SOLUCIÓN PROPUESTA

Balanceadores de carga virtuales

Marca: F5

Modelo: F5 BIG-IP VE 1GB

SKU: F5-BIG-LTM-VE-1G-V23 (BIGIP VIRTUAL EDITION: LOCAL TRAFFIC MANAGER 1 GBPS (V17.1.X V23.X)

Soporte: F5-SVC-BIG-VE+PREL13 (Level 1-3 Premium Service for BIG-IP Virtual Edition (24x7) (VersionPlus only)

Add-on: F5-ADD-BIG-AWF-VE-1G (BIG-IP ADD-ON: ADVANCED WEB APPLICATION FIREWALL VIRTUAL LICENSE 1G)

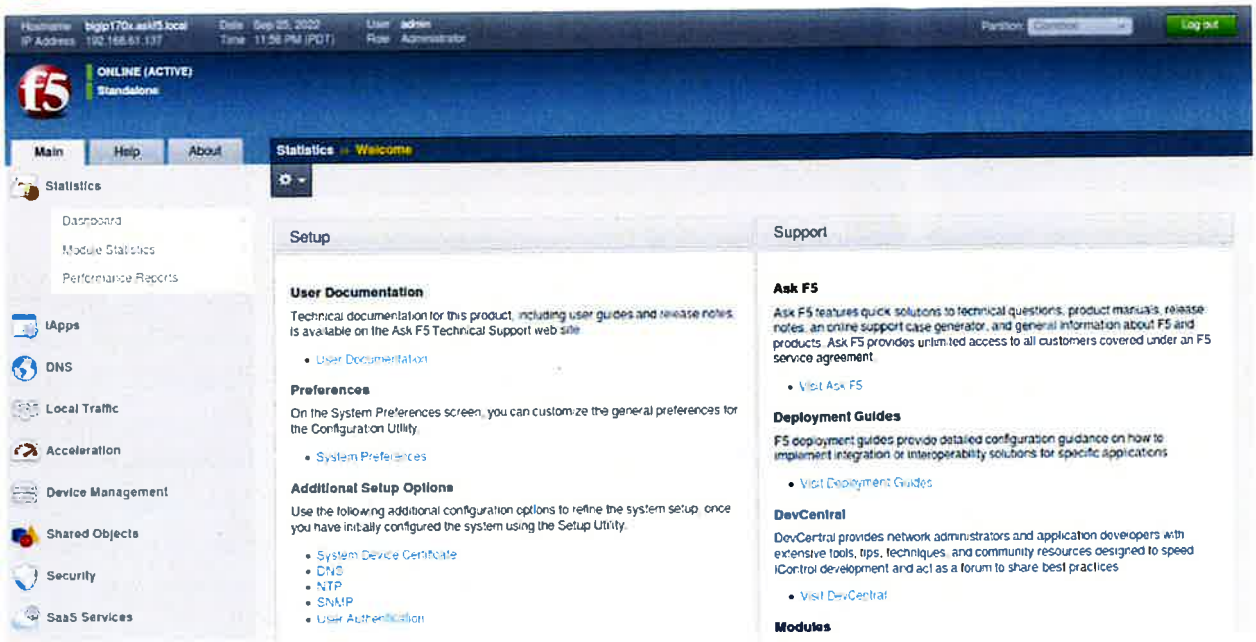
Soporte add-on: F5-SVC-BIG-VE+PREL13 (Level 1-3 Premium Service for BIG-IP Virtual Edition (24x7) (VersionPlus only)

Cantidad: 2

Tiempo: 3 años.

Wagner Peña

IPX SRL
RNC 130-850151
Santo Domingo, R.D.



Descripción de la Solución

Las ediciones virtuales (VE) de F5 BIG-IP son los controladores de entrega de aplicaciones virtuales (vADC) más escalables del sector, facilitando el procesamiento de tráfico de aplicaciones de alto rendimiento en todos los hipervisores y plataformas en la nube líderes y simplificando la transición del hardware al software.

Las VE ofrecen los mismos servicios de entrega de aplicaciones líderes del mercado, incluyendo gestión avanzada del tráfico, seguridad de aplicaciones, aceleración de aplicaciones, DNS, firewall de red y gestión de acceso seguro, que se ejecutan en hardware F5 diseñado específicamente para este fin. Esta similitud permite reutilizar y replicar en las VE las configuraciones y políticas de servicio de los dispositivos F5 existentes, simplificando las migraciones a la nube. Las VE se pueden aprovisionar y configurar fácilmente de forma automática tanto por operadores de red como por desarrolladores, lo que permite integrarlas en las canalizaciones de CI/CD existentes y garantiza que todas las aplicaciones

C/ Francisco Prats Ramírez #810, esq. Privada, El Millón. Santo Domingo, D.N.
Tel.: 809-532-4143

IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Wagner Peña

se implementen con las capacidades necesarias de seguridad, cumplimiento y gestión del tráfico. Cuando se utiliza junto con F5

BIG-IQ Centralized Management, puede crear, aprovisionar y administrar rápidamente servicios de aplicaciones en cualquier lugar, al tiempo que obtiene visibilidad del estado y el rendimiento de sus aplicaciones multi-nube, todo desde un punto de control centralizado.

Características y especificaciones de la solución ofertada

- Ofrecemos dos F5 BIG-IP VE en modalidad de alta disponibilidad
- Los F5 BIG-IP VE es una plataforma virtual dedicada exclusivamente a funciones de entrega y optimización de aplicaciones.
- El sistema operativo de la solución que es TMOS es especializado y diseñado específicamente para balanceo de carga y servicios de aplicaciones, no se basa en sistemas operativos genéricos.
- El desempeño solicitado se alcanza por la solución de manera independiente, sin requerir la agregación de múltiples appliances.
- Los F5 BIG-IP VE son compatible con entornos de virtualización líderes en el mercado: VMware ESXi, Linux KVM, Microsoft Hyper-V, Nutanix AHV, XenServer y Xen Project.
- La licencia inicial ofertada contempla 1 Gbps de capacidad de procesamiento de tráfico.
- La solución realiza balanceo de tráfico de aplicaciones basadas en TCP/UDP, incluidos servicios web.
- El F5 BIG-IP VE permite la definición de direcciones IP y puertos virtuales que distribuyan peticiones hacia granjas de servidores.

Wagner Peña

expert IPX SRL RNC 130-850151 Santo Domingo, R.D.

C/ Francisco Prats Ramírez #810, esq. Privada, El Millón, Santo Domingo, D.N.
Tel.: 809-532-4642

- F5 BIG-IP VE cuenta con arquitectura Full-Proxy, diferenciando claramente conexiones de cliente y servidor.
- F5 BIG-IP VE soporta la incorporación gradual de nuevos servidores al balanceo para evitar saturación inicial de conexiones.
- F5 BIG-IP VE permite la persistencia de conexiones basada en múltiples parámetros del paquete completo, incluyendo IP origen/destino, cookies, hash, campos SIP, sesiones SSL y credenciales de escritorio remoto.
- F5 BIG-IP VE soporta múltiples algoritmos de balanceo de manera nativa: Round Robin, Proporcional, Dinámico,Respuesta más rápida, Conexiones mínimas, entre otros
- F5 BIG-IP VE cuenta con monitoreo avanzado de salud deservidores y aplicaciones mediante métodos de red (Ping, TCP/UDP, HTTP/S), servicios de aplicaciones (LDAP, SMTP, SQL, RADIUS, SIP, etc.), y scripts personalizados.
- El F5 BIG-IP VE soporta el control dinámico de ancho de banda y balanceo basado en carga de los servidores (ej.memoria RAM).
- El F5 BIG-IP VE tiene soporte para APIs imperativas y declarativas para automatización de configuraciones (incluyendo REST).
- Permite la modificación de contenido HTML sin necesidad de scripting y soportar protocolos de administración de tráfico como MQTT y NetFlow.
- El F5 BIG-IP VE Soporta extensibilidad mediante scripting estructurado (TCL) y moderno (Node.js), así como funcionalidades de geolocalización offline
- El F5 BIG-IP VE tiene el stack TLS que soporta funcionalidades avanzadas: Session ID, Session Ticket, OCSP Stapling, ALPN, Forward Secrecy y Dynamic Record Sizing.

expert
IPX SRL
RNC 130-85051
Santo Domingo, R.D.

Wagner Pina

C/ Francisco Prats Ramírez #10, Piantini, Millón, Santo Domingo, D.N.
Tel.: 809-532-4642

- Cuenta con soporte para algoritmos criptográficos modernos y tradicionales: AES, AES-GCM, SHA, RSA, DSA, ECC, Diffie-Hellman y Camellia.
- Incluye firmado criptográfico de cookies y compatibilidad con integración de dispositivos HSM (ej. CloudHSM, Thales, Equinix).
- El F5 BIG-IP VE cuenta con capacidad de Proxy SSL para desencriptar, optimizar y reencriptar tráfico sin terminar la sesión SSL.
- Los F5 BIG-IP VE soporta protocolos de seguridad adicionales como STARTTLS, HSTS y sistemas de reputación IP para bloqueo de conexiones a hosts maliciosos.
- Los F5 BIG-IP VE permite caching, compresión HTTP, multiplexación de conexiones y optimización TCP.
- Los F5 BIG-IP VE soporta compresión GZIP compatible con navegadores estándar.
- Los F5 BIG-IP VE soportan HTTP/2 actuando como gateway.
- Los F5 BIG-IP VE permite modificar y gestionar etiquetas de caché por objeto.
- Los F5 BIG-IP VE incluye Adaptive Forward Error Correction para TCP y UDP.
- La solución incluye un WAF integrado de capa 7, que no es un sistema separado, para minimizar latencia y simplificar gestión.
- El WAF permite la personalización avanzada de políticas, creación automática de reglas, herencia de configuraciones y soporte a múltiples aplicaciones.
- Soporta modelos de seguridad positiva y negativa, aprendizaje automático de comportamiento y protección frente al Top 10 de OWASP.

expert IPX SRL RNC 130-85015 Santo Domingo, R.D.

Wagner Pestrana

C/ Francisco Prats Ramírez #30, esq. Privada, El Millón, Santo Domingo, D.N.
Tel.: 809-532-4642

- Incluye protección de APIs REST y GraphQL, validación de definiciones Swagger/OpenAPI, así como servicios web XML.
- Soporta integración con herramientas DevSecOps y exportación/importación de políticas en formatos estándar (JSON, XML).
- Incluye la protección avanzada contra bots, scraping, DoS/DDoS de capa 7 y ataques como XSS, CSRF, SQLi, manipulación de cookies y otros.
- Ofrece las capacidades de ofuscación de parámetros sensibles, cifrado dinámico en navegador y protección de sesiones y logins contra fuerza bruta.
- Incluye reportes alineados a normativa PCI DSS y permitir integración con antivirus vía ICAP y con firewalls de base de datos (ej. Guardium)
- La solución soporta VLAN 802.1q, agregación de enlaces 802.3ad, NAT y SNAT.
- La solución soporta conectividad dual IPv4/IPv6 y funcionar como gateway entre ambas.
- La solución soporta enrutamiento dinámico: BGP, RIP, OSPF, IS-IS.
- Los F5 BIG-IP VE soportan dominios de enrutamiento con gateways independientes.
- Los F5 BIG-IP VE incluyen capacidades de rate shaping.
- La solución tiene manejo integrado de tráfico avanzando: por Geolocalización, Balanceo por Latencia, DNSSEC y monitorización profunda de aplicaciones.
- La solución cuenta con resilencia DNS con caching, rate-limiting y protección contra ataques.

expert IPX SRL RNC 130-950151 Santo Domingo, R.D.

Wagner Peña

C/ Francisco Prats Ramírez #8, 0, esq. Pri Mill, El Millón, Santo Domingo, D.N.
Tel.: 809-532-4642

- La solución ofrece acceso de gestión por CLI (SSH) y consola web segura (HTTPS).
- La solución puede integrarse con AD, LDAP, RADIUS y TACACS+, SSO y MFA integrado para autenticación de administradores.
- La solución cuenta con la combinación VPN+SSO+MFA en el mismo appliance.
- La solución soporta alertas centralizadas vía Syslog, SMTP y SNMP.
- La administración la solución esta separada del plano de datos de tráfico.
- Los F5 BIG-IP VE incluye módulo de administración remota (lights out), dashboards personalizables y reportes detallados sobre tráfico y aplicaciones.
- Los F5 BIG-IP VE ofrecen plantillas predefinidas para aplicaciones empresariales (ej. Oracle, Microsoft, SAP, IBM) y permitir creación de plantillas personalizadas.

Servicios de soporte y licenciamiento de fabrica

- Incluimos las licencias completas para balanceo de carga y firewall de aplicaciones web.
- Se incluye el soporte por parte del fabricante 24x7 para todos los módulos licenciados.
- Incluimos las licencias que habilitan funcionalidades avanzadas sin requerir dispositivos adicionales.
- Todo el licenciamiento, soporte y mantenimiento está incluido por un periodo mínimo de 3 años.

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Wagner Peña

C/ Francisco Prats Ramírez #810, esq. Privada, Millón, Santo Domingo, D.N.
Tel.: 809-532-4642

Tiempo y Condiciones de Garantía de la Solución Ofertada

La solución ofertada incluye un paquete de soporte y garantía F5 Premium 24x7 (F5-SVC-BIG-VE+PREL13) con una vigencia de tres (3) años, cumpliendo con los requisitos establecidos en el pliego. Este nivel de garantía asegura la continuidad operativa, la estabilidad de la plataforma y el acompañamiento técnico especializado durante toda la vida útil del servicio.

Durante el período de garantía, la Junta Central Electoral contará con:

1. Cobertura Premium 24x7 del Fabricante

La garantía incluye acceso continuo, las 24 horas del día, los 365 días del año, al equipo global de ingenieros certificados de F5. Esto proporciona atención inmediata ante cualquier incidente crítico y soporte especializado en funciones avanzadas de balanceo de carga, WAF, seguridad, tráfico L4/L7 y automatización.

2. Tiempos de Respuesta Garantizados

El soporte Premium ofrece atención prioritaria, incluyendo:

- Respuesta para eventos Severity 1 (site down) en un plazo aproximado de 30 minutos.
- Acompañamiento continuo hasta la resolución del incidente.
- Alineado con el pliego, garantizamos un SLA máximo de 12 horas para cualquier incidente reportado.

3. Actualizaciones, Mejoras y Parches

Durante los 3 años de garantía, la institución recibe:

- Acceso inmediato a todas las actualizaciones de software, nuevas versiones, mejoras funcionales y parches de seguridad publicados por F5.
- Descarga ilimitada de versiones y releases a través del portal oficial AskF5.

C/ Francisco Prats Ramírez #10, esq. Privada, El Millón, Santo Domingo, D.N.
Tel.: 809-532-4642

IPX SRL
RNC 130-850151
Santo Domingo, R.D.

4. Asistencia Técnica Especializada

El servicio incluye:

- Soporte técnico experto de nivel 1 a 3 para la plataforma F5 BIG-IP VE.
- Validación y troubleshooting de iRules, verificación de sintaxis, lógica funcional y apoyo en problemas operativos.
- Acceso al WebSupport Portal, para apertura y seguimiento de casos, envío de archivos diagnósticos y comunicación directa con ingenieros de soporte.

5. Proactive Case Management

El soporte Premium permite:

- Notificar mantenimientos programados sobre la plataforma.
- Asignación anticipada de ingenieros para soporte durante ventanas de trabajo críticas.
- Reducción de tiempos de diagnóstico ante cambios o actualizaciones.

6. Recursos de Autoayuda y Comunidad Técnica

El oferente provee acceso a:

- La base de conocimiento oficial AskF5, con guías, manuales, documentación, hotfixes y alertas de seguridad.
- La comunidad especializada DevCentral, con más de 300,000 usuarios expertos, ejemplos de configuraciones y mejores prácticas.

7. Reemplazo Avanzado (RMA)

Aunque la solución es virtual, el soporte Premium incluye:

- Derecho a reemplazos avanzados de licenciamiento o fallos atribuibles al software.

C/ Francisco Prats Ramírez #810, ens. Paraíso, El Millón, Santo Domingo, D.N.
Tel.: 809-532-4642

- Opciones de Expedited RMA (si aplicara hardware complementario), disponibles para adquisición.

8. Alcance de la Garantía

El servicio de garantía cubre:

- Todas las funciones licenciadas de la solución.
- Fallas, bugs, errores operativos y correcciones de la plataforma.
- Acompañamiento para asegurar operación continua, estable y segura.

Servicios de soporte de IP Expert IPX SRL

- Garantizamos la compatibilidad e integración con la infraestructura actual.
- Como parte de la propuesta IP Expert IPX SRL brindara soporte técnico y mantenimiento durante el periodo de la garantía.
- Como parte de la propuesta IP Expert IPX SRL brinda soporte técnico disponible 8x5.
- Incluimos la capacitación técnica al personal en la operación y administración de los nuevos componentes.
- Como parte de la propuesta IP Expert IPX SRL contamos con un tiempo máximo de respuesta para incidentes de 12 horas.

Wagner Peña

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

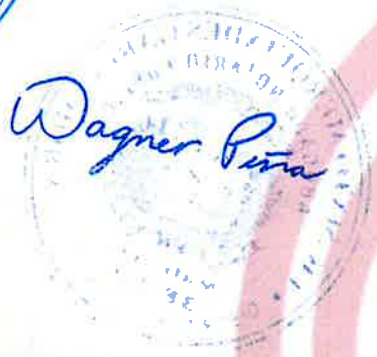
C/ Francisco Prats Ramírez #81[illegible] El Millón, Santo Domingo, D.N.
Tel.: 809-532-4642

Servicio de Implementación de la solución ofertada

- Incluimos la instalación y configuración de todos los componentes de la solución ofertada.
- La implementación de la solución será realizada por el personal profesional requerido, compuesto por:
    - Un Gerente de Proyecto
    - Un Ingeniero de la solución
    - Un Ingeniero de Integración

Tiempo de entrega

- El tiempo de entrega de la solución es en un plazo no mayor a treinta (30) días hábiles contados a partir de la recepción de la orden.



C/ Francisco Prats Ramírez #810, esq. Privada, El Millón, Santo Domingo, D.N.
Tel.: 809-532-4642


LIC. SIXTO MERQUIADES GARCIA VIORA
ABOGADO NOTARIO PUBLICO
Matricula
3E - 62
DISTRITO NACIONAL RD

Información Técnica Complementaria

QUÉ HAY DENTRO

Wagner Peña

Acceso sencillo, seguro y sin interrupciones a cualquier aplicación, en cualquier lugar

Las aplicaciones son puertas de enlace a tus datos críticos y sensibles. El acceso simple y seguro a tus aplicaciones es fundamental, pero hoy en día el acceso a aplicaciones es extremadamente complejo. Las aplicaciones pueden alojarse en cualquier lugar: en la nube pública, en una nube privada, en las instalaciones o en un centro de datos. Garantizar que los usuarios tengan acceso seguro y autenticado en cualquier momento y lugar, solo a la
Las aplicaciones a las que están autorizados a acceder ahora supone un desafío importante. Existen diferentes métodos de acceso a aplicaciones para gestionar estas complejidades. Existen diversas fuentes para la identidad autorizada del usuario, así como para tratar con aplicaciones que requieren métodos modernos o tradicionales de autenticación y autorización, inicio de sesión único (SSO), federación y más, además de la experiencia de acceso del usuario para dar soporte y considerar.

Con la transformación digital afectando a todos los aspectos de una empresa hoy en día, las aplicaciones nativas en la nube y Software como Servicio (SaaS) son ahora el estándar de las aplicaciones empresariales. Sin embargo, muchas organizaciones descubren que no pueden o no quieren migrar todas sus aplicaciones a la nube. Puede haber aplicaciones clásicas o personalizadas críticas que no deberían
o no puede soportar la migración a la nube pública ni ser fácilmente reemplazada por una aplicación SaaS. Las aplicaciones se alojan en una variedad de ubicaciones, con métodos de autenticación y autorización diferentes y muchas veces dispares que no pueden comunicarse entre sí y no funcionan sin problemas entre SSO o identidades federadas existentes, que no pueden soportar los medios de identidad más recientes como Identidad como Servicio (IDaaS) y no están equipados para soportar autenticación multifactor (MFA).

F5® BIG-IP® Access Policy® Manager (APM) es una solución proxy de gestión de accesos segura, flexible y de alto rendimiento que gestiona el acceso global a tu red, la nube,

ICSA labs CERTIFIED SSL VPN FIREWALL - CORPORATE

BIG-IP APM consolida acceso remoto, móvil, de red, virtual y web. Con BIG-IP APM, puedes crear, hacer cumplir y centralizar políticas de acceso a aplicaciones simples, dinámicas e inteligentes para todas tus aplicaciones, independientem ente de dónde o cómo estén alojadas.

Wagner Peña

Wagner Peña

BENEFICIOS CLAVE

Simplifica el acceso a todas las aplicaciones : ponte el acceso seguro a aplicaciones locales y en la nube con un solo inicio de sesión vía SSO. Incluso funciona para aplicaciones que no pueden soportar autenticación moderna como como Lenguaje de Marcado de Aserción de Seguridad (SAML), o OAuth y OpenID Connect (OIDC).

Acceso a aplicaciones de confianza cero El Proxy Consciente de la Identidad (IAP) ofrece una validación del modelo de confianza cero para el acceso a aplicaciones basada en la conciencia de identidad y el contexto granular, asegurando cada solicitud de acceso a la aplicación sin necesidad de VPN.

Acceso web seguro
Controla el acceso a aplicaciones y contenidos web centralizando la autenticación, autorización e inspección de endpoints mediante proxy de aplicación web.

Centralizar y gestionar el control de acceso
Consolidar la gestión de accesos remotos, móviles, de red, virtuales y web en una única interfaz de control con federación adaptativa de identidad, SSO y MFA mediante políticas aplicadas dinámicamente, basadas en el contexto y conscientes de la identidad.

Autenticación y autorización simplificadas
Federación adaptativa de identidades, SSO y MFA que emplean SAML, OAuth y OIDC para una experiencia de usuario fluida y segura en todas las aplicaciones.

PUENTE SEGURO APLICACIÓN A CCESS

Los protocolos modernos de autenticación y autorización —incluyendo Secure Assertion Markup Language (SAML) y OAuth con OpenID Connect (OIDC)— reducen la dependencia del usuario respecto a las contraseñas, aumentan la seguridad y mejoran la experiencia y productividad del usuario. Sin embargo, no todas las aplicaciones soportan protocolos modernos de autenticación y autorización. Muchas aplicaciones, como las clásicas o las creadas a medida, soportan autenticación clásica
y métodos de autorización, como Kerberos, NT LAN Manager (NTLM), RADIUS, basados en cabeceras y más. Esto complica aún más el acceso y la seguridad de las aplicaciones. La necesidad de soportar protocolos diferentes y dispares que no pueden compartir información de autenticación y autorización de usuarios dificulta el uso de SSO y MFA. Eso, a su vez, afecta negativamente a la experiencia del usuario y a la seguridad de las aplicaciones. También dificulta adaptar la contraseña corporativa moderna política de cambios periódicos de contraseña y aumenta los costes organizativos a medida que se requieren múltiples métodos de acceso.

BIG-IP APM sirve como puente entre protocolos y métodos modernos y clásicos de autenticación y autorización. Para aplicaciones que no pueden soportar protocolos modernos de autenticación y autorización, como SAML y OAuth con OIDC, pero que sí lo soportan métodos clásicos de autenticación, el BIG-IP APM convierte las credenciales del usuario al estándar de autenticación adecuado soportado por la aplicación. BIG-IP APM garantiza que los usuarios u organizaciones puedan usar SSO para acceder a cualquier aplicación en cualquier lugar—independientemente de su ubicación (en las instalaciones, en un centro de datos, en una nube privada o en la nube pública como aplicación nativa en la nube o SaaS), o si soporta o no autenticación moderna o clásica y
autorización. Esto ayuda a reducir el número de contraseñas que los usuarios deben crear, recordar y utilizar, ayudando a frenar la oleada de ataques basados en credenciales. Permite el cumplimiento de las políticas corporativas modernas de cambios periódicos de contraseña para combatir el robo de credenciales. Eso
también reduce el coste para las organizaciones de tener que comprar y mantener soluciones de acceso separadas para aplicaciones alojadas localmente, en un centro de datos y en una nube privada, en comparación con la nube nativa y las aplicaciones SaaS.

BIG-IP APM soporta opciones de federación de identidad y SSO al soportar conexiones iniciadas tanto por proveedores de identidad SAML (IdP) como por proveedores de servicios (SP) que aprovechan SAML 2.0. F5 soporta el consumo de tokens JOU, lo que permite a BIG-IP APM consumir tokens JWT cifrados de proveedores SAML IdP. Esto permite que BIG-IP APM mantenga el secreto entre el emisor o el token y el destinatario. BIG-IP APM permite a los administradores habilitar y desactivar de forma centralizada el acceso autorizado por usuarios a cualquier aplicación habilitada por identidad, independientemente de dónde esté alojada, ahorrando tiempo y aumentando la productividad administrativa.

BENEFICIOS CLAVE (CONT.)

Defiende tus eslabones más débiles Protege contra la pérdida de datos, malware y acceso fraudulento a dispositivos con controles integrales y continuos de integridad y seguridad en los endpoints.

APIs de protección Habilitar la autenticación segura para APIs REST e integrar archivos OpenAPI o "swagger" para garantizar acciones de autenticación adecuadas mientras ahorra tiempo y costes.

Hazlo todo a gran escala Soporta a todos los usuarios de forma sencilla, rápida y rentable, sin compensaciones en rendimiento en cuanto a seguridad, incluso en los entornos más exigentes.

Esto ayuda a prevenir ataques como la interceptación de códigos de autorización al habilitar tokens secretos dinámicos. PKCE permite que las aplicaciones realicen solicitudes directas al proveedor del token, añadiendo una capa extra de seguridad para las aplicaciones públicas.

SUPPOR T PARA ID AAS

Con soporte para SSO y tickets Kerberos en múltiples dominios, el APM BIG-IP permite tipos adicionales de autenticación, como las Common Access Cards (CAC) del Gobierno Federal de EE. UU. y el uso de IDaaS —como Azure Active Directory (Azure AD), Okta y otros— para acceder a todas las aplicaciones independientemente de la ubicación o del soporte moderno de autenticación y autorización. Por ejemplo, los usuarios pueden iniciar sesión automáticamente en aplicaciones y servicios de backend que forman parte de un ámbito Kerberos. Esto proporciona un flujo de autenticación fluido una vez que el usuario ha sido autenticado mediante un mecanismo de autenticación de usuario soportado. BIG-IP APM también es compatible con tarjetas inteligentes con proveedores de credenciales, para que los usuarios puedan conectar sus dispositivos a su red antes de iniciar sesión.

SUPPOR T PARA MFA

A través del extenso ecosistema de socios de F5, BIG-IP APM también se integra con la mayoría de las soluciones de MFA líderes, incluyendo las de Cisco Duo, Okta, Azure AD y otros. Al integrarse con tu solución de MFA existente, BIG-IP APM permite la autenticación adaptativa, permitiendo emplear diversas formas de autenticación de uno, dos o múltiples factores basadas en la identidad del usuario, el contexto y el acceso a la aplicación. Además, para ayudarte a desplegar MFA, BIG-IP APM incluye autenticación con contraseña de un solo uso (OTP) mediante correo electrónico o SMS.

Después de que el usuario ha iniciado sesión en una aplicación, puede requerirse un método adicional de autenticación para asegurar un acceso seguro a aplicaciones y archivos críticos o especialmente sensibles. Esto se conoce comúnmente como autenticación step-up. BIG-IP APM soporta autenticación step-up para autenticación de un solo y varios factores. Cualquier variable de sesión puede usarse para activar la autenticación step-up, y puedes utilizar capacidades adicionales de autenticación o elegir entre nuestras ofertas de socios. Además, cualquier variable de sesión puede formar parte de la ramificación de políticas de acceso (como la ramificación de URL) por política de solicitud. Las políticas de autenticación step-up pueden basarse en aplicaciones, partes seguras de aplicaciones, URI web sensibles, ampliación de sesiones o cualquier variable de sesión.

Muchas soluciones de autenticación utilizan codificación de aplicaciones, agentes de servidor web separados o proxies especializados que presentan importantes problemas de gestión, coste y escalabilidad. Con control AAA, BIG-IP APM te permite aplicar

APLICACIÓN CERO TRUST A CCESS

Muchas organizaciones —posiblemente incluida la suya— están avanzando rápidamente hacia la adopción de una arquitectura de seguridad de confianza cero. Los pilares de una arquitectura de seguridad de confianza cero son la identidad y el contexto.

Un enfoque de seguridad de confianza cero significa adoptar la mentalidad de que los atacantes ya han infiltrado tu red y están acechando, esperando una oportunidad para lanzar un ataque. Elimina la idea de un insider de confianza dentro de un perímetro de red definido, asumiendo, en el mejor de los casos, un perímetro de red limitado y seguro. Fomenta no confiar nunca en los usuarios, incluso si ya han sido autenticados, autorizados y han recibido acceso a aplicaciones y recursos. Un enfoque de seguridad cero confianza aplica derechos de privilegio mínimo al acceso de los usuarios, permitiendo que los usuarios accedan solo a aquellas aplicaciones y recursos para los que están autorizados, y restringiendo su acceso a una sola aplicación o recurso a la vez.

La conciencia de identidad y contexto también es lo que define el Proxy Consciente de la Identidad (IAP). La IAP permite el acceso seguro a aplicaciones específicas mediante un enfoque detallado de autenticación y autorización de usuarios. Los IAP solo permiten el acceso por solicitud a la aplicación, lo cual es muy diferente del enfoque de acceso a la red amplia de las VPNs que aplican acceso basado en sesión, que no es un enfoque de confianza cero. Con este enfoque, la VPN se vuelve opcional para acceder a aplicaciones. El IAP permite la creación y aplicación de políticas de acceso a aplicaciones granulares basadas en atributos contextuales, como la identidad del usuario, la integridad del dispositivo y la ubicación del usuario. La IAP se basa en controles de acceso a nivel de aplicación, no en reglas de la capa de red. Las políticas configuradas reflejan la intención y el contexto del usuario y la aplicación. La IAP requiere una raíz fuerte de identidad confiable para verificar a los usuarios y para hacer cumplir estrictamente lo que están autorizados a acceder.

El Proxy Identity Aware es clave tanto para una arquitectura de seguridad de confianza cero como para el BIG IP APM F5. BIG-IP APM y F5 Access Guard entregan un Proxy Identity Aware utilizando un modelo de validación cero confianza en cada solicitud de acceso a la aplicación. Proporcionando a usuarios autenticados y autorizados acceso seguro a aplicaciones específicas, aprovecha el proxy de acceso de primera clase de F5. BIG-IP APM centraliza la identidad y autorización del usuario. La autorización se basa en los principios del acceso menos privilegiado.

A través de la PAI, BIG-IP APM examina, termina o autoriza solicitudes de acceso a aplicaciones. Las políticas dentro de BIG-IP APM pueden crearse para:

- Verificar la identidad del usuario
- Comprueba el tipo de dispositivo y la postura
- Validar la autorización del usuario
- Confirmar la integridad y sensibilidad de la aplicación
- Confirma la disponibilidad de fecha y hora

- Limitar o detener el acceso si la ubicación del usuario o la postura de su dispositivo se considera incorrecta, inapropiada o insegura
- Solicita formas adicionales de autenticación—incluida la autenticación multifactor (MFA)—si la ubicación del usuario o la naturaleza sensible de las aplicaciones o sus datos lo justifican
- Y más

Los datos del análisis de comportamiento de usuarios y entidades (UEBA) y otros motores de riesgo impulsados por API pueden integrarse sin problemas, añadiendo otro nivel de seguridad y control de acceso a aplicaciones.

BIG-IP APM verifica la postura de seguridad de los dispositivos del usuario mediante F5 Access Guard, una extensión de navegador que coordina con BIG-IP APM. Sin embargo, el APM BIG-IP y el F5 Access Guard van más allá de simplemente comprobar la integridad del dispositivo en la autenticación para realizar comprobaciones continuas y continuas de la postura del dispositivo, asegurando que los dispositivos de usuario no solo cumplan, sino que cumplan con las políticas de seguridad de los endpoints durante todo el acceso a la aplicación. Si BIG-IP APM detecta algún cambio en la integridad del dispositivo, puede limitar o detener el acceso a las aplicaciones, deteniendo posibles ataques antes incluso de que puedan lanzarse.

Un flujo de trabajo de configuración guiado permite a las organizaciones alojar aplicaciones web protegidas por un Proxy Identity Aware en un webtop, proporcionando a los usuarios un único catálogo de sus aplicaciones. Ofrece una experiencia de usuario fluida, ya que los usuarios pueden acceder a las aplicaciones independientemente de dónde estén alojadas. También simplifica el flujo de trabajo administrativo, permitiendo a los administradores seleccionar, modificar y modificar fácilmente las aplicaciones accesibles por un grupo de usuarios específico.

BIG-IP APM, a través de la aplicación en aplicación (IAP), también simplifica el acceso a aplicaciones para trabajadores remotos o desde casa, facilita y asegura mejor la accesibilidad de las aplicaciones, eliminando opcionalmente la necesidad de VPNs.

SEGURIDAD ROBUSTA DE ENDPOINTS

BIG-IP APM inspecciona y evalúa los dispositivos finales de los usuarios antes de la autenticación y durante todo el acceso a la aplicación con F5 Access Guard. F5 Access Guard examina la postura de seguridad del dispositivo y determina si el dispositivo forma parte del dominio corporativo. Según los resultados, BIG-IP APM aplicará listas dinámicas de control de acceso (ACLs) para desplegar seguridad contextual. El APM BIG-IP y el F5 Access Guard incluyen comprobaciones de inspección de endpoints preconfiguradas e integradas, incluyendo comprobaciones por tipo de sistema operativo, software antivirus, cortafuegos, archivo, proceso, validación y comparación de valores de registro (solo Windows), así como dirección MAC del dispositivo, ID de CPU e ID de HDD. Para dispositivos móviles con iOS o Android, la inspección de endpoint de BIG-IP APM verifica el estado UDID del dispositivo móvil y el jailbreak o root.

UN CCESS BASADO EN RIESGO USANDO MOTORES DE RIESGO TERCEROS - PAR TY (HTTP CONNEC TOR)

Muchas organizaciones han desplegado análisis de comportamiento de usuarios y entidades (UEBA) o motores de riesgo de terceros. La capacidad de aprovechar un UEBA o motor de riesgo existente para incorporar análisis en tiempo real y datos de riesgo dentro de sus políticas de control de acceso puede ayudar a esas organizaciones garantizar que el acceso a redes, nubes, aplicaciones e incluso APIs se regule en función de un perfil de riesgo. También es importante abordar el acceso basado en riesgos a redes, nubes, aplicaciones y APIs que se activa por una variedad de variables relevantes.

A través de su HTTP Connector, BIG-IP APM se integra con UEBA de terceros y motores de riesgo, aprovechando su evaluación de riesgos mediante APIs REST como parte de sus controles de acceso basados en políticas. Esto permite un acceso basado en riesgos a redes, nubes, aplicaciones y APIs, mejorando aún más la solución de IAP cero confianza de BIG-IP APM. El HTTP Connector de BIG-IP APM aprovecha disparadores basados en grupos de usuarios, dominios y red para aumentar la aplicabilidad del acceso basado en riesgos. El acceso basado en riesgos mejora la seguridad, proporcionando mayor visibilidad y análisis para determinar si conceder o denegar el acceso a tus redes, nube, aplicaciones y APIs.

INTEGRACIÓN INTELIGENTE CON IDENTIDAD Y UN CCESS MANA GEMENT (IAM)

F5 colabora con los principales proveedores de gestión de identidad y acceso (IAM) tanto locales como en la nube, como Microsoft, Okta y Ping Identity. Esta integración permite el uso local y remoto de usuarios SSO vía SAML, OAuth o FIDO2 (U2F) a aplicaciones basadas en instalaciones o en un centro de datos. Para las organizaciones que no desean replicar su almacén de credenciales de usuario en la nube con IDaaS o ofertas IAM basadas en la nube, trabajando con sus socios, F5 y BIG-IP APM trabajan para ayudar a estas organizaciones a mantener el control de las credenciales de usuario locales. Esto se logra creando un puente entre la oferta del proveedor IAM y los servicios locales de autenticación. Este puente, o cadena de proveedores de identidad, utiliza SAML para federar la identidad del usuario.

UNIFICAR UN CCESS A PARTIR DE CUALQUIER DISPOSITIVO

BIG-IP APM está situado entre tus aplicaciones y tus usuarios, proporcionando un punto estratégico de control de acceso a las aplicaciones. Protege tus aplicaciones públicas proporcionando políticas detalladas para el acceso de usuario consciente de la identidad y el contexto, mientras consolida tu infraestructura de acceso. Asegura el acceso remoto y móvil a aplicaciones, redes y nubes mediante VPN SSL o acceso a aplicaciones de confianza cero. BIG-IP APM converge y consolida todo el acceso—red, nube, aplicación y API—dentro de una única interfaz de gestión. También permite y simplifica la creación de políticas de acceso dinámicas fáciles de gestionar.

BIG-IP APM incluye un portal de aplicaciones web dinámico o webtop. El webtop BIG-IP APM muestra solo las aplicaciones autorizadas y disponibles para un usuario según su identidad y contexto—independientemente de dónde estén alojadas las aplicaciones—localmente, en un centro de datos, en una nube privada, en una nube pública o ofrecidas como servicio.

Wagner Peña

BIG-IP APM activa el modo de Seguridad de la Capa de Transporte de Datagramas (DTLS), que soporta DTLS 2.0 para conexiones remotas que aseguran y tunelan aplicaciones sensibles al retardo. Soporta cifrado IPsec para el tráfico entre sucursales o centros de datos.
VPN por aplicación mediante una aplicación
El túnel a través de BIG-IP APM permite acceder a una aplicación específica sin el riesgo de seguridad de abrir un túnel de acceso a red completo.

F5 BIG-APM permite el acceso seguro a aplicaciones, redes y nubes a través del cliente BIG-IP Edge y el acceso F5. El cliente BIG-IP Edge está disponible para Apple MacOS, Microsoft Windows, plataformas Linux, Chromebooks, e incluye soporte para Windows en dispositivos ARM64. F5 Access es un cliente móvil opcional para garantizar el acceso seguro desde dispositivos móviles compatibles con Apple iOS y Google Android, y está disponible para descargar en la Apple App Store o Google Play.

BIG-IP Edge Client y F5 Access se integran con soluciones líderes en gestión de dispositivos móviles (MDM) y gestión de movilidad empresarial (EMM), incluyendo VMware Horizon ONE (AirWatch), Microsoft Intune e IBM MaaS360, para realizar comprobaciones de seguridad e integridad de dispositivos y para ofrecer acceso VPN por aplicación sin intervención del usuario. Las políticas contextuales se asignan en función del estado de seguridad del dispositivo. Estas políticas habilitan, modifican o desactivan el acceso a aplicaciones, red y nube desde el dispositivo. Los atributos de hardware pueden asignarse al rol del usuario para permitir puntos adicionales de decisión de control de acceso. Un limpiador de caché del navegador elimina automáticamente cualquier dato sensible al final de la sesión del usuario.

Se soportan biometrías, como el acceso por huella dactilar, para abrir y acceder al Cliente Edge F5. Esto simplifica el acceso, ya que el usuario ya no necesitará crear, recordar e introducir una credencial de usuario/contraseña para acceder al Cliente Edge. También hace que el acceso al Cliente Edge sea más seguro, ya que los usuarios reutilizan contraseñas o crean pares simples de nombre de usuario/contraseña, facilitando así el hackeo de los atacantes.

BIG-IP APM también soporta autenticación de servidores mediante Delegación Limitada de Certificado de Cliente (C3D). Al emplear C3D, BIG-IP APM aborda la autenticación basada en certificados, limitando la necesidad y el uso de credenciales. Con C3D, las organizaciones pueden implementar protocolos de cifrado más sólidos y los últimos intercambios de claves, así como emplear autenticación de certificados de cliente, habilitar el cifrado de extremo a extremo en entornos de proxy inverso, aprovechar Perfect Forward Secrecy (PFS) y validar certificados de cliente utilizando el Protocolo de Estado de Certificados en Línea (OCSP).

UN CCESS TRANSPARENTE PARA TODAS LAS APLICACIONES

A medida que las organizaciones se centran en reducir la fricción de los usuarios y aumentar la agilidad, su necesidad de proporcionar un acceso fluido a todas las aplicaciones se convierte en una prioridad. BIG-IP APM permite a las organizaciones reducir la fricción para que los usuarios accedan remotamente (SSL VPN). También reduce la fricción en aplicaciones web. BIG-IP APM soporta SSO tanto en acceso remoto como en aplicaciones web con un único inicio de sesión para dispositivos Apple Mac o Microsoft Windows (a través de
Windows Hello For Business). Las organizaciones pueden soportar el inicio de sesión del usuario mediante tokens U2F (como claves Yubico) o FIDO2 sin contraseña a través del Cliente Edge F5 para reducir la fricción del usuario y aumentar la seguridad de acceso a las aplicaciones.

SIMPLIFICAR LA APLICACIÓN DE VIRUS A CCESS

Los despliegues virtuales de escritorio y aplicaciones deben escalar para satisfacer las necesidades de miles de usuarios y cientos de conexiones por segundo. BIG-IP APM sirve como puerta de entrada para entornos de aplicaciones virtuales. Incluye soporte nativo para Microsoft Remote Desktop Protocol (RDP), soporte nativo para proxies web seguros para Citrix XenApp y XenDesktop, y acceso a proxies de seguridad para VMware Horizon. Los administradores pueden controlar la entrega y los componentes de seguridad de soluciones de virtualización empresarial mediante la gestión unificada de acceso, seguridad y políticas de BIG-IP APM. Estas capacidades escalables y de alto rendimiento simplifican el acceso y control del usuario en entornos de escritorio virtual alojados. BIG-IP APM ofrece soporte virtual sencillo y amplio para aplicaciones y escritorios.

BIG-IP APM soporta autenticación de dos factores vía RSA SecureID y RADIUS a través del cliente nativo para despliegues de VMware End User Computing (EUC). BIG-IP APM es compatible con Citrix Virtual Apps and Desktops y Citrix StoreFront. BIG-IP APM, cuando se integra con el protocolo Microsoft RDP, permite el acceso remoto al escritorio necesario para instalar componentes en el lado del cliente o ejecutar Java. Permite que Microsoft RDP esté disponible para su uso en nuevas plataformas, como dispositivos Apple iOS y Google Android. También permite clientes RDP nativos en plataformas no Windows como Mac OS y Linux, donde anteriormente solo se soportaba un cliente basado en Java. El soporte RDP de BIG-IP APM funciona con cualquier navegador web o aplicación RDP de Microsoft, Apple o Google.

PRO TEC TING API

Las APIs son el tejido conectivo en las arquitecturas de aplicaciones modernas. Los atacantes están aprovechando las APIs para lanzar ataques, porque están listas para ser explotadas: muchas organizaciones exponen las APIs al público y a sus socios de la cadena

de suministro o las dejan sin protección sin querer.
Mientras los atacantes explotan APIs para lanzar ataques, las organizaciones pueden garantizar la seguridad de las APIs mediante

autenticación, especialmente si es adaptable y está protegida por políticas de autenticación y autorización coherentes y flexibles. BIG-IP APM permite la autenticación segura para APIs REST. También garantiza que se tomen las acciones de autorización adecuadas. BIG-IP APM integra OpenAPI existentes, o archivos "swagger", ahorrando tiempo, recursos humanos y costes al desarrollar políticas de protección de API, asegurando al tiempo que existen políticas de protección de API precisas.

OBTENCIÓN DE CREDENCIALES

Las credenciales de usuario son como las llaves del reino: todo lo que un atacante tiene que hacer es robar un conjunto de credenciales de usuario y podrá disfrutar de acceso sin restricciones a la red, las nubes y las aplicaciones de tu organización.

La protección de credenciales de BIG-IP APM, como parte de una licencia opcional de BIG-IP DataSafe™, protege las credenciales contra robos y reutilizaciones. Protege contra ataques Man-in-the-Browser (MitB) mediante cifrado adaptable y en tiempo real, y cifra las credenciales de usuario introducidas en su webtop. BIG-IP APM, junto con BIG-IP DataSafe, hace que las credenciales sean ilegibles e inutilizables, incluso en el improbable caso de que un atacante las robe con éxito. BIG-IP APM también garantiza la seguridad de inicio de sesión para todas las aplicaciones asociadas mediante federación.

F 5 DEFENSA DISTRIBUIDA DE LA BO-T — CONSTRUIDA EN LA GRAN PLATAFORMA IP

Los bots causan un dolor financiero significativo mediante el scraping que ralentiza el rendimiento, el rescalping y el acaparamiento de inventario que frustran a los clientes fieles, la enumeración de códigos de tarjetas regalo para robar saldos, la creación de cuentas falsas para cometer fraude y el crepitado de credenciales —la prueba de credenciales robadas— que conduce a la toma de control de cuentas.

Los bots persistentes avanzados de hoy en día son más sofisticados que nunca, evadiendo muchas defensas estándar de bots disponibles dentro de los WAF. Los delincuentes reconfigurarán bots para saltarse defensas en cuestión de horas, utilizar millones de direcciones IP válidas, resolver rápidamente CAPTCHAs, imitar comportamientos humanos e introducir una sutil aleatoriedad.

Para adelantarse a los atacantes, F5® Distributed Cloud Bot Defense utiliza una recopilación de señales enriquecida en el lado del cliente, ofuscación de código líder en la industria, recopilación agregada de telemetría e IA para una eficacia a largo plazo sin precedentes y casi cero falsos positivos, manteniendo el acceso para bots buenos. Y dado que F5 defiende los sitios más atacados en la web —incluidos los de los bancos,

minoristas y aerolíneas más grandes del mundo— F5 está preparada cuando estos ataques tengan como objetivo tu organización.

Despliega Distributed Cloud Bot Defense directamente desde tu IP BIG-IP o a través de un conector adecuado para tu aplicación, con servicios de soporte adaptados a tus necesidades, desde autoservicio hasta servicio gestionado.

EDITOR VISUAL DE POLÍTICAS (VPE)

Gracias a su avanzado Editor Visual de Políticas (VPE) gráfico, BIG-IP APM hace que diseñar y gestionar políticas de control de acceso granulares, tanto individuales como grupales, sea rápido y sencillo. Con VPE, puedes crear y editar políticas de acceso dinámicas completas de forma eficiente con solo unos clics. El VPE de BIG-IP APM puede definir reglas por ruta de URL. Centralizando y simplificando la gestión de políticas contextuales, puedes dirigir de forma eficiente el acceso detallado de los usuarios a aplicaciones, redes y nubes.

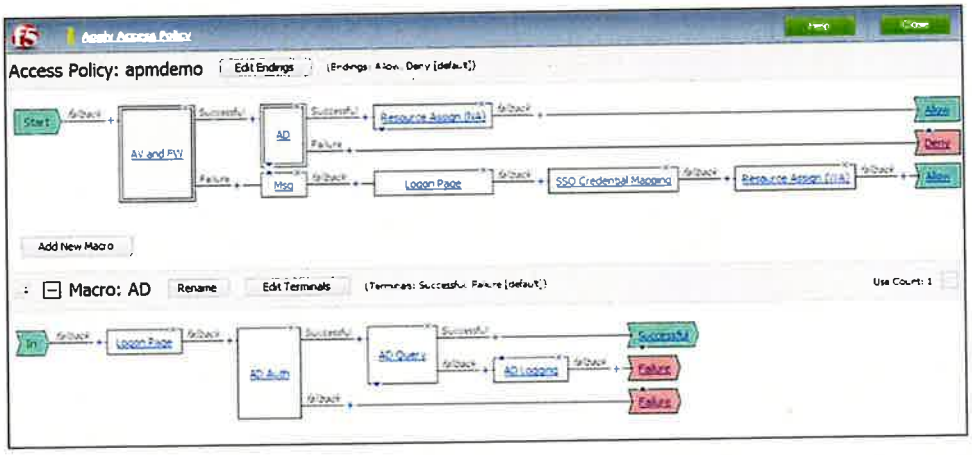


Figura 1: El VPE avanzado BIG-IP APM facilita la creación, modificación y gestión de políticas de acceso granulares basadas en aplicaciones, usuarios, red/nube y vulnerabilidades.

BIG-IP APM te permite diseñar políticas de acceso para autenticación y autorización, así como comprobaciones de seguridad en los endpoints, haciendo cumplir el cumplimiento de los usuarios con las políticas corporativas y las normativas del sector. Se puede definir un solo perfil de acceso para todas las conexiones que provengan de cualquier dispositivo, o puedes crear varios perfiles de acceso para diferentes métodos de acceso desde distintos dispositivos.

BIG-IP APM impone la autenticación de acceso mediante ACLs y autoriza a los usuarios con ACLs de capa 4 y capa 7 aplicadas dinámicamente en una sesión. Tanto las ACL de nivel 4 como las de nivel 7 se soportan en función de la postura del endpoint como punto de aplicación de políticas. El acceso individual y grupal a aplicaciones y redes aprobadas está permitido por BIG-IP APM utilizando ACLs dinámicas L7 por sesión (HTTP). El VPE en BIG-IP APM puede usarse para crear, modificar y gestionar ACLs de forma rápida y sencilla.

UNA CONFIGURACIÓN GUIADA POR CCESS (UN GC)

BIG-IP APM incluye una capacidad de Configuración Guiada por Acceso (AGC) que simplifica el despliegue y la gestión del acceso a aplicaciones. El AGC guía a tu administrador paso a paso en un proceso de configuración y despliegue de BIG-IP APM, ahorrándote

y el tiempo y coste de despliegue de tu administrador. El AGC de BIG-IP APM también permite a tu administrador integrar y gestionar de forma rápida y sencilla aplicaciones clásicas críticas para la misión, como SAP ERP y Oracle PeopleSoft, en Azure AD. Este acceso guiado simplificado elimina numerosos pasos previamente requeridos en Azure AD para salvar la brecha de acceso entre aplicaciones que soportan autenticación moderna y aplicaciones que soportan métodos clásicos de autenticación, reduciendo considerablemente la carga administrativa implicada en la modernización de dichas aplicaciones.

Figura 2: La configuración guiada por acceso de BIG-IP APM AHORRA TIEMPO Y COSTE DE DESPLIEGUE.

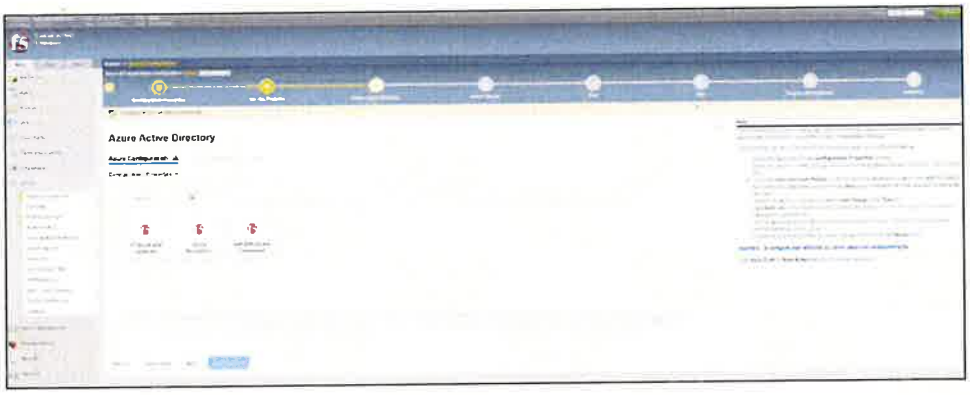


Figura 3: La configuración guiada por acceso de F5 BIG-IP APM permite una incorporación rápida y sencilla y gestión de aplicaciones personalizadas y clásicas, como SAP ERP y Oracle PeopleSoft, con Azure AD.

CENTRALIZAR UN MANA DE POLÍTICA DE CCESS

Si tienes múltiples despliegues de APM BIG-IP, F5 BIG-IQ Centralized® Management te ayudará a gestionarlos de forma eficiente. Puede gestionar políticas para hasta 100 instancias BIG-IP APM, permitiéndote importar, comparar, editar y actualizar políticas de acceso granulares entre múltiples dispositivos de usuario.

Con BIG-IQ Centralized Management y BIG-IP APM, puedes importar configuraciones desde una instancia maestra "source" de BIG-IP APM, simplificando la distribución de políticas de acceso. También puedes
editar objetos específicos de dispositivo o ubicación directamente en BIG-IQ Centralized Management y hacer que se propaguen a lo largo de tu despliegue APM DE BIG-IP. Puedes ver fácilmente las diferencias entre las configuraciones de acceso actuales y propuestas.

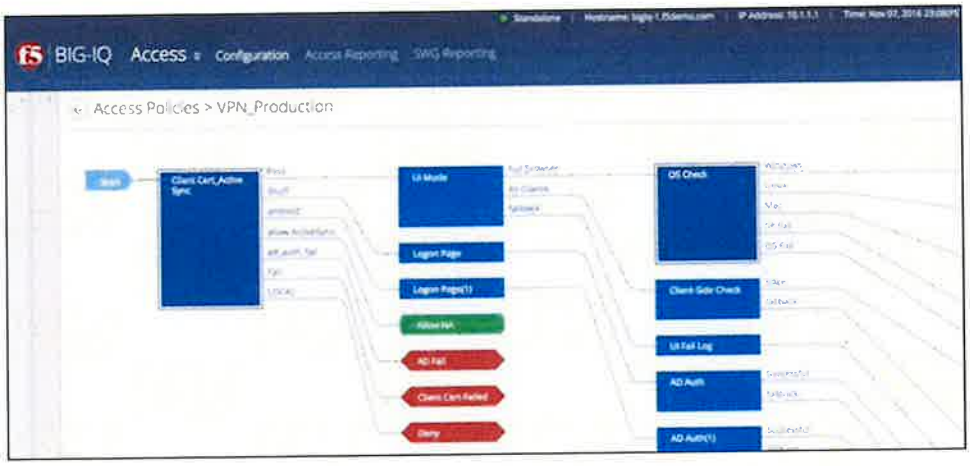


Figura 4: La Gestión Centralizada de BIG-IQ permite la importación, comparación, edición y actualización de políticas de acceso en múltiples dispositivos desde una única interfaz.

MEJORAR LA VISIBILIDAD Y LA REPERCUSIÓN

Una vista detallada de los registros y eventos proporciona detalles de la sesión de política de acceso. Con informes disponibles a través de BIG-IQ Centralized Management, BIG-IP APM te ayuda a obtener mayor visibilidad sobre el acceso a aplicaciones y las tendencias de tráfico, agregar datos para la forense a largo plazo, acelerar respuestas a incidentes e identificar problemas e imprevistos antes de que los usuarios puedan experimentarlos.

BIG-IP APM puede personalizar informes con datos y estadísticas granulares para informes y análisis inteligentes. Ejemplos incluyen informes detallados de sesiones por:

- Fallos de acceso
- Usuarios
- Recursos consultados
- Uso en grupo
- Geolocalización IP

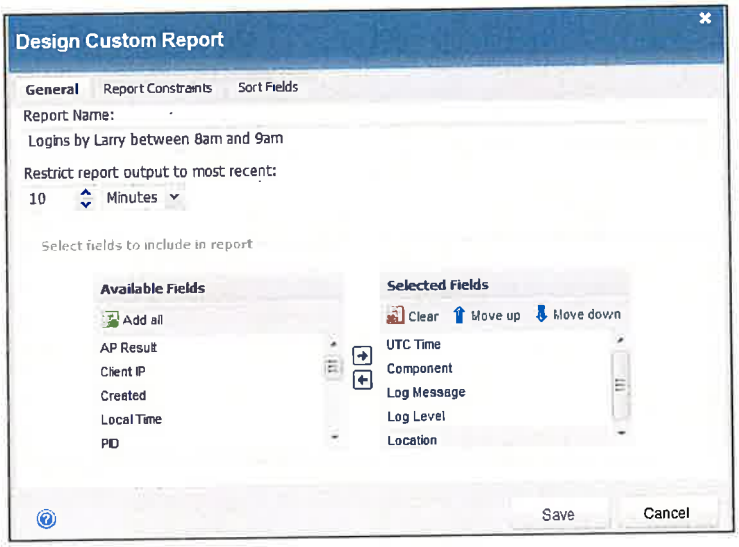


Figura 5: Los informes personalizados proporcionan datos y estadísticas detalladas para un análisis inteligente.

BIG-IP APM se integra con la Gestión Centralizada de BIG-IQ para ofrecer una mayor visibilidad a través de informes de acceso y registros. Ofrece informes analíticos y registros basados en dispositivos y grupos, para que puedas aumentar tu conocimiento sobre el acceso y análisis de los usuarios. También te ayuda a tomar medidas rápidas si es necesario, incluyendo la terminación de sesiones de acceso específicas. Además, ofrece una exportación en CSV de los datos de informes BIG-IP APM, por lo que está accesible para informes personalizados. La vista personalizada de panel de BIG-IQ Centralized Management te ayuda a visualizar mejor tendencias y contextos de relaciones con mayor facilidad. Esto mejora tu tiempo de respuesta si surgen problemas. A través de esta visión holística del acceso a aplicaciones y red, puedes comprender mejor la eficacia de las políticas de acceso que has establecido, localizar y abordar puntos débiles, y mejorar tus respuestas a problemas y preocupaciones.

Figura 6: El panel completo de gestión centralizada de BIG-IQ para BIG-IP APM te ayuda a visualizar mejor las tendencias y los contextos de relaciones.

Libro blanco F5

TMOS: Redefiniendo la solución

Este documento aborda la arquitectura F5 TMOS, una colección de características y funciones en tiempo real, diseñada y construida específicamente como una solución de proxy completa con la potencia y el rendimiento requeridos en la infraestructura de red actual.

Por KJ (Ken) Salchow, Jr.
Gerente de Marketing Técnico

Contenido

Resumen ejecutivo

Históricamente, ha habido dos maneras de diseñar dispositivos de red de entrega de aplicaciones: priorizar el rendimiento o la inteligencia. En el mercado, los clientes tradicionalmente han optado por las soluciones con el mejor rendimiento. Por ello, la mayoría de los proveedores han basado sus dispositivos en diseños más rápidos, basados en paquetes, en lugar de la arquitectura basada en proxy, de menor rendimiento. A medida que ha aumentado la necesidad de inteligencia en estos dispositivos, los proveedores se encuentran en una posición delicada: cuanta más inteligencia añaden para satisfacer la demanda de los clientes, más se asemejan a un proxy y peor es su rendimiento.

Inicialmente, F5 optó por la solución basada en paquetes, pero simultáneamente comenzó a abordar el problema de raíz, creando una solución inteligente que también ofrece un alto rendimiento. El resultado es el F5 TMOS.®Arquitectura, un conjunto de características y funciones en tiempo real, diseñada y construida específicamente como una solución de proxy completa con la potencia y el rendimiento necesarios en la infraestructura de red actual.

Basado en paquetes frente a basado en proxy

Para comprender cuán único y potente es TMOS, es importante examinar detenidamente la historia de estos dispositivos de red de entrega de aplicaciones y el dilema entre velocidad e inteligencia con soluciones basadas en paquetes y basadas en proxies.

¿Qué es un diseño basado en paquetes?

Un dispositivo de red con diseño basado en paquetes (o paquete a paquete) se sitúa en medio de un flujo de comunicaciones, pero no es un extremo de dichas comunicaciones; simplemente las reenvía. A menudo, un dispositivo que opera paquete a paquete tiene cierto conocimiento de los protocolos que lo atraviesan, pero dista mucho de ser un verdadero extremo de protocolo. La velocidad de estos dispositivos se basa principalmente en no tener que comprender toda la pila de protocolos, lo que reduce el trabajo necesario para gestionar el tráfico. Por ejemplo, con TCP/IP, este tipo de dispositivo podría comprender los protocolos lo suficientemente bien como para reescribir las direcciones IP y los puertos TCP; aproximadamente la mitad de la pila completa.

A medida que las redes se volvieron más complejas y aumentó la necesidad de inteligencia, comenzaron a surgir diseños basados en paquetes más avanzados (incluido BIG-IP).®(productos de F5). Estos dispositivos conocían TCP/IP lo suficientemente bien como para comprender tanto el establecimiento como la finalización de la conexión TCP, modificar las cabeceras TCP/IP e incluso insertar datos en

Wagner Ponce

Flujos TCP. Dado que estos sistemas podían insertar datos en flujos TCP y modificar su contenido, también debían reescribir los valores de secuencia (SEQ) y acuse de recibo (ACK) de los paquetes que se enviaban entre el cliente y el servidor. Los productos BIG-IP de F5 comprendían TCP/IP y HTTP lo suficientemente bien como para identificar solicitudes HTTP individuales y podían enviar diferentes solicitudes a distintos servidores, reutilizando las conexiones que el dispositivo BIG-IP ya tenía abiertas.

Si bien todo esto es posible utilizando una arquitectura paquete por paquete muy sofisticada (los dispositivos BIG-IP son algunos de los diseños más sofisticados de este tipo hasta la fecha), requirió un motor de seguimiento de estado muy complejo para comprender los protocolos TCP/IP y HTTP lo suficientemente bien como para reescribir el contenido de los encabezados, insertar datos y mantener sus propias conexiones con clientes y servidores.

A pesar de esta creciente complejidad, los diseños basados en paquetes siguen siendo menos complejos y más rápidos que los diseños tradicionales basados en proxies, ya que tienen la ventaja de requerir solo un pequeño porcentaje de la lógica necesaria para un proxy completo.

¿Qué es un diseño basado en proxy (proxy completo)?

Un diseño de proxy completo es lo opuesto a un diseño paquete a paquete. En lugar de tener un conocimiento mínimo de las comunicaciones que fluyen a través del dispositivo, un proxy completo comprende completamente los protocolos y actúa como punto final y origen de los mismos. La conexión entre un cliente y el proxy completo es totalmente independiente de la conexión entre el proxy completo y el servidor; mientras que en un diseño paquete a paquete, existe esencialmente un canal de comunicación directo entre el cliente y el servidor (aunque el dispositivo intermedio puede manipular los paquetes que se transmiten).

Dado que el proxy completo es un punto final de protocolo real, debe implementar completamente los protocolos tanto como cliente como servidor (un diseño basado en paquetes no lo requiere). Esto también significa que el proxy completo puede tener su propio comportamiento de conexión TCP, como el almacenamiento en búfer, las retransmisiones y las opciones TCP. Con un proxy completo, cada conexión es única y puede tener su propio comportamiento de conexión TCP. Esto implica que un cliente que se conecta al dispositivo proxy completo probablemente tendrá un comportamiento de conexión diferente al que el proxy completo podría usar para comunicarse con los servidores de backend. Por lo tanto, un proxy completo permite la optimización de cada conexión de forma única, independientemente del origen y el destino. Además, un proxy completo comprende y procesa cada protocolo como lo haría un cliente o servidor real, utilizando capas. Tomando HTTP como ejemplo, primero se procesa el protocolo IP, luego TCP y finalmente HTTP; y cada capa desconoce las capas inferiores.

Redefiniendo la solución

Es sabido que las soluciones basadas en proxies, o al menos la inteligencia que ofrecían, eran la solución definitiva. Sin embargo, el rendimiento muy superior de los diseños de enrutamiento paquete a paquete compensó con creces su inteligencia limitada. Durante un tiempo, esta fue una solución aceptable para la mayoría de las redes empresariales.

A medida que crece la necesidad de mayor inteligencia, las soluciones basadas en paquetes experimentan rápidamente las mismas limitaciones de rendimiento que siempre han afectado a las soluciones basadas en proxies. Además, la complejidad de desarrollo de las soluciones basadas en paquetes se acerca rápidamente a la de los diseños basados en proxies. A pesar de los drásticos aumentos en la potencia del hardware y el software, los diseños basados en paquetes no pueden satisfacer la demanda de inteligencia y rendimiento. Ya no es aceptable tener que elegir entre ellos.

Si bien las soluciones basadas en paquetes tuvieron su momento, ese momento ya pasó. Ahora resulta evidente que sacrificar la inteligencia en aras del rendimiento no proporcionó una solución viable. La verdadera solución consiste en desarrollar una solución basada en proxies con el mismo rendimiento que la solución basada en paquetes.

TMOS

TMOS es un término colectivo que describe la arquitectura completamente personalizada y diseñada específicamente para este fin, en cuyo desarrollo F5 invirtió años y una cantidad significativa de recursos como base para los futuros productos de F5. En términos generales, TMOS es:

- **Una colección de módulos**

  Cada módulo realiza una función específica. Por ejemplo, existe un módulo controlador de red, un módulo Ethernet, un módulo ARP, un módulo IP, un módulo TCP, etc. Cada componente del sistema es autónomo, lo que reduce su complejidad y facilita el desarrollo futuro. Añadir compatibilidad con nuevos protocolos es tan sencillo como agregar un nuevo módulo. Este diseño también permite una reutilización más sencilla. Si un nuevo protocolo de aplicación se ejecutara sobre TCP/IP, sería muy fácil interconectar los módulos para que el nuevo protocolo accediera a los datos de TCP/IP sin necesidad de comprender los protocolos de nivel inferior.

- **Autocontenido y autónomo**

  Muchos usuarios han observado que un dispositivo basado en TMOS ejecuta una distribución de Linux, lo cual se puede apreciar al administrarlo mediante la línea de comandos. Es importante destacar que este sistema Linux no interviene en ningún aspecto del tráfico que fluye a través de TMOS. TMOS cuenta con su propia CPU, memoria y bus de sistema dedicados para el acceso a los periféricos. Cuando un dispositivo basado en TMOS recibe paquetes, todo, desde la conexión por cable hasta el bus de sistema, desde el subsistema de red hasta el subsistema de gestión de memoria, se encuentra completamente aislado dentro de TMOS. Linux no interviene ni tiene conocimiento de nada de esto; ni siquiera el kernel de Linux. El sistema Linux se utiliza únicamente para tareas de administración, como la línea de comandos o la interfaz gráfica web.

  La razón es sencilla: un sistema operativo ideal para la gestión de tráfico de alta velocidad no lo es como sistema operativo de propósito general. Por lo tanto, conviene usar un sistema operativo de propósito general para tareas generales, como la gestión, y dejar la gestión del tráfico al sistema operativo diseñado para ello: TMOS.

- **Un sistema operativo en tiempo real**

  Un sistema operativo en tiempo real implica que TMOS no cuenta con un planificador de CPU preventivo. Para los sistemas operativos de propósito general, disponer de un planificador preventivo en el núcleo es muy conveniente, ya que permite que todos los procesos obtengan una distribución equitativa del tiempo de CPU y muchos de ellos se ejecuten prácticamente al mismo tiempo. En un sistema operativo de propósito específico y altamente optimizado como TMOS, dicho planificador no resulta adecuado, pues añade una sobrecarga innecesaria. TMOS se diseñó y optimizó para que cada componente del sistema realice las operaciones necesarias y, a continuación, permita la ejecución del siguiente componente. Esto reduce significativamente la sobrecarga de la planificación de la CPU al eliminar las interrupciones, los cambios de contexto y la mayor parte del trabajo que normalmente realizaría un planificador. Además, permite un control total sobre cuándo y en qué orden se produce el procesamiento.

- **Tanto el hardware como el software**

  Gracias a su diseño modular inherente, TMOS no tiene por qué ser gestionado por software o hardware. Con TMOS, todo puede realizarse mediante software utilizando módulos altamente optimizados y diseñados específicamente para este fin; sin embargo, las operaciones que consumen muchos recursos también pueden delegarse a hardware especializado. Por ejemplo, TMOS cuenta con su propia pila SSL y puede procesar SSL completamente por software, pero es mucho más rápido delegar las operaciones criptográficas a circuitos integrados de aplicación específica (ASIC) SSL especializados. Disponer de una tecnología de software completa permite una flexibilidad prácticamente ilimitada, y contar con hardware especializado para la delegada de tareas permite una escalabilidad rentable hasta alcanzar niveles de rendimiento líderes en el sector.

• **Impulsado por eventos**

La combinación de modularidad y procesamiento en tiempo real otorga a TMOS la capacidad única de modificar su comportamiento en función de eventos reales y en tiempo real. Cada evento, desde el inicio de la conexión del cliente hasta el procesamiento de la carga útil —incluso el tráfico de retorno del servidor al cliente— representa una oportunidad para que TMOS ajuste su comportamiento a las necesidades actuales. Esta funcionalidad convierte a TMOS en la solución más adaptable y flexible del mercado.

• Inspección estatal

La arquitectura principal de TMOS se basa en un proxy completo de alta velocidad que realiza una inspección con estado del flujo de tráfico, al igual que un firewall con estado. Mientras el tráfico de conexión se redirige a través de TMOS, las reglas iRules de F5●El motor tiene acceso completo (capas 2-7) a ese tráfico y puede establecer diversas reglas (basadas en las características del tráfico, las ACL o la lógica de negocio). Por ejemplo, las acciones de las reglas pueden ser Descartar, Bloquear, Redirigir, Registrar o Transformar.

• Filtrado dinámico de paquetes

Por defecto, al igual que un firewall, TMOS tiene una política de "denegación total". Una importante ventaja de seguridad de TMOS es que su proxy completo oculta por completo la pila de red de los servicios de backend. Las iRules de F5 en TMOS permiten el control dinámico del flujo de tráfico de las aplicaciones, como el control dinámico de las políticas de modelado de tráfico en función de la aplicación (no solo del protocolo TCP o de red), la solicitud o el contenido de la respuesta. El flujo de tráfico también se puede filtrar, redirigir o bloquear dinámicamente en la misma capa de aplicación, como HTTP, o paquete por paquete, por ejemplo, mediante UDP, SCP o TCP.

Todos estos elementos convierten a TMOS en una solución extremadamente potente y adaptable. La combinación de modularidad en un sistema operativo autónomo, en tiempo real y basado en eventos, le confiere a TMOS capacidades sin precedentes. Por ejemplo, TMOS puede utilizar tres pilas de red completamente únicas, diseñadas para satisfacer los requisitos de implementación. En primer lugar, está la pila FastL4: un diseño TCP/UDP de estado limitado o tradicional paquete a paquete para gestionar cualquier alta velocidad de conexión, pero con requisitos de funcionalidad limitada (capa 4 e inferiores). A continuación, está la pila FastHTTP: una pila TCP/HTTP de estado limitado que representa un diseño paquete a paquete extremadamente avanzado para gestionar altas velocidades de conexión con mayores requisitos de inteligencia HTTP (capa 7). Por último, está el Fast Application Proxy: la pila predeterminada basada en proxy completo, que representa la cúspide del diseño basado en proxy. El hecho de que TMOS pueda utilizar componentes de software y hardware indistintamente permite que toda la pila FastL4 se ejecute completamente en el ASIC Packet Velocity de F5.

(PVA) si el sistema está equipado con el hardware PVA. La elección del enfoque más adecuado depende exclusivamente del cliente.

Por sí solo, cualquiera de estos descriptores de alto nivel diferenciaría a TMOS de cualquier solución existente, ya sea basada en paquetes o en proxies. Esta arquitectura, por sí sola, bastaría para revolucionar el mercado de las redes de entrega de aplicaciones, pero incluso la mejor arquitectura construida con componentes de baja calidad resulta en una solución deficiente. Los componentes, o módulos, con los que se construye TMOS la convierten en una solución verdaderamente superior.

Llevándolo al siguiente nivel

Lo que hace extraordinaria la arquitectura TMOS son los módulos personalizados creados para soportarla. Entre los más importantes se encuentran algunos de los más utilizados: TCP Express. ™ Proxy de aplicación rápido™y iRules.

TCP Express

Los diseños paquete por paquete simplemente no pueden proporcionar lo que TMOS puede con el El conjunto de características de TCP Express. Existen empresas que cuentan con un proxy completo, pero este se ve limitado por ser simplemente un componente de un sistema UNIX de propósito general. Les resulta imposible alcanzar el rendimiento de un sistema operativo personalizado en tiempo real, diseñado para proporcionar una conectividad de red de baja latencia y de última generación. Simplemente, no es posible añadir este tipo de funcionalidad una vez diseñado el producto; requiere un compromiso arquitectónico fundamental con la conectividad de red de alto rendimiento y baja latencia.

TCP Express es un conjunto de mejoras de eficiencia de TCP, en forma de estándares de Internet (RFC), y cientos de funciones y ajustes personalizados de F5 basados en nuestra amplia experiencia práctica. TMOS es compatible con todas las mejoras de eficiencia de TCP modernas, incluidas:

- Reconocimientos tardíos y selectivos (RFC 2018)
- Notificación explícita de congestión (ECN), (RFC 3168)
- Retransmisiones limitadas y rápidas (RFC 3042 y RFC 2582)
- Arranque lento con prevención de congestión (RFC 2581)
- Ventanas de congestión inicial adaptativas (RFC 3390)
- Marcas de tiempo y escalado de ventanas (RFC 1323)

- Arranque lento de TCP (RFC 3390)
- Control de retardo de ancho de banda y muchos más (Vegas, NewReno, etc.)

Estas características, junto con más de cien otras, buscan alcanzar el máximo rendimiento en cualquier escenario de conexión. Cada dispositivo con el que interactúa TMOS presenta un escenario de red diferente. Para lograr el máximo rendimiento en todos los dispositivos conectados, TMOS debe reaccionar de forma inteligente a los requisitos específicos de cada dispositivo y de cada conexión. No basta con admitir una o dos optimizaciones TCP avanzadas. Tampoco basta con desarrollar optimizaciones propias y optimizar el producto en el entorno de producción. Se requiere una optimización TCP completa, extensiones personalizadas y exhaustivas pruebas en entornos reales, además de un sistema operativo optimizado en tiempo real y con baja latencia, para alcanzar un rendimiento óptimo. Todo esto debe implementarse de forma conjunta para obtener un beneficio real significativo, tal y como lo ha hecho F5 con TMOS.

Proxy de aplicación rápida

El componente Fast Application Proxy de TMOS, la pila de proxy completa, es otro factor diferenciador clave. Esto es lo que permite a TMOS ofrecer más funciones de aceleración y optimización que cualquier otra solución anterior o posterior. Normalmente, la lógica de inspección o inteligencia sacrifica velocidad, y es lógico: cuanta más carga de trabajo se requiere por conexión, menos conexiones se pueden gestionar. Lo que hace que Fast Application Proxy sea tan único es que, al aprovechar el hardware de forma transparente cuando es posible, junto con un sistema operativo personalizado de alto rendimiento en tiempo real (TMOS), logra un rendimiento verdaderamente inigualable, a la vez que ofrece todas las ventajas de un diseño de proxy completo. Además, Fast Application Proxy proporciona la fluidez de aplicación necesaria para implementar otros módulos de TMOS, entre ellos:

- Compresión HTTP
  - Almacenamiento en caché de múltiples tiendas
- Aceleración SSL
- Caché rápida
  - Almacenamiento en cola de contenido
- Compresión inteligente
  - Calidad de servicio/Términos de servicio
- Modelado de velocidad L7

Todo encaja a la perfección. TMOS proporciona una arquitectura que permite al Fast Application Proxy ofrecer inteligencia y rendimiento; y el Fast Application Proxy, gracias a la arquitectura TMOS, permite el uso inteligente de numerosos módulos adicionales, tanto de hardware como de software, que proporcionan un rendimiento aún mayor.

iRules

Las iRules son una de las funcionalidades más exclusivas de TMOS. Se trata de scripts creados con el lenguaje de comandos de herramientas (TCL) estándar, con extensiones F5 personalizadas que permiten a los usuarios crear funciones únicas que se activan a partir de eventos de TMOS. Si bien las reglas en sí son fáciles de crear y comprender, este módulo las compila en bytecode, el cual ejecuta acciones como la lectura y escritura de cookies HTTP mediante llamadas a funciones personalizadas y altamente optimizadas en el núcleo de TMOS. La combinación de estas dos tecnologías clave permite que el texto simple de la regla TCL se convierta en bytecode de alto rendimiento que realiza la inspección y manipulación de forma nativa en TMOS, lo que resulta en una gran rapidez.

Desde el lanzamiento inicial de TMOS, los clientes de F5 han encontrado cientos de maneras de aprovechar la potencia del motor iRules en TMOS. Por ejemplo:

- Limitación de la velocidad del DNS.
- Implementar un proxy SMTP para inspeccionar y dirigir mensajes individuales.
- Reordenar las cookies HTTP para facilitar su análisis en los sistemas de back-end.
- Autenticar las conexiones de usuario con un servidor RADIUS de backend utilizando credenciales almacenadas en una cookie HTTP.
- Implementar un analizador LDAP simple para inspeccionar los parámetros de las solicitudes LDAP bind().
- Utilizar selectivamente el recifrado SSL en los servidores back-end solo para determinadas URL HTTP. Y exigir selectivamente certificados de cliente SSL en función de URL HTTP.
- Crear e insertar un valor de ID de sesión personalizado en una solicitud HTTP, que el servidor devolverá en la respuesta. A continuación, se inspecciona la respuesta y se verifica que coincida con la solicitud. De no ser así, se registra la información completa de la sesión y las últimas 100 solicitudes.
- Multiplexación de solicitudes CORBA/IIOP.

No existe otro dispositivo en el mundo capaz de implementar este tipo de lógica tan sofisticada mediante su conjunto de funciones de inspección. Se trata de iRules sencillas que toman

Aprovechar la flexibilidad sin parangón de TMOS y su arquitectura basada en eventos. Además, si bien no podemos atribuirlo directamente a TMOS, iRules y su desarrollo han dado lugar a su propia comunidad de desarrolladores, que supera los 7000 miembros en todo el mundo:Centro de desarrollo .

Si bien TCP Express, el Fast Application Proxy e iRules son solo tres de los muchos componentes únicos y altamente optimizados construidos sobre y dentro de TMOS, presentan una visión amplia del hecho de que TMOS no se limita a una arquitectura innovadora, sino que también incluye los componentes de vanguardia para hacer que esa arquitectura cobre vida.

El desarrollo de diseños basados en paquetes surgió de la necesidad de proporcionar dispositivos de red para la entrega de aplicaciones que ofrecieran un rendimiento excepcional, además de cierta inteligencia, aunque menor que la de sus contrapartes basadas en proxies. La capacidad de estos dispositivos para satisfacer las necesidades de las redes actuales ha llegado a su fin, y la mayoría de los proveedores se encuentran en la misma situación inicial: necesitan ofrecer la inteligencia de un proxy completo con los requisitos de rendimiento aún mayores de las redes actuales. La elección de una arquitectura basada en paquetes ha demostrado ser una decisión poco acertada.

F5 comprendió desde el principio que la única solución a largo plazo era una arquitectura basada en proxy diseñada para ofrecer rendimiento y una flexibilidad sin precedentes para afrontar cualquier desafío futuro. El resultado de esta visión, junto con un importante tiempo de desarrollo e inversión, es TMOS. TMOS es la primera arquitectura de proxy completamente diseñada para este fin: modular, autónoma, en tiempo real y basada en eventos, con la capacidad de utilizar hardware y software de forma transparente y unilateral para lograr el máximo rendimiento e inteligencia. Además, TMOS va más allá de una arquitectura revolucionaria y establece un nuevo estándar para cada uno de sus componentes. Desde TCP Express, que garantiza las conexiones de red más eficientes tanto para el cliente como para el servidor, hasta el Fast Application Proxy, que proporciona inteligencia y rendimiento, pasando por iRules, que permiten el control y la personalización completos de todas estas funciones y de los numerosos componentes de aceleración, seguridad y disponibilidad de aplicaciones, TMOS es, sencillamente, la única solución de Application Delivery Networking que no parte de cero. TMOS ya es la solución ideal.

F5 Networks, Inc.401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Sede corporativa
info@f5.com

Redes F5
Asia-Pacífico
apacinfo@f5.com

F5 Networks Ltd.
Europa/Oriente Medio/África
emeainfo@f5.com

Redes F5
Japón KK
f5j-info@f5.com

CS01-00035 0111

QUÉ HAY DENTRO

Acceso sencillo, seguro y sin interrupciones a cualquier aplicación, en cualquier lugar

Las aplicaciones son puertas de enlace a tus datos críticos y sensibles. El acceso simple y seguro a tus aplicaciones es fundamental, pero hoy en día el acceso a aplicaciones es extremadamente complejo. Las aplicaciones pueden alojarse en cualquier lugar: en la nube pública, en una nube privada, en las instalaciones o en un centro de datos. Garantizar que los usuarios tengan acceso seguro y autenticado en cualquier momento y lugar, solo a la
Las aplicaciones a las que están autorizados a acceder ahora supone un desafío importante. Existen diferentes métodos de acceso a aplicaciones para gestionar estas complejidades. Existen diversas fuentes para la identidad autorizada del usuario, así como para tratar con aplicaciones que requieren métodos modernos o tradicionales de autenticación y autorización, inicio de sesión único (SSO), federación y más, además de la experiencia de acceso del usuario para dar soporte y considerar.

Con la transformación digital afectando a todos los aspectos de una empresa hoy en día, las aplicaciones nativas en la nube y Software como Servicio (SaaS) son ahora el estándar de las aplicaciones empresariales. Sin embargo, muchas organizaciones descubren que no pueden o no quieren migrar todas sus aplicaciones a la nube. Puede haber aplicaciones clásicas o personalizadas críticas que no deberían
o no puede soportar la migración a la nube pública ni ser fácilmente reemplazada por una aplicación SaaS. Las aplicaciones se alojan en una variedad de ubicaciones, con métodos de autenticación y autorización diferentes y muchas veces dispares que no pueden comunicarse entre sí y no funcionan sin problemas entre SSO o identidades federadas existentes, que no pueden soportar los medios de identidad más recientes como Identidad como Servicio (IDaaS) y no están equipados para soportar autenticación multifactor (MFA).

F5® BIG-IP® Access Policy® Manager (APM) es una solución proxy de gestión de accesos segura, flexible y de alto rendimiento que gestiona el acceso global a tu red, la nube, aplicaciones e interfaces de programación de aplicaciones (APIs). A través de una única interfaz de gestión,
BIG-IP APM consolida acceso remoto, móvil, de red, virtual y web. Con BIG-IP APM, puedes crear, hacer cumplir y centralizar políticas de acceso a aplicaciones simples, dinámicas e inteligentes para todas tus aplicaciones, independientemente de dónde o cómo estén alojadas.

BENEFICIOS CLAVE

Simplifica el acceso a todas las aplicaciones : ponte el acceso seguro a aplicaciones locales y en la nube con un solo inicio de sesión vía SSO. Incluso funciona para aplicaciones que no pueden soportar autenticación moderna como como Lenguaje de Marcado de Aserción de Seguridad (SAML), o OAuth y OpenID Connect (OIDC).

Acceso a aplicaciones de confianza cero El Proxy Consciente de la Identidad (IAP) ofrece una validación del modelo de confianza cero para el acceso a aplicaciones basada en la conciencia de identidad y el contexto granular, asegurando cada solicitud de acceso a la aplicación sin necesidad de VPN.

Acceso web seguro
Controla el acceso a aplicaciones y contenidos web centralizando la autenticación, autorización e inspección de endpoints mediante proxy de aplicación web.

Centralizar y gestionar el control de acceso
Consolidar la gestión de accesos remotos, móviles, de red, virtuales y web en una única interfaz de control con federación adaptativa de identidad, SSO y MFA mediante políticas aplicadas dinámicamente, basadas en el contexto y conscientes de la identidad.

Autenticación y autorización simplificadas
Federación adaptativa de identidades, SSO y MFA que emplean SAML, OAuth y OIDC para una experiencia de usuario fluida y segura en todas las aplicaciones.

PUENTE SEGURO APLICACIÓN A CCESS

Los protocolos modernos de autenticación y autorización —incluyendo Secure Assertion Markup Language (SAML) y OAuth con OpenID Connect (OIDC)— reducen la dependencia del usuario respecto a las contraseñas, aumentan la seguridad y mejoran la experiencia y productividad del usuario. Sin embargo, no todas las aplicaciones soportan protocolos modernos de autenticación y autorización. Muchas aplicaciones, como las clásicas o las creadas a medida, soportan autenticación clásica
y métodos de autorización, como Kerberos, NT LAN Manager (NTLM), RADIUS, basados en cabeceras y más. Esto complica aún más el acceso y la seguridad de las aplicaciones. La necesidad de soportar protocolos diferentes y dispares que no pueden compartir información de autenticación y autorización de usuarios dificulta el uso de SSO y MFA. Eso, a su vez, afecta negativamente a la experiencia del usuario y a la seguridad de las aplicaciones. También dificulta adaptar la contraseña corporativa moderna
política de cambios periódicos de contraseña y aumenta los costes organizativos a medida que se requieren múltiples métodos de acceso.

BIG-IP APM sirve como puente entre protocolos y métodos modernos y clásicos de autenticación y autorización. Para aplicaciones que no pueden soportar protocolos modernos de autenticación y autorización, como SAML y OAuth con OIDC, pero que sí lo soportan
métodos clásicos de autenticación, el BIG-IP APM convierte las credenciales del usuario al estándar de autenticación adecuado soportado por la aplicación. BIG-IP APM garantiza que los usuarios u organizaciones puedan usar SSO para acceder a cualquier aplicación en cualquier lugar—independientemente de su ubicación (en las instalaciones, en un centro de datos, en una nube privada o en la nube pública como aplicación nativa en la nube o SaaS), o si soporta o no autenticación moderna o clásica y
autorización. Esto ayuda a reducir el número de contraseñas que los usuarios deben crear, recordar y utilizar, ayudando a frenar la oleada de ataques basados en credenciales. Permite el cumplimiento de las políticas corporativas modernas de cambios periódicos de contraseña para combatir el robo de credenciales. Eso
también reduce el coste para las organizaciones de tener que comprar y mantener soluciones de acceso separadas para aplicaciones alojadas localmente, en un centro de datos y en una nube privada, en comparación con la nube nativa y las aplicaciones SaaS.

BIG-IP APM soporta opciones de federación de identidad y SSO al soportar conexiones iniciadas tanto por proveedores de identidad SAML (IdP) como por proveedores de servicios (SP) que aprovechan SAML 2.0. F5 soporta el consumo de tokens JOU, lo que permite a BIG-IP APM consumir tokens JWT cifrados de proveedores SAML IdP. Esto permite que BIG-IP APM mantenga el secreto entre el emisor o el token y el destinatario. BIG-IP APM permite a los administradores habilitar y desactivar de forma centralizada el acceso autorizado por usuarios a cualquier aplicación habilitada por identidad, independientemente de dónde esté alojada, ahorrando tiempo y aumentando la productividad administrativa.

El soporte para el estándar abierto OAuth 2.0 para autorizaciones permite que BIG-IP APM actúe como cliente, como delegado de autorización para aplicaciones SaaS y puede mejorar la protección y autorización de APIs para servicios web.

BIG-IP APM soporta Proof Key for Code Exchance (PKCE), un flujo de autorización más seguro basado en OAuth 2.0 que mejora la seguridad para todos los clientes OAuth (incluidos móviles y públicos).

BENEFICIOS CLAVE (CONT.)

Defiende tus eslabones más débiles Protege contra la pérdida de datos, malware y acceso fraudulento a dispositivos con controles integrales y continuos de integridad y seguridad en los endpoints.

APIs de protección Habilitar la autenticación segura para APIs REST e integrar archivos OpenAPI o "swagger" para garantizar acciones de autenticación adecuadas mientras ahorra tiempo y costes.

Hazlo todo a gran escala Soporta a todos los usuarios de forma sencilla, rápida y rentable, sin compensaciones en rendimiento en cuanto a seguridad, incluso en los entornos más exigentes.

Esto ayuda a prevenir ataques como la interceptación de códigos de autorización al habilitar tokens secretos dinámicos. PKCE permite que las aplicaciones realicen solicitudes directas al proveedor del token, añadiendo una capa extra de seguridad para las aplicaciones públicas.

SUPPOR T PARA ID AAS

Con soporte para SSO y tickets Kerberos en múltiples dominios, el APM BIG-IP permite tipos adicionales de autenticación, como las Common Access Cards (CAC) del Gobierno Federal de EE. UU. y el uso de IDaaS —como Azure Active Directory (Azure AD), Okta y otros— para acceder a todas las aplicaciones independientemente de la ubicación o del soporte moderno de autenticación y autorización. Por ejemplo, los usuarios pueden iniciar sesión automáticamente en aplicaciones y servicios de backend que forman parte de un ámbito Kerberos. Esto proporciona un flujo de autenticación fluido una vez que el usuario ha sido autenticado mediante un mecanismo de autenticación de usuario soportado. BIG-IP APM también es compatible con tarjetas inteligentes con proveedores de credenciales, para que los usuarios puedan conectar sus dispositivos a su red antes de iniciar sesión.

SUPPOR T PARA MFA

A través del extenso ecosistema de socios de F5, BIG-IP APM también se integra con la mayoría de las soluciones de MFA líderes, incluyendo las de Cisco Duo, Okta, Azure AD y otros. Al integrarse con tu solución de MFA existente, BIG-IP APM permite la autenticación adaptativa, permitiendo emplear diversas formas de autenticación de uno, dos o múltiples factores basadas en la identidad del usuario, el contexto y el acceso a la aplicación. Además, para ayudarte a desplegar MFA, BIG-IP APM incluye autenticación con contraseña de un solo uso (OTP) mediante correo electrónico o SMS.

Después de que el usuario ha iniciado sesión en una aplicación, puede requerirse un método adicional de autenticación para asegurar un acceso seguro a aplicaciones y archivos críticos o especialmente sensibles. Esto se conoce comúnmente como autenticación step-up. BIG-IP APM soporta autenticación step-up para autenticación de un solo y varios factores. Cualquier variable de sesión puede usarse para activar la autenticación step-up, y puedes utilizar capacidades adicionales de autenticación o elegir entre nuestras ofertas de socios. Además, cualquier variable de sesión puede formar parte de la ramificación de políticas de acceso (como la ramificación de URL) por política de solicitud. Las políticas de autenticación step-up pueden basarse en aplicaciones, partes seguras de aplicaciones, URI web sensibles, ampliación de sesiones o cualquier variable de sesión.

Muchas soluciones de autenticación utilizan codificación de aplicaciones, agentes de servidor web separados o proxies especializados que presentan importantes problemas de gestión, coste y escalabilidad. Con control AAA, BIG-IP APM te permite aplicar políticas de acceso personalizadas en muchas aplicaciones y obtener visibilidad centralizada de tu entorno de autorización. Puedes consolidar tu infraestructura AAA, eliminar niveles redundantes y simplificar la gestión para reducir los gastos de capital y operativos.

APLICACIÓN CERO TRUST A CCESS

Muchas organizaciones —posiblemente incluida la suya— están avanzando rápidamente hacia la adopción de una arquitectura de seguridad de confianza cero. Los pilares de una arquitectura de seguridad de confianza cero son la identidad y el contexto.

Un enfoque de seguridad de confianza cero significa adoptar la mentalidad de que los atacantes ya han infiltrado tu red y están acechando, esperando una oportunidad para lanzar un ataque. Elimina la idea de un insider de confianza dentro de un perímetro de red definido, asumiendo, en el mejor de los casos, un perímetro de red limitado y seguro. Fomenta no confiar nunca en los usuarios, incluso si ya han sido autenticados, autorizados y han recibido acceso a aplicaciones y recursos. Un enfoque de seguridad cero confianza aplica derechos de privilegio mínimo al acceso de los usuarios, permitiendo que los usuarios accedan solo a aquellas aplicaciones y recursos para los que están autorizados, y restringiendo su acceso a una sola aplicación o recurso a la vez.

La conciencia de identidad y contexto también es lo que define el Proxy Consciente de la Identidad (IAP). La IAP permite el acceso seguro a aplicaciones específicas mediante un enfoque detallado de autenticación y autorización de usuarios. Los IAP solo permiten el acceso por solicitud a la aplicación, lo cual es muy diferente del enfoque de acceso a la red amplia de las VPNs que aplican acceso basado en sesión, que no es un enfoque de confianza cero. Con este enfoque, la VPN se vuelve opcional para acceder a aplicaciones. El IAP permite la creación y aplicación de políticas de acceso a aplicaciones granulares basadas en atributos contextuales, como la identidad del usuario, la integridad del dispositivo y la ubicación del usuario. La IAP se basa en controles de acceso a nivel de aplicación, no en reglas de la capa de red. Las políticas configuradas reflejan la intención y el contexto del usuario y la aplicación. La IAP requiere una raíz fuerte de identidad confiable para verificar a los usuarios y para hacer cumplir estrictamente lo que están autorizados a acceder.

El Proxy Identity Aware es clave tanto para una arquitectura de seguridad de confianza cero como para el BIG IP APM F5. BIG-IP APM y F5 Access Guard entregan un Proxy Identity Aware utilizando un modelo de validación cero confianza en cada solicitud de acceso a la aplicación. Proporcionando a usuarios autenticados y autorizados acceso seguro a aplicaciones específicas, aprovecha el proxy de acceso de primera clase de F5. BIG-IP APM centraliza la identidad y autorización del usuario. La autorización se basa en los principios del acceso menos privilegiado.

A través de la PAI, BIG-IP APM examina, termina o autoriza solicitudes de acceso a aplicaciones. Las políticas dentro de BIG-IP APM pueden crearse para:

- Verificar la identidad del usuario
- Comprueba el tipo de dispositivo y la postura
- Validar la autorización del usuario
- Confirmar la integridad y sensibilidad de la aplicación
- Confirma la disponibilidad de fecha y hora

- Limitar o detener el acceso si la ubicación del usuario o la postura de su dispositivo se considera incorrecta, inapropiada o insegura
- Solicita formas adicionales de autenticación—incluida la autenticación multifactor (MFA)—si la ubicación del usuario o la naturaleza sensible de las aplicaciones o sus datos lo justifican
- Y más

Los datos del análisis de comportamiento de usuarios y entidades (UEBA) y otros motores de riesgo impulsados por API pueden integrarse sin problemas, añadiendo otro nivel de seguridad y control de acceso a aplicaciones.

BIG-IP APM verifica la postura de seguridad de los dispositivos del usuario mediante F5 Access Guard, una extensión de navegador que coordina con BIG-IP APM. Sin embargo, el APM BIG-IP y el F5 Access Guard van más allá de simplemente comprobar la integridad del dispositivo en la autenticación para realizar comprobaciones continuas y continuas de la postura del dispositivo, asegurando que los dispositivos de usuario no solo cumplan, sino que cumplan con las políticas de seguridad de los endpoints durante todo el acceso a la aplicación. Si BIG-IP APM detecta algún cambio en la integridad del dispositivo, puede limitar o detener el acceso a las aplicaciones, deteniendo posibles ataques antes incluso de que puedan lanzarse.

Un flujo de trabajo de configuración guiado permite a las organizaciones alojar aplicaciones web protegidas por un Proxy Identity Aware en un webtop, proporcionando a los usuarios un único catálogo de sus aplicaciones. Ofrece una experiencia de usuario fluida, ya que los usuarios pueden acceder a las aplicaciones independientemente de dónde estén alojadas. También simplifica el flujo de trabajo administrativo, permitiendo a los administradores seleccionar, modificar y modificar fácilmente las aplicaciones accesibles por un grupo de usuarios específico.

BIG-IP APM, a través de la aplicación en aplicación (IAP), también simplifica el acceso a aplicaciones para trabajadores remotos o desde casa, facilita y asegura mejor la accesibilidad de las aplicaciones, eliminando opcionalmente la necesidad de VPNs.

SEGURIDAD ROBUSTA DE ENDPOINTS

BIG-IP APM inspecciona y evalúa los dispositivos finales de los usuarios antes de la autenticación y durante todo el acceso a la aplicación con F5 Access Guard. F5 Access Guard examina la postura de seguridad del dispositivo y determina si el dispositivo forma parte del dominio corporativo. Según los resultados, BIG-IP APM aplicará listas dinámicas de control de acceso (ACLs) para desplegar seguridad contextual. El APM BIG-IP y el F5 Access Guard incluyen comprobaciones de inspección de endpoints preconfiguradas e integradas, incluyendo comprobaciones por tipo de sistema operativo, software antivirus, cortafuegos, archivo, proceso, validación y comparación de valores de registro (solo Windows), así como dirección MAC del dispositivo, ID de CPU e ID de HDD. Para dispositivos móviles con iOS o Android, la inspección de endpoint de BIG-IP APM verifica el estado UDID del dispositivo móvil y el jailbreak o root.

UN CCESS BASADO EN RIESGO USANDO MOTORES DE RIESGO TERCEROS - PAR TY (HTTP CONNEC TOR)

Muchas organizaciones han desplegado análisis de comportamiento de usuarios y entidades (UEBA) o motores de riesgo de terceros. La capacidad de aprovechar un UEBA o motor de riesgo existente para incorporar análisis en tiempo real y datos de riesgo dentro de sus políticas de control de acceso puede ayudar a esas organizaciones
garantizar que el acceso a redes, nubes, aplicaciones e incluso APIs se regule en función de un perfil de riesgo. También es importante abordar el acceso basado en riesgos a redes, nubes, aplicaciones y APIs que se activa por una variedad de variables relevantes.

A través de su HTTP Connector, BIG-IP APM se integra con UEBA de terceros y motores de riesgo, aprovechando su evaluación de riesgos mediante APIs REST como parte de sus controles de acceso basados en políticas. Esto permite un acceso basado en riesgos a redes, nubes, aplicaciones y APIs, mejorando aún más la solución de IAP cero confianza de BIG-IP APM. El HTTP Connector de BIG-IP APM aprovecha disparadores basados en grupos de usuarios, dominios y red para aumentar la aplicabilidad del acceso basado en riesgos. El acceso basado en riesgos mejora la seguridad, proporcionando mayor visibilidad y análisis para determinar si conceder o denegar el acceso a tus redes, nube, aplicaciones y APIs.

INTEGRACIÓN INTELIGENTE CON IDENTIDAD Y UN CCESS MANA GEMENT (IAM)

F5 colabora con los principales proveedores de gestión de identidad y acceso (IAM) tanto locales como en la nube, como Microsoft, Okta y Ping Identity. Esta integración permite el uso local y remoto de usuarios SSO vía SAML, OAuth o FIDO2 (U2F) a aplicaciones basadas en instalaciones o en un centro de datos. Para las organizaciones que no desean replicar su almacén de credenciales de usuario en la nube con IDaaS o ofertas IAM basadas en la nube, trabajando con sus socios, F5 y BIG-IP APM trabajan para ayudar a estas organizaciones a mantener el control de las credenciales de usuario locales. Esto se logra creando un puente entre la oferta del proveedor IAM y los servicios locales de autenticación. Este puente, o cadena de proveedores de identidad, utiliza SAML para federar la identidad del usuario.

UNIFICAR UN CCESS A PARTIR DE CUALQUIER DISPOSITIVO

BIG-IP APM está situado entre tus aplicaciones y tus usuarios, proporcionando un punto estratégico de control de acceso a las aplicaciones. Protege tus aplicaciones públicas proporcionando políticas detalladas para el acceso de usuario consciente de la identidad y el contexto, mientras consolida tu infraestructura de acceso. Asegura el acceso remoto y móvil a aplicaciones, redes y nubes mediante VPN SSL o acceso a aplicaciones de confianza cero. BIG-IP APM converge y consolida todo el acceso—red, nube, aplicación y API—dentro de una única interfaz de gestión. También permite y simplifica la creación de políticas de acceso dinámicas fáciles de gestionar.

BIG-IP APM incluye un portal de aplicaciones web dinámico o webtop. El webtop BIG-IP APM muestra solo las aplicaciones autorizadas y disponibles para un usuario según su identidad y contexto—independientemente de dónde estén alojadas las aplicaciones—localmente, en un centro de datos, en una nube privada, en una nube pública o ofrecidas como servicio.

BIG-IP APM activa el modo de Seguridad de la Capa de Transporte de Datagramas (DTLS), que soporta DTLS 2.0 para conexiones remotas que aseguran y tunelan aplicaciones sensibles al retardo. Soporta cifrado IPsec para el tráfico entre sucursales o centros de datos. VPN por aplicación mediante una aplicación
El túnel a través de BIG-IP APM permite acceder a una aplicación específica sin el riesgo de seguridad de abrir un túnel de acceso a red completo.

F5 BIG-APM permite el acceso seguro a aplicaciones, redes y nubes a través del cliente BIG-IP Edge y el acceso F5. El cliente BIG-IP Edge está disponible para Apple MacOS, Microsoft Windows, plataformas Linux, Chromebooks, e incluye soporte para Windows en dispositivos ARM64. F5 Access es un cliente móvil opcional para garantizar el acceso seguro desde dispositivos móviles compatibles con Apple iOS y Google Android, y está disponible para descargar en la Apple App Store o Google Play.

BIG-IP Edge Client y F5 Access se integran con soluciones líderes en gestión de dispositivos móviles (MDM) y gestión de movilidad empresarial (EMM), incluyendo VMware Horizon ONE (AirWatch), Microsoft Intune e IBM MaaS360, para realizar comprobaciones de seguridad e integridad de dispositivos y para ofrecer acceso VPN por aplicación sin intervención del usuario. Las políticas contextuales se asignan en función del estado de seguridad del dispositivo. Estas políticas habilitan, modifican o desactivan el acceso a aplicaciones, red y nube desde el dispositivo. Los atributos de hardware pueden asignarse al rol del usuario para permitir puntos adicionales de decisión de control de acceso. Un limpiador de caché del navegador elimina automáticamente cualquier dato sensible al final de la sesión del usuario.

Se soportan biometrías, como el acceso por huella dactilar, para abrir y acceder al Cliente Edge F5. Esto simplifica el acceso, ya que el usuario ya no necesitará crear, recordar e introducir una credencial de usuario/contraseña para acceder al Cliente Edge. También hace que el acceso al Cliente Edge sea más seguro, ya que los usuarios reutilizan contraseñas o crean pares simples de nombre de usuario/contraseña, facilitando así el hackeo de los atacantes.

BIG-IP APM también soporta autenticación de servidores mediante Delegación Limitada de Certificado de Cliente (C3D). Al emplear C3D, BIG-IP APM aborda la autenticación basada en certificados, limitando la necesidad y el uso de credenciales. Con C3D, las organizaciones pueden implementar protocolos de cifrado más sólidos y los últimos intercambios de claves, así como emplear autenticación de certificados de cliente, habilitar el cifrado de extremo a extremo en entornos de proxy inverso, aprovechar Perfect Forward Secrecy (PFS) y validar certificados de cliente utilizando el Protocolo de Estado de Certificados en Línea (OCSP).

UN CCESS TRANSPARENTE PARA TODAS LAS APLICACIONES

A medida que las organizaciones se centran en reducir la fricción de los usuarios y aumentar la agilidad, su necesidad de proporcionar un acceso fluido a todas las aplicaciones se convierte en una prioridad. BIG-IP APM permite a las organizaciones reducir la fricción para que los usuarios accedan remotamente (SSL VPN). También reduce la fricción en aplicaciones web. BIG-IP APM soporta SSO tanto en acceso remoto como en aplicaciones web con un único inicio de sesión para dispositivos Apple Mac o Microsoft Windows (a través de
Windows Hello For Business). Las organizaciones pueden soportar el inicio de sesión del usuario mediante tokens U2F (como claves Yubico) o FIDO2 sin contraseña a través del Cliente Edge F5 para reducir la fricción del usuario y aumentar la seguridad de acceso a las aplicaciones.

SIMPLIFICAR LA APLICACIÓN DE VIRUS A CCESS

Los despliegues virtuales de escritorio y aplicaciones deben escalar para satisfacer las necesidades de miles de usuarios y cientos de conexiones por segundo. BIG-IP APM sirve como puerta de entrada para entornos de aplicaciones virtuales. Incluye soporte nativo para Microsoft Remote Desktop Protocol (RDP), soporte nativo para proxies web seguros para Citrix XenApp y XenDesktop, y acceso a proxies de seguridad para VMware Horizon. Los administradores pueden controlar la entrega y los componentes de seguridad de soluciones de virtualización empresarial mediante la gestión unificada de acceso, seguridad y políticas de BIG-IP APM. Estas capacidades escalables y de alto rendimiento simplifican el acceso y control del usuario en entornos de escritorio virtual alojados. BIG-IP APM ofrece soporte virtual sencillo y amplio para aplicaciones y escritorios.

BIG-IP APM soporta autenticación de dos factores vía RSA SecureID y RADIUS a través del cliente nativo para despliegues de VMware End User Computing (EUC). BIG-IP APM es compatible con Citrix Virtual Apps and Desktops y Citrix StoreFront. BIG-IP APM, cuando se integra con el protocolo Microsoft RDP, permite el acceso remoto al escritorio necesario para instalar componentes en el lado del cliente o ejecutar Java. Permite que Microsoft RDP esté disponible para su uso en nuevas plataformas, como dispositivos Apple iOS y Google Android. También permite clientes RDP nativos en plataformas no Windows como Mac OS y Linux, donde anteriormente solo se soportaba un cliente basado en Java. El soporte RDP de BIG-IP APM funciona con cualquier navegador web o aplicación RDP de Microsoft, Apple o Google.

PRO TEC TING API

Las APIs son el tejido conectivo en las arquitecturas de aplicaciones modernas. Los atacantes están aprovechando las APIs para lanzar ataques, porque están listas para ser explotadas: muchas organizaciones exponen las APIs al público y a sus socios de la cadena de suministro o las dejan sin protección sin querer.

Mientras los atacantes explotan APIs para lanzar ataques, las organizaciones pueden garantizar la seguridad de las APIs mediante

autenticación, especialmente si es adaptable y está protegida por políticas de autenticación y autorización coherentes y flexibles. BIG-IP APM permite la autenticación segura para APIs REST. También garantiza que se tomen las acciones de autorización adecuadas. BIG-IP APM integra OpenAPI existentes, o archivos "swagger", ahorrando tiempo, recursos humanos y costes al desarrollar políticas de protección de API, asegurando al tiempo que existen políticas de protección de API precisas.

OBTENCIÓN DE CREDENCIALES

Las credenciales de usuario son como las llaves del reino: todo lo que un atacante tiene que hacer es robar un conjunto de credenciales de usuario y podrá disfrutar de acceso sin restricciones a la red, las nubes y las aplicaciones de tu organización.

La protección de credenciales de BIG-IP APM, como parte de una licencia opcional de BIG-IP DataSafe™, protege las credenciales contra robos y reutilizaciones. Protege contra ataques Man-in-the-Browser (MitB) mediante cifrado adaptable y en tiempo real, y cifra las credenciales de usuario introducidas en su webtop. BIG-IP APM, junto con BIG-IP DataSafe, hace que las credenciales sean ilegibles e inutilizables, incluso en el improbable caso de que un atacante las robe con éxito. BIG-IP APM también garantiza la seguridad de inicio de sesión para todas las aplicaciones asociadas mediante federación.

F 5 DEFENSA DISTRIBUIDA DE LA BO-T — CONSTRUIDA EN LA GRAN PLATAFORMA IP

Los bots causan un dolor financiero significativo mediante el scraping que ralentiza el rendimiento, el rescalping y el acaparamiento de inventario que frustran a los clientes fieles, la enumeración de códigos de tarjetas regalo para robar saldos, la creación de cuentas falsas para cometer fraude y el crepitado de credenciales —la prueba de credenciales robadas— que conduce a la toma de control de cuentas.

Los bots persistentes avanzados de hoy en día son más sofisticados que nunca, evadiendo muchas defensas estándar de bots disponibles dentro de los WAF. Los delincuentes reconfigurarán bots para saltarse defensas en cuestión de horas, utilizar millones de direcciones IP válidas, resolver rápidamente CAPTCHAs, imitar comportamientos humanos e introducir una sutil aleatoriedad.

Para adelantarse a los atacantes, F5® Distributed Cloud Bot Defense utiliza una recopilación de señales enriquecida en el lado del cliente, ofuscación de código líder en la industria, recopilación agregada de telemetría e IA para una eficacia a largo plazo sin precedentes y casi cero falsos positivos, manteniendo el acceso para bots buenos. Y dado que F5 defiende los sitios más atacados en la web —incluidos los de los bancos, minoristas y aerolíneas más grandes del mundo— F5 está preparada cuando estos ataques tengan como objetivo tu organización.

Despliega Distributed Cloud Bot Defense directamente desde tu IP BIG-IP o a través de un conector adecuado para tu aplicación, con servicios de soporte adaptados a tus necesidades, desde autoservicio hasta servicio gestionado.

EDITOR VISUAL DE POLÍTICAS (VPE)

Gracias a su avanzado Editor Visual de Políticas (VPE) gráfico, BIG-IP APM hace que diseñar y gestionar políticas de control de acceso granulares, tanto individuales como grupales, sea rápido y sencillo. Con VPE, puedes crear y editar políticas de acceso dinámicas completas de forma eficiente con solo unos clics. El VPE de BIG-IP APM puede definir reglas por ruta de URL. Centralizando y simplificando la gestión de políticas contextuales, puedes dirigir de forma eficiente el acceso detallado de los usuarios a aplicaciones, redes y nubes.

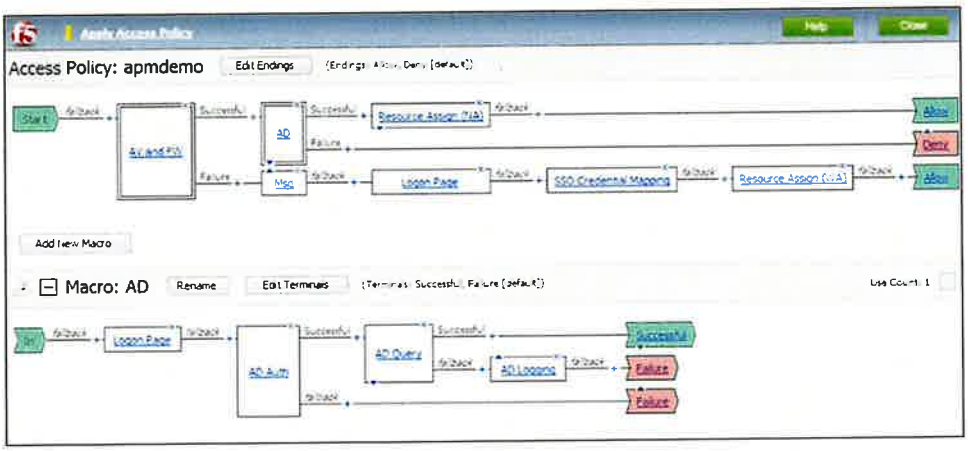


Figura 1: El VPE avanzado BIG-IP APM facilita la creación, modificación y gestión de políticas de acceso granulares basadas en aplicaciones, usuarios, red/nube y vulnerabilidades.

BIG-IP APM te permite diseñar políticas de acceso para autenticación y autorización, así como comprobaciones de seguridad en los endpoints, haciendo cumplir el cumplimiento de los usuarios con las políticas corporativas y las normativas del sector. Se puede definir un solo perfil de acceso para todas las conexiones que provengan de cualquier dispositivo, o puedes crear varios perfiles de acceso para diferentes métodos de acceso desde distintos dispositivos.

BIG-IP APM impone la autenticación de acceso mediante ACLs y autoriza a los usuarios con ACLs de capa 4 y capa 7 aplicadas dinámicamente en una sesión. Tanto las ACL de nivel 4 como las de nivel 7 se soportan en función de la postura del endpoint como punto de aplicación de políticas. El acceso individual y grupal a aplicaciones y redes aprobadas está permitido por BIG-IP APM utilizando ACLs dinámicas L7 por sesión (HTTP). El VPE en BIG-IP APM puede usarse para crear, modificar y gestionar ACLs de forma rápida y sencilla.

UNA CONFIGURACIÓN GUIADA POR CCESS (UN GC)

BIG-IP APM incluye una capacidad de Configuración Guiada por Acceso (AGC) que simplifica el despliegue y la gestión del acceso a aplicaciones. El AGC guía a tu administrador paso a paso en un proceso de configuración y despliegue de BIG-IP APM, ahorrándote

y el tiempo y coste de despliegue de tu administrador. El AGC de BIG-IP APM también permite a tu administrador integrar y gestionar de forma rápida y sencilla aplicaciones clásicas críticas para la misión, como SAP ERP y Oracle PeopleSoft, en Azure AD. Este acceso guiado simplificado elimina numerosos pasos previamente requeridos en Azure AD para salvar la brecha de acceso entre aplicaciones que soportan autenticación moderna y aplicaciones que soportan métodos clásicos de autenticación, reduciendo considerablemente la carga administrativa implicada en la modernización de dichas aplicaciones.

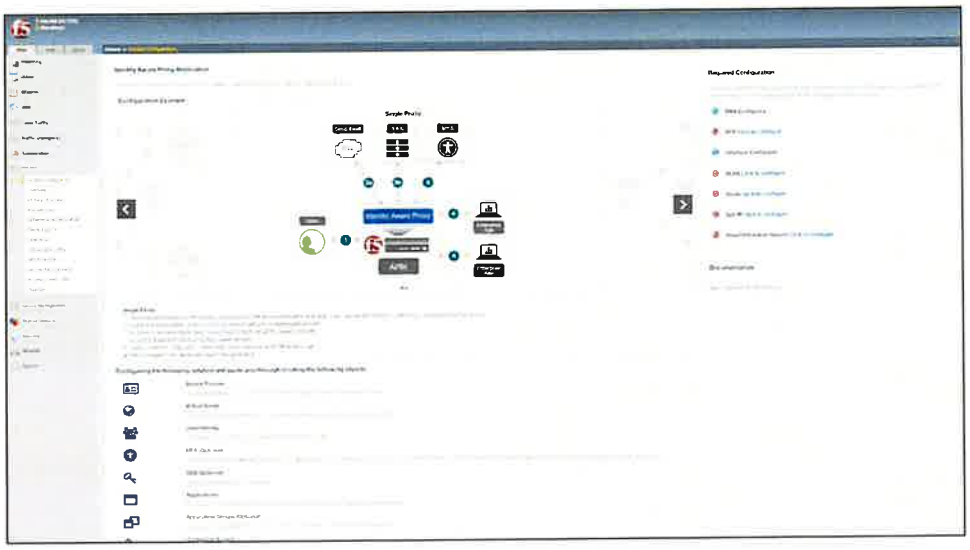


Figura 2: La configuración guiada por acceso de BIG-IP APM AHORRA TIEMPO Y COSTE DE DESPLIEGUE.

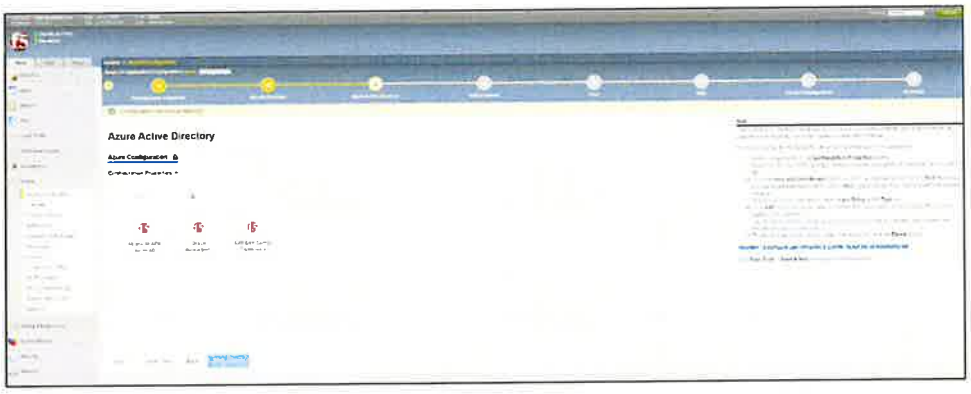


Figura 3: La configuración guiada por acceso de F5 BIG-IP APM permite una incorporación rápida y sencilla y gestión de aplicaciones personalizadas y clásicas, como SAP ERP y Oracle PeopleSoft, con Azure AD.

CENTRALIZAR UN MANA DE POLÍTICA DE CCESS

Si tienes múltiples despliegues de APM BIG-IP, F5 BIG-IQ Centralized® Management te ayudará a gestionarlos de forma eficiente. Puede gestionar políticas para hasta 100 instancias BIG-IP APM, permitiéndote importar, comparar, editar y actualizar políticas de acceso granulares entre múltiples dispositivos de usuario.

Con BIG-IQ Centralized Management y BIG-IP APM, puedes importar configuraciones desde una instancia maestra "source" de BIG-IP APM, simplificando la distribución de políticas de acceso. También puedes
editar objetos específicos de dispositivo o ubicación directamente en BIG-IQ Centralized Management y hacer que se propaguen a lo largo de tu despliegue APM DE BIG-IP. Puedes ver fácilmente las diferencias entre las configuraciones de acceso actuales y propuestas.

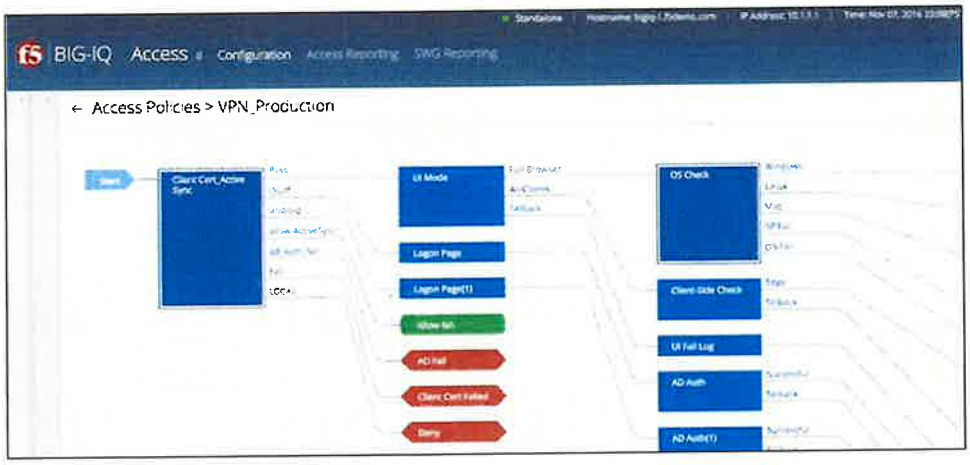


Figura 4: La Gestión Centralizada de BIG-IQ permite la importación, comparación, edición y actualización de políticas de acceso en múltiples dispositivos desde una única interfaz.

MEJORAR LA VISIBILIDAD Y LA REPERCUSIÓN

Una vista detallada de los registros y eventos proporciona detalles de la sesión de política de acceso. Con informes disponibles a través de BIG-IQ Centralized Management, BIG-IP APM te ayuda a obtener mayor visibilidad sobre el acceso a aplicaciones y las tendencias de tráfico, agregar datos para la forense a largo plazo, acelerar respuestas a incidentes e identificar problemas e imprevistos antes de que los usuarios puedan experimentarlos.

BIG-IP APM puede personalizar informes con datos y estadísticas granulares para informes y análisis inteligentes. Ejemplos incluyen informes detallados de sesiones por:

- Fallos de acceso
- Usuarios
- Recursos consultados
- Uso en grupo
- Geolocalización IP

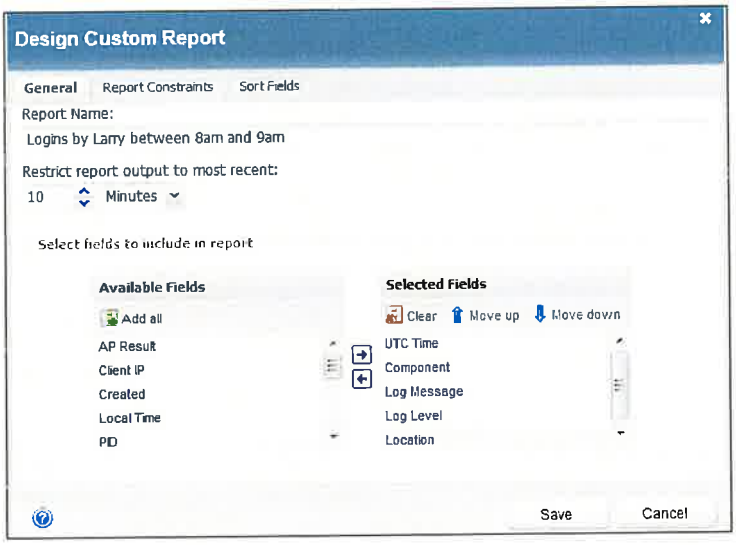


Figura 5: Los informes personalizados proporcionan datos y estadísticas detalladas para un análisis inteligente.

BIG-IP APM se integra con la Gestión Centralizada de BIG-IQ para ofrecer una mayor visibilidad a través de informes de acceso y registros. Ofrece informes analíticos y registros basados en dispositivos y grupos, para que puedas aumentar tu conocimiento sobre el acceso y análisis de los usuarios. También te ayuda a tomar medidas rápidas si es necesario, incluyendo la terminación de sesiones de acceso específicas. Además, ofrece una exportación en CSV de los datos de informes BIG-IP APM, por lo que está accesible para informes personalizados. La vista personalizada de panel de BIG-IQ Centralized Management te ayuda a visualizar mejor tendencias y contextos de relaciones con mayor facilidad. Esto mejora tu tiempo de respuesta si surgen problemas. A través de esta visión holística del acceso a aplicaciones y red, puedes comprender mejor la eficacia de las políticas de acceso que has establecido, localizar y abordar puntos débiles, y mejorar tus respuestas a problemas y preocupaciones.

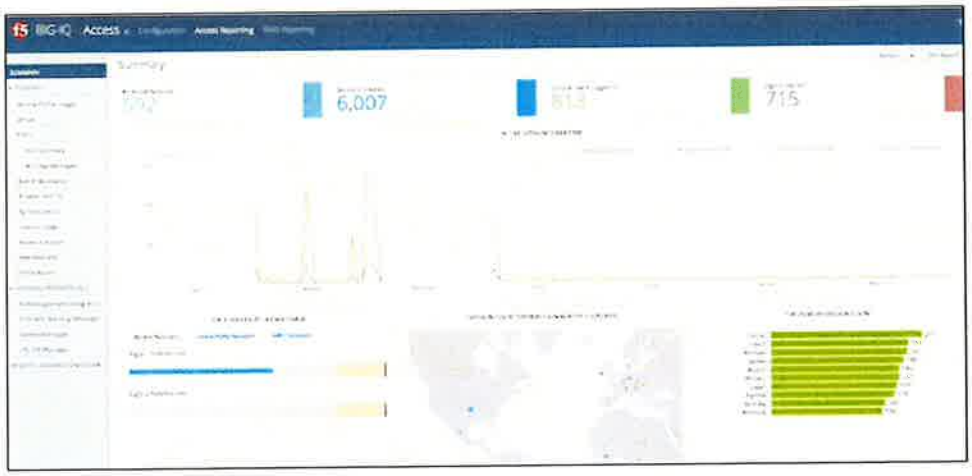


Figura 6: El panel completo de gestión centralizada de BIG-IQ para BIG-IP APM te ayuda a visualizar mejor las tendencias y los contextos de relaciones.

Además del panel de acceso disponible a través de BIG-IQ Centralized Management for BIG-IP APM, el panel de políticas de acceso en el sistema BIG-IP ofrece una visión rápida de la salud del acceso. Puedes ver la plantilla predeterminada de sesiones activas, rendimiento de acceso a la red, nuevas sesiones y conexiones de acceso a la red, o crear vistas personalizadas
Usando el selector de ventanas del panel. Al arrastrar y soltar las estadísticas deseadas en el cristal de la ventana, obtienes una comprensión en tiempo real de la salud del acceso.

FLEXIBILIDAD Y, ALTO RENDIMIENTO Y ALABILIDAD SIN IGUAL.

BIG-IP APM ofrece acceso flexible a aplicaciones, red y nube, manteniendo a tus usuarios productivos y permitiendo que tu organización escale de forma rápida y rentable.

BIG-IP APM puede desplegarse de diversas formas para cubrir tus necesidades específicas de acceso. BIG-IP APM puede ser:

- Desplegado como módulo adicional para BIG-IP LTM para proteger aplicaciones públicas
- Entregado como un dispositivo BIG-IP independiente o como chasis independiente F5 VIPRION®
- Incluido con una BIG IP LTM Virtual Edition (VE) para ofrecer acceso flexible a aplicaciones en entornos virtualizados
- Funcionan en ediciones virtuales de alta gama y ediciones virtuales de alto rendimiento
- Ofrecido en una plataforma Turbo SSL

Además de estar licenciado para estas plataformas, BIG-IP APM también puede estar licenciado como el mejor paquete de la oferta Good-Better-Best de F5, como parte del Acuerdo de Licencia Empresarial (ELA) de F5 para BIG-IP VEs, y de modelos de licencias por suscripción.

BIG-IP APM está disponible en una plataforma de chasis y en todos los appliances BIG-IP. Es compatible con el entorno de Multiprocesamiento™ Virtual en Clúster (vCMP) F5. El hipervisor vCMP ofrece la capacidad de ejecutar múltiples instancias de BIG-IP APM, lo que resulta en multitenencia y efectividad
separación. Con vCMP, los administradores de red pueden virtualizar mientras alcanzan un mayor nivel de redundancia y control.

BIG-IP APM ofrece descarga SSL a velocidades de red y soporta hasta 3.000 inicios de sesión por segundo. Para organizaciones con una base de usuarios de aplicaciones web en constante crecimiento, esta solución escala de forma rápida y rentable.

El uso de BIG-IP APM se basa en dos tipos de sesiones de usuario: sesiones de acceso y sesiones de uso concurrente de conexión (CCU). Las sesiones de acceso se aplican a sesiones de autenticación, IAP, VDI y situaciones similares. CCU es aplicable para acceso a la red, como acceso VPN completo y aplicación

túneles o acceso a la web. La plataforma BIG-IP y la plataforma VIPRION —ambas compatibles con BIG-IP APM— gestionan exponencialmente más sesiones de acceso que sesiones CCU en casos de uso como autenticación, SAML, SSO y proxy forward. Esto significa que si tienes la intención de usar BIG-IP APM para autenticación, VDI y similares, el número de sesiones soportadas en VIPRION puede llegar hasta 2 millones, y la plataforma BIG-IP puede soportar hasta 1 millón.

Características de BIG-IP APM

Ya sea ejecutándose como módulo independiente o incluido en la plataforma BIG-IP, o en un blade de chasis VIPRION, BIG-IP APM se basa en el inteligente y modular sistema operativo F5 TMOS®, que ofrece visión, flexibilidad y control para ayudarte a habilitar mejor el acceso a aplicaciones, red y nube.

LAS GRANDES CARACTERÍSTICAS DE LOS APM DE IP INCLUYEN:

- Aplicación granular de políticas de acceso
- Creación y gestión de políticas conscientes de la identidad y del contexto
- Enrutamiento de políticas
- Soporte para el Proxy Consciente de la Identidad (IAP) que permite el acceso a aplicaciones de confianza cero
- Autorización basada en contexto con ACLs dinámicas L4/L7
- Soporte para federación de identidades SAML 2.0
- Soporte para el protocolo de autorización OAuth 2.0
- Federación simplificada de identidades para aplicaciones con atributos multivalorados
- Soporte SSO para autenticación clásica (Kerberos, basada en cabeceras, etc.), caché de credenciales, OAuth 2.0, SAML 2.0 y FIDO2 (U2F)
- Integra con soluciones SSO de terceros
- Caché de credenciales y proxy para SSO
- Uniendo métodos modernos de autenticación y autorización (SAML, OAuth/OIDC) y los métodos clásicos de autenticación y autorización
- Soporte para la Clave de Prueba OIDC para el intercambio de códigos (PKCE)
- Soporte para autenticación basada en SAML usando BIG-IP Edge Client y acceso F5 para Android y iOS
- Soporte para la vinculación de artefactos SAML
- Soporte para el perfil SAML ECP
- Autenticación de servidores AAA y alta disponibilidad
- Soporte para autenticación step-up
- Soporte de cifrado web JSON para clientes públicos
- Autenticación multifactor (MFA) mediante contraseña de un solo uso (OTP)
- Integración fluida con soluciones MFA de terceros
- Modo DTLS 2.0 para entregar y asegurar aplicaciones
- Acceso remoto SSL VPN

LAS GRANDES CARACTERÍSTICAS DE LOS APM DE IP INCLUYEN (CON T):

- Acceso siempre conectado
- Establecer un túnel VPN siempre activo (con inicio de sesión en el sistema operativo de Windows y cliente BIG-IP Edge para Windows)
- Soporte amplio para plataformas de cliente (véase F5 BIG-IP APM Matrices de Compatibilidad de Clientes para cada versión de BIG-IP)
- Soporte robusto para navegadores web (véase F5 BIG-IP APM Client Compatibility Matrices para cada versión)
- Comprobaciones continuas de integridad y seguridad en los puntos finales
- Soporte para seguridad en endpoints y VPN sin complementos para navegadores web
- Cifrado IPsec de sitio a sitio
- Túneles de aplicación
- "Webtops" dinámicos, basados en la identidad del usuario
- Integración con productos líderes de proveedores IAM (Microsoft, Okta, Ping Identity)
- Métodos de autenticación: formulario, certificado, Kerberos SSO, SecurID, básico, token RSA, tarjeta inteligente, factor N
- Protección de credenciales de usuario
- Protección y autorización de la API
- Acceso basado en riesgos aprovechando UEBA de terceros y motores de riesgo (HTTP Connector)
- Soporte para Identity-as-a-Service (IDaaS), incluyendo Azure Active Directory y Okta
- Editor Visual de Políticas (VPE) y Configuración Guiada por Acceso (AGC)
- Agente de geolocalización IP (en VPE)
- Soporte para certificados de máquina Windows
- Integración con el Administrador de Credenciales de Windows
- Soporte para páginas de inicio de sesión externas
- Soporte para control de acceso al servidor virtual BIG-IP LTM
- Escala hasta 2 millones de sesiones de acceso concurrentes
- BIG-IP Edge Client y F5 Access se integran con VMware Horizon ONE (AirWatch), Microsoft Intune e IBM MaaS360
- Integración del cliente de borde BIG-IP con Windows en ARM64
- Exportación e importación de políticas de acceso mediante BIG-IQ Centralized Management
- Tiempos de espera configurables
- Monitor de control de salud para la contabilidad RADIUS
- Soporte de variables URI de aterrizaje
- Soporte de caché/proxy DNS
- Soporta Google reCAPTCHA v2 para autenticación y autenticación contextual
- Listo para IPv6
- Hojas de estilo para una página de inicio de sesión personalizada
- Informes avanzados centralizados con Splunk
- vCMP
- Lenguaje de scripting F5 iRules®
- Proxy completo
- Capas BIG-IP APM y BIG-IP ASM

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Plataformas F5 BIG-IP

Por favor, consulte las hojas de datos de hardware del sistema BIG-IP, VIPRION y Virtual Edition para más detalles. Para información sobre el soporte específico de módulos para cada plataforma, consulte las últimas notas de versión en AskF5. Para la lista completa de hipervisores soportados, consulte la Matriz de Hipervisores Soportados por VE. Las plataformas F5 pueden gestionarse mediante un único panel de cristal con la Gestión Centralizada BIG-IQ.

Electrodomésticos BIG-IP iSeries

Ediciones Virtuales BIG-IP

Chasis VIPRION

Servicios Globales F5

F5 Global Services ofrece apoyo, formación y consultoría de primer nivel para ayudarte a sacar el máximo partido a tu inversión en F5. Ya sea proporcionando respuestas rápidas a preguntas, formando equipos internos o gestionando implementaciones completas desde el diseño hasta el despliegue, F5 Global Services puede ayudar a garantizar que tus aplicaciones sean siempre seguras, rápidas y fiables. Para más información sobre F5 Global Services, contacta con consulting@f5.com o visita f5.com/support.

Para saber más sobre BIG-IP APM, visita f5.com/apm.

BIG-IP DNS

QUÉ HAY DENTRO

ICSA labs CERTIFIED FIREWALL - CORPORATE

Hiperescala y protege tu DNS mientras optimizas la entrega global de aplicaciones

Escalar y proteger cada entorno ayuda a proteger tu negocio frente a interrupciones de sitios y mejora el rendimiento del DNS y de las aplicaciones. Proteger las infraestructuras DNS frente a los últimos ataques de denegación de servicio distribuida (DDoS) y proteger las respuestas de consultas DNS de las redirecciones que envenenan la caché ayudará a mantener tu negocio online y viable. Para alcanzar plenamente estos objetivos, necesitas formas eficientes de monitorizar la infraestructura DNS y la salud de las aplicaciones, así como escalar bajo demanda.

F5® BIG-IP® DNS distribuye DNS y solicitudes de aplicaciones de usuario basándose en políticas empresariales, condiciones de centros de datos y servicios en la nube, ubicación del usuario y rendimiento de las aplicaciones. La plataforma BIG-IP ofrece los servicios DNS de alto rendimiento de F5 con visibilidad, informes y análisis; hiperescala y asegura las respuestas DNS geográficamente para sobrevivir a ataques DDoS; ofrece una solución DNSSEC en tiempo real; y garantiza una alta disponibilidad de aplicaciones globales en todos los entornos de nube.

BENEFICIOS CLAVE

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Hyperscale DNS hasta 100 millones de RPS con un chasis completamente cargado
BIG-IP DNS hiperescala DNS autoritativo hasta 100 millones de respuestas de consulta por segundo (RPS) y controla el tráfico DNS.
Garantiza que los usuarios sean
Conectado al mejor sitio y ofrece escalado bajo demanda para DNS y aplicaciones globales.

Protege contra ataques DNS y garantiza la disponibilidad
Asegurar la disponibilidad y protección de DNS y aplicaciones durante ataques DDoS o picos de volumen de DNS. Mitigar amenazas DNS bloqueando el acceso a dominios IP maliciosos.

Mejorar el rendimiento global de las aplicaciones
Envía a los usuarios de la app a la nube o a la web local con el mejor rendimiento basado en la aplicación, la geolocalización, el negocio y las condiciones de red.

Despliega de forma flexible, escala a medida que crezcas y gestiona con eficiencia
BIG-IP DNS ofrece una gestión global flexible de aplicaciones en entornos virtuales y multi-nube. La interfaz web proporciona una configuración DNS sencilla con menús centralizados;
Registro avanzado, estadísticas e informes junto con exportación a analítica de terceros.

Wagner Peña

RENDIMIENTO DNS INIGUALABLE

BIG-IP DNS ofrece un rendimiento hiperescalable capaz de manejar incluso las aplicaciones y sitios web más concurridos. Cuando las aplicaciones sufren un aumento de volumen en consultas DNS debido a peticiones legítimas o ataques DDoS, BIG-IP DNS gestiona las solicitudes con procesamiento multinúcleo y F5 DNS Express™, aumentando drásticamente el rendimiento autoritario de DNS hasta 50 millones de RPS para responder rápidamente a todas las consultas.

Esta escalabilidad ayuda a tu organización a ofrecer la mejor calidad de servicio (QoS) para tus usuarios, eliminando al mismo tiempo el bajo rendimiento de las aplicaciones. DNS Express mejora las funciones estándar del servidor DNS al descargar las respuestas DNS como un servidor DNS autoritativo. BIG-IP DNS acepta transferencias de zonas de registros DNS desde el servidor DNS principal y responde a las consultas DNS de forma autoritativa.

Los beneficios y características del procesamiento multinúcleo y DNS Express incluyen:

- Respuesta de alta velocidad y protección contra ataques DDoS con DNS en memoria
- Replicación DNS autorizada en múltiples despliegues de servicios BIG-IP o DNS para respuestas más rápidas
- DNS y DNSSEC autorizados en multi-nubes para recuperación ante desastres y respuestas rápidas y seguras
- Rendimiento DNS escalable para la calidad de la experiencia de la aplicación y el servicio
- La capacidad de consolidar servidores DNS y aumentar el ROI

En casos de volúmenes muy altos para aplicaciones y servicios o un ataque DDoS por DNS, el DNS BIG-IP con DNS Express activado y en Modo de Respuesta Rápida (RRM) escala hasta 100 millones de RPS. Extiende la disponibilidad con un rendimiento y seguridad inigualables—absorbiendo y respondiendo a consultas hasta el 200 por ciento de los límites normales. Consulta la página 17 para las métricas de rendimiento
y detalles.

DNS C A CHING Y RESOLUCIÓN

La latencia DNS puede reducirse activando una caché DNS en BIG-IP DNS y haciendo que responda inmediatamente a las solicitudes del cliente. BIG-IP DNS puede consolidar la caché y aumentar la tasa de aciertos de la caché. Esto reduce la latencia DNS hasta un 80 por ciento, con la caché DNS F5 reduciendo el número de consultas DNS para el mismo sitio. Cuando se utiliza en hardware de la plataforma VIPRION® F5, la caché DNS hiperescala para un rendimiento máximo de respuesta a consultas y ofrece escalabilidad lineal a través de chasis multihoja. Además de la caché, el DNS de BIG-IP permite que el dispositivo realice su propia resolución DNS sin necesidad de usar un solucionador DNS ascendente.

Los perfiles de caché disponibles para seleccionar para múltiples cachés incluyen:

- Caché transparente
- Sitio BIG-IP DNS entre cliente y DNS interno/externo
- Caché en caliente
- Caching resolver
- Sin respuesta en caché - BIG-IP DNS envía solicitudes con respuestas devueltas para resolución y almacenamiento en caché
- Validación del resolvedor de caché

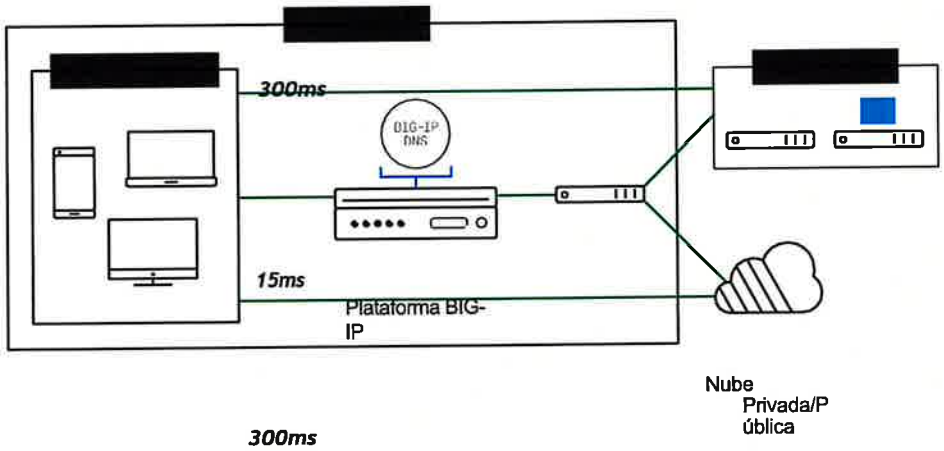


Figura 1: BIG-IP DNS soporta todos los despliegues DNS comunes que sean autorizados o localmente DNS resuelto. Las solicitudes de zona específicas que no están en caché se reenvían a servidores de nombres para una resolución DNS más rápida, permitiendo a los usuarios recibir respuestas rápidas.

BIG-IP DNS reduce el tiempo medio de respuesta y la latencia del DNS para dispositivos móviles y de escritorio de una media de 300 milisegundos (ms) y 100 ms respectivamente a tan solo 15 ms, dependiendo de la carga de trabajo.

APLICACIONES SEGURAS

Los ataques de denegación de servicio por DNS, el envenenamiento de caché y el secuestro de DNS amenazan la disponibilidad y seguridad de tus aplicaciones. BIG-IP DNS protege contra ataques DNS y te permite crear políticas que proporcionan una capa adicional de protección para tus aplicaciones y datos.

Las características de protección contra ataques DNS incluyen:

- Dispositivo reforzado—BIG-IP DNS está certificado por ICSA Labs como cortafuegos de red y resiste ataques comunes de gotas de lágrima, ICMP y demonios.
- Protección contra ataques DNS—BIG-IP DNS ofrece validación de protocolos integrada en software para eliminar automáticamente UDP de alto volumen, consultas DNS, inundaciones de NXDOMAIN y paquetes malformados. Puedes usar BIG-IP DNS en hardware para mitigar estos ataques de alto volumen.

- Balanceo de carga DNS—La plataforma BIG-IP puede usarse para hacer front-end a servidores DNS estáticos. Si la solicitud DNS es para un nombre controlado por la plataforma BIG-IP, los servicios DNS F5 responderán a la solicitud.
- Control de seguridad—F5 iRules® para DNS puede ayudarte a crear políticas que bloqueen solicitudes de sitios fraudulentos.
- Filtrado de paquetes—BIG-IP DNS utiliza filtrado de paquetes para limitar o denegar el acceso a los sitios web según el origen, destino o puerto.

Cortafuegos DNS

El DDoS en DNS, el envenenamiento de la caché de LDNS y otros ataques DNS no deseados y picos de volumen pueden causar caídas de DNS y pérdida de productividad. Estos ataques y picos de tráfico aumentan el volumen de forma drástica y pueden dejar fuera de servicio los servidores DNS.

BIG-IP DNS, con funcionalidad de seguridad, escala, rendimiento y control, ofrece beneficios al firewall DNS. Protege al DNS de ataques como ataques DDoS por reflexión o amplificación y otras consultas y respuestas DNS no deseadas que reducen el rendimiento del DNS.

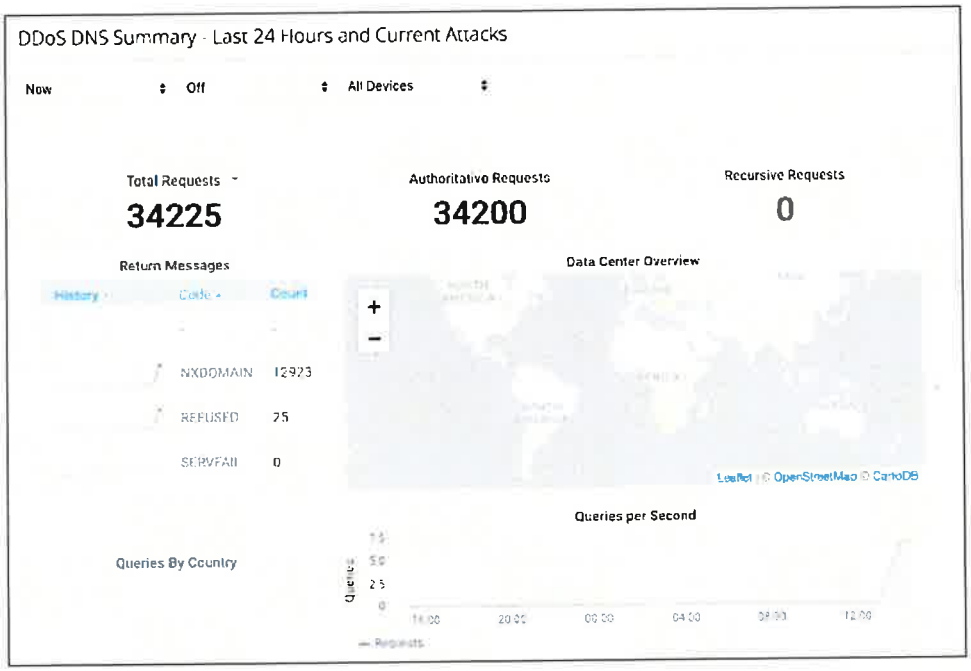


Figura 2: Visualiza los ataques DDoS por DNS, las 25 principales URLs de ataque, las consultas por segundo (QPS) y por país según esté disponible, y otro tráfico DNS como Respuestas por Segundo (RPS) por tipos de registro para obtener una visión completa del rendimiento de tu DNS y ataques no deseados.

Además, puedes mitigar amenazas complejas de seguridad DNS bloqueando el acceso a dispositivos maliciosos Dominios IP con Zonas de Política de Respuesta. Con BIG-IP DNS, puedes instalar un servicio de filtrado de dominios de terceros como SURBL o Spamhaus y prevenir la infección del cliente o interceptar respuestas infectadas a fuentes conocidas de malware y virus. Los servicios de cortafuegos DNS F5 reducen los costes de resolución de infecciones y aumentan la productividad del usuario.

INCLUYEN:

- Inspección y validación del protocolo
- Tipo de registro DNS ACL*
- DNS autoritativo de alto rendimiento, que escala las respuestas exponencialmente
- Hiperescalado autoritativo de DNS hasta un 200% para absorber ataques DDoS
- Reducción de la latencia y hiperescalado de la caché DNS
- Balanceo de carga DNS
- Inspección con estado (nunca acepta respuestas no solicitadas)
- Certificación ICSA Labs (puede desplegarse en la DMZ)
- La capacidad de escalar entre dispositivos usando IP Anycast
- Respuestas seguras (DNSSEC)
- Límites de tasa de respuesta de DNSSEC
- El soporte DNS sobre HTTPS resuelve consultas y mitiga ataques
- Control DNS completo usando DNS iRules
- Alerta de umbral DDoS*
- Mitigación de amenazas bloqueando el acceso a dominios IP maliciosos
- Registro e informes DNS
- Código DNS reforzado F5 (no protocolo BLINK)

*Requiere aprovisionar el Gestor Avanzado de Cortafuegos BIG-IP para acceder a la funcionalidad.

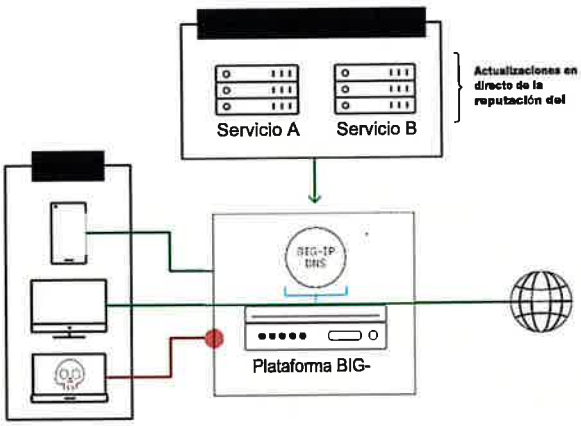


Figura 3: Reducir el riesgo de comunicación por malware y virus y mitigar las amenazas DNS bloqueando el acceso a dominios IP maliciosos con un servicio de reputación de dominio como SURBL o Spamhaus.

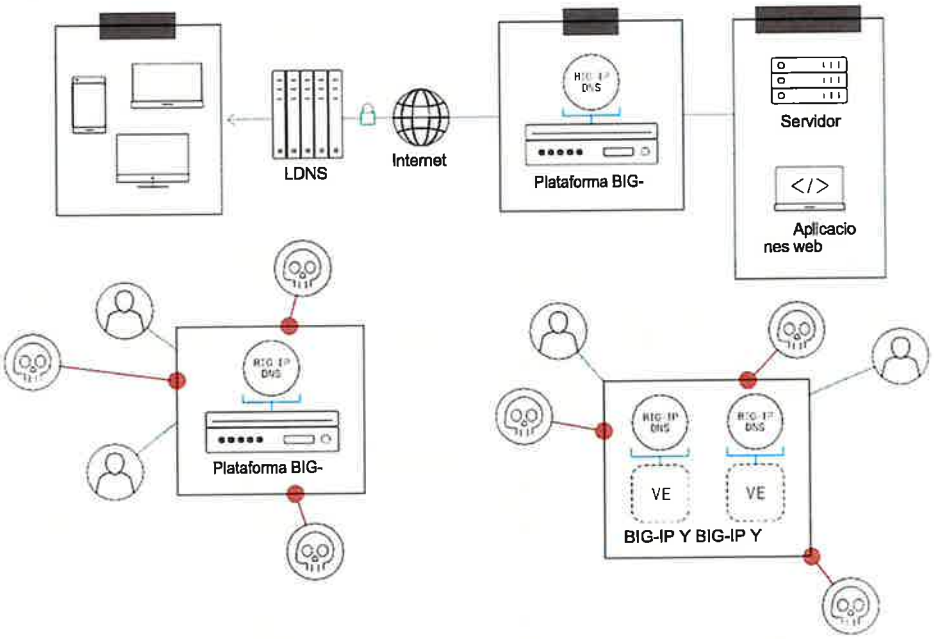


Figura 4: BIG-IP DNS mantiene las aplicaciones disponibles con servicios de cortafuegos que protegen la infraestructura DNS de ataques de alto volumen y paquetes malformados.

Firma completa de DNSSEC

Con el soporte DNSSEC DE BIG-IP, puedes firmar y cifrar digitalmente tus respuestas a consultas DNS. Esto permite al resolver determinar la autenticidad de la respuesta, evitando el secuestro de DNS y el envenenamiento de caché. Además, recibe todos los beneficios del balanceo global de carga del servidor mientras proteges tus respuestas a consultas DNS. Alternativamente, si una zona ya ha sido firmada, BIG-IP DNS gestiona las respuestas estáticas de DNSSEC para un mayor rendimiento.

Gestión centralizada de claves DNSSEC

Muchas organizaciones de TI han estandarizado o quieren estandarizar dispositivos compatibles con FIPS y claves DNSSEC seguras. Puedes usar BIG-IP DNS con tarjetas FIPS que ofrecen soporte 140-2 para asegurar tus claves. Además, BIG-IP DNS integra y utiliza módulos de seguridad de hardware (HSM) de Thales para su implementación, gestión centralizada y manejo seguro de claves DNSSEC, reduciendo OpEx y proporcionando consolidación y cumplimiento FIPS.

Soporte de dominio de primer nivel para DNSSEC

Para los administradores DNS que desean delegar a otros subdominios seguros, el DNS BIG-IP permite una gestión sencilla de DNSSEC como dominio de primer nivel, convirtiéndose en una zona principal.

Validación DNSSEC

En la mayoría de las redes, los resolvers DNS descargan solicitudes de registros DNSSEC y cálculos criptográficos para validar que la respuesta DNS recibida está correctamente firmada. Las respuestas DNSSEC que llegan a la red requieren altas cargas de CPU en los servidores de resolución DNS.

DNS sobre HTTPS

DNS sobre HTTPS (DOH) es un DNS cifrado usando SSL para protección total. Está totalmente habilitado por navegadores web populares y puede generar retrasos y problemas de seguridad para proveedores de servicios y empresas que no pueden terminar ni responder a estas consultas de DNS. F5 BIG-IP DNS permite que tu red descifre y resuelva consultas DNS por HTTPS sin afectar las respuestas por segundo (RPS). Además, el soporte para DoH elimina HTTPS como
Vector de suplantación DNS para ataques de amplificación maliciosa y protege la última milla con encapsulación de mensajes DNS.

DNS sobre TLS

El DNS sobre TLS (DoT) garantiza que las solicitudes y respuestas DNS no sean manipuladas ni falsificadas mediante ataques en la ruta. DoT añade cifrado TLS encima de la transmisión protocolo de control (TCP), que se utiliza para consultas DNS. DoT es un protocolo que autentica la comunicación entre un cliente DNS y un servidor DNS. Utiliza firmas criptográficas para la transmisión segura. DNS sobre TLS o DoT, es un estándar para cifrar consultas DNS y mantenerlas seguras y privadas. DoT utiliza el mismo protocolo de seguridad, TLS, para cifrar y autenticar comunicaciones.

Wagner Peña

Claves ECDSA

BIG-IP DNS ofrece soporte para claves del Algoritmo de Firma Digital de Curva Elíptica (ECDSA) para DNSSEC. Además de cumplir con los requisitos de seguridad modernos de una amplia variedad de sectores, ECDSA proporciona el mismo nivel de fuerza criptográfica que las claves RSA que actualmente soporta BIG-IP, pero con claves mucho más pequeñas. Esto supone un aumento significativo en la seguridad al usar tamaños de clave similares y permite una firma y verificación más rápidas.

DESPLIEGA F5 CLOUD BO-T DE DEFENSA DISTRIBUIDA DIRECTAMENTE DESDE TU BIG - IP

Los bots causan un dolor financiero significativo mediante el scraping que ralentiza el rendimiento, el rescalping y el acaparamiento de inventario que frustran a los clientes fieles, la enumeración de códigos de tarjetas regalo para robar saldos, la creación de cuentas falsas para cometer fraude y el crepitado de credenciales —la prueba de credenciales robadas— que conduce a la toma de control de cuentas.

Los bots persistentes avanzados de hoy en día son más sofisticados que nunca. Para adelantarse a los atacantes, F5 Distributed Cloud Bot Defense utiliza una recolección rica de señales del lado del cliente, ofuscación de código líder en la industria, recopilación agregada de telemetría e IA para una eficacia a largo plazo sin precedentes y casi cero falsos positivos, manteniendo el acceso para bots buenos. Y dado que F5 defiende los sitios más dirigidos a la web —incluidos los de los mayores bancos, minoristas y aerolíneas del mundo— F5 está preparado cuando estos ataques tengan como objetivo tu organización.

Despliega Distributed Cloud Bot Defense directamente desde BIG-IP o a través de un conector adecuado para tu aplicación, con servicios de soporte adaptados a tus necesidades, desde autoservicio hasta servicio gestionado.

Balanceo de carga global avanzado

BIG-IP DNS incluye las capacidades de distribución de tráfico más avanzadas de la industria para adaptarse a las necesidades de cualquier organización o aplicación desplegada globalmente.

- Round robin
- Disponibilidad global
- Persistencia LDNS
- Disponibilidad de aplicaciones
- Geografía
- Capacidad de servidor virtual
- Menos conexiones
- Paquetes por segundo
- Tiempo de ida y vuelta
- Lúpulo
- Tasa de completación de paquetes
- QoS definido por el usuario
- Relación dinámica
- LDNS
- Proporción
- Kilobytes por segundo

Con la validación DNSSEC DE BIG-IP, los administradores pueden descargar y validar fácilmente DNSSEC en el lado del cliente usando BIG-IP DNS para resolver. Esto resulta en un rendimiento DNS superior y en un aumento dramático en la respuesta del sitio hacia los usuarios.

APLICACIONES DISPONIBLES EN GRAN MEDIDA

BIG-IP DNS ofrece disponibilidad global de aplicaciones y un monitoreo sofisticado de salud que soporta una amplia variedad de tipos de aplicaciones, dando a las organizaciones la flexibilidad para adaptarse rápidamente y mantenerse competitivas.

Estas funciones de disponibilidad global y monitorización de la salud incluyen:

- Balanceo global de carga—BIG-IP DNS proporciona una gestión integral y de aplicaciones de alto rendimiento para entornos híbridos.
- Balanceo de carga por relación dinámica—BIG-IP DNS enruta a los usuarios al mejor recurso en función de métricas de sitio y red (por ejemplo, basándose en el número de saltos entre el cliente y el DNS local).
- Persistencia en área amplia—Para asegurar que las conexiones de usuario persistan entre aplicaciones y centros de datos, BIG-IP DNS sincroniza datos, propaga el DNS local y mantiene la integridad de la sesión.
- Balanceo de carga geográfica—BIG-IP DNS incluye una base de datos IP que identifica la ubicación a nivel continental, país y estado/provincia para conectar a los usuarios con la aplicación o servicio más cercano y lograr el mejor rendimiento.
- Mapeo de topología personalizado—Con BIG-IP DNS, las organizaciones pueden configurar mapas de topología personalizados. Al definir y guardar agrupaciones regionales personalizadas, puedes configurar la topología en función de políticas de tráfico de aplicaciones intranet que coincidan con tu infraestructura interna.
- Monitorización de infraestructuras—BIG-IP DNS verifica la salud de toda la infraestructura, eliminando puntos únicos de fallo y desviando el tráfico de aplicaciones desde sitios con bajo rendimiento.

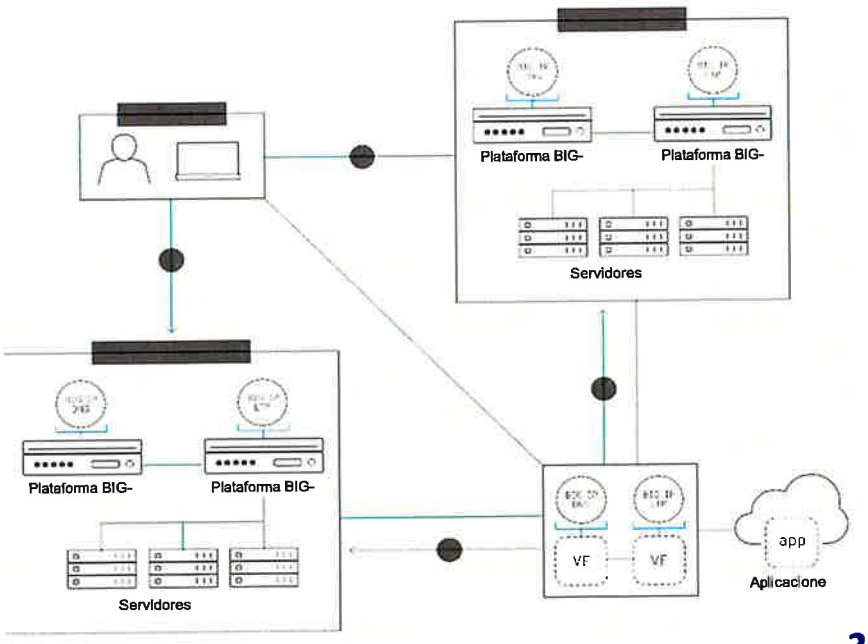


Figura 5: BIG-IP DNS garantiza que los usuarios estén siempre conectados al mejor sitio. ❶ El usuario consulta DNS local para resolver dominios y consultas DNS locales DNS DE GRAN IP. Usos de BIG-IP DNS métricas recogidas para cada sitio y Identifica el mejor servidor. BIG-IP El DNS responde al DNS local con IP dirección ❹ El usuario está conectado a Best sitio local o en multi-nube.

Wagner Piña

Monitorización de la salud de la aplicación

BIG-IP DNS mejora la experiencia de la aplicación al monitorizar inteligentemente la disponibilidad de recursos. Amplía la resiliencia de las aplicaciones seleccionando y utilizando de forma flexible las mejores soluciones BIG-IP disponibles para la monitorización de la salud. BIG-IP DNS reduce el tiempo de inactividad de las aplicaciones y permite una fácil disponibilidad con múltiples configuraciones en la monitorización de aplicaciones.

Las aplicaciones sofisticadas actuales requieren controles de salud inteligentes para determinar la disponibilidad. En lugar de depender de una sola comprobación de salud, BIG-IP DNS agrega múltiples monitores para que puedas comprobar el estado de la aplicación en varios niveles. Esto resulta en la mayor disponibilidad, mejora la fiabilidad y elimina falsos positivos para reducir los gastos de gestión.

BIG-IP DNS ofrece soporte predefinido y lista para la monitorización de la salud para más de 18 aplicaciones diferentes, incluyendo SAP, Oracle, LDAP y mySQL. BIG-IP DNS realiza un seguimiento dirigido de estas aplicaciones para determinar con precisión su estado de salud, reducir los tiempos de inactividad y mejorar la experiencia del usuario.

Recuperación ante desastres/planificación de la continuidad del negocio

Además de realizar comprobaciones completas de disponibilidad del sitio, puedes definir las condiciones para trasladar todo el tráfico a un centro de datos de respaldo, fallar sobre todo un sitio o controlar solo las aplicaciones afectadas.

SIMPLE MANA GEMENT

Gestionar una red distribuida y de múltiples sitios desde un solo punto es un desafío enorme. BIG-IP DNS ofrece herramientas que te ofrecen una visión global de tu infraestructura con los medios para gestionar la red y añadir políticas para garantizar la máxima disponibilidad para tu negocio.
Aplicaciones críticas. Gestionar la infraestructura global desde una interfaz centralizada con características que incluyen

- Interfaz de usuario basada en la web.
- Menús DNS y GSLB optimizados y centralizados para una configuración rápida.
- Gestión eficiente de listas y objetos para una visibilidad completa de los recursos globales.
- Nombres únicos de objetos para reducir la administración y construir políticas empresariales.
- Mejora de la gestión de aplicaciones distribuidas como parte de un grupo colectivo.
- Ayuda contextual para información sobre objetos, comandos y ejemplos de configuración.

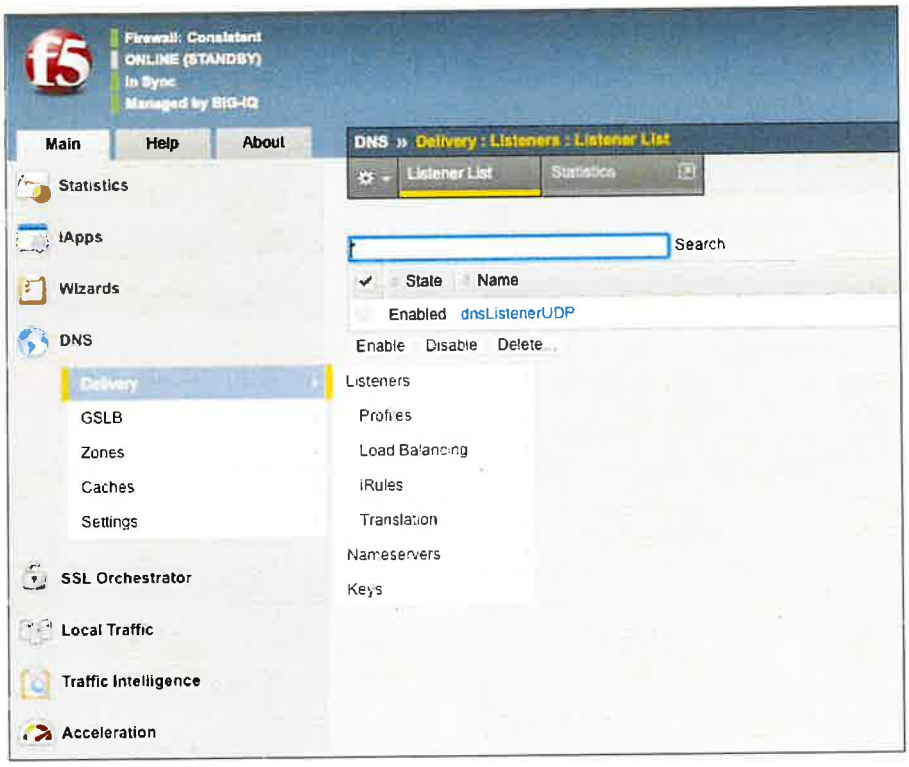


Figura 6: Reducir el tiempo de despliegue de entrega de DNS con secuencias de configuración y gestión centralizadas y fáciles de encontrar.

Wagner Peña

- **Potente interfaz de línea** de comandos—La interfaz de línea de comandos TMSH ofrece búsqueda integrada, ayuda contextual y transacciones en modo batch.
- **Configuración y sincronización automatizadas**: Autosync automatiza y protege múltiples dispositivos BIG-IP DNS, eliminando la difícil gestión jerárquica común en el DNS.
- **Mejora la escala y el análisis con dispositivos N+1 ilimitados**—En una situación de conmutación por error, cuando los servicios DNS BIG-IP forman parte de un grupo de Clúster de Servicios de Dispositivos (DSC), la solución BIG-IP funciona a su máxima capacidad—en todos los appliances o ediciones virtuales sincronizadas con servicios DNS y GSLB. BIG-IP DNS ofrece aplicaciones y servicios altamente escalables, realizando análisis inteligentes de todo el tráfico entrante para comprender mejor patrones y anomalías.
- **Configuraciones GSLB escalables y** optimizadas—Sincronización Incremental ofrece un alto rendimiento para despliegues de gran tamaño. Con más dispositivos sincronizados, los cambios de configuración ocurren rápidamente. Para despliegues grandes con configuraciones GSLB y cambios rápidos de usuario, puedes proteger los cambios guardando manualmente cuando te resulte más conveniente.
- **Recuperación de configuración**—AutoDiscovery permite recuperar configuraciones de instancias BIG-IP distribuidas, eliminando configuraciones repetidas entre dispositivos.
- **Centros de datos y grupos de sincronización**—Crear grupos lógicos de equipos de red para asegurar un uso eficiente de la monitorización y la recopilación de métricas para compartir de forma inteligente con los miembros del grupo lógico.

- **Gestión distribuida de aplicaciones**: puedes definir dependencias entre servicios de aplicación y gestionarlos como un grupo, construyendo políticas escalables de distribución de tráfico y mejorando la eficiencia con un control granular de los objetos.
- **iRules**—Utiliza el lenguaje de scripting F5 iRules para personalizar la distribución del tráfico global. BIG-IP DNS analiza profundamente el tráfico DNS para personalizar el tráfico de aplicaciones hacia el centro de datos, pool o servidor virtual deseado. Esto reduce la latencia, aumenta la protección contra ataques y mejora el rendimiento.
- **Personaliza el tráfico con QoS**—Diseña decisiones de tráfico y desarrolla fácilmente algoritmos personalizados de balanceo de carga utilizando métricas de calidad de servicio en iRules, como el tiempo de ida y vuelta, saltos, ratio de impacto, tasa de paquetes, topología y más.
- **DNS iRules**—Gestiona consultas, respuestas y acciones DNS para una infraestructura DNS rápida y personalizada. Por ejemplo, configura DNS iRules con filtrado para protección y reportes.

- **F5 ZoneRunner™**—ZoneRunner es una herramienta integrada de gestión de archivos de zonas DNS que simplifica y reduce el riesgo de mala configuración. Basado en la última versión de BIND, ZoneRunner ofrece:
  - Población automática de protocolos comúnmente utilizados.
  - Comprobación de validación/errores para entradas de archivos de zona.
  - Importación de zonas desde un servidor externo o un archivo.
  - Búsquedas automáticas inversas.
  - Creación, edición y búsqueda sencillas de todos los registros.
  - Gestión sencilla de los registros NAPTR para requisitos LTE y 4G.

Balanceo de carga entre entornos de contenedores

Al migrar a la nube pública y contenedores, los ingenieros y arquitectos necesitan una solución robusta para el balanceo de carga entre clústeres (balanceo global de carga) en despliegues multi-nube. F5 BIG-IP DNS apunta a aplicaciones en clústeres de contenedores para servicios de escalabilidad, enrutamiento y seguridad habilitando el soporte para Server Name Indication (SNI) al usar el monitor HTTPS.

Monitor de salud DNS

El monitor de salud del DNS disponible en BIG-IP DNS y BIG-IP® Local Traffic™ Manager (LTM) monitoriza el estado del servidor DNS y ayuda a configurar el DNS en función de los informes. El monitor de salud DNS detecta si los servidores funcionan al máximo rendimiento y ayuda a reconfigurar para obtener respuestas óptimas.

Wagner Pina

Tala de alta velocidad

Puedes gestionar fácilmente DNS y el registro global de aplicaciones para una visibilidad y planificación rápida de la red. El registro a alta velocidad de consultas y respuestas DNS, syslog y los registros globales de decisiones de balanceo de carga del servidor mejoran la información sobre los datos para permitir un reconocimiento rápido de red mediante búsquedas y visualización rápidas y profundas.

Figura 7: Entiende la salud de tu DNS desde segundos hasta años comparando las principales IPs de origen, nombres de dominio y IP amplios y el TPS para informes.

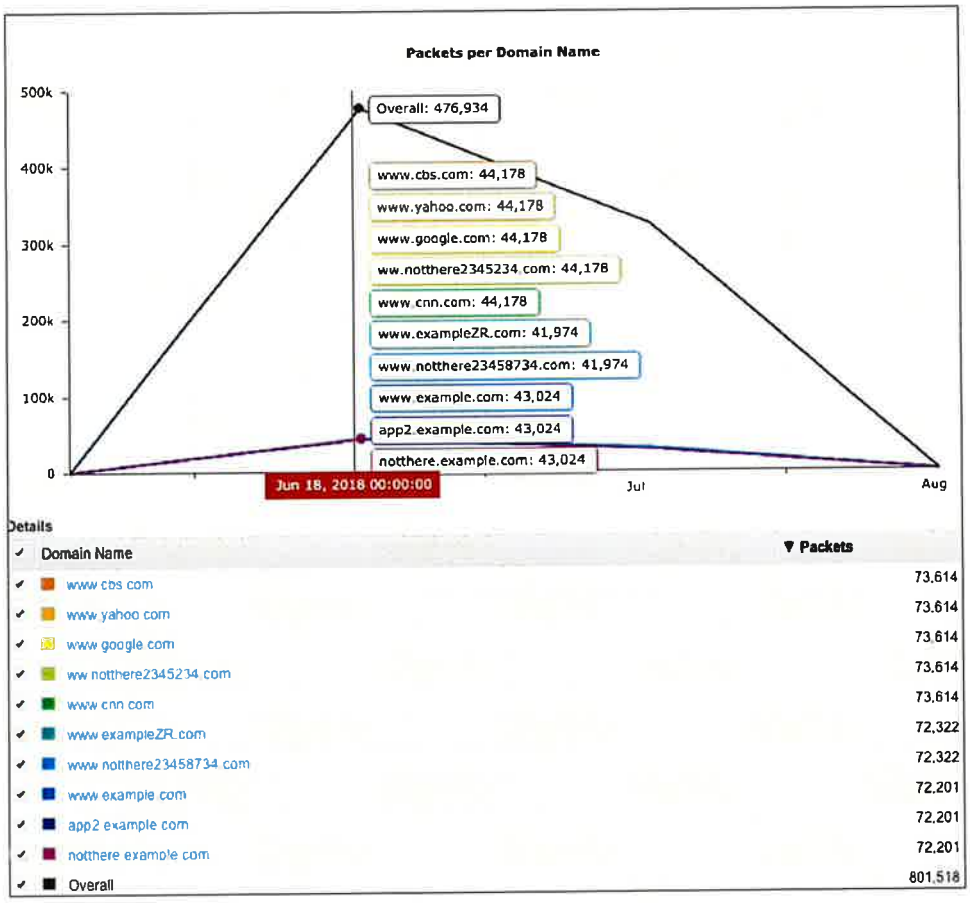
Estadísticas detalladas mejoradas del DNS

BIG-IP DNS ofrece estadísticas avanzadas de DNS para administradores, con datos detallados mejorados para perfiles como el número de tipos de consulta (A, CNAME, NS, RRSIG, AAAA, SRV y "otros" tipos) con solicitudes, respuestas y conteos porcentuales. Las estadísticas son por perfil y por dispositivo para una visibilidad rápida y planificación de capacidad de la infraestructura de entrega DNS. Las estadísticas detalladas de DNS se pueden ver en el perfil DNS o en informes analíticos.

Informes y análisis avanzados de DNS

F5 Analytics proporciona informes y análisis avanzados de DNS de aplicaciones, servidores virtuales, nombres de consulta, tipos de consulta, IPs de clientes, nombres más solicitados y mucho más para inteligencia empresarial, planificación de capacidades, informes de retorno de inversión, resolución de problemas, métricas de rendimiento y ajustes, permitiendo la máxima optimización del DNS e infraestructura global de aplicaciones.

Figura 8: Los administradores pueden gestionar fácilmente el DNS mediante analítica con informes avanzados y análisis de acciones para una rápida visibilidad de la entrega e infraestructura del DNS.



Wagner Pena

VENTAJAS DE LA VISIBILIDAD DNS

- Visualiza y gestiona la configuración y las políticas en dispositivos DNS.
- Añadir BIG-IP DNS y BIG-IP LTM Dispositivos a grupos de sincronización existentes.
- Analiza la información de conexión de F5 iQuery® para ayudar a identificar problemas en los grupos de sincronización DNS.
- Consulta estadísticas de alto nivel en toda tu infraestructura DNS que muestran el estado de los grupos y dispositivos de sincronización DNS.
- Consulta estadísticas DNS tanto en tiempo real como históricas.

Gestión Centralizada BIG-IQ

La Gestión Centralizada F5® BIG-IQ® proporciona un punto central de control para los dispositivos físicos y virtuales F5 y para las soluciones que se ejecutan en ellos. Simplifica la gestión, ayuda a garantizar el cumplimiento normativo y te proporciona las herramientas necesarias para entregar tus aplicaciones de forma segura y eficaz. BIG-IQ gestiona licencias, políticas, certificados SSL de BIG-IP, imágenes y configuraciones.

BIG-IQ ofrece una gestión centralizada de BIG-IP DNS, incluyendo la capacidad de crear, recuperar, actualizar y eliminar todos los objetos de balanceo de carga global del servidor (GSLB); herramientas para desplegar y revertir políticas GSLB; y la capacidad de gestionar configuraciones de escuchadores y perfiles DNS.

Figura 9: La integración con BIG-IQ muestra visibilidad avanzada del DNS con solicitudes, respuestas y conocimientos de consultas no gestionadas para análisis en profundidad.

INTEGRACIÓN DE RED

BIG-IP DNS está diseñado para encajar en tu red actual y en tus planes de futuro. Las características de integración incluyen:

- **Soporte de aplicaciones de gestión SNMP**—BIG-IP DNS integra sus MIBs y un agente SNMP con DNS. Esto permite que las aplicaciones de gestión SNMP lean datos estadísticos sobre el rendimiento del DNS de BIG-IP.
- **Integración de** terceros—BIG-IP DNS comunica e integra con una amplia variedad de dispositivos de red. Esto incluye soporte para varios tipos de hosts remotos, como agentes SNMP, cachés de terceros, servidores, routers y balanceadores de carga para diagnosticar el estado de los endpoints de red.
- **Soporte IPv6/IPv4**—Facilitar la transición a IPv6 proporcionando servicios de pasarela DNS y traducción para soluciones híbridas IPv6 e IPv4 y gestionando servidores DNS IPv6 e IPv4. BIG-IP LTM configurado con NAT64 transforma IPv6 a IPv4 para esos entornos solo IPv4.

- **Integración IP Anycast:** los volúmenes de consulta DNS dirigidos a una sola dirección IP, ya sea legítimo o durante un ataque DoS, se gestionan fácilmente distribuyendo la carga entre múltiples dispositivos DNS BIG-IP geográficos. Los gestores de red se dan cuenta de estos beneficios:
  - Mejora del rendimiento y fiabilidad del usuario
  - Latencia de red reducida para transacciones DNS
  - Capacidad para escalar la infraestructura DNS para gestionar la carga de solicitudes DNS a una sola dirección IP
  - Menores tasas de paquetes de consulta perdidos, reduciendo los tiempos de espera y reintentos DNS
  - Aumento de ingresos porque se atiende a más usuarios y se protege el valor de marca

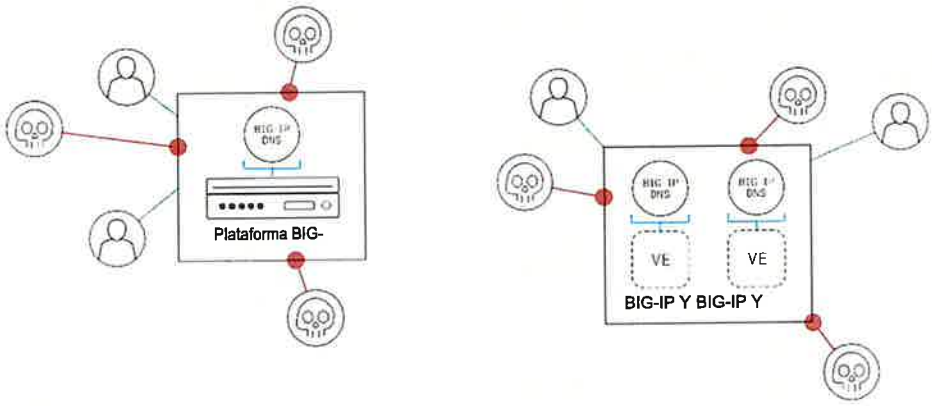


Figura 10: BIG-IP DNS e integración IP Anycast distribuyen la carga de solicitudes DNS dirigiendo solicitudes IP individuales a múltiples dispositivos locales.

Wagner Pena

- **Balanceo global de carga de servidores en entornos virtuales y en la nube**—Crear fácilmente instancias virtuales de BIG-IP DNS. Proporcionar una entrega DNS flexible y disponibilidad global de aplicaciones encaminando a los usuarios hacia aplicaciones en entornos físicos, virtuales y en la nube.

DERECHO ARCHITECA

La avanzada arquitectura de BIG-IP DNS te da total flexibilidad para controlar la entrega de aplicaciones sin crear cuellos de botella de tráfico.

La arquitectura BIG IP DNS incluye:

- **TMOS®**—El sistema operativo F5, TMOS, proporciona un sistema unificado para la entrega óptima de DNS y aplicaciones, dándote visibilidad, flexibilidad y control total en todos los servicios BIG-IP.
- **Rendimiento de consultas y respuestas y escalabilidad**—Escalar linealmente en plataformas más grandes y chasis multi-blade para aumentar el rendimiento integrando funciones en TMOS. BIG-IP DNS puede ser provisionado para plataformas que soportan Multiprocesamiento™ Virtual en Clúster F5 (vCMP®).

GRANDES - PLATAFORMAS IP

Solo la plataforma ADC de próxima generación y lista para la nube de F5 ofrece una agilidad similar a la de DevOps con la escala, profundidad de seguridad y protección de inversión necesarias tanto para los establecidos como para los establecidos
Aplicaciones emergentes. Los nuevos dispositivos BIG-IP® iSeries ofrecen programabilidad rápida y sencilla, orquestación amigable con el ecosistema y un rendimiento récord de hardware definido por software. Los clientes ahora pueden acelerar las nubes privadas y asegurar datos críticos a gran escala, reduciendo el TCO y preparando sus infraestructuras de aplicaciones para el futuro. Las soluciones F5 pueden desplegarse rápidamente mediante integraciones con herramientas de gestión de configuración de código abierto y sistemas de orquestación.

Además de la iSeries, F5 ofrece sistemas modulares de chasis y palas VIPRION diseñados específicamente para el rendimiento y para una verdadera escalabilidad lineal bajo demanda sin interrupciones empresariales. La nueva plataforma VELOS es la siguiente generación de los sistemas basados en chasis, líderes en la industria de F5, que ofrecen un rendimiento, escalabilidad y personalización sin precedentes en un solo sistema ADC. El software BIG-IP® edición virtual (VE) funciona en servidores comerciales y soporta la gama más amplia de hipervisores y requisitos de rendimiento. Los VEs proporcionan agilidad, movilidad y un despliegue rápido de servicios de aplicaciones en centros de datos definidos por software y entornos en la nube.

La solución de próxima generación Application Delivery Controller (ADC), F5 rSeries, conecta infraestructuras tradicionales y modernas con una plataforma reestructurada y orientada a API, diseñada para satisfacer las necesidades de tus aplicaciones tradicionales y emergentes. La nueva F5 rSeries ofrece niveles de rendimiento sin precedentes, una arquitectura totalmente automatizable y la máxima fiabilidad, seguridad y control de acceso para tus aplicaciones críticas.

Wagner Pat...

Consulta las hojas de datos de hardware del sistema BIG-IP, VIPRION, VLOS y Virtual Edition para más detalles. Para información sobre el soporte específico de módulos para cada plataforma, consulte las últimas notas de versión en AskF5. Para la lista completa de hipervisores soportados, consulte la Matriz de Hipervisores Soportados por VE.

Además, F5 ofrece la Gestión Centralizada BIG-IQ® para la gestión de un solo panel de todos los dispositivos F5, permitiendo la orquestación de las políticas de entrega de aplicaciones F5.

Electrodomésticos BIG-IP iSeries

Chasis VIPRION

Electrodomésticos rSeries

Chasis VELOS

Ediciones Virtuales BIG-IP

Wagner Peña

SERVICIOS EN LA NUBE F 5

Ahora puedes provisionar y configurar fácilmente los servicios que necesitas tus apps en minutos. Construidos en un modelo de pago por uso, los servicios en la nube F5 ofrecen precios predecibles, flexibilidad y la capacidad de escalar automáticamente para satisfacer la demanda cambiante. Transfiere tus servicios DNS locales y zonas a los servicios en la nube F5:

- **DNS Cloud Service**—Provisionar y configurar fácilmente los servicios DNS con unos pocos clics; empezar a responder consultas en cuestión de minutos tras la activación.
- **Servicio en la Nube DNS Load** Balancer — Asegura alta disponibilidad y rendimiento de las aplicaciones con el sencillo e inteligente Servicio en la Nube F5 DNS Load Blancer.

DNS ENCENDIDO - BAJO DEMANDA

Los administradores tienen la opción de añadir escalado bajo demanda DNS y GSLB con límite de velocidad y capacidad límite de objetos según deseen a los appliances BIG-IP DNS o BIG-IP LTM. Esta opción soporta requisitos para el rendimiento exacto del tráfico, lo que resulta en un CapEx y OpEx más bajos. La escala bajo demanda incluye los siguientes servicios: DNS, GSLB y DNSSEC. Las estadísticas de la interfaz de usuario muestran la capacidad nominal de las instancias, como el RPS de consulta y los límites de objetos, que ofrecen detalles rápidos del tráfico para facilitar la planificación de capacidad. Contacta con tu representante de ventas o distribuidor regional de F5 para más información.

CONSULTA DNS RPS RENDIMIENTO MÁXIMO

Los servicios BIG-IP DNS ofrecen respuesta de consulta por segundo (RPS) con alta escalabilidad de rendimiento. La siguiente tabla enumera muchas plataformas BIG-IP con DNS Express habilitado para responder de consulta DNS autoritativa con las capacidades máximas por plataforma.

Plataforma	RPS de consulta máxima
Edición Virtual	250,000*
R2600	590,000
r2800	1,100,000
R4600	1,800,000
R4800	2,500,000
R5600	2,700,000
R5800	3,800,000
R5900	4,900,000
R10600	5,000,000
R10800	5,700,000
R10900	6,900,000
i2600	240,000
i2800	500,000
i4600	480,000
i4800	880,000
i5600	1,000,000
i5800, i5820 FIPS	1,500,000
i7600	1,500,000
i7800, i7820 FIPS	2,300,000
NEBS de los años 10150	990,000
FIPS 10350v, NEBS	1,800,000
i10600	2,000,000
i10800	2,900,000
i11400-DS	1,200,000
i11600 (DS)	1,800,000
i11800 (DS)	4,500,000
i15600	4,100,000
i15800	8,100,000
VELOS CX410 Chasis completo (8 palas)	
CUCHILLA VELOS BX110	2,500,000
VIPRION 2200 Chasis Completo (2 palas)	
VIPRION 2400 Chasis completo (4 palas)	
VIPRION B2250 Blade	2,100,000
VIPRION 4480 Chasis Completo (4 palas)	
VIPRION 4800 Chasis Completo (8 palas)	
Hoja VIPRION B4450	6,400,000

*BIG-IP DNS Edición Virtual está disponible en incrementos de 250,000 RPS. Para 5050 y superiores, el Modo de Respuesta Rápida (RRM—véase página 2) ofrece hasta el 200 por ciento del RPS máximo normal de consulta cuando está activado. **Consulta F5 Sales o revendedor para más detalles.**

LICENCIAS SIMPLIFICADAS

Satisfacer las necesidades de tus aplicaciones en un entorno dinámico nunca ha sido tan fácil. F5's te ofrece la flexibilidad de provisionar módulos avanzados bajo demanda, al mejor precio.

- Decide qué soluciones son adecuadas para el entorno de tu aplicación con las soluciones de F5.
- Especifica las suscripciones que necesitas en entornos de nube híbrida.
- Proporciona los módulos necesarios para ejecutar tus aplicaciones con las ofertas Good, Better, Best de F5.
- Haz la transición hacia arriba o hacia abajo con los Acuerdos de Licencia Empresarial.
- Implementa una flexibilidad completa de la aplicación con la posibilidad de desplegar tus módulos en una plataforma virtual o física .

SERVICIOS GLOBAL F 5

F5 Global Services ofrece apoyo, formación y consultoría de primer nivel para ayudarte a sacar el máximo partido a tu inversión en F5. Ya sea proporcionando respuestas rápidas a preguntas, formando equipos internos o gestionando implementaciones completas desde el diseño hasta el despliegue,
F5 Global Services puede ayudar a garantizar que tus aplicaciones sean siempre seguras, rápidas y disponibles. Para más información sobre F5 Global Services, contacte con consulting@f5.com o visite F5 Servicios Profesionales.

DEV CENTRAL

Wagner Peña

La comunidad técnica de F5 DevCentral™ es una fuente activa y comprometida para los mejores artículos técnicos, tutoriales, foros de discusión, código compartido, medios y mucho más relacionado con la entrega de DNS y la red global de aplicaciones.

MÁS INFORMACIÓN

Para saber más sobre BIG-IP DNS, busca en f5.com para encontrar estos y otros recursos.

Páginas web
Entrega DNS
Balanceo de Carga Global de
Servidores DevCentral

Hoja técnica
Hoja de datos de hardware del
sistema BIG-IP Edición
VirtualEdición
BICICLETAS
VIPRION
Hoja de datos de hardware rSeries

Artículos y vídeos
Introducción a los servicios DNS y al balanceo global de carga
de servidores (vídeo) El DNS es clave para los clientes
conectados
Abordar DNS basado en la nube—Es hora de moverse
DNS cifrado - Mitigación del impacto del DoT y DoH para los proveedores de
servicios ¿Qué es un ataque de amplificación de DNS?

Estudios de caso
El banco mejora la experiencia del usuario con acceso siempre disponible, rápido y seguro a los servicios bancarios utilizando el proveedor SaaS F5 que garantiza alta disponibilidad y resiliencia para aplicaciones críticas de clientes con F5
Everbridge gestiona el tráfico y la seguridad en proveedores globales de nube y el centro de datos local Shawbrook Bank recluta a F5 para acelerar y escalar la transformación digital

Gestor de Tráfico Local BIG-IP

QUÉ HAY DENTRO

Entrega de aplicaciones con escala, automatización y personalización

Las aplicaciones impulsan la innovación y la rentabilidad, permitiendo que tu empresa aproveche la computación en la nube, la movilidad y las redes definidas por software (SDN). Tu organización, desde los equipos de AppDev y DevOps hasta Infraestructura y Operaciones de TI, depende de que tus servicios de aplicaciones e infraestructura de red funcionen al máximo rendimiento con seguridad centrada en las apps para afrontar los retos de hoy —y del mañana.

F5® BIG-IP® Local Traffic™ Manager (LTM) entrega tus aplicaciones a los usuarios de forma fiable, segura y optimizada. Obtienes la extensibilidad y flexibilidad de los servicios de aplicación con la programabilidad que necesitas para gestionar tu infraestructura en la nube, virtual y física. Con BIG-IP LTM, tienes el poder de escalar, automatizar y personalizar los servicios de aplicación de forma más rápida y predecible.

BENEFICIOS CLAVE

Escalar las aplicaciones de forma rápida y fiable
Optimiza para las aplicaciones web actuales con HTTP/2 para asegurar que tus clientes y usuarios tengan acceso a las aplicaciones que necesitan—cuando las necesiten.

Automatiza y personaliza con infraestructura programable
Controla tus aplicaciones—desde la conexión y el tráfico hasta la configuración y gestión—con F5® iRules® LX para la programabilidad de la red, con soporte Node.js lenguajes en BIG-IP. Utiliza la Cadena de Herramientas de Automatización F5 para un enfoque declarativo que permita provisionar, configurar y gestionar los appliances de forma eficiente.

Migra a entornos virtuales y en la nube .
Realiza la coherencia operativa y cumple con las necesidades empresariales en entornos físicos, virtuales y en la nube, con flexibilidad y escalabilidad en el despliegue.

Simplifica el despliegue y la gestión de aplicaciones F5® definidas por el usuario y las plantillas FAST facilitan el despliegue, la gestión y la obtención de una visibilidad completa de tus aplicaciones.

Asegura tus aplicaciones críticas
Protege las aplicaciones que gestionan tu negocio con un rendimiento y una visibilidad SSL líderes en la industria.

RECURSOS RELEVANTES

Balanceo de Carga de tus Aplicaciones

Visibilidad, control y rendimiento SSL

Despliega políticas coherentes en cualquier nube

Problemas de rendimiento de la app

INTELIGENCIA DE APLICACIÓN

Gestión del tráfico de aplicaciones

BIG-IP LTM incluye balanceo de carga estático y dinámico para eliminar puntos únicos de fallo. Los proxies de aplicación te dan conocimiento de protocolo para controlar el tráfico de tus aplicaciones más importantes. BIG-IP LTM también monitoriza los niveles dinámicos de rendimiento de los servidores en un grupo, asegurando que tus aplicaciones no solo estén siempre activas, sino que también sean más fáciles de escalar y gestionar.

Entrega segura de aplicaciones

BIG-IP LTM ofrece un rendimiento SSL líder en la industria y una visibilidad para el tráfico entrante y saliente, por lo que puedes proteger de forma rentable toda tu experiencia de usuario cifrando todo, desde el cliente hasta el servidor. También protege contra ataques DDoS potencialmente paralizantes y proporciona servicios ICAP para su integración con la protección contra la pérdida de datos y la protección contra virus.

Optimización de la entrega de aplicaciones

BIG-IP LTM escala de forma espectacular, mejorando los tiempos de carga de las páginas y la experiencia del usuario con HTTP/2, caché inteligente, amplia optimización y gestión de conexiones, compresión, rendimiento RAMCache, F5 TCP Express™ y F5 OneConnect™. También
toma decisiones en tiempo real de protocolo y gestión del tráfico basadas en las condiciones de la aplicación y del servidor, permite la personalización y programabilidad de reglas, así como la descarga de contenido TCP y contenido.

Visibilidad y monitorización de aplicaciones

Monitoriza exactamente cómo está funcionando tu aplicación para usuarios reales basándote en los tiempos de respuesta de la aplicación, las condiciones de la red y el contexto del usuario. F5 Analytics recoge estadísticas específicas de la aplicación, como la URL, el rendimiento y la latencia del servidor, reportadas en diferentes niveles del servicio. BIG-IP LTM facilita la integración con tus herramientas existentes utilizando estándares industriales como sFlow, SNMP y syslog.

Visibilidad de protocolos IoT

BIG-IP LTM permite el soporte de clientes IoT, publicando información útil a los Brokers MQTT (servidores) a través del protocolo MQTT. Los Brokers MQTT envían entonces información a todos los suscriptores de esta información y el soporte MQTT permite a BIG-IP LTM aprovechar el balanceo de carga del tráfico MQTT para los clientes IoT de los clientes.

Wagner Pena

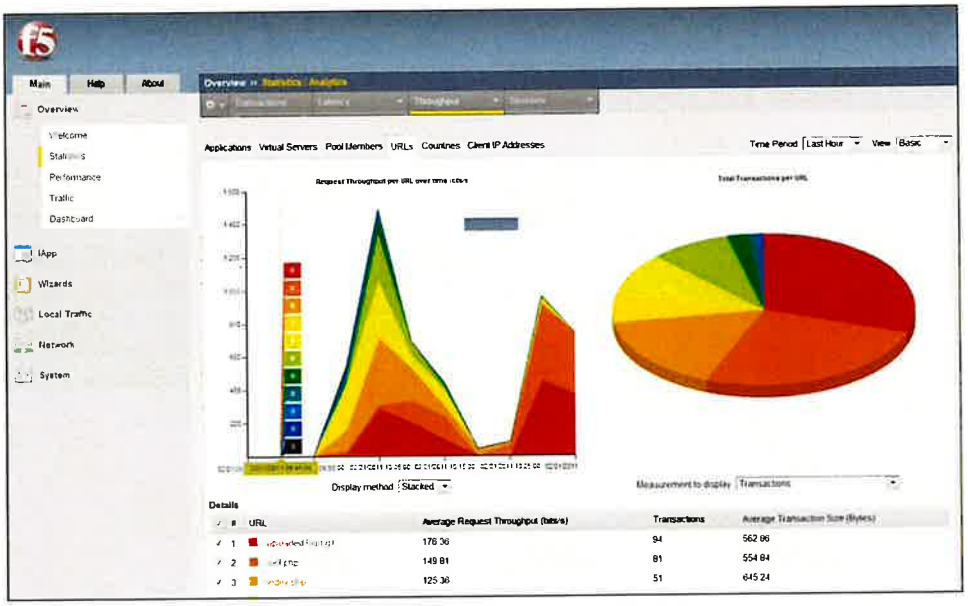


Figura 1: F5 Analytics proporciona estadísticas en tiempo real a nivel de aplicación.

UNA UTOMACIÓN Y ENTRADA DE CONTENEDORES

RECURSO RELEVANTE

Integración en entornos de contenedores

F5 Automation Toolchain permite gestionar los servicios de red y aplicaciones como la gestión del tráfico y la seguridad de aplicaciones, mediante APIs simples y declarativas en lugar de configuraciones imperativas manuales tradicionales.

En el núcleo de la Cadena de Herramientas de Automatización F5 está la Extensión de Servicios de Aplicación 3 (AS3), que permite a administradores y desarrolladores automatizar servicios de aplicación de capa 4–7. AS3 también proporciona una base sostenible para habilitar la estrategia de Infraestructura como Código (IaC) de F5 y su futura integración con soluciones de orquestación, SDN y NFV de terceros.

La incorporación declarativa F5 permite la provisión inicial de soluciones F5, así como la configuración de objetos de capa 2–3 como dominios de ruta, rutas, auto-IPs y VLANs. La Extensión de Incorporación Declarativa, al igual que la Extensión Application Services 3, acepta una declaración JSON que define el estado final deseado mediante una única API REST.

La Extensión de Streaming de Telemetría F5 es una extensión iControl LX que agrega, normaliza y reenvía estadísticas y eventos a aplicaciones de consumo como Splunk, Azure Log Analytics, AWS CloudWatch, AWS S3, Graphite y más. Esta herramienta utiliza un modelo declarativo, lo que significa que proporcionas una declaración JSON en lugar de un conjunto de comandos imperativos.

La Pasarela de Servicios API de F5 es un contenedor Docker independiente de TMOS que ejecuta el framework iControl LX de F5 y proporciona un vehículo ligero, rápido, portátil e independiente de TMOS para que los clientes aprovechen iControl LX.

La Cadena de Herramientas de Automatización F5 ofrece un enfoque de automatización orientado a procesos. Utiliza los componentes de la Automation Toolchain para provisionar, configurar y gestionar eficientemente los servicios que soportan tus aplicaciones. La cadena de herramientas de automatización está disponible, de forma gratuita, en GitHub y Docker Hub.

Las integraciones del ecosistema F5 con Ansible, Terraform, Puppet, Chef y Cisco ACI te ayudan a simplificar la orquestación y la gestión de configuración en nubes públicas y privadas y locales, ofreciendo redes definidas por software con automatización basada en políticas y aumentando la velocidad de despliegue de aplicaciones mediante provisión automatizada.

Wagner Peña

F5 Container Ingress Services (CIS) facilita la entrega de servicios avanzados de aplicaciones a tus despliegues de contenedores, permitiendo el enrutamiento HTTP con control de entrada, balanceo de carga y rendimiento en la entrega de aplicaciones, así como servicios de seguridad robustos.

Contenedores Ingress Services integra fácilmente soluciones BIG-IP con entornos nativos de contenedores, como Kubernetes, y sistemas de orquestación y gestión de contenedores PaaS, como RedHat OpenShift.

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

INFRAESTRUCTURA PROGRAMABLE

Políticas locales de tráfico

Las políticas de tráfico local de BIG-IP® son una colección estructurada y basada en datos de reglas creadas al poblar tablas en una interfaz web. Las tablas de políticas se rellenan usando un inglés legible; No se requieren habilidades de programación. Estas políticas te permiten inspeccionar, analizar, modificar, enrutar, redirigir, descartar o manipular el tráfico, y resolver casos de uso comunes previamente cubiertos
por simples iRules. Por ejemplo, podrías crear una política que determine si un cliente está usando un dispositivo móvil y luego redirigir las solicitudes desde dispositivos móviles a la URL correspondiente del sitio web móvil.

iReglas

El lenguaje de scripting F5 iRules®—la interfaz de scripting de tráfico de F5—permite el análisis programático, la manipulación y la detección de todos los aspectos del tráfico en tus redes. Los clientes implementan rutinariamente reglas de mitigación de seguridad, soportan nuevos protocolos y corrigen errores relacionados con la aplicación en tiempo real. Con iRules robustas y flexibles, puedes desarrollar soluciones de forma rápida y rápida que puedes desplegar con confianza en múltiples aplicaciones.

iRules LX

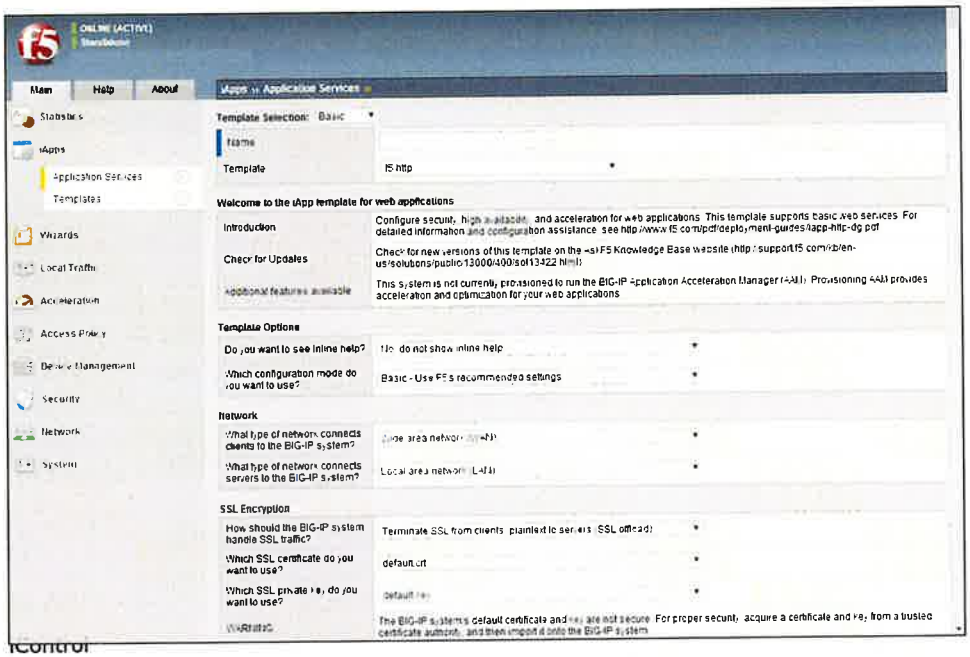
iRules LX es la siguiente etapa de evolución de la programabilidad de red que aporta soporte Node.js lenguajes a la plataforma BIG-IP. Node.js permite a los desarrolladores de JavaScript acceder a más de 250.000 paquetes npm que facilitan la escritura y el mantenimiento del código. Los equipos de desarrollo pueden acceder y trabajar en código con el nuevo entorno iRules LX Workspace y el nuevo complemento disponible para el IDE Eclipse, que puede usarse para compilaciones de integración continua.

iApps y FAST

F5 iApps y plantillas FAST son herramientas potentes que te permiten desplegar, gestionar y analizar los servicios de aplicaciones empresariales en su conjunto, en lugar de gestionarlas individualmente

Configuración y objetos. iApps y FAST te ofrecen mayor visibilidad y control sobre la entrega de aplicaciones, y te ayudan a desplegar en horas en lugar de semanas. Este enfoque centrado en la aplicación alinea la red con tus aplicaciones y adapta la entrega de las aplicaciones a las necesidades del negocio.

Figura 2: Las plantillas de iApps simplifican el despliegue de aplicaciones.



iControl

Las APIs y SDK de iControl® F5 permiten la automatización e integración de aplicaciones personalizadas en todos los aspectos de BIG-IP LTM y otros módulos de BIG-IP. iControl se entrega tanto en APIs REST como SOAP para ajustarse al modelo que mejor se adapte a tu organización. Con iControl, todos los aspectos de la configuración BIG-IP LTM, incluyendo la mayoría de los módulos BIG-IP —desde la provisión de dispositivos y aplicaciones hasta la optimización y la salud e inicio de soporte— pueden automatizarse programáticamente para lograr infraestructuras dinámicas.

iCall

F5 iCall® es un potente framework de scripting, basado en TMSH (la interfaz de línea de comandos del F5 TMOS® Shell) y Tcl, que ayuda a los clientes a mantener su entorno y reducir los tiempos de inactividad automatizando tareas. Monitoriza eventos y ejecuta scripts para resolver problemas de forma rápida y predecible. iCall permite a los administradores reaccionar a eventos específicos ejecutando servicios en el plano de gestión, como generar un volcado de pila TCP en caso de fallo, ejecutar una iApp específica para reconfigurar la configuración de servicios de red de la aplicación o ajustar los pesos de balanceo de carga en los servicios de la aplicación en función de un cambio en los datos de monitorización de salud.

RECURSOS RELEVANTES

Optimizar el rendimiento del ADC

Servicios de aplicaciones consistentes en cualquier nube

INFRAESTRUCTURA DISPONIBLE PARA LA INFRAESTRUCTURA

Listo para la nube

BIG-IP LTM facilita la coherencia operativa y el cumplimiento de las necesidades empresariales en entornos físicos, virtuales y en la nube, eliminando la fricción de la migración de aplicaciones entre arquitecturas físicas tradicionales y en la nube. Disponible en nubes públicas y para migración a través de multi-cloud. Aprende más en la sección de datos de la Edición Virtual BIG-IP.

ScaleN

La tecnología F5 ScaleN® utiliza el chasis F5 VIPRION®, los Clústeres de Servicios de Dispositivo y las capacidades de escalado del Multiprocesamiento™ Virtual en Clúster F5 (vCMP) para permitir soluciones más eficientes, elásticas y multiinquilino para centros de datos, nubes y despliegues híbridos. ScaleN va más allá de las limitaciones tradicionales de la infraestructura y ofrece múltiples modelos de escalabilidad y consolidación para ayudarte a satisfacer las necesidades específicas de tu negocio.

Redes virtuales

El módulo de servicios BIG-IP® SDN soporta de forma nativa VXLAN y NVGRE para ofrecer capacidades de pasarela con BIG-IP LTM que conecta redes virtuales y tradicionales. Esto te permite mantener las cosas simples, aplicando servicios de red de entrega de aplicaciones tanto en redes virtuales como tradicionales.

Enrutamiento avanzado

El Módulo Avanzado de Enrutamiento™ BIG-IP® permite a BIG-IP LTM proporcionar capacidades de enrutamiento de red como BGP, RIP, OSPF, ISIS y BFD para mejorar la interoperabilidad dentro de la red, aumentando la resiliencia y capacidad de tu red.

ACTO MITIGACIÓN

Despliega F5 Distributed Cloud Bot Defense directamente desde tu IP BIG-IP

Los bots causan un dolor financiero significativo mediante el scraping que ralentiza el rendimiento, el rescalping y el acaparamiento de inventario que frustran a los clientes fieles, la enumeración de códigos de tarjetas regalo para robar saldos, la creación de cuentas falsas para cometer fraude y el crepitado de credenciales —la prueba de credenciales robadas— que conduce a la toma de control de cuentas.

Los bots avanzados y persistentes de hoy en día son más sofisticados que nunca. Para adelantarse a los atacantes, F5 Distributed Cloud Bot Defense utiliza una recolección rica de señales del lado del cliente, ofuscación de código líder en la industria, recopilación agregada de telemetría e IA para una eficacia a largo plazo sin precedentes y casi cero falsos positivos, manteniendo el acceso para bots buenos. Y dado que F5 defiende los sitios más atacados en la web —incluidos los de los bancos, minoristas y aerolíneas más grandes del mundo— F5 está preparada cuando estos ataques tengan como objetivo tu organización.

Despliega F5 Distributed Cloud Bot Defense directamente desde tu BIG-IP o a través de un conector adecuado para tu aplicación, con servicios de soporte adaptados a tus necesidades, desde autoservicio hasta servicio gestionado.

GRANDES - PLATAFORMAS IP

Solo la plataforma ADC de próxima generación y lista para la nube de F5 ofrece una agilidad similar a la de DevOps con la escala, profundidad de seguridad y protección de inversión necesarias tanto para aplicaciones consolidadas como emergentes. Los dispositivos BIG-IP® iSeries ofrecen programabilidad rápida y sencilla, orquestación compatible con el ecosistema y un rendimiento de hardware definido por software que rompe récords. Como
como resultado, los clientes pueden acelerar las nubes privadas y asegurar datos críticos a gran escala, al tiempo que reducen el TCO y preparan sus infraestructuras de aplicaciones para el futuro. Las soluciones F5 pueden desplegarse rápidamente mediante integraciones con herramientas de gestión de configuración de código abierto y sistemas de orquestación.

Además de la iSeries, F5 ofrece sistemas modulares de chasis y palas VIPRION diseñados específicamente para el rendimiento y para una verdadera escalabilidad lineal bajo demanda sin interrupciones empresariales. Los sistemas VIPRION aprovechan la tecnología de clustering ScaleN de F5 para poder añadir blades sin necesidad de reconfigurar o reiniciar.

La plataforma VELOS® de F5 es la siguiente generación de los sistemas basados en chasis líderes en la industria de F5, que ofrece un rendimiento y escalabilidad sin precedentes en un único Controlador de Entrega de Aplicaciones (ADC). Puedes escalar la capacidad sin problemas añadiendo blades modulares en un chasis, sin interrupciones, y VELOS permite una mezcla de tenants tradicionales de BIG-IP así como de próxima generación de BIG-IP en el futuro.

La solución ADC de próxima generación, F5 rSeries, conecta las infraestructuras tradicionales y modernas con una plataforma reestructurada y API-first, diseñada para satisfacer las necesidades de tus aplicaciones tradicionales y emergentes. La nueva F5 rSeries ofrece algo sin precedentes niveles de rendimiento, una arquitectura totalmente automatizable y la máxima fiabilidad, seguridad y control de acceso para tus aplicaciones críticas.

Las Ediciones Virtuales (VEs) del software BIG-IP se ejecutan en servidores comerciales y soportan la variedad de hipervisores y requisitos de rendimiento. Los VEs proporcionan agilidad, movilidad y un despliegue rápido de servicios de aplicaciones en centros de datos definidos por software y entornos en la nube.

Consulte las hojas técnicas de hardware del sistema BIG-IP, VIPRION, VELS y Virtual Edition para conocer Más detalles. Para información sobre el soporte específico de módulos para cada plataforma, consulte las últimas notas de versión en AskF5. Para la lista completa de hipervisores soportados, consulte la Matriz de Hipervisores Soportados por VE.

expert
where knowledge meets action
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Wagner Pérez

Con la Gestión Centralizada BIG-IQ®, puedes gestionar las plataformas F5 con una visión de cristal único, incluyendo:

- Electrodomésticos BIG-IP iSeries
- Electrodomésticos rSeries
- Ediciones Virtuales BIG-IP
- Chasis VIPRION
- Chasis VELOS

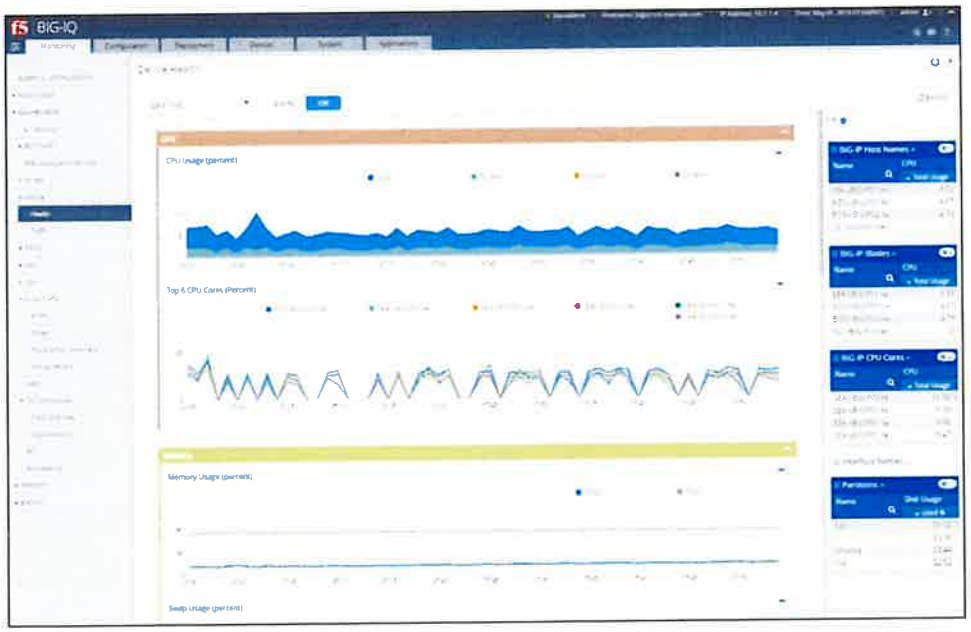


Figura 3: Gestiona la salud de tu appliance BIG-IP y registra el uso de CPU y memoria de plataformas físicas y virtuales, blades de hardware y núcleos con BIG-IQ. Utiliza registros y reportes para entender las tendencias generales y detectar áreas que necesitan corrección. Gestionar fácilmente políticas, certificados y gestión de licencias para enviarlas a todos los ADCs BIG-IP para un control centralizado de la infraestructura de servicios de aplicaciones.

LICENCIAS FLEXIBLES PARA ADAPTARSE A TUS NECESIDADES

Para alinearse con diferentes directrices de compra, BIG-IP Next también puede estar licenciado mediante una variedad de modelos de consumo. Elige el modelo de licencias que mejor se adapte a tus necesidades, incluyendo suscripción, perpetuo o el programa de servicios públicos:

- **Suscripción**—Las suscripciones renovables de uno a tres años proporcionan ahorros iniciales e incluyen acceso al soporte premium de F5.
- **Perpetuo**: Una inversión única en CapEx proporciona la propiedad total de la solución.
- **Utilidad**: El modelo de pago por uso incluye acceso a soporte premium F5 sin necesidad de compromiso a largo plazo.

Wagner Pina

SERVICIOS GLOBAL F 5

F5 Global Services ofrece apoyo, formación y consultoría de primer nivel para ayudarte a sacar el máximo partido a tu inversión en F5. Ya sea proporcionando respuestas rápidas a preguntas, formando equipos internos o gestionando implementaciones completas desde el diseño hasta el despliegue, F5 Global Services puede ayudar a garantizar que tus aplicaciones sean siempre seguras, rápidas y fiables. Para más información sobre F5 Global Services, contacta con consulting@f5.com o visita f5.com/support.

DEV CENTRAL

La comunidad técnica de DevCentral® de F5 es una fuente activa y comprometida para los mejores artículos técnicos, tutoriales, foros de discusión, código compartido, medios y mucho más relacionado con la programabilidad y la red de entrega de aplicaciones.

BIG - FUNCIONES DE IP LTM

Gestión del tráfico de aplicaciones

- Balanceo inteligente de carga
- Soporte de protocolos de aplicación (HTTP/2, SSL/TLS, SIP, etc.)
- Monitorización de la salud de la aplicación
- Gestión del estado de la conexión de aplicaciones
- F5 OneConnect
- Enrutamiento avanzado (BGP, DESCANSO EN PAZ, OSPF, ISIS, BFD)
- Servicios SDN (VXLAN, NVGRE)

Optimización de la entrega de aplicaciones

- Compresión adaptativa simétrica
- Caché y compresión de la RAM
- TCP Express
- Pasarela HTTP/2

Entrega segura de aplicaciones

- Conexión SSL y espejado de sesión
- Servicios híbridos de criptomonedas (Descarga SSL por hardware para BIG-IP VE)
- Descarga de cifrado SSL/TLS (acelerada por hardware)
- Agilidad del algoritmo (GCM, ECC, Camellia, DSA, RSA)
- Soporte para Suite B incluyendo secreto hacia adelante
- HSM interno/de red/nube (FIPS 140-2)
- Visibilidad SSL

Visibilidad y monitorización de aplicaciones

- Analítica F5
- Panel de rendimiento
- Tala de alta velocidad
- sFlow

Infraestructura programable

- iRules e iRules LX para la programabilidad en planos de datos
- iCall para scripting basado en eventos en el plano de control
- iApps para la gestión y despliegue de configuración a nivel de aplicación
- iControl para la Gestión API (SOAP, RESTO)

Automatización e ingreso de contenedores

- Cadena de herramientas de automatización para configuraciones declarativas de servicios de aplicaciones
- Application Services 3 Extension (AS3) automatiza los servicios de las Capa 4-7
- Incorporación declarativa para provisiones y configuraciones iniciales
- Streaming de telemetría para exportación de flujo de datos a analítica de terceros
- Plantillas FAST para configuraciones declarativas de servicios de aplicación
- Servicios de entrada de contenedores para la automatización de servicios de aplicaciones de contenedores

Integraciones de ecosistemas

- Plantillas de Ansible para la automatización de servicios de aplicaciones
- Módulos Terraform para la automatización del despliegue
- Cisco ACI y F5 BIG-IP para tejido de red integrado y control
- Títere para la automatización de configuraciones y servicios de aplicaciones
- Chef para integraciones de gestión de configuración
- F5 Defensa Distribuida de Bots en la Nube para mitigación de ataques

ScaleN

- Escalado bajo demanda
- Clúster de aplicaciones totalmente activo

MÁS INFORMACIÓN

Para saber más sobre BIG-IP LTM, visita f5.com para encontrar estos y otros recursos.

Telaraña

Gestor de Tráfico Local BIG-
IP DevCentral

Hojas de datos

Hardware del Sistema
BIG-IP Ediciones
Virtuales rSeries
BICICLETAS
VIPRION

Artículos y guías

Estado de la Estrategia de Aplicaciones 2021: Desentrañando el estado actual y futuro de la seguridad y entrega de aplicaciones
3 consejos para mantener un portafolio de aplicaciones de alto rendimiento Elige soluciones avanzadas en la nube que escalen en el futuro Balanceo de carga de tus aplicaciones

Estudios de caso

Varolii: proveedor SaaS garantiza alta disponibilidad y resiliencia para aplicaciones críticas de clientes con F5 Motorists Insurance Group ofrece a los clientes una experiencia fluida con la solución F5 + Okta Pandora escala para atender a decenas de millones de usuarios de radio por Internet con la solución F5 MarketAxess aumenta la productividad con la automatización F5 y Ansible

Casos de uso

Desplegar políticas coherentes en cualquier nube Integrar en entornos contenedores
Solucionar problemas de rendimiento de las aplicaciones Integrarse en las canalizaciones CI/CD

F5 Advanced WAF

FICHA TÉCNICA

Contenido

Protección proactiva de aplicaciones

Las aplicaciones son fundamentales para su negocio. Sin la protección adecuada, pueden convertirse en un vector de ataque que, en última instancia, puede provocar una filtración de datos. Considere esta alarmante estadística: las organizaciones tienen un promedio de 765 aplicaciones web y estas aplicaciones son el objetivo inicial de las filtraciones de datos el 53 % de las veces.[1]

Proteja su organización y su reputación manteniendo la confidencialidad, la disponibilidad y el rendimiento de las aplicaciones que son fundamentales para su negocio con F5® soluciones de firewall de aplicaciones web (WAF).

Las soluciones F5 WAF se implementan en más centros de datos que cualquier WAF empresarial del mercado. El conjunto integral de soluciones F5 WAF incluye conjuntos de reglas administrados para Amazon Web Services (AWS); servicio administrado, de autoservicio y basado en la nube en F5 Silverline® plataforma de entrega de servicios basada en la nube; integración del controlador de entrega de aplicaciones (ADC) con F5 BIG-IP® Application Security Manager™ (ASM)[2]; y F5 Advanced Web Application Firewall™ (Advanced WAF).

Advanced WAF redefine la seguridad de las aplicaciones para abordar las amenazas más frecuentes a las que se enfrentan las organizaciones hoy en día:

- Ataques automatizados y bots que sobrecargan las soluciones de seguridad existentes.
- Ataques web que roban credenciales y obtienen acceso no autorizado a las cuentas de usuario.
- Ataques a la capa de aplicación que evaden la seguridad estática basada en la reputación y las firmas manuales.
- Nuevas superficies de ataque y amenazas debido a la rápida adopción de las API.

El WAF avanzado se basa en la tecnología probada de F5 y va más allá de la seguridad reactiva, como las firmas estáticas y la reputación, para detectar y mitigar de forma proactiva los bots, proteger las credenciales y los datos confidenciales, y defenderse contra la denegación de servicio (DoS) de las aplicaciones.

El WAF avanzado ofrece protecciones flexibles y completas dondequiera que residan las aplicaciones y sin comprometer el rendimiento. El WAF avanzado se ofrece como dispositivo, edición virtual y como servicio gestionado, lo que proporciona servicios WAF automatizados que cumplen con los requisitos complejos de implementación y administración, al tiempo que protegen sus aplicaciones con gran precisión. Es la solución más eficaz para proteger las aplicaciones y los datos modernos de las amenazas existentes y emergentes, al tiempo que se mantiene el cumplimiento de los mandatos normativos clave.

Wagner Peña

[1] Informe de protección de aplicaciones de 2018

[2] BIG-IP ASM se sigue ofreciendo a través de las licencias F5 Good/Better/Best.

Beneficios clave

Proteja las aplicaciones web y móviles de los bots maliciosos

F5 protege los activos, aplicaciones y datos confidenciales más valiosos de una organización contra bots, ataques automatizados, web scrapers y exploits. El WAF avanzado extiende la protección contra bots a las aplicaciones móviles a través del SDK móvil F5 Anti-Bot, lo que proporciona una implementación rápida de la protección contra bots móviles a través de un portal web fácil de usar sin necesidad de realizar cambios en la aplicación o el dispositivo móvil. Las aplicaciones con protección contra bots móviles integrada son compatibles con las tiendas de aplicaciones de proveedores y de terceros.

Proteja las credenciales y los datos confidenciales contra el robo y el abuso

El WAF avanzado protege las credenciales y los datos confidenciales contra el robo y el abuso, lo que evita las filtraciones de datos y mitiga los ataques automatizados que aprovechan las credenciales robadas previamente. F5 BIG-IP DataSafe™El cifrado de la capa de aplicación en Advanced WAF enmascara los campos confidenciales directamente en el navegador web del usuario, lo que hace que los datos robados por ciberdelincuentes a través de ataques del lado del cliente sean inútiles. Con BIG-IP DataSafe, los clientes pueden cifrar los datos a nivel de campo de forma transparente, sin necesidad de realizar cambios en los clientes ni en los servidores web. La mitigación integral de ataques de fuerza bruta, incluida la protección contra el relleno de credenciales, defiende contra los ataques automatizados que aprovechan las credenciales robadas previamente.

Defensa contra ataques sofisticados de denegación de servicio (DoS) de aplicaciones

Advanced WAF descubre y crea huellas digitales de patrones de tráfico nuevos e inusuales sin intervención humana, distinguiendo y aislando el tráfico potencialmente malicioso del tráfico legítimo. Esta capacidad de mitigación automatizada se basa en un ciclo de retroalimentación continua del comportamiento del cliente y la carga del servidor. Si se detecta un comportamiento anómalo, Advanced WAF crea automáticamente una firma dinámica y comienza a mitigar el ataque. La eficacia de la mitigación se supervisa a través del ciclo de retroalimentación continua. Los falsos positivos se reducen, mientras que la precisión y el rendimiento mejoran mediante el ajuste continuo de la mitigación a medida que el ataque comienza, evoluciona o se detiene.

Mitigación de campañas de amenazas sofisticadas

Las campañas de amenazas proporcionan firmas específicas para proteger a las organizaciones de ataques generalizados que a menudo están coordinados por el crimen organizado y los estados nación. Basándose en la investigación de F5 Labs, las campañas de amenazas proporcionan inteligencia crítica para identificar y mitigar ataques sofisticados con actualizaciones casi en tiempo real. Los metadatos se utilizan para determinar tanto las solicitudes maliciosas como la intención maliciosa, y la alta precisión de las firmas de las campañas de amenazas bloquea inmediatamente las amenazas activas con bajos falsos positivos y sin ciclo de aprendizaje.

Proteger las API

A medida que las aplicaciones web se expanden de conectadas a colaborativas mediante el uso extensivo de interfaces de programación de aplicaciones (API), Advanced WAF garantiza que los métodos de API se apliquen en las URL. También protege las aplicaciones contra ataques a la API que suelen pasar desapercibidos para los firewalls tradicionales. Con un mecanismo de defensa único que protege las API XML, JSON y GTW mediante la limitación de velocidad, el análisis de comportamiento y la antiautomatización, Advanced WAF detecta automáticamente las amenazas a la interfaz de programación de aplicaciones, aplica reglas de política estrictas para cada caso de uso y bloquea ataques y tipos de contenido especiales, cerrando la puerta trasera a las amenazas de las aplicaciones. Con F5 Access Manager™, la protección de la API mejora mediante la autenticación integral y la aplicación de tokens.

Wagner Peña

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

230

Garantizar la seguridad y el cumplimiento de las aplicaciones

Obtenga seguridad integral contra ataques sofisticados de capa 7, bloqueando las amenazas que evaden los WAF tradicionales y permitiendo el cumplimiento de las principales normativas.

Active la protección inmediatamente

Simplifique la seguridad con políticas predefinidas, miles de firmas listas para usar y un enfoque optimizado para la administración de políticas que reduce los gastos operativos.

Parchee las vulnerabilidades rápidamente

Identifique y resuelva las vulnerabilidades de las aplicaciones en minutos con la integración líder de pruebas de seguridad de aplicaciones dinámicas (DAST) y el parcheo virtual automático.

Implemente de forma flexible

Implemente como un dispositivo, en entornos virtuales o en la nube, y como un servicio administrado que admite servicios multiinquilino, al tiempo que incorpora inteligencia externa que protege contra amenazas de IP conocidas.

Defiéndase con protecciones avanzadas comprobadas

Defiéndase con tecnología altamente programable que adapta dinámicamente las políticas, detiene de forma proactiva los bots y los ataques DoS, y demuestra una eficacia de seguridad general del 99.89 %.

Amplíe el conocimiento de las amenazas

Comprenda fácilmente su estado de seguridad con un análisis forense detallado, visibilidad completa del tráfico HTTP y WebSocket, y una rica información sobre todos los eventos y tipos de usuarios.

Garantice una protección integral contra amenazas

El volumen y la sofisticación de los ataques hacen que mantenerse al día sobre los tipos de amenazas de seguridad y las medidas de protección sea un desafío para los administradores de aplicaciones y los equipos de seguridad. Con capacidades líderes en la industria y una flexibilidad superior, F5 Advanced WAF ofrece seguridad avanzada y rentable para las aplicaciones web y móviles más recientes

El WAF avanzado protege las credenciales contra el robo y el abuso, y asegura cualquier parámetro contra la manipulación del lado del cliente mediante la validación de los parámetros de inicio de sesión y el flujo de la aplicación para prevenir la navegación forzada y las fallas lógicas. También permite a las organizaciones protegerse eficazmente contra los ataques de aplicaciones de capa 7 existentes y emergentes, previniendo costosas filtraciones de datos, frustrando ataques DoS y manteniendo el cumplimiento. El WAF avanzado es el primer WAF líder que admite la transición de AJAX/HTTP a WebSockets para una mayor eficiencia y menor sobrecarga con datos de transmisión bidireccionales. El WAF avanzado también proporciona visibilidad del tráfico de WebSocket, lo que permite a las empresas realizar la transición para proteger las sesiones de chat y las fuentes de información en streaming (como los tickers de bolsa) contra la exposición, la manipulación y el robo de datos. Los usuarios se benefician de una extensa base de datos de firmas, actualizaciones dinámicas de firmas, integración con DAST y la flexibilidad de F5 iRules® scripting para la personalización y la extensibilidad

Las organizaciones confían en Advanced WAF para proteger las aplicaciones web más visitadas del mundo, dondequiera que se encuentren, con el más alto nivel de seguridad y sin comprometer el rendimiento. Advanced WAF permite a las organizaciones detectar y mitigar las amenazas de capa 7, incluyendo web scraping, inyección web, fuerza bruta, CSRF, amenazas web JSON, URL con alto volumen de DoS y ataques de día cero, proporcionando alertas tempranas y mitigando las amenazas según la política.

Wagner Pina

IPX SRL
RNC 130-850151
Santo Domingo, R.D.

231

Defiende automáticamente contra múltiples amenazas simultáneas de capa de aplicación, incluyendo ataques DoS sigilosos de bajo ancho de banda. Advanced WAF también detiene el secuestro de sesión en el navegador e informa sobre ataques regulares y repetidos desde direcciones IP.

Utilizando capacidades de aprendizaje automático, perfiles dinámicos, métodos únicos de detección de anomalías y políticas basadas en riesgos, Advanced WAF puede imponer las protecciones necesarias para evitar que incluso los ataques más sofisticados lleguen a los servidores. Cuando se combina con F5 BIG-IP Local Traffic Manager™(LTM), Advanced WAF filtra los ataques y acelera las aplicaciones para una mejor experiencia de usuario

Wagner Peña

Investigación de seguridad experta continua

El equipo de investigación de seguridad de F5 ayuda a garantizar el desarrollo continuo de firmas, políticas y capacidades de WAF avanzado. Los investigadores exploran foros y recursos de terceros, investigan ataques, realizan ingeniería inversa de malware y analizan vulnerabilidades para determinar métodos eficaces de detección y mitigación que protejan contra amenazas de día cero, ataques DoS y otras amenazas evasivas o en evolución. El WAF avanzado ofrece una protección mejorada gracias a los avances tecnológicos, las actualizaciones periódicas de firmas, la inteligencia sobre amenazas y el fortalecimiento de las capacidades existentes.

Defiéndase con protecciones proactivas contra bots

Se requiere una defensa permanente para identificar y protegerse eficazmente contra ataques DoS automatizados, web scraping y ataques de fuerza bruta antes de que se produzcan. F5 ofrece capacidades de defensa proactiva contra bots que proporcionan controles efectivos para prevenir estos ataques. Mediante métodos de defensa avanzados y la comparación de reputación para identificar usuarios no humanos (como desafíos JavaScript y CAPTCHA, geolocalización y otras técnicas), Advanced WAF ralentiza las solicitudes para distinguir los bots y las descarta antes de que lleguen al servidor. Advanced WAF inspecciona exhaustivamente la interacción del usuario, analiza el estado del servidor y detecta anomalías en las transacciones para ayudar a identificar bots que podrían eludir los desafíos del cliente/aplicación, los límites de velocidad establecidos y otros métodos de detección estándar. También mitiga automáticamente los ataques de capa 7 que muestran un cambio inusual en los patrones de solicitud. A diferencia de otras soluciones, Advanced WAF proporciona a los expertos en seguridad un mayor control sobre la aplicación de la defensa contra bots, permitiéndoles forzar acciones adicionales (como el registro de alta velocidad en acciones de bloqueo o desafío, desafíos JavaScript, anulaciones de URI, redirecciones HTML personalizadas y más) antes de que se apliquen las mitigaciones. Las capacidades de defensa contra bots de Advanced WAF proporcionan los métodos de prevención más eficaces, lo que le permite identificar actividad automatizada sospechosa, categorizar los bots detectados y mitigar los ataques con el mayor nivel de precisión. El SDK móvil F5 Anti-Bot, junto con Advanced WAF, extiende la protección integral contra bots de F5 a las aplicaciones móviles sin necesidad de modificar el código de la aplicación.

Seguimiento de intentos de usuarios maliciosos

Distinguir a los usuarios autorizados de los ciberdelincuentes cada vez que se visita un sitio web ayuda a minimizar el riesgo de seguridad y a prevenir la actividad maliciosa. Con Advanced WAF, los equipos de seguridad de aplicaciones pueden emplear técnicas de seguimiento de identificación de dispositivos para identificar usuarios finales específicos, sesiones de aplicaciones y atacantes. Esta capacidad única permite a TI distinguir fácilmente el tráfico humano del tráfico de bots, detectar visitantes recurrentes, prevenir intentos maliciosos y ayudar a los WAF a mitigar con mayor precisión los ataques de fuerza bruta, el secuestro de sesiones, el web scraping y los ataques DoS.

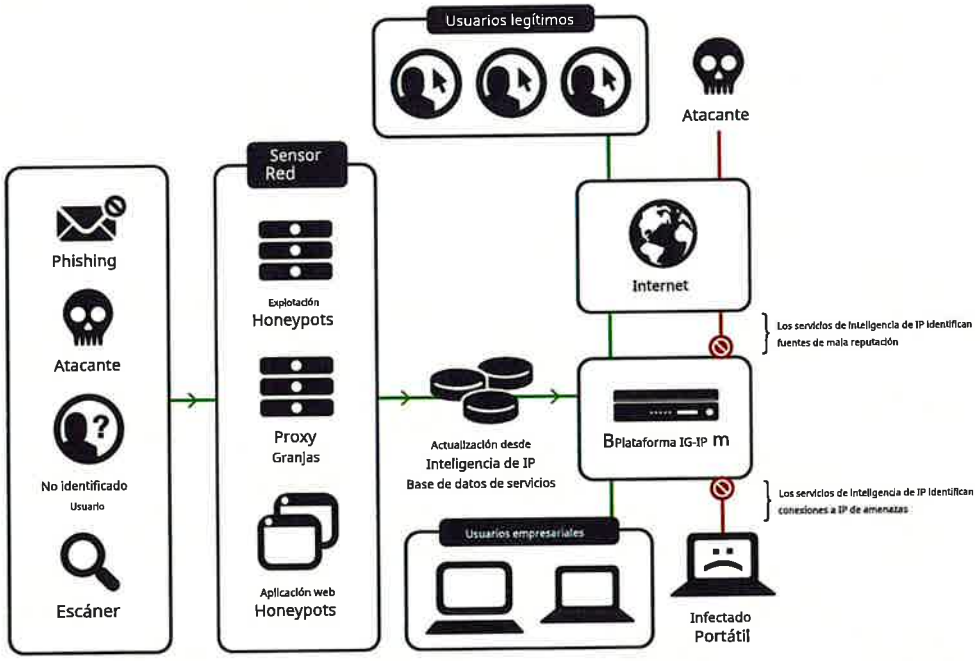
232

El seguimiento de la identificación del dispositivo permite que Advanced WAF identifique el mismo navegador, incluso cuando los usuarios cambian de sesión o de IP de origen. Cuando está activado, Advanced WAF captura y guarda las características y atributos únicos del dispositivo, determina qué clientes son sospechosos y mitiga las amenazas según la configuración predefinida. Ya sea una amenaza automatizada, un ataque DoS, un navegador sin interfaz gráfica o un usuario humano, Advanced WAF puede distinguir entre atacantes recurrentes y visitantes de clientes para cada caso de uso de WAF.

Bloquear direcciones IP maliciosas

La entrega del contenido de Internet actual, rico y complejo, a los usuarios puede exponer a una organización a una variedad de ataques potencialmente maliciosos provenientes de direcciones IP que cambian rápidamente. El tráfico de botnets entrante y saliente, como la actividad de DoS y malware, puede penetrar las capas de seguridad de la organización.Servicios de inteligencia de IP de F5 mejora las decisiones de seguridad automatizadas con inteligencia de reputación de IP. Al identificar las direcciones IP y las categorías de seguridad asociadas con la actividad maliciosa, los Servicios de inteligencia de IP pueden incorporar listas dinámicas de direcciones IP amenazantes de terceros en la plataforma F5, lo que agrega contexto y automatización a las decisiones de bloqueo del WAF avanzado. Esto agrega granularidad a las reglas del WAF avanzado, lo que permite a los administradores configurar una alarma, detener el tráfico o bloquear completamente las IP según una categoría de reputación de IP específica, al tiempo que incluyen en la lista blanca las direcciones IP aprobadas

Además, Advanced WAF reduce la mitigación computacionalmente pesada de amenazas provenientes de direcciones IP maliciosas conocidas con una capacidad única de bloqueo de IP (lista negra acelerada). En lugar de desperdiciar ciclos en el tráfico de IP con mal comportamiento, Advanced WAF incluye inmediatamente en la lista negra las IP que fallan repetidamente en los desafíos o que experimentan altas tasas de bloqueo. Esto bloquea temporalmente las IP maliciosas en el hardware de la capa de red hasta que las fuentes de inteligencia de IP estén actualizadas.



Los servicios de inteligencia de IP recopilan datos de reputación para su uso por las soluciones de F5.

Habilitación del cifrado seguro

A medida que la creciente demanda de protección de datos impulsa el crecimiento del tráfico cifrado, es importante hacer la transición a Perfect Forward Secrecy (PFS) y al mismo tiempo protegerse contra los ataques SSL/TLS que amenazan la seguridad de las aplicaciones y la información en tránsito. Advanced WAF protege contra los intentos maliciosos de eludir SSL/TLS y comprometer las claves privadas, las contraseñas de usuario y otra información confidencial. Proporciona una terminación SSL/TLS completa y descifra y vuelve a cifrar el tráfico terminado, lo que permite una inspección y mitigación completas de las amenazas maliciosas ocultas. Cuando Advanced WAF se combina con BIG-IP LTM, las organizaciones también obtienen una mitigación integral de DDoS SSL/TLS y protección de descarga SSL/TLS para protegerse contra ataques SSL/TLS, incluidos los ataques de inundación SSL, POODLE, Heartbleed y varias herramientas de descifrado de memoria.

Identificar comportamiento anómalo

Con Advanced WAF, el departamento de TI puede detectar fácilmente el tráfico que no se ajusta al comportamiento normal y que evade las protecciones volumétricas habituales, como un aumento o disminución inusual de la latencia o la tasa de transacciones. Advanced WAF puede identificar y bloquear de forma única los fallos excesivos de autenticación de direcciones IP que generan un alto volumen de intentos de inicio de sesión, así como otras anomalías en el patrón de tráfico típico. Estas incluyen sesiones abiertas a altas tasas o que solicitan demasiado tráfico. El análisis de comportamiento y el aprendizaje automático en Advanced WAF supervisan automáticamente el tráfico de clientes y servidores en busca de anomalías en un ciclo de retroalimentación continua.

Parchear las vulnerabilidades inmediatamente

Advanced WAF se integra con los principales escáneres de vulnerabilidades de aplicaciones web para permitirle administrar fácilmente las evaluaciones, descubrir vulnerabilidades y aplicar políticas específicas desde una única ubicación. Estas capacidades únicas facilitan la mitigación casi instantánea de los resultados de la evaluación de aplicaciones, lo que garantiza la protección mientras los desarrolladores corrigen el código vulnerable, aplicando parches en minutos en lugar de semanas o meses. Con Advanced WAF, los administradores pueden importar los resultados de las pruebas de los escáneres DAST, incluidos los escáneres de WhiteHat, IBM y QualysGuard, y superponer una política basada en vulnerabilidades (obtenida de las integraciones de escáneres F5) sobre una política de implementación rápida o de SharePoint existente. Cuando se combina con WhiteHat Sentinel, Advanced WAF también detecta e informa al escáner sobre los cambios recientes en el sitio web. Esto garantiza el escaneo de URL y parámetros que de otro modo se pasarían por alto y la aplicación de políticas específicas, lo que permite a las organizaciones proteger sus aplicaciones inmediatamente después de la actualización

La compatibilidad con Advanced WAF DAST ayuda a TI a ofrecer seguridad web de última generación mediante servicios simples, precisos y automatizados. Estos servicios protegen los activos en un entorno de amenazas dinámico con evaluaciones más completas, cero falsos positivos y más parches virtuales manuales y automatizados que cualquier otra solución WAF.

Aplicar bloqueo basado en geolocalización

Los ataques están aumentando desde diversas fuentes globales. Advanced WAF le permite bloquear estos ataques según la geolocalización: estados, países o regiones. Los administradores pueden seleccionar fácilmente geolocalizaciones permitidas o prohibidas para una aplicación estricta de las políticas y protección contra ataques. El bloqueo basado en geolocalización también protege contra patrones de tráfico anómalos de países o regiones específicos y permite la limitación del tráfico según la ubicación. La protección basada en geolocalización de Advanced WAF se puede aplicar a un desafío CAPTCHA y para proteger la caché de RAM y otros recursos de los ataques DDoS.

Wagner Peña

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

234

Inspeccionar SMTP y FTP

Advanced WAF habilita las comprobaciones de seguridad de SMTP y FTP para proteger contra el spam, Ataques virales, robo de directorios y fraude. Con la configuración predeterminada, los administradores pueden configurar fácilmente perfiles de seguridad para inspeccionar el tráfico FTP y SMTP en busca de vulnerabilidades de red y cumplimiento de protocolos. La configuración predeterminada también permite activar alarmas o bloquear solicitudes por infracciones.

Las comprobaciones de seguridad SMTP permiten la validación del correo entrante mediante varios criterios, al tiempo que se deniegan o permiten métodos de llamada comunes utilizados para atacar los servidores de correo. Además, los administradores pueden establecer límites de velocidad en el número de mensajes entrantes, crear listas grises y negras, y validar los registros DNS SPF. Se pueden activar infracciones de FTP para solicitudes anónimas, pasivas o activas; comandos FTP específicos; longitud de la línea de comandos; e intentos de inicio de sesión excesivos. Los administradores pueden utilizar la configuración predeterminada de SMTP/FTP para una configuración sencilla o personalizar los perfiles para abordar riesgos específicos y garantizar de forma más eficaz el cumplimiento del protocolo.

Wagner Peña

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Agilizar el aprendizaje, la implementación y la administración

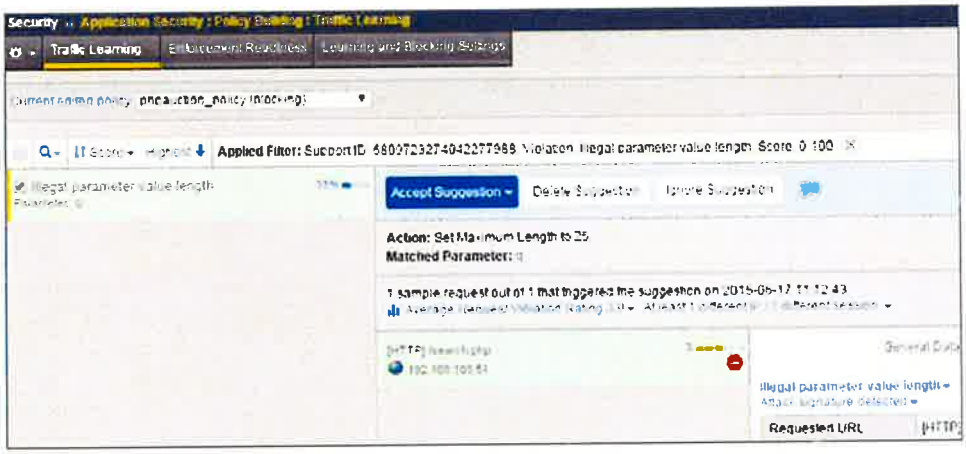
Las organizaciones desean activar las protecciones de inmediato sin una amplia experiencia en seguridad. F5 Advanced WAF simplifica y automatiza la configuración y la implementación de políticas con políticas de seguridad predefinidas que proporcionan protección inmediata para aplicaciones comunes como Microsoft Outlook Web Access, Lotus Domino Mail Server, Oracle E-Business Financials y Microsoft SharePoint. Las políticas validadas también sirven como punto de partida para la creación de políticas más avanzadas. Esto permite incluso a los usuarios principiantes implementar rápidamente políticas y proteger de inmediato las aplicaciones con poco o ningún tiempo de configuración

Aprendizaje unificado y creación dinámica de políticas

En el corazón de Advanced WAF se encuentra el motor de aprendizaje unificado y creación dinámica de políticas, que automatiza la creación y el ajuste de políticas para aumentar la eficiencia operativa y la escalabilidad. El motor de creación de políticas crea automáticamente políticas de seguridad en torno a las violaciones de seguridad, estadísticas avanzadas y heurísticas a lo largo del tiempo. También comprende el comportamiento esperado para lograr un filtrado de tráfico más preciso.

Al examinar cientos o miles de solicitudes y respuestas, el motor de creación de políticas completa la política de seguridad con elementos legítimos con mayor precisión que otros WAF. Las políticas generadas dinámicamente se colocan inicialmente en el entorno de pruebas y luego se mueven automáticamente desde allí y se aplican a medida que cumplen con los umbrales de reglas para la estabilización.
El motor de creación de políticas admite la adaptación y el aprendizaje automáticos de políticas tras la ocurrencia de violaciones o a medida que se observan nuevos parámetros. El mantenimiento de políticas se simplifica mediante una interfaz gráfica de usuario con una vista de una sola página de todas las sugerencias de aprendizaje. Las acciones con un solo clic le permiten explorar, buscar, aceptar e ignorar posibles sugerencias para ajustes de políticas, lo que refuerza las políticas con facilidad.

235



La interfaz gráfica de usuario de aprendizaje mejorada ofrece una vista de una sola página de todas las sugerencias de aprendizaje.

Administración y supervisión centralizadas

Cuando implementa varios dispositivos Advanced WAF, F5 BIG-IQ®La gestión centralizada centraliza la administración de toda su infraestructura F5. Los administradores obtienen una vista consolidada de todos los dispositivos F5, lo que ayuda a gestionar mejor las relaciones entre los dispositivos, reducir los costes de TI y minimizar los errores de configuración.

Advanced WAF proporciona una API abierta que admite una fácil integración con plataformas virtuales en la nube/aaS y soluciones de administración de políticas de terceros. Los ingenieros pueden configurar y administrar completamente las políticas de Advanced WAF desde una interfaz programática que admite todas las tareas de administración de políticas, incluida la configuración de inicio de sesión, el aprendizaje, el ajuste semiautomático, las consultas de utilización y la supervisión del estado. La API REST de Advanced WAF expone toda la gama de entidades de políticas de Advanced WAF para admitir modelos abiertos de WAF como servicio.

Aproveche los informes completos y prácticos

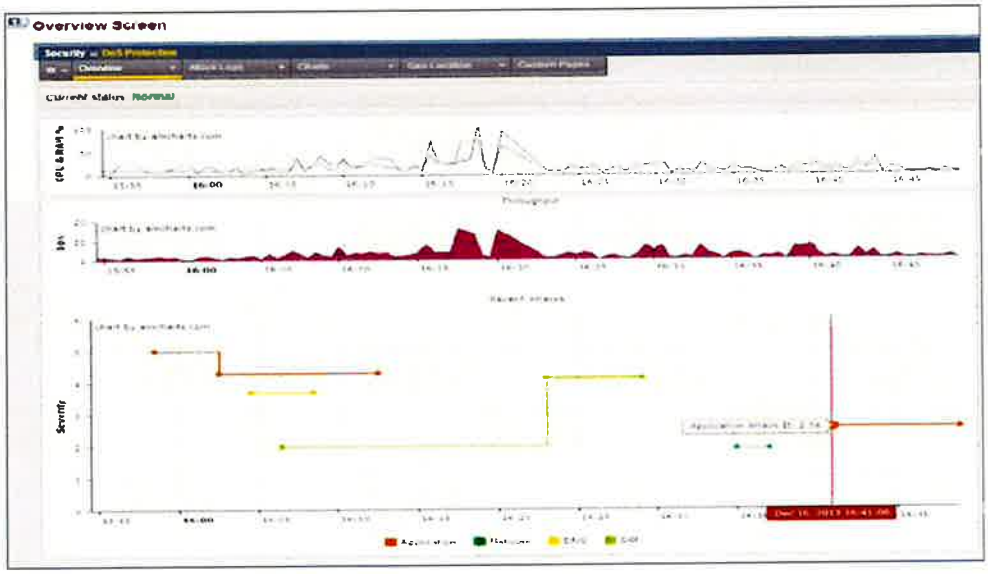
F5 Advanced WAF proporciona potentes capacidades de generación de informes que le permiten analizar fácilmente las solicitudes entrantes, realizar un seguimiento de las tendencias en las infracciones mediante la correlación de eventos, generar informes de seguridad, evaluar posibles ataques y tomar decisiones de seguridad informadas. Para expertos en seguridad o generalistas, Advanced WAF proporciona información clara y discernible con una visibilidad completa de los ataques y los cambios en el panorama de amenazas

La pantalla de resumen de Advanced WAF muestra las políticas de seguridad activas, los eventos y ataques de seguridad, las estadísticas de anomalías y las estadísticas de red y tráfico. La información se puede guardar o enviar como archivo adjunto de correo electrónico. Las capacidades de supervisión muestran cómo se accede a la aplicación y cómo se comporta. La API REST única admite integraciones sencillas con servicios SIEM o de administración de nivel superior. Advanced WAF también ofrece paneles, gráficos, informes y estadísticas predefinidos y personalizables, que destacan los ataques DoS y de fuerza bruta, el web scraping y la aplicación de IP, el estado del seguimiento de sesiones y mucho más.

Wagner Peña

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

236



La pantalla de resumen de seguridad proporciona una vista sencilla de lo que sucede en su sistema.

Análisis forense en profundidad y seguridad de la base de datos

Para un análisis de amenazas más profundo, Advanced WAF se integra con soluciones de indexación y búsqueda de alta velocidad como Splunk. Estas soluciones ofrecen una mayor visibilidad de las tendencias de ataques y tráfico, la agregación de datos a largo plazo y la identificación de amenazas imprevistas antes de que se produzca la exposición. Advanced WAF también admite informes de bases de datos para una vista en tiempo real de la actividad de la base de datos y las instrucciones SQL generadas por los usuarios front-end. Las soluciones de indexación y búsqueda se combinan con Advanced WAF para proporcionar información forense más completa para una mayor eficacia de seguridad al mitigar las amenazas.

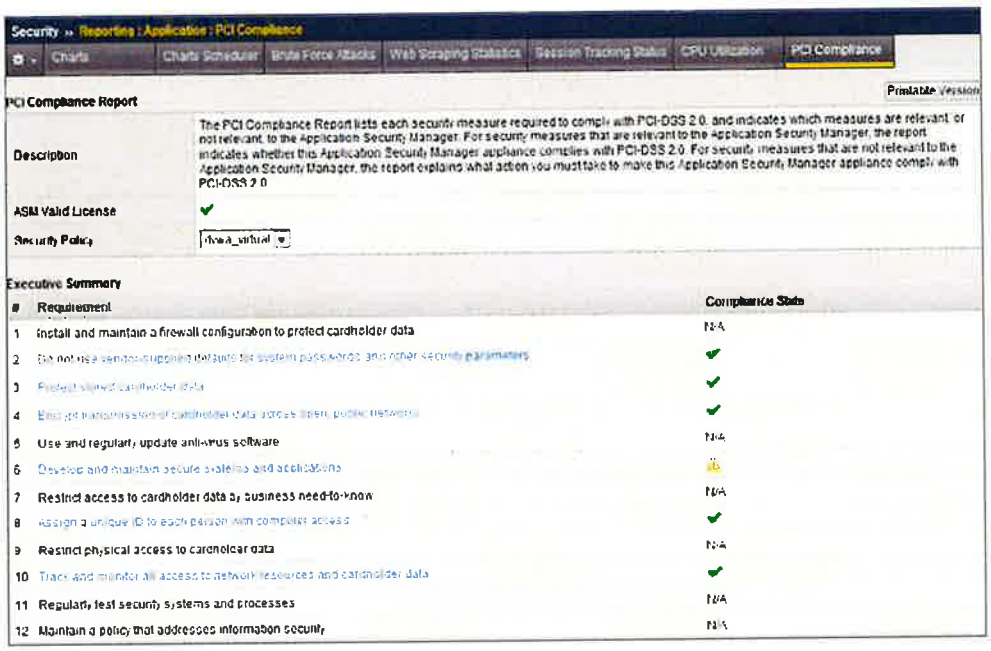
Mantener el cumplimiento de los mandatos de la industria y las normativas

El WAF avanzado facilita a las organizaciones la comprensión y el mantenimiento del cumplimiento normativo. La protección de seguridad integrada, el registro y la generación de informes, y la auditoría remota ayudan a las organizaciones a cumplir con los estándares de seguridad de la industria (incluidos PCI DSS, HIPAA, Basilea II, FFIEC y SOX) de forma rentable y sin necesidad de múltiples dispositivos, cambios en las aplicaciones ni reescrituras. Con los informes PCI, el WAF avanzado enumera las medidas de seguridad requeridas, determina si se cumple con la normativa y detalla los pasos necesarios para lograr el cumplimiento.

Wagner Peña

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

237



Mantener el cumplimiento con los mandatos normativos y de la industria.

Cumplir con los requisitos de implementación complejos

La explosión del Internet de las Cosas (IoT) ha tenido un impacto tremendo en las organizaciones. El número de aplicaciones web que deben administrarse y protegerse ha aumentado drásticamente. Además, el creciente enfoque en la implementación de aplicaciones híbridas significa que las aplicaciones empresariales ahora residen en múltiples entornos: centro de datos, nube privada y nube pública. Como resultado de estos cambios, se necesitan nuevos requisitos para proteger las aplicaciones y migrar los servicios WAF del centro de datos a la nube.

Modelos de implementación de WAF híbridos

F5 Advanced WAF ofrece opciones flexibles que permiten a los administradores implementar fácilmente servicios de firewall cerca de la aplicación. Los administradores también pueden migrar políticas de seguridad reforzadas desde dispositivos de centro de datos a Advanced WAF Virtual Edition (VE) en entornos de nube virtual y privada. Advanced WAF ofrece la misma calidad de protección y escalabilidad con una edición de dispositivo y software. Las políticas e iRules se pueden mover sin problemas entre dispositivos de hardware y dispositivos virtuales sin actualizaciones manuales.

La tecnología WAF de F5 admite la seguridad de las aplicaciones en cualquier entorno, ya sea implementada en hardware de F5, como una edición virtual o como un servicio basado en la nube totalmente administrado

El firewall de aplicaciones web F5 Silverline se basa en F5 Advanced WAF, pero se proporciona a través de la plataforma de servicios de aplicaciones en la nube Silverline y es implementado, configurado y administrado completamente por los expertos altamente especializados del Centro de Operaciones de Seguridad (SOC) de F5. Con soporte experto 24x7x365 para proteger las aplicaciones web y los datos (y permitir el cumplimiento de los estándares de seguridad de la industria), el servicio de firewall de aplicaciones web Silverline proporciona protección de aplicaciones sin necesidad de inversión de capital ni experiencia en seguridad.

Wagner Pena

expert IPX SRL RNC 130-850151 Santo Domingo, R.D.

238

Ejecución de varias instancias de Advanced WAF

Advanced WAF utiliza F5 ScaleN®con F5 Virtual Clustered Multiprocessing™(vCMP) para proporcionar la implementación de seguridad de aplicaciones más rentable para administrar implementaciones a gran escala, ya sea que sea un proveedor de servicios administrados que ofrece WAF como servicio o simplemente administre una gran cantidad de dispositivos Advanced WAF

Con Advanced WAF y sistemas habilitados para vCMP, los administradores pueden consolidar fácilmente varios firewalls en un solo dispositivo y asignar recursos de Advanced WAF de una manera más flexible y aislada para diferentes clientes, grupos, aplicaciones y servicios. vCMP le permite ejecutar varias instancias de Advanced WAF en una sola plataforma F5 con aislamiento de firewall de alta densidad mediante una combinación de hardware y software. Los firewalls de invitados se pueden agrupar para facilitar la administración y el mantenimiento, y para garantizar la coherencia en toda la infraestructura de firewall. vCMP le permite consolidar y administrar mejor su infraestructura de seguridad, lo que garantiza la eficiencia y el cumplimiento de los acuerdos de nivel de servicio (SLA) con una infraestructura de servicio WAF dinámica y flexible.

Servicios de seguridad de F5

Los administradores de TI necesitan una solución consolidada de firewall de red y aplicaciones web para defenderse de ataques multicapa, como eventos de red y de capa 7. F5 Advanced WAF, junto con F5 Web Fraud Protection, F5 BIG-IP Advanced Firewall Manager™(AFM) y F5 BIG-IP DNS, cubre el espectro de amenazas: mitiga los ataques de capa 3 a capa 7, proporciona protección contra el fraude del lado del cliente y protege la infraestructura DNS. Cuando se utiliza con F5 Access Manager®(AM), Advanced WAF proporciona acceso contextual y basado en políticas con una administración simplificada de autenticación, autorización y contabilidad (AAA) para aplicaciones web. Como componente de los servicios de seguridad integrales de F5, Advanced WAF se beneficia de otros módulos de F5 para habilitar la seguridad del centro de datos, una amplia protección de aplicaciones y capacidades de administración de acceso.

Advanced WAF, junto con otros módulos de BIG-IP, consolida la protección de aplicaciones y la administración de acceso en una única plataforma de seguridad de alto rendimiento

Características y especificaciones de F5 Advanced WAF

Firewall de aplicaciones web

Implementación	
Asistente de implementación rápida con sugerencias de autoayuda	Sí
Aprendizaje unificado y creador de políticas	Sí, con creación de políticas manual y automatizada
Preparación de políticas	Sí
Compatibilidad con dominios de ruta	Sí
VE, dispositivo o servicio gestionado	Sí, los servicios gestionados requieren una licencia Silverline

Seguridad WAF	
Cifrado de capa de aplicación	Sí
Mitigación de ataques de fuerza bruta	Sí
Protección contra relleno de credenciales	Sí
Protección contra denegación de servicio (DoS) conductual	Sí, protección para todas las aplicaciones
Detección de DoS y DDoS de capa 7, incluyendo: DoS HASH, Slowloris, inundaciones, Keep-Dead, bomba XML	Sí
Prevención de web scraping	Sí
Prevención de OWASP Top 10	Sí
Defensa automatizada contra ataques y detección de bots	Sí
Protecciones avanzadas contra amenazas, incluyendo: inyecciones web, fuga de datos, secuestro de sesión, ataques HPP, desbordamientos de búfer, shellshock	Sí
Protección contra bots móviles	Sí, con el SDK móvil F5 Anti-Bot
Bloqueo de geolocalización	Sí
Servicios de reputación de inteligencia IP	Sí, con F5 IP Intelligence Services
Terminación SSL con recifrado	Sí
Correlación de incidentes y violaciones de seguridad	Sí
Compatibilidad con la certificación del lado del cliente	Sí
Autenticación de cliente	LDAP, RADIUS; más métodos disponibles con F5 Access Manager
Seguridad de la base de datos	Sí, con firewall de Oracle Database
Verificación de respuesta	Sí
Puntuación de riesgo de violación	Sí
Cifrado y descifrado de servicios web	Sí, y con validación de firmas
Detección de ID de dispositivo e huella digital	Sí
Actualizaciones de firmas en vivo	Sí
Filtrado de tráfico WebSocket	Sí
Bloqueo de IP (lista negra de capa 3 en hardware)	Requiere licencia de F5 BIG-IP AFM

Wagner Pena

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

240

Informes y análisis

Gráficos e informes personalizables	Sí
Informe general de seguridad	Sí, capacidades de desglose a detalles granulares
Informe combinado de ataques de red y aplicaciones	Sí, con la implementación combinada de F5 BIG-IP AFM y F5 WAF
Monitoreo del estado del WAF	Sí
Compatibilidad con el cumplimiento de PCI-DSS, HIPAA, SOX, Basilea II	PCI-DSS, HIPAA, SOX, Basilea II
Administración e informes centrales con control de acceso basado en roles	Sí, requiere administración centralizada F5 BIG-IQ
Sincronización automática de políticas entre dispositivos WAF	Sí

Otro

Integración de iRules y caché rápida	Sí
Informes SNMP	Sí
API REST	Sí
Compatibilidad con ICAP	Sí
Integración con DAST	Sí: WhiteHat, QualysGuard e IBM
Protección contra fraude	Sí: requiere licencia de F5 Fraud Protection Service
Aceleración SSL	Sí: fundamental para la plataforma BIG-IP

Compatibilidad con la plataforma BIG-IP y TMOS

Multitenencia	Sí: con F5 vCMP
Alta disponibilidad	Sí: activo-pasivo o activo-activo
Compatibilidad con sistemas operativos de 64 bits	Sí
Aceleración de aplicaciones	Sí: requiere F5 BIG-IP LTM
Optimización TCP	Sí
Control avanzado de velocidad y QoS	Sí
F5 IPv6 Gateway™	Sí
Filtrado de puertos IP	Sí
Compatibilidad con VLAN	Sí
Certificados SSL seguros desde el acceso	Sí
Se integra con BIG-IP AFM y F5 AM para una seguridad completa del centro de datos con gestión de identidad y acceso	Sí

Wagner Pena

F5 Advanced WAF

F5 Advanced WAF está disponible como solución independiente o como módulo adicional para BIG-IP Local Traffic Manager (LTM) en cualquier plataforma F5 y en BIG-IP LTM Virtual Edition (VE).
F5 Access Manager (AM) está disponible como módulo adicional para el dispositivo independiente Advanced WAF. F5 AM Lite (con 10 licencias de usuario gratuitas) se incluye con cualquier compra de Advanced WAF independiente. Para obtener especificaciones físicas detalladas, consulte laHoja de datos de hardware del sistema BIG-IP .

Wagner Peña

Plataformas BIG-IP

Solo la plataforma de controlador de entrega de aplicaciones (ADC) de próxima generación y lista para la nube de F5 proporciona agilidad similar a la de DevOps con la escala, la profundidad de seguridad y la protección de la inversión necesarias tanto para aplicaciones establecidas como emergentes. Los nuevos dispositivos F5 BIG-IP iSeries ofrecen una programabilidad rápida y sencilla, una orquestación compatible con el ecosistema y un rendimiento de hardware definido por software sin precedentes. Como resultado, los clientes pueden acelerar las nubes privadas y proteger los datos críticos a escala, al tiempo que reducen el costo total de propiedad (TCO) y preparan sus infraestructuras de aplicaciones para el futuro. Las soluciones de F5 se pueden implementar rápidamente mediante integraciones con herramientas de administración de configuración y sistemas de orquestación de código abierto.

Además de iSeries, F5 ofrece VIPRION®Chasis modular y sistemas blade diseñados específicamente para el rendimiento y para una verdadera escalabilidad lineal bajo demanda sin interrupción del negocio. Los sistemas VIPRION aprovechan la tecnología de clustering ScaleN de F5 para que pueda agregar blades sin reconfigurar ni reiniciar.

Las ediciones virtuales del software F5 se ejecutan en servidores estándar y admiten la gama de hipervisores y requisitos de rendimiento. Estas ediciones virtuales proporcionan agilidad, movilidad y una rápida implementación de servicios de aplicaciones en centros de datos definidos por software y entornos de nube. Consulte lasHojas de datos de hardware del sistema F5 ,VIPRION yEdición virtual para obtener más detalles. Para obtener información sobre la compatibilidad con módulos específicos para cada plataforma, consulte las notas de la versión más reciente enAskF5 . Para obtener la lista completa de hipervisores compatibles, consulte laMatriz de hipervisores compatibles con VE .

Las plataformas F5 se pueden administrar a través de un único panel de control con BIG-IQ Centralized Management.

Dispositivo BIG-IP iSeries

Chasis VIPRION

Ediciones virtuales de BIG-IP

242

Ediciones virtuales

F5 Advanced WAF Virtual Edition (VE) puede ayudarle a satisfacer las necesidades de su entorno virtualizado al escalar a 20 núcleos/vCPU.

F5 Advanced WAF VE

Hipervisores compatibles:	• VMware vSphere Hypervisor 4.0, 4.1, 5.0 y 5.1 y vCloud Director 1.5 • Citrix XenServer 5.6 y 6.0 • Microsoft Hyper-V para Windows Server 2008 R2 y 2012 • KVM – Linux Kernel 2.6.32 (RHEL 6.2/6.3, CentOS 6.2/6.3)

Advanced WAF VE también está disponible como una imagen de máquina de Amazon para su uso en Amazon Web Services.

amazon web services | Partner Network

Wagner Pérez

243

Servicios globales de F5

F5 Global Services ofrece soporte, capacitación y consultoría de clase mundial para ayudarle a sacar el máximo provecho de su inversión en F5. Ya sea proporcionando respuestas rápidas a sus preguntas, capacitando a equipos internos o gestionando implementaciones completas desde el diseño hasta la implementación, F5 Global Services puede ayudarle a garantizar que sus aplicaciones sean siempre seguras, rápidas y confiables. Para obtener más información sobre F5 Global Services, póngase en contacto conconsulting@f5.com o visite f5.com/support .

Más información

Para obtener más información sobre F5 Advanced WAF, visitef5.com para encontrar estos y otros recursos.

Recursos adicionales

Descripción general de F5 Advanced WAF

Las amenazas avanzadas a las aplicaciones requieren un WAF avanzado.

Informe de protección de aplicaciones de F5 Labs 2018

Libros electrónicos

Los bots son un problema para el negocio

Relleno de credenciales | Una epidemia de seguridad. OWASP Top 10 y más allá

Informe

Cuadrante mágico de Gartner para firewalls de aplicaciones web, 2018

Wagner Peña

F5 Networks, Inc.401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 f5.com

Américas info@f5.com
Asia-Pacífico apacinfo@f5.com
Europa/Oriente Medio/África emeainfo@f5.com
Japón f5j-info@f5.com

Wagner Peña

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Los servicios de entrega de aplicaciones basados en software son fundamentales para mantener la infraestructura de aplicaciones adaptable y segura que exigen las empresas que están en proceso de transformación digital. F5 acelera tu transición a la nube y a las arquitecturas definidas por software con plataformas virtuales de entrega de aplicaciones que ofrecen una forma ágil, flexible y eficiente de desplegar servicios avanzados de aplicaciones y seguridad.

Muchas empresas han tenido o planean desplegar aplicaciones en múltiples entornos en la nube, tanto públicos como privados, lo que dificulta la implementación de servicios de aplicación avanzados, consistentes y conformes para cada aplicación de su cartera. Además, están ampliando más allá de las aplicaciones monolíticas tradicionales y desplegando arquitecturas de aplicaciones más modernas y dinámicas, incluyendo contenedores y microservicios con requisitos únicos.

Estandarizar los servicios de aplicaciones F5 acelera la migración hacia y entre nubes, al tiempo que proporciona servicios coherentes y avanzados tanto para aplicaciones monolíticas como modernas que funcionan en esos entornos, ayudándote a soportar y gestionar más fácilmente tu creciente cartera de aplicaciones multi-nube.

Las Ediciones Virtuales (VEs) F5® BIG-IP® son los controladores virtuales de entrega de aplicaciones (vADCs) más escalables de la industria, facilitando el procesamiento de tráfico de aplicaciones de alto rendimiento en todos los principales hipervisores y plataformas en la nube, y facilitando la transición del hardware al software. Los VEs ofrecen todos los mismos servicios de entrega de aplicaciones líderes en el mercado —incluyendo gestión avanzada de tráfico, seguridad de aplicaciones, aceleración de aplicaciones, DNS, cortafuegos de red y gestión de accesos seguros— que funcionan en hardware diseñado específicamente para F5. Esta similitud permite reutilizar y replicar configuraciones y políticas de servicios de los appliances F5 existentes en los VEs, simplificando las migraciones a la nube. Los VEs pueden ser fácilmente provisionados y configurados automáticamente por operadores de red y desarrolladores, permitiendo integrarlos en las canalizaciones CI/CD existentes y asegurando que todas las aplicaciones se desplieguen con las capacidades necesarias de seguridad, cumplimiento y gestión del tráfico. Cuando se utiliza junto con F5 BIG-IQ® Centralized Management, puedes crear, provisionar y gestionar rápidamente servicios de aplicaciones en cualquier lugar, ganando visibilidad sobre la salud y el rendimiento de tus aplicaciones multi-nube, todo desde un punto de control centralizado.

Wagner Peña

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

MÓDULOS BIG-IP DISPONIBLES:

- Gestor de Tráfico Local (LTM) de BIG-IP
- BIG-IP DNS
- Gestor Avanzado de Cortafuegos BIG-IP (AFM)
- Gestor de Políticas de Acceso BIG-IP (APM)
- WAF avanzado
- SSL Orchestrator
- NAT de grado portador BIG-IP (CGNAT)
- Gestor de Aplicación de Políticas (PEM) de BIG-IP

Beneficios clave

Aumentar la agilidad multi-nube
Rápido, y fácilmente, inicia, desactiva o migra los servicios de entrega de aplicaciones a través del centro de datos y la nube pública, utilizando opciones de despliegue instantáneo según sea necesario.

Acelerar despliegues con automatización
Automatizar la inserción de servicios de aplicaciones con F5 Automation Toolchain. Permite la provisión declarativa y la configuración de BIG-IP VE en entornos cloud e integración con herramientas de automatización y CI/CD como Ansible, Jenkins y Terraform.

Optimiza los servicios de aplicaciones y seguridad Implementa servicios robustos de gestión de seguridad y tráfico para mantener tus aplicaciones disponibles, protegidas y conformes, independientemente de la ubicación de despliegue.

Utilizar arquitecturas de aplicaciones modernas
La integración nativa con entornos de orquestación de contenedores te permite implementar servicios avanzados de aplicaciones tan dinámicos como tus contenedores.

Soporte para requisitos de alto rendimiento en la nube
Haz la transición del hardware al software sin los típicos problemas de degradación del rendimiento.

Obtener flexibilidad máxima de despliegue y consumo
Despliega BIG-IP VE en la gama más amplia de plataformas de hipervisores y nube soportadas, con la libertad de consumir mediante acuerdos de licencia perpetuos, de utilidad, suscripción o empresa (ELA).

Escenarios principales de la nube

Los VEs BIG-IP pueden utilizarse para ofrecer un conjunto consistente de servicios avanzados de aplicación en los cuatro escenarios principales de la nube descritos a continuación: nube privada/centro de datos definido por software (SDDC), nube pública, nube multi/híbrida y colocation con interconexión en la nube.

NUBE PRIVADA USANDO SOFTWARE - DEFINED ARCHITEC TURES

Las empresas están migrando a nubes privadas/SDDC para lograr agilidad, reducir el tiempo de llegada a la venta de aplicaciones y proporcionar control a los propietarios y desarrolladores de aplicaciones mediante un autoservicio
portal o catálogo. Una nube privada o SDDC que utilice servicios de aplicaciones F5 es ideal para acelerar el despliegue de aplicaciones, permitir cambios dinámicos en el centro de datos y adaptar los servicios de infraestructura a las cargas de trabajo mediante un modelo por aplicación. Los productos y soluciones de F5 se integran con las principales plataformas tecnológicas de nube privada, incluyendo OpenStack, VMware,
Cisco y Microsoft Azure Stack. F5 ofrece plantillas de soluciones en la nube y soporta herramientas de código abierto como Heat, Ansible y herramientas de máquinas virtuales abiertas para orquestar y automatizar el despliegue de servicios de entrega de aplicaciones y seguridad.

Flexibilidad y alto rendimiento en una arquitectura híbrida de dos niveles

Algunas empresas están adoptando una arquitectura de dos niveles como parte de su transformación SDDC. En el borde de la red está el nivel de aplicación que proporciona servicios de puerta principal —incluyendo gestión de tráfico L4, cortafuegos DDoS o descarga SSL— para todo el tráfico que entra en la red, basándose en las políticas generales de negocio y seguridad. Los servicios que gestionan tráfico de alto volumen requieren el mayor rendimiento y escalabilidad, un caso en el que el hardware dedicado y diseñado específicamente puede ser más rentable que los servidores comerciales. El nivel por aplicación gestiona la pila de aplicaciones dentro del centro de datos, que aprovecha software altamente escalable y flexible para ofrecer servicios avanzados de aplicaciones y seguridad por aplicación. Este modelo híbrido de centro de datos de dos niveles (véase la Figura 1) ofrece lo mejor de ambos mundos: hardware donde se necesita y agilidad del software cercana a la app.

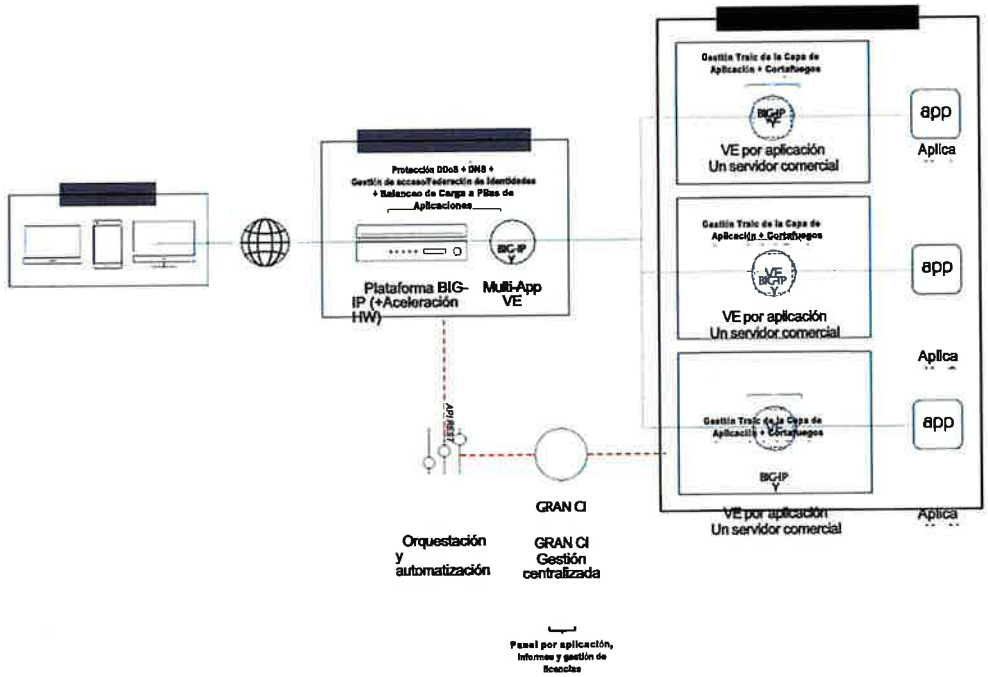


Figura 1: Arquitectura de dos niveles con hardware F5 o VE multiapp compartido en el borde y VE por aplicación.

DESPLIEGUE APLICACIONES EN Y UN ENTORNO DE NUBE PÚBLICA CRUZADA S

Desplegar aplicaciones en las principales nubes públicas te da la flexibilidad y escalabilidad que deseas, sin los costes de inversión y capital asociados a la creación de centros de datos privados adicionales. Utilizar servicios de aplicaciones y seguridad F5 proporcionados por BIG-IP VEs ofrece los siguientes beneficios:

- **Arquitecturas repetibles en entornos cloud**: a medida que expandes y adoptas nuevas nubes, reutiliza la misma arquitectura segura, validada y compatible para acelerar la adopción multi-cloud y simplificar las operaciones.

- **Reducción de la proliferación de herramientas y de la complejidad operativa**: estandarizar servicios familiares que son agnósticos en la nube hace que desplegar y mantener aplicaciones en entornos cloud sea más rápido y sencillo.

Wagner Peña

- **Niveles consistentes de disponibilidad, rendimiento y seguridad**: proporcionan a tus clientes una excelente experiencia de usuario mientras protegen tanto tus ingresos como tu reputación.
- **Tiempo de salida al mercado más** rápido: aprovisionar rápidamente servicios avanzados de aplicaciones al lanzar nuevas aplicaciones o migrar aplicaciones existentes a la nube pública.
- **Integración profunda con proveedores de nube pública**: escalar dinámicamente los servicios de aplicaciones mediante la integración con AWS Auto Scaling, o aplicar fácilmente la seguridad avanzada de aplicaciones con una solución de firewall de aplicaciones web (WAF) preconfigurada y lista para usar en el Centro de Seguridad de Azure.
- **Modelos de licenciamiento flexibles**: consume con un modelo de licenciamiento que apoye los requisitos de tu negocio, ya sea mediante suscripción, Programa de Consumo Flexible (FCP), pago por uso o de forma perpetua.

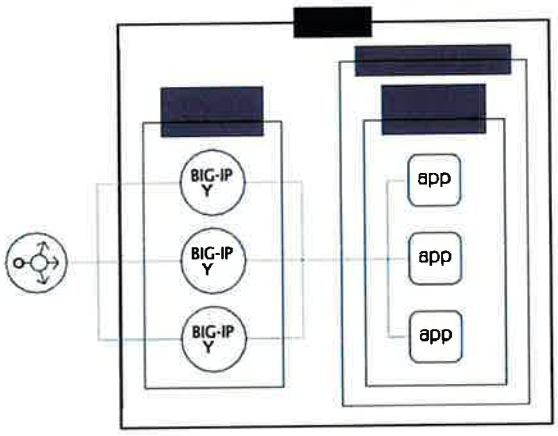


Figura 2: GRANDES VEs de IP desplegados dentro de una arquitectura de autoescalado—ya sea dentro o entre zonas de disponibilidad—para garantizar que tus aplicaciones estén disponibles y sean seguros, optimizando los costes a medida que escalaran para adaptarse a la demanda

APLICACIÓN POR TABILIDAD: UN ENTORNO HÍBRIDO Y MULTI-NUBE

A pesar de los numerosos beneficios de los despliegues en la nube pública, las empresas suelen evitar trasladar todas las aplicaciones o datos a la nube pública debido a la percepción de pérdida de control, riesgo, cumplimiento normativo y falta de soporte para el diseño de aplicaciones heredadas. Como resultado, muchos optan por hacerlo operan dentro de un modelo híbrido de nube o multi-nube híbrida, en el que parte de sus operaciones se desarrollan en la nube pública mientras que los componentes que no pueden moverse a la nube o que requieren un seguimiento avanzado de seguridad y cumplimiento permanecen en las instalaciones. En algunos escenarios, las aplicaciones operan en diferentes entornos para aumentar la redundancia o permitir una mayor

capacidad de escalabilidad cuando sea necesario. F5 aumenta la portabilidad de estas aplicaciones mientras reduce la carga de gestión al proporcionar un conjunto de servicios de aplicación estandarizados que pueden reutilizarse dondequiera que una app esté ejecutándose o donde se reimplemente. En la Figura 3,

Las aplicaciones front-end orientadas a Internet se despliegan en la nube pública, mientras que las cargas de trabajo críticas con mayores requisitos de seguridad y cumplimiento se ejecutan localmente. Una conexión directa conecta ambos entornos para reducir la latencia.

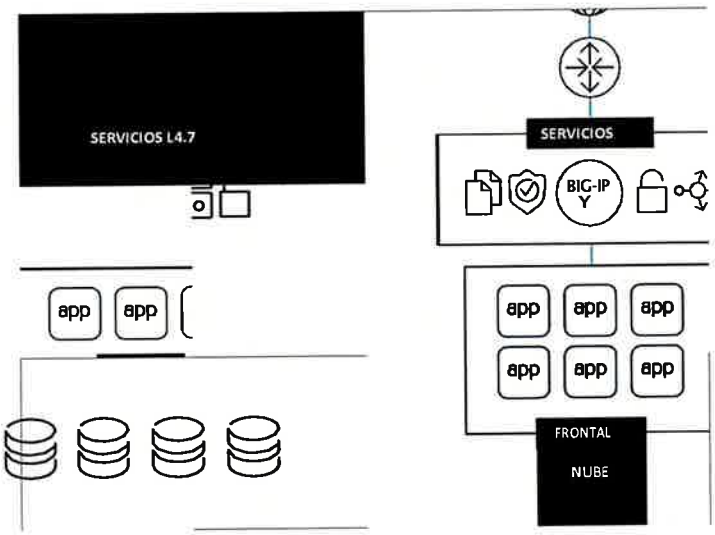


Figura 3: Despliegue de nube híbrida con BIG-IP Virtual Editions que soportan aplicaciones en nube pública y centros de datos.

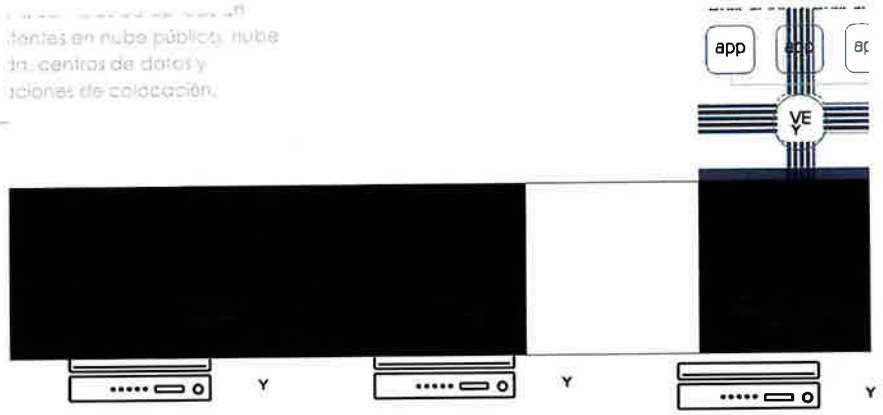
DESPLIEGUES DE COLOCACIÓN CON DIREC T CONNEC T A LA NUBE PÚBLICA

Muchas empresas operan su cartera de aplicaciones en un modelo de nube híbrida similar al mostrado en la Figura 3. Pero, para algunos, puede haber un aumento de latencia asociado debido a grandes distancias entre sus centros de datos y las ubicaciones en el borde de la nube. Para estas organizaciones, la mejor opción es desplegar aplicaciones locales dentro de una instalación de colocación y usar conexiones directas para conectar ambos extremos de su arquitectura híbrida. F5 BIG-IP VE también puede desplegarse en estas instalaciones de colocación y usarse para proporcionar inserción de servicios de aplicaciones,
tanto para aplicaciones desplegadas en la colocation como para las que se ejecutan en la nube pública. Como resultado, se pueden implementar servicios de aplicación consistentes para aplicaciones que se ejecutan en diferentes entornos de nube.

Wagner Pina

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

...tentes en nube pública, nube
...n, centros de datos y
...iciones de colocación.



expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Wagner Pastor

Integración con Frameworks SDN

Las redes definidas por software (SDN) logran agilidad, flexibilidad y eficiencia en costes en términos de superar la complejidad de la infraestructura de redes en los centros de datos actuales. SDN busca operacionalizar la red mediante virtualización y abstracción, similar a lo ocurrido con servidores y almacenamiento. Sin embargo, aunque SDN se ha centrado en la conectividad L2–3 sin estado, sigue existiendo la necesidad de servicios L4–7 con estado y conscientes del flujo. A través de sus alianzas con Technology Alliance, F5 está completando la visión SDN integrando sus servicios inteligentes de entrega de aplicaciones con arquitecturas líderes de SDN (VMware NSX, Cisco ACI) mediante plug-ins BIG-IP y APIs REST. Además, las plataformas BIG-IP pueden funcionar como gateways SDN, conectando redes virtualizadas y arquitecturas de red tradicionales para proporcionar una transición suave y protección de inversión.

Wagner Pena

Lograr un rendimiento comparable al hardware con software

Un obstáculo importante de la adopción de la nube entre las grandes empresas, y especialmente los proveedores de servicios, es la reducción del rendimiento que suele asociarse a la transición del hardware al software. Esto significa que, para muchos, la promesa de mayor agilidad y escalabilidad en el despliegue que ofrece la nube puede no valer la pena sacrificar la baja latencia y la alta respuesta que ofrece su centro de datos.

BIG-IP Virtual Edition (VE) es el ADC virtual más escalable y de alto rendimiento disponible, capaz de soportar tarjetas de 100Gbps en una sola instancia, lo que significa que no tienes que elegir entre agilidad y alto rendimiento: puedes tener ambos. A continuación, algunos ejemplos de cómo se ha ampliado BIG-IP VE para ofrecer un rendimiento aún mayor.

- **VEs de alto rendimiento**—Estas instancias de VE no están limitadas por un límite de rendimiento, sino que se licencian por el número de núcleos de vCPU que se pueden asignar. Eso te permite optimizar el hardware del host subyacente y alcanzar 85Gbps+ de rendimiento en L4.
- **Soporte SR-IOV y tarjeta de interfaz de red avanzada (NIC)**: El controlador de BIG-IP VE está optimizado para interactuar directamente con las tarjetas de red subyacentes utilizando virtualización de E/S de raíz única (SR-IOV), mejorando significativamente el rendimiento en rendimiento y reduciendo la latencia.
  SR-IOV puede habilitarse en AWS usando AWS ENA, en Azure con Azure Accelerated Networking, y en entornos de nube privada con ciertas tarjetas de conexión Intel, Mellanox, Broadcom y Emulex.
- **Procesamiento criptográfico y de compresión acelerado**—BIG-IP VE puede descargar funciones criptográficas intensivas en computación y compresión utilizando la tecnología Quick Assist de Intel, liberando ciclos de CPU para centrarse en otras

tareas importantes de la aplicación.

- **Descarga a SmartNIC habilitada para** FPGA—Descarga diversas tareas intensivas en computación a una Smart NIC Intel de alto rendimiento, incluyendo mitigación DDoS y NAT de grado portador
  (CGNAT) y transmisión de tráfico de capa 4. Hacerlo mejora significativamente el rendimiento en más de un 30%, mientras reduce la presión sobre los recursos de computación de BIG-IP VE hasta en un 80%.

Wagner Pastor

Servicios de aplicaciones dinámicas para entornos de contenedores

Las organizaciones están adoptando rápidamente entornos contenedores para desarrollar aplicaciones más ágiles y portátiles, normalmente utilizando marcos de gestión y orquestación para coordinar la provisión y automatización de estas cargas de trabajo. Pero estas aplicaciones aún necesitan servicios como descarga SSL, enrutamiento y protección de aplicaciones web

F5 Container Ingress Services (CIS) es una solución de integración de contenedores que ayuda a desarrolladores y equipos de sistemas a gestionar el control de entrada de puerta principal y los servicios avanzados de entrega de aplicaciones y seguridad para despliegues de contenedores y Plataforma como Servicio (PaaS). CIS integra BIG-IP VE con entornos nativos de contenedores y sistemas de orquestación, incluyendo Kubernetes y Red Hat OpenShift. Esa integración permite enrutamiento dinámico Ingress HTTP, balanceo de carga y seguridad para los contenedores a medida que se ponen en marcha.

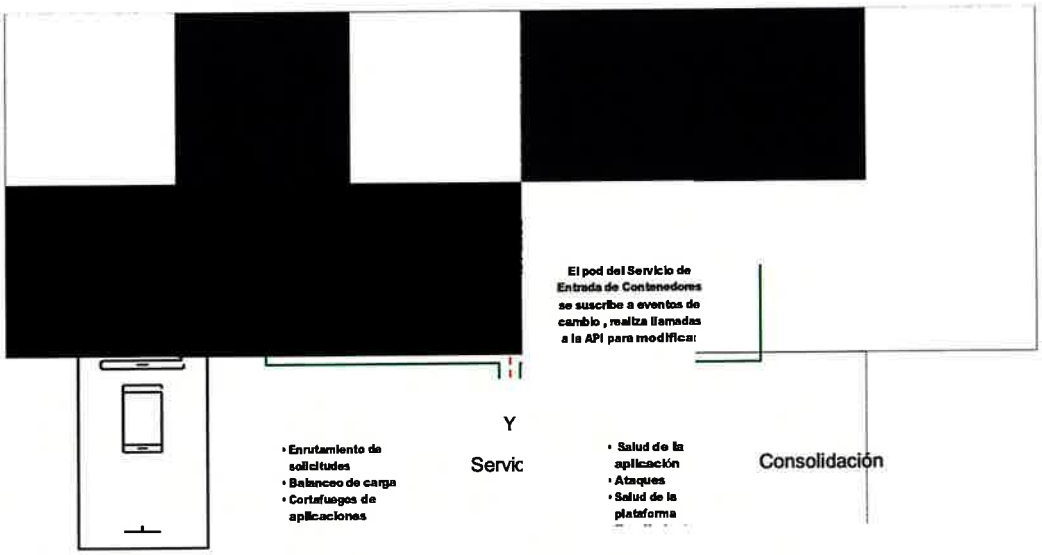


Figura 5: BIG-IP VE proporcionando servicios de aplicación de puerta principal a contenedores usando Servicios de Entrada de Contenedores F5.

Automatización, Orquestación y Programabilidad

F5 ofrece muchas formas de programar la estructura de servicios de aplicación y la red, permitiendo a las organizaciones reaccionar en tiempo real a eventos operativos y empresariales, automatizar el despliegue y configuración, e integrarse fácilmente en sistemas de orquestación propios o de terceros.

- **F5 Automation Toolchain:** Proporciona un conjunto de herramientas de automatización de código abierto que hacen más rápido y fácil desplegar y configurar BIG-IP VE mediante interfaces declarativas simples pero potentes, todas ellas que pueden consumirse como parte de una pipeline completa de CI/CD. Incluye:
  - **Incorporación declarativa** para el aprovisionamiento L1–3
  - **Extensión de servicios de aplicación 3 (AS3)** para configuración L4–7
  - **Transmisión de telemetría** para agregar, normalizar y reenviar estadísticas y eventos de aplicaciones a herramientas analíticas de terceros
- **Plantillas de soluciones en la nube F5:** Permite el despliegue automático y el arranque de BIG IP VEs en todos los principales entornos de nube pública y privada y en una amplia gama de topologías arquitectónicas, incluyendo HA y autoescalado.
- **Extensión de Conmutación por Conmutación en la Nube (CFE) F5:** Una extensión iControl LX que proporciona funcionalidad de conmutación por error L3 en entornos en la nube, reemplazando efectivamente el ARP gratuito (GARP).
- **F5 iRules:** Scripting que proporciona control y visibilidad granular del tráfico, permitiendo personalización, respuesta rápida a errores en el código de la aplicación y vulnerabilidades de seguridad, y soporte para nuevos protocolos.

Visita el repositorio GitHub de F5 para obtener información adicional sobre la cadena de herramientas de automatización F5, plantillas de soluciones en la nube y otras extensiones e integraciones de código abierto.

Gestión Centralizada de BIG-IP VE

F5 BIG-IQ Centralized Management proporciona un punto de control unificado para toda tu cartera F5, asegurando que estés al tanto de dispositivos, módulos y licencias, ayudándote a ofrecer la óptima disponibilidad, rendimiento y seguridad de aplicaciones. Proporciona un único panel de cristal para gestionar y desplegar dispositivos F5, incluyendo módulos clave de BIG-IP como BIG-IP Local Traffic Manager (LTM), BIG-IP Application Security Manager (ASM), BIG IP Advanced Firewall Manager (AFM), BIG-IP Access Policy Manager (APM) y BIG-IP DNS, así como otras soluciones F5 como SSL Orchestrator, Secure Web Gateway, DDoS Hybrid Defender, WebSafe y MobileSafe.

Utilizar la Gestión Centralizada de BIG-IQ para:

- Copia de seguridad automática de imágenes y configuraciones.
- Monitoriza los paneles, los informes y las alertas.
- Proporcionar control de acceso basado en roles (RBAC).
- Obtén análisis detallados por aplicación.
- Gestiona licencias BIG IP VE.
- Asegura políticas de seguridad y gestión del tráfico coherentes en toda tu infraestructura.
- Crear, aprovisionar y desplegar nuevos dispositivos y servicios de aplicaciones con BIG-IP.
- Alinearse con las prácticas modernas de desarrollo y los flujos de trabajo CI/CD a través de la Automation Toolchain.
- Asigna y gestiona identidades y certificados de máquinas mediante integraciones con Venafi.

La gestión de licencias VE de BIG-IQ permite automatizar despliegues virtuales ADC a gran escala, incluidos VE por aplicación, en nubes compatibles con suscripción F5 o licencias ELA. Con BIG-IQ Centralized Management, puedes crear y provisionar licencias VE individuales a partir de un único pool de licencias bajo demanda. Cuando los requisitos de recursos disminuyan, puedes desactivar el VE y devolverlo al pool de licencias para su uso futuro.

Características técnicas

Disponibles en una variedad de opciones de rendimiento, las ediciones virtuales F5 pueden dimensionarse y configurarse para adaptarse a los servicios de aplicación requeridos. El rendimiento máximo se basa en los rangos de rendimiento y recursos asignados con licencia VE aplicable (número de núcleos de CPU/memoria).

Requisitos mínimos de recursos: 1 vCPU, 2 GB de RAM y 10 GB de disco.

RENDIMIENTO CON LICENCIA VE

Rendimiento	Incipiente	Máximo*
Peticiones L7 por segundo	3,000	450,000
Conexiones L4 por segundo	2,000	135,000
Rendimiento de L4	25 Mbps	10 Gbps**
Conexiones concurrentes máximas en L4	1 millón	10 millones

Figura 4: Rendimiento BIG-IP con Dell PowerEdge R620 con Intel Xeon CPU E5-2670 0 @ 2.6GHz e Intel 82599EB 10-Gigabit SFP+ NIC configurado para PCI pasado con soporte para SR-IOV.

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

SSL	Incipiente	Máximo*
SSL RSA TPS (lavas de 2K)	900	3,800
Rendimiento SSL (RSA)	23 Mbps	4 Gbps
SSL ECC TPS	1,200	20,000***
Rendimiento SSL (ECC)	23 Mbps	5,4 Gbps
Compresión de software	**Incipiente**	**Máximo***
Rendimiento de compresión	20 Mbps	4 Gbps
DNS	**Incipiente**	**Máximo***
Respuesta de consulta por segundo	1,000	250,000

Nota: Las especificaciones BIG-IP APM se mantienen en este artículo support.f5.com.

* [illegible] askf5.com [illegible]
** El rendimiento en 10 [illegible] SR-IOV
[illegible] BIG-IP TMOS v12.[illegible]

Figura 7: Rendimiento de BIG-IP LTM VE en un servidor SuperMicro 2U con dos procesadores Intel® Xeon® Scalable 8-28 núcleos (2,7GHz) y tarjeta Intel XL710 40G— configurado para SR-IOV usando hipervisor VMware ESXi 6.5. VE de alto rendimiento licenciado para 24 vCPUs ejecutando BIG-IP TMOS v15.x y posteriores requerido.

ALTO RENDIMIENTO VE

Rendimiento	Máximo*
Peticiones L7 por segundo	4,6 millones
Conexiones L4 por segundo	1,4 millones
Rendimiento de L4	85 Gbps**
SSL	**Máximo***
SSL RSA TPS (lavas de 2K)	30,000
Rendimiento SSL (RSA)	32 Gbps
SSL ECC TPS	100,000
Rendimiento SSL (ECC)	37 Gbps

Figura 8: Rendimiento BIG-IP LTM VE en la plataforma Neon City con 2x procesador Intel Xeon® Gold E5 6230N. Intel® QuickAssist Adapter 8970 con 3x funciones físicas QAT (punto final) y tarjeta de red Intel XL710 40G – configurado para SR-IOV usando KVM CentOS 7.5. Licencias VE de alto rendimiento para 16 vCPUs (para ECC) y 20 vCPUs (para RSA), ejecutando BIG-IP TMOS v14.1.0.3 y posteriores.

SSL con Intel QAT	Máximo*
SSL RSA TPS (lavas de 2K)	95,000
Rendimiento SSL (RSA)	60 Gbps
SSL ECC TPS	59,000
Rendimiento SSL (ECC)	46 Gbps
BIG-IP DNS	**Máximo***
Query responsas per second	1,8 millones

Figura 9: VE de alto rendimiento (6vCPU/16GB RAM) con hadilitado y Intel FPGA PAC N3000 SmartNIC

BIG - IP VE PARA SMAR TNICS

	Mitigación del tamaño del ataque DDoS	Utilización de la CPU en VE
Protección DDoS sin SmartNIC	2,5 Gbps	100%
Protección DDoS con SmartNIC	40 Gbps	27%
	Rendimiento de L4	**Utilización de la CPU en VE**
CGNAT (NAT44 NAPT) sin SmartNIC	37 Gbps	87%
CGNAT (NAT44 NAPT) con SmartNIC	48 Gbps	4%
	Rendimiento de L4	**Utilización de la CPU en VE**
Aceleración L4 sin SmartNIC	36 Gbps	81%
Aceleración L4 con SmartNIC	48 Gbps	4%

Nota: Las especificaciones BIG-IP APM se mantienen en este artículo support.f5.com

SUPPOR TED HYPERVISORS Y DISTRIBUCIONES LINUX

F5 ofrece las opciones de despliegue más flexibles del sector, con soporte en todas las principales plataformas de virtualización.

Figura 10: Soporte BIG IP VE F5 para los hipervisores líderes. (Para la lista completa de versiones soportadas, por favor Vea a la matriz de hipervisores soportados por VE en ask.f5.com)

	Laboratorio	25 Mbps	200 Mbps	1 Gbps	3 Gbps	5 Gbps	10 Gbps
VMware vSphere	•	•	•	•	•	•	•
KVM y Community Xen	•	•	•	•	•	•	•
Microsoft Hyper-V	•	•	•	•	•		

* Las especificaciones de rendimiento [illegible] askf5.com [illegible]
** [illegible] KVM CentOS 7.5

Figura 11: Hipervisores de alto rendimiento soportados por VE Nota: El controlador paravirtualizado de alto rendimiento se utiliza como controlador predeterminado para el rendimiento con licencia y el VE de alto rendimiento.

	Alta Performance. SR-IOV	Alta Performance. Controlador paravirtualizado
KVM	•	• (Virtio)
VMware vSphere	•	• (Vmxnet3)

APOYO TED PUBLIC CLOUD IAAS PARA VIDERS

F5 ofrece soporte para los principales proveedores de nube pública, incluyendo Amazon Web Services, Microsoft Azure, Google Cloud Platform e IBM Cloud.

Figura 12: Soporte F5 BIG-IP VE para los principales proveedores de IaaS en la nube pública. Para más detalles y una lista de proveedores de nube validados, visite F5.com

	Laboratorio	25 Mbps	200 Mbps	1 Gbps	3 Gbps	5 Gbps	10 Gbps*	HPVE*
Amazon Web Services** y GovCloud	•	•	•	•	•†	•	•	• (20G)***
Amazon IC Marketplace		•	•	•				
Microsoft Azure y Gobierno	•	•	•	•	•†	•	• (10G)****	• (10G)****
Google Cloud Platform	•	•	•	•		•	•	•
VMware en IBM Cloud††		•	•	•		•		
Alibaba Cloud International		•	•	•		•	•	
Infraestructura Oracle Cloud†		•	•	•		•	•	

Azure Accelerated Networking

Por favor, consulta esta matriz de soporte en askf5.com para saber más sobre el soporte para BIG-IP VE en la nube. También puedes aprovechar la herramienta BIG-IP Image Generator para crear imágenes VE personalizadas para lanzamientos o hot-fixes específicos de TMOS que pueden no estar disponibles en marketplaces en la nube.

Ediciones virtuales F5 BIG-IP: Licencias y elecciones simplificadas

Las ediciones virtuales F5 están disponibles para todos los módulos BIG-IP y pueden adquirirse según el nivel de rendimiento, desde la licencia de laboratorio no productivo de 10M hasta las licencias de producción de 25 Mbps, 200 Mbps, 1 Gbps, 3 Gbps, 5 Gbps y 10 Gbps. A medida que aumentan los requisitos de rendimiento, F5
Ofrece licencias de actualización de pago a medida que creces. Además, F5 ofrece licencias de VE de Alto Rendimiento sin límites de rendimiento y permite aumentar el número de vCPUs para incrementar el rendimiento—hasta un máximo de 24 vCPUs.

Las Ediciones Virtuales BIG-IP están disponibles en una variedad de modelos de licencia para adaptarse a tu negocio y presupuesto individual, así como a los requisitos de presupuesto, incluyendo:

- **Perpetual (Bring-your-own-license)**—Compra única de CapEx, que soporta 3 lanzamientos de software importantes .
- **Suscripción**—de 1 a 3 años con actualizaciones de versión ilimitadas y soporte premium incluidos
- **Utilidad (Pago por uso)**—Facturación por horas o mensuales para máxima flexibilidad y sin compromiso a largo plazo
- **Programa de Consumo Flexible (FCP):** suscripción de 3 años con máxima flexibilidad arquitectónica en entornos híbridos, protección presupuestaria anual y soporte premium incluidos.

Las ofertas de paquetes Good, Better, Best de F5 te ofrecen el mejor valor gracias a la flexibilidad para proporcionar módulos avanzados adicionales de gestión de tráfico de aplicaciones y seguridad según sea necesario.

Transición a BIG-IP Next Virtual Edition

BIG-IP Next es el software de próxima generación de BIG-IP, diseñado para ofrecer mayores capacidades de automatización, escalabilidad y facilidad de uso para organizaciones que ejecutan aplicaciones locales, en la nube o en el exterior. En esencia, sigue siendo la misma BIG-IP que los clientes de F5
Saber y confiar, simplemente diseñado y rediseñado para el futuro. Las potentes APIs declarativas son la base del diseño API-first de BIG-IP Next, haciendo que sea más rápido y sencillo para los equipos de DevOps, NetOps y otros equipos que dependen de BIG-IP gestionar y automatizar sus despliegues de BIG-IP. Una capa de software completamente reestructurada y moderna también proporciona la base para una escala significativamente mejorada en el plano de control, una huella en la nube reducida, actualizaciones rápidas de instancias y mucho más.

BIG-IP Next estará disponible en formato Virtual Edition para su despliegue en entornos de nube pública y privada a partir de 2022. El nuevo marco de software requerirá relativamente menos recursos físicos para funcionar que la actual Edición Virtual BIG-IP, lo que ayudará a reducir los costes y el consumo energético en la nube. Optimizaciones adicionales dentro de la nueva arquitectura también permiten que BIG-IP Next Virtual Edition se desarrolle en un periodo de tiempo más corto para apoyar entornos de aplicaciones más dinámicos.

Para más información sobre BIG-IP Next Virtual Edition, contacta con un representante de ventas de F5

Empieza hoy mismo

Comprueba por ti mismo cómo BIG-IP Virtual Editions puede ofrecer una forma ágil, flexible y eficiente de desplegar y optimizar servicios de aplicaciones.

Descarga la prueba gratuita de BIG-IP VE

Empieza a probar cómo puedes hacer tu aplicación rápida, segura y disponible con un BIG IP VE completo—incluyendo la Gestión Centralizada BIG-IQ—en el entorno que elijas. Descarga ahora una prueba de 30 días de un BIG-IP VE. Por favor, revisa la documentación de "Cómo empezar".

Consigue una licencia de evaluación completa

Solicita una licencia de evaluación gratuita para acceder a las últimas versiones de las ediciones virtuales F5.

Compra BIG-IP para tu laboratorio de desarrollo

Construye, pruebe, configure y prepare módulos BIG-IP en su laboratorio de desarrollo.

Prueba con BIG IP VEs en la nube pública

Prueba los BIG IP VEs a través de proveedores de nube pública con pruebas gratuitas y facturación por horas de pago por uso. Descubre cómo empezar en AWS, Azure y GCP viendo los vídeos.

Servicios Globales F5

Las exigencias para ti y tus equipos son altas. Hay que equilibrar la implementación rápida de soluciones empresariales manteniendo un nivel muy alto de disponibilidad de soluciones. Por ello, F5 Global Services y sus socios ofrecen consultoría, apoyo y formación de primer nivel para ayudarte a sacar el máximo partido a tu inversión en F5. Ya sea proporcionando respuestas rápidas a preguntas, formando equipos internos o gestionando implementaciones completas desde el diseño hasta el despliegue, F5 Global Services y sus socios pueden ayudar a garantizar que tus aplicaciones escalen y sean siempre seguras, rápidas y disponibles. Para más información sobre F5 Global Services, contacta con consulting@f5.com o visita f5.com/ soporte.

DevCentral

La comunidad de usuarios de F5 DevCentral™, con más de 200.000 miembros, es tu fuente para documentación técnica adicional, foros de discusión, blogs, medios y mucho más relacionado con BIG-IP Virtual Editions, servicios de aplicación en centros de datos virtualizados y despliegues en la nube.

Más información

Para saber más sobre la familia de productos BIG-IP, visita f5.com para encontrar estos y otros recursos:

Hojas de datos

Gestor local de tráfico BIG-IP BIG-IP DNS
BIG-IP Gestor Avanzado de Cortafuegos BIG-IP WAF avanzado
Gestor de políticas de acceso BIG-IP NAT de grado operador
Gestor de Aplicación de Políticas BIG-IP, Servicios de Entrada de Contenedores de Gestión Centralizada BIG-IQ

Páginas web

Ediciones Virtuales Computación en la Nube
Plantillas de soluciones en la nube F5 en AWS
F5 on Azure F5 on GCP
F5 en IBM Cloud F5 en Alibaba F5 en VMware
F5 en OpenStack
Utilidad de migración de la cadena de herramientas de automatización F5

Estudios de caso

American Systems lanza EMNS seguros para miembros del servicio con F5 y Microsoft Azure
Maximus agiliza operaciones con F5 en AWS
Ricacorp Properties refuerza la seguridad de sitios web con F5 en Microsoft Azure

Documentos técnicos

Migración de cargas de trabajo de aplicaciones de nivel 1 a AWS con F5
Cómo añadir servicios de entrega de aplicaciones F5 a OpenStack
La plataforma BIG-IP y Microsoft Azure: Servicios de Aplicaciones en la Nube

Visión general

Visión general de la solución FIPS de VE
Automatiza el despliegue de BIG-IP VE con plantillas de solución en la nube F5


expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

BIG-IP Local

Administrador de tráfico

QUÉ HAY DENTRO

Aplicación ción D entrega con S Cale, Automatización on, y Cu stomiz ación

Las aplicaciones impulsan la innovación y la rentabilidad, lo que permite a su empresa aprovechar la computación en la nube, la movilidad y las redes definidas por software (SDN). Su organización, desde los equipos de desarrollo de aplicaciones y DevOps hasta la infraestructura y las operaciones de TI, depende de que sus servicios de aplicaciones e infraestructura de red funcionen con el máximo rendimiento y con seguridad centrada en las aplicaciones para afrontar los desafíos de hoy y del futuro.

F5® BIG-IP® Local Traffic Manager™ (LTM)Entrega sus aplicaciones a los usuarios de forma confiable, segura y optimizada. Obtiene la extensibilidad y flexibilidad de los servicios de aplicaciones con la programabilidad que necesita para administrar su infraestructura en la nube, virtual y física. Con BIG-IP LTM, tiene el poder de escalar, automatizar y personalizar los servicios de aplicaciones de forma más rápida y predecible.

BENEFICIOS CLAVE

Escale las aplicaciones de forma rápida y confiable Optimice para las aplicaciones web actuales con HTTP/2 para garantizar que sus clientes y usuarios tengan acceso a las aplicaciones que necesitan, cuando las necesiten.

Automatice y personalice con infraestructura programable

Controle sus aplicaciones, desde la conexión y el tráfico hasta la configuración y la administración, con F5® iRules® LX para la programabilidad de la red, con compatibilidad con el lenguaje Node.js en BIG-IP. Utilice laCadena de herramientas de automatización de F5para un enfoque declarativo para aprovisionar, configurar y administrar dispositivos de manera eficiente.

Migre a entornos virtuales y en la nube Logre coherencia operativa y cumpla con las necesidades comerciales en entornos físicos, virtuales y en la nube con flexibilidad de implementación y escalabilidad.

Simplifique la implementación y la administración de aplicaciones Las plantillas F5 iApps® y FAST definidas por el usuario facilitan la implementación, la administración y la obtención de una visibilidad completa de sus aplicaciones

Proteja sus aplicaciones críticas Proteja las aplicaciones que impulsan su negocio con un rendimiento y una visibilidad SSL líderes en la industria.

RECURSOS RELEVANTES

Balanceo de carga de sus aplicaciones

Visibilidad, control y rendimiento SSL

Implemente políticas coherentes en cualquier nube

Solucione problemas de la aplicación

Problemas de rendimiento

INTELIGENCIA DE APLICACIONES

Administración del tráfico de aplicaciones

BIG-IP LTM incluye balanceo de carga estático y dinámico para eliminar puntos únicos de falla. Los proxies de aplicaciones le brindan conocimiento del protocolo para controlar el tráfico de sus aplicaciones más importantes. BIG-IP LTM también realiza un seguimiento de los niveles de rendimiento dinámico de los servidores en un grupo, lo que garantiza que sus aplicaciones no solo estén siempre disponibles, sino que también sean más fáciles de escalar y administrar.

Entrega segura de aplicaciones

BIG-IP LTM ofrece un rendimiento y una visibilidad SSL líderes en la industria para el tráfico entrante y saliente, lo que le permite proteger de forma rentable toda la experiencia del usuario cifrando todo desde el cliente hasta el servidor. También defiende contra ataques DDoS potencialmente paralizantes y proporciona servicios ICAP para la integración con la protección contra la pérdida de datos y la protección antivirus.

Optimización de la entrega de aplicaciones

BIG-IP LTM escala drásticamente, mejorando los tiempos de carga de las páginas y la experiencia del usuario con HTTP/2, almacenamiento en caché inteligente, amplia optimización y administración de conexiones, compresión, rendimiento de RAMCache, F5 TCP Express™ y F5 OneConnect™. También toma decisiones de administración de protocolo y tráfico en tiempo real basadas en las condiciones de la aplicación y del servidor, permite la personalización y la programabilidad de reglas, y la descarga de TCP y contenido.

Visibilidad y monitoreo de aplicaciones

Supervise con precisión el rendimiento de su aplicación para usuarios reales en función de los tiempos de respuesta de la aplicación, las condiciones de la red y el contexto del usuario. F5 Analytics captura estadísticas específicas de la aplicación, como la URL, el rendimiento y la latencia del servidor, que se informan en diferentes niveles del servicio. BIG-IP LTM facilita la integración con sus herramientas existentes mediante estándares de la industria como sFlow, SNMP y syslog.

Visibilidad del protocolo IoT

BIG-IP LTM permite la compatibilidad con clientes IoT, publicando información útil en los brokers MQTT (servidores) a través del protocolo MQTT. Los brokers MQTT envían información a todos los suscriptores de esta información y la compatibilidad con MQTT permite a BIG-IP LTM aprovechar el equilibrio de carga del tráfico MQTT para los clientes IoT de los clientes.

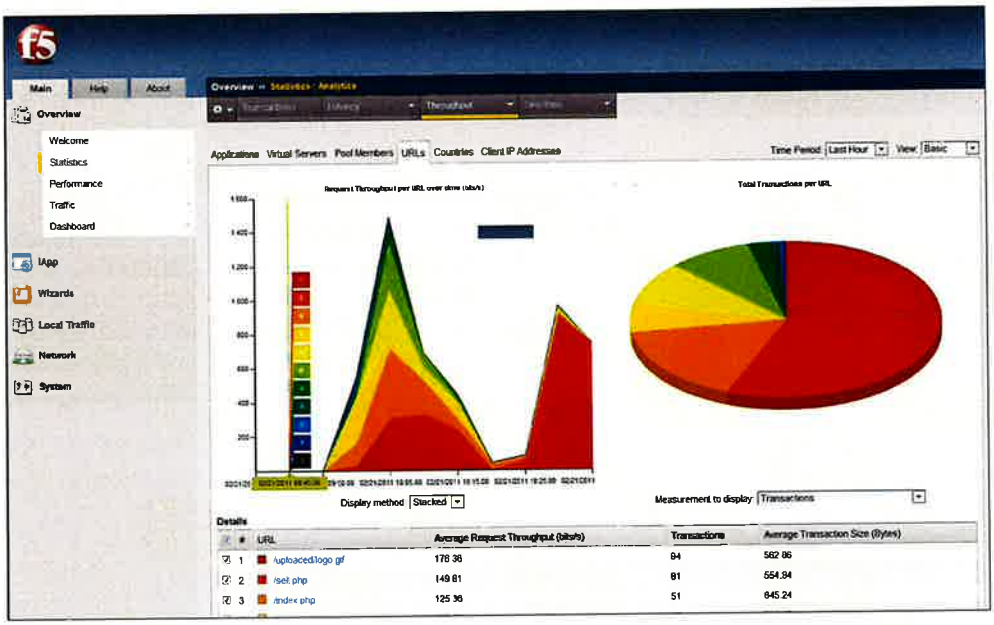


Figura 1: F5 Analytics proporciona estadísticas en tiempo real a nivel de aplicación.

RECURSO RELEVANTE

Integración en entornos de contenedores

AUTOMATIZACIÓN Y CONTENEDORES

Cadena de herramientas de automatización de F5Permite que los servicios de red y de aplicaciones, como la gestión del tráfico y la seguridad de las aplicaciones, se gestionen mediante programación, a través de API declarativas sencillas en lugar de las configuraciones imperativas manuales tradicionales.

En el núcleo de la cadena de herramientas de automatización de F5 se encuentra la extensión Application Services 3 (AS3), que permite a los administradores y desarrolladores automatizar los servicios de aplicaciones de las capas 4 a 7. AS3 también proporciona una base sostenible para habilitar la estrategia de infraestructura como código (IaC) de F5 y la futura integración con soluciones de orquestación, SDN y NFV de terceros

La incorporación declarativa de F5 permite el aprovisionamiento inicial de soluciones F5, así como la configuración de objetos de capa 2 y 3, como dominios de enrutamiento, rutas, direcciones IP propias y VLAN. La extensión de incorporación declarativa, al igual que la extensión de Application Services 3, acepta una declaración JSON que define el estado final de incorporación deseado mediante una única API REST.

La extensión de transmisión de telemetría de F5 es una extensión de iControl LX que agrega, normaliza y reenvía estadísticas y eventos a aplicaciones de consumo como Splunk, Azure Log Analytics, AWS CloudWatch, AWS S3, Graphite y más. Esta herramienta utiliza un modelo declarativo, lo que significa que se proporciona una declaración JSON en lugar de un conjunto de comandos imperativos.

El F5 API Services Gateway es un contenedor Docker independiente de TMOS que ejecuta el marco de trabajo iControl LX de F5 y proporciona un vehículo ligero, rápido, portátil e independiente de TMOS para que los clientes aprovechen iControl LX.

La cadena de herramientas de automatización de F5 ofrece un enfoque basado en procesos para la automatización. Utilice los componentes de la cadena de herramientas de automatización para aprovisionar, configurar y administrar de manera eficiente los servicios que admiten sus aplicaciones.La cadena de herramientas de automatizaciónestá disponible de forma gratuita en GitHubyDocker Hub.

Las integraciones del ecosistema F5 con Ansible, Terraform, Puppet, Chef y Cisco ACI le ayudan a simplificar la orquestación y la gestión de la configuración en nubes públicas y privadas, así como en entornos locales, ofreciendo redes definidas por software con automatización basada en políticas y aumentando la velocidad de implementación de aplicaciones mediante el aprovisionamiento automatizado.

F5 Container Ingress Services (CIS) facilita la entrega de servicios de aplicaciones avanzados a sus implementaciones de contenedores, habilitando el control de entrada, el enrutamiento HTTP, el equilibrio de carga y el rendimiento de entrega de aplicaciones, así como servicios de seguridad robustos.

Container Ingress Servicesintegra fácilmente las soluciones BIG-IP con entornos de contenedores nativos, como Kubernetes, y sistemas de orquestación y gestión de contenedores PaaS, como Red Hat OpenShift.

ESTRUCTURA DE INFRAESTRUCTURA DE PROGRAMACIÓN

Políticas de tráfico local

Las políticas de tráfico local de BIG-IP® son una colección estructurada de reglas basadas en datos, creadas mediante la introducción de tablas en una interfaz web. Las tablas de políticas se rellenan con inglés legible; no se requieren conocimientos de programación. Estas políticas permiten inspeccionar, analizar, modificar, enrutar, redirigir, descartar o manipular el tráfico, y resolver casos de uso comunes que antes se cubrían con iRules simples. Por ejemplo, puede crear una política que determine si un cliente está utilizando un dispositivo móvil y, a continuación, redirigir las solicitudes de dispositivos móviles a la URL del sitio web móvil correspondiente.

iRules

El lenguaje de scripting F5 iRules® (la interfaz de scripting de tráfico de F5) permite el análisis, la manipulación y la detección programática de todos los aspectos del tráfico en sus redes. Los clientes implementan de forma rutinaria reglas de mitigación de seguridad, admiten nuevos protocolos y corrigen errores relacionados con las aplicaciones en tiempo real. Con iRules, robusto y flexible, puede desarrollar de forma fácil y rápida soluciones que puede implementar con confianza en múltiples aplicaciones.

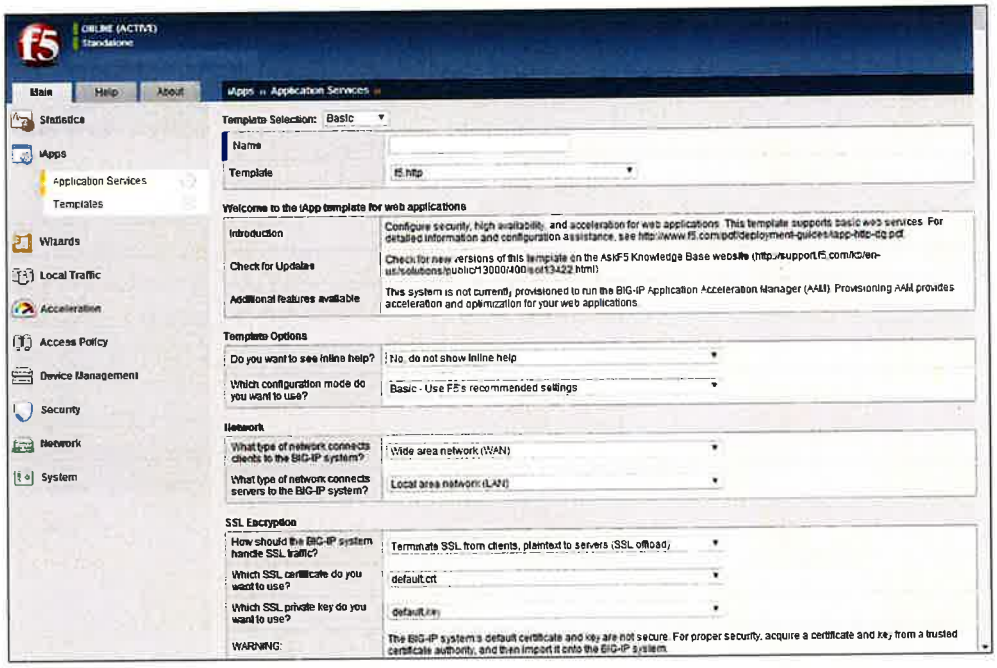
iRules LX

iRules LX es la siguiente etapa de evolución para la programabilidad de redes que trae soporte para el lenguaje Node.js a la plataforma BIG-IP. Node.js permite a los desarrolladores de JavaScript acceder a más de 250,000 paquetes npm que facilitan la escritura y el mantenimiento del código. Los equipos de desarrollo pueden acceder y trabajar en el código con el nuevo entorno de espacio de trabajo de iRules LX y el nuevo complemento disponible para el IDE de Eclipse, que se puede usar para compilaciones de integración continua.

iApps y FAST

Las plantillas de F5 iApps y FAST son herramientas poderosas que le permiten implementar, administrar y analizar los servicios de aplicaciones empresariales en su conjunto, en lugar de administrar individualmente la configuración y los objetos. iApps yFASTle brindan mayor visibilidad y control sobre la entrega de aplicaciones y le ayudan a implementar en horas en lugar de semanas. Este enfoque centrado en las aplicaciones alinea la red con sus aplicaciones y adapta la entrega de aplicaciones a las necesidades comerciales.

Figura 2: Las plantillas de iApps simplifican las implementaciones de aplicaciones



iControl

Las API y el SDK de F5 iControl® permiten la automatización e integración de aplicaciones personalizadas en todos los aspectos de BIG-IP LTM y otros módulos de BIG-IP. iControl se ofrece como API REST y SOAP para adaptarse al modelo más adecuado para su organización. Con iControl, todos los aspectos de la configuración de BIG-IP LTM, incluidos la mayoría de los aspectos de todos los módulos de BIG-IP (desde el aprovisionamiento de dispositivos y aplicaciones hasta el ajuste de aplicaciones y el inicio de soporte y estado), se pueden automatizar mediante programación para lograr infraestructuras dinámicas.

iCall

F5 iCall® es un potente marco de scripting, basado en TMSH (la interfaz de línea de comandos de F5 TMOS® Shell) y Tcl, que ayuda a los clientes a mantener su entorno y reducir el tiempo de inactividad mediante la automatización de tareas. Supervisa los eventos y ejecuta scripts para resolver problemas de forma rápida y predecible. iCall permite a los administradores reaccionar a eventos específicos mediante la ejecución de servicios en el plano de administración, como generar un volcado de pila TCP en caso de fallo, ejecutar una iApp específica para reconfigurar los ajustes del servicio de red de la aplicación o ajustar los pesos de equilibrio de carga en los servicios de la aplicación en función de un cambio en los datos de supervisión del estado.

RECURSOS RELEVANTES

Optimizar el rendimiento de ADC

Servicios de aplicaciones consistentes en cualquier nube

ESTRUCTURA DE INFRAESTRUCTURA ESCALABLE

Preparado para la nube

BIG-IP LTM facilita la consecución de la coherencia operativa y el cumplimiento de las necesidades empresariales en entornos físicos, virtuales y en la nube, eliminando la fricción de la migración de aplicaciones entre arquitecturas físicas y en la nube tradicionales. Disponible en nubes públicas y para la migración a través de múltiples nubes. Obtenga más información enHoja de datos de BIG-IP Virtual Edition.

ScaleN

La tecnología F5 ScaleN® utiliza el chasis F5 VIPRION®, los clústeres de servicios de dispositivos y las capacidades de escalado de F5 Virtual Clustered Multiprocessing™ (vCMP) para habilitar soluciones más eficientes, elásticas y multiinquilino para centros de datos, nubes e implementaciones híbridas. ScaleN va más allá de las limitaciones de la infraestructura tradicional y ofrece múltiples modelos de escalabilidad y consolidación para ayudarle a satisfacer sus necesidades comerciales específicas.

Redes virtuales

El módulo de servicios SDN de BIG-IP® admite de forma nativa VXLAN y NVGRE para ofrecer capacidades de puerta de enlace con BIG-IP LTM, que conecta redes virtuales y tradicionales. Esto le permite mantener las cosas simples, aplicando servicios de red de entrega de aplicaciones tanto en redes virtuales como tradicionales.

Enrutamiento avanzado

El módulo BIG-IP® Advanced Routing™ permite que BIG-IP LTM proporcione capacidades de enrutamiento de red como BGP, RIP, OSPF, ISIS y BFD para una interoperabilidad mejorada dentro de la red, lo que aumenta la resiliencia y la capacidad de su red.

MITIGACIÓN DE ATAQUES

Implemente F5 Distributed Cloud Bot Defense directamente desde su BIG-IP

Los bots causan importantes pérdidas financieras a través del scraping que ralentiza el rendimiento, la reventa y el acaparamiento de inventario que frustran a los clientes leales, la enumeración de códigos de tarjetas de regalo para robar saldos, la creación de cuentas falsas para cometer fraude y el relleno de credenciales (la prueba de credenciales robadas) que conduce a la toma de control de cuentas.

Los bots avanzados y persistentes de hoy en día son más sofisticados que nunca. Para adelantarse a los atacantes, F5 Distributed Cloud Bot Defense utiliza una rica recopilación de señales del lado del cliente, ofuscación de código líder en la industria, recopilación de telemetría agregada e IA para una eficacia a largo plazo sin precedentes y una tasa de falsos positivos casi nula, al tiempo que mantiene el acceso para los bots legítimos. Y debido a que F5 defiende los sitios más atacados de la web, incluidos los de los bancos, minoristas y aerolíneas más grandes del mundo, F5 está preparado cuando estos ataques se dirigen a su organización

Implemente F5 Distributed Cloud Bot Defense directamente desde su BIG-IP o a través de un conector adecuado para su aplicación, con servicios de soporte adaptados a sus necesidades, desde autoservicio hasta servicio gestionado.

BIG-IPPL AT FO RMS

Solo la plataforma ADC de última generación de F5, preparada para la nube, ofrece la agilidad de DevOps con la escalabilidad, la seguridad integral y la protección de la inversión necesarias tanto para aplicaciones consolidadas como emergentes. Los dispositivos BIG-IP® iSeries ofrecen una programación rápida y sencilla, una orquestación compatible con el ecosistema y un rendimiento de hardware definido por software sin precedentes. Como resultado, los clientes pueden acelerar las nubes privadas y proteger los datos críticos a gran escala, a la vez que reducen el coste total de propiedad (TCO) y preparan sus infraestructuras de aplicaciones para el futuro. Las soluciones de F5 se pueden implementar rápidamente mediante integraciones con herramientas de gestión de configuración y sistemas de orquestación de código abierto.

Además de la iSeries, F5 ofrece los sistemas modulares de chasis y blade VIPRION, diseñados específicamente para el rendimiento y para una verdadera escalabilidad lineal bajo demanda sin interrupciones en el negocio. Los sistemas VIPRION aprovechan la tecnología de clustering ScaleN de F5, lo que le permite agregar blades sin reconfigurar ni reiniciar.

La plataforma F5 VELOS® es la próxima generación de sistemas basados en chasis líderes en la industria de F5, que ofrece un rendimiento y una escalabilidad sin precedentes en un único Application Delivery Controller (ADC). Puede escalar la capacidad sin problemas agregando blades modulares en un chasis, sin interrupciones, y VELOS permite una combinación de inquilinos BIG-IP tradicionales, así como inquilinos BIG-IP de próxima generación en el futuro

La solución ADC de próxima generación, F5 rSeries, cierra la brecha entre las infraestructuras tradicionales y modernas con una plataforma rediseñada, basada en API, diseñada para satisfacer las necesidades de sus aplicaciones tradicionales y emergentes. La nueva F5 rSeries ofrece niveles de rendimiento sin precedentes, una arquitectura totalmente automatizable y la mayor confiabilidad, seguridad y control de acceso para sus aplicaciones críticas.

Las ediciones virtuales (VE) del software BIG-IP se ejecutan en servidores estándar y admiten la gama de hipervisores y requisitos de rendimiento. Las VE proporcionan agilidad, movilidad y una rápida implementación de servicios de aplicaciones en centros de datos definidos por software y entornos de nube.

Consulte lasHardware del sistema BIG-IP,VIPRION,VELOSyEdición virtualpara obtener más detalles. Para obtener información sobre la compatibilidad con módulos específicos para cada plataforma, consulte las notas de la versión más reciente enAskF5. Para obtener la lista completa de hipervisores compatibles, consulte laMatriz de hipervisores compatibles con VE.

ConAdministración centralizada BIG-IQ®Puede administrar las plataformas F5 con una vista unificada, incluyendo:

- Dispositivos BIG-IP iSeries
- Dispositivos rSeries
- Ediciones virtuales BIG-IP
- Chasis VIPRION
- Chasis VELOS

Figura 3 Administre el estado de su dispositivo BIG-IP y realice un seguimiento del uso de CPU y memoria de las plataformas físicas y virtuales, las tarjetas de hardware y los núcleos con BIG-IQ. Utilice el registro y la generación de informes para comprender las tendencias generales y detectar las áreas que necesitan corrección. Administre fácilmente las políticas, los certificados y la administración de licencias para implementarlos en todos los ADC de BIG-IP en un control centralizado de la infraestructura de servicios de aplicaciones.

LICENCIAS FLEXIBLES PARA SATISFACER SUS NECESIDADES

Para adaptarse a las diferentes directivas de compra, BIG-IP Next también se puede licenciar mediante una variedad de modelos de consumo. Elija el modelo de licencia que mejor se adapte a sus necesidades, incluyendo suscripción, perpetua o el programa de uso:

- **Suscripción**—Las suscripciones renovables de uno a tres años ofrecen ahorros iniciales y acceso al soporte premium de F5.
- **Perpetua**—Una inversión única de CapEx proporciona la propiedad completa de la solución.
- **Uso**—El modelo de pago por uso incluye acceso al soporte premium de F5 sin necesidad de un compromiso a largo plazo.

F 5 GLO BA LSERVICES

F5 Global Services ofrece soporte, capacitación y consultoría de clase mundial para ayudarle a sacar el máximo provecho de su inversión en F5. Ya sea proporcionando respuestas rápidas a preguntas, capacitando a equipos internos o gestionando implementaciones completas desde el diseño hasta la implementación, F5 Global Services puede ayudar a garantizar que sus aplicaciones sean siempre seguras, rápidas y confiables. Para obtener más información sobre F5 Global Services, comuníquese conconsulting@f5.com o visitef5.com/support.

DE VC CENTRAL

LaF5 DevCentral® comunidad técnica es una fuente activa y comprometida de los mejores artículos técnicos, prácticos, foros de discusión, código compartido, contenido multimedia y más relacionados con la programabilidad y las redes de entrega de aplicaciones.

BIG - IP LT MFE AT URES

Administración del tráfico de aplicaciones

- Balanceo de carga inteligente
- Compatibilidad con protocolos de aplicaciones (HTTP/2, SSL/TLS, SIP, etc.)
- Monitoreo del estado de las aplicaciones
- Administración del estado de conexión de las aplicaciones
- F5 OneConnect
- Enrutamiento avanzado (BGP, RIP, OSPF, ISIS, BFD)
- Servicios SDN (VXLAN, NVGRE)

Optimización de la entrega de aplicaciones

- Compresión adaptativa simétrica
- Caché y compresión de RAM
- TCP Express
- Puerta de enlace HTTP/2

Entrega segura de aplicaciones

- Duplicación de conexión y sesión SSL
- Servicios criptográficos híbridos (descarga de SSL por hardware para BIG-IP VE)
- Descarga de cifrado SSL/TLS (aceleración por hardware)
- Agilidad algorítmica (GCM, ECC, Camellia, DSA, RSA)
- Compatibilidad con Suite B, incluyendo confidencialidad directa
- HSM interno/de red/en la nube (FIPS 140-2)
- Visibilidad SSL

Visibilidad y monitoreo de aplicaciones

- F5 Analytics
- Panel de rendimiento
- Registro de alta velocidad
- sFlow

Infraestructura programable

- iRules e iRules LX para la programabilidad del plano de datos
- ICall para scripting del plano de control basado en eventos
- iApps para la administración y el despliegue de la configuración a nivel de aplicación
- iControl para la API de administración (SOAP, REST)

Automatización y entrada de contenedores

- Cadena de herramientas de automatización para configuraciones declarativas de servicios de aplicaciones
- La extensión Application Services 3 (AS3) automatiza los servicios de las capas 4 a 7
- Incorporación declarativa para el aprovisionamiento y las configuraciones iniciales
- Transmisión de telemetría para la exportación de flujos de datos a análisis de terceros
- Plantillas FAST para configuraciones declarativas de servicios de aplicaciones
- Servicios de entrada de contenedores para la automatización de servicios de aplicaciones de contenedores

Integraciones del ecosistema

- Plantillas de Ansible para la automatización de servicios de aplicaciones
- Módulos de Terraform para la automatización de la implementación
- Cisco ACIy F5 BIG-IP para una estructura y control de red integrados
- Puppet para la automatización de configuraciones y servicios de aplicaciones
- Chef para integraciones de gestión de configuración
- F5 Distributed Cloud Bot Defense para la mitigación de ataques

ScaleN

- Escalado bajo demanda
- Agrupamiento de aplicaciones totalmente activas

MÁS INFORMACIÓN

Para obtener más información sobre BIG-IP LTM, visitef5.compara encontrar estos y otros recursos.

Web

BIG-IP Local Traffic Manager
DevCentral

Hojas de datos

Hardware del sistema BIG-IP
BIG-IP Virtual Editions
rSeries
VELOS
VIPRION

Artículos y guías

Estado de la estrategia de aplicaciones 2021: Analizando el estado actual y futuro de la seguridad y la entrega de aplicaciones
3 consejos para mantener un portafolio de aplicaciones de alto rendimiento.
Elija soluciones avanzadas en la nube que se adapten al futuro. Balanceo de carga de sus aplicaciones.

Casos de estudio

Varolii: proveedor de SaaS garantiza un alto tiempo de actividad y resiliencia para aplicaciones críticas de clientes con F5. Motorists Insurance Group ofrece a sus clientes una experiencia fluida con la solución F5 + Okta. Pandora escala para dar servicio a decenas de millones de usuarios de radio por Internet con la solución F5. MarketAxess aumenta la productividad con la automatización de F5 y Ansible.

Casos de uso

Implemente políticas consistentes en cualquier nube.
Intégrelo en entornos de contenedores. Solucione problemas de rendimiento de las aplicaciones. Intégrelo en canalizaciones de CI/CD

Soporte estándar y premium

HOJA TÉCNICA DE SERVICIOS DE SOPORTE TÉCNICO

¿Qué hay dentro?

Mantén tu solución F5 con soporte rápido y fiable

En un mundo donde el cambio es la única constante, dependes de tu tecnología F5® para cumplir, sin importar los rumbo que tome tu negocio. A medida que surgen desafíos, encontrar rápidamente la mejor solución para tu empresa puede marcar la diferencia entre una crisis informática y la agilidad informática.

Tanto el soporte estándar (10x5) como el premium (24x7) incluyen asistencia remota tanto en línea como por teléfono, soporte proactivo para mantenimiento planificado, reemplazo anticipado de autorización de devolución de materiales (RMA), actualizaciones de software y ayuda con las reglas® F5 iRules. Puedes actualizar el soporte estándar o premium con Servicios RMA Acelerados y Paquetes Adicionales de Mantenimiento. Además, F5 ofrece muchos recursos gratuitos de autoservicio para ayudarte a sacar el máximo partido a tu inversión en F5.

Principales beneficios

Mantén tu negocio en marcha
Recibe ayuda rápida y experta con preguntas o problemas relacionados con tu tecnología F5, para que puedas seguir ofreciendo los servicios de los que depende tu negocio.

Prepárate para eventos conocidos
Soporte acelerado para mantenimiento programado y minimizar el tiempo dedicado a abrir un nuevo caso.

Aumentar la flexibilidad
Aprovecha al máximo la flexibilidad que ofrecen los scripts de iRules para personalizar tus dispositivos F5. Con soporte Standard y Premium, los expertos de F5 ofrecen asistencia con iRules en la resolución de problemas, la comprobación de sintaxis y la validación de la lógica.

Mejora el ROI
Obtén más valor de tu inversión utilizando los recursos de F5.com para buscar en la base de conocimiento, ampliar tus habilidades e interactuar con la comunidad de desarrolladores de F5.

Características de soporte estándar y premium

Desde ingenieros de soporte de red formados en F5 hasta herramientas online y descargas de software, encontrarás una variedad de recursos F5 para ofrecer el nivel adecuado de apoyo a tu organización.

La diferencia entre los niveles de soporte estándar y premium está en las horas de soporte.

Asistencia experta cuando la necesites

Cuenta con el soporte de F5 para que te brinde la ayuda que necesitas, cuando la necesites. La organización mundial de atención al cliente de F5 ha implementado un Sistema de Gestión de Calidad compatible con la norma ISO 9001:2015 que garantiza que F5 cumpla con los procesos y procedimientos documentados y continúa mejorando la prestación de atención al cliente. Con el cumplimiento de la ISO, puedes estar seguro de que recibirás un servicio excelente de forma constante.

Centros de Soporte de Redes

Los Centros de Soporte de Red F5 están estratégicamente ubicados para socios y clientes en APAC, Japón, EMEA y Norteamérica. La dispersión global de los Centros de Soporte de Red permite a F5 ofrecer soporte en varios idiomas a través de ingenieros de soporte nativos que están disponibles cuando tú lo estés, durante tu jornada laboral.

- El horario estándar de soporte es de lunes a viernes, de 8:00 a 18:00, hora local.
- El horario de soporte premium es las 24 horas del día, los 365 días del año.

Ingenieros de Soporte de Redes

Los ingenieros de soporte de redes de F5 tienen un amplio conocimiento de la tecnología F5 y reciben formación continua en las últimas características y actualizaciones de los productos F5. Cuando contactes con el Soporte Técnico, tu llamada será dirigida al mejor experto en la materia para tu caso.

WebSupport Portal

El Portal WebSupport de F5 te ofrece más flexibilidad y acceso rápido a los Centros de Soporte de Red de F5, en cualquier momento. Crea rápidamente nuevos casos de soporte, recibe un número de caso automatizado, lee detalles y actualizaciones del caso, sube archivos adjuntos para solucionar problemas y mucho más.
La ayuda online siempre está disponible.

Gestión proactiva de casos

Con la gestión proactiva de casos, puedes alertar al Soporte F5 sobre el mantenimiento programado próximo de tus dispositivos F5. Así, si necesitas ayuda, ahorrarás el tiempo dedicado a abrir un nuevo caso y a proporcionar archivos de diagnóstico, y los ingenieros de soporte de red F5 podrán ser asignados rápidamente a tu caso.

Soporte iRules

F5 proporcionará soporte básico para iRules existentes para:

- Consulta la sintaxis de iRule
- Asistencia en la resolución de problemas en iRules
- Validar la lógica de iRule frente a los requisitos funcionales para el esfuerzo razonable de F5

El iRule debió estar funcionando antes de contactar con el soporte de F5. Los Servicios de Soporte de F5 no proporcionarán concepto, diseño, autoría ni creación de iRule. Se ofrece asistencia adicional a través de DevCentral y los servicios de consultoría F5.

Actualizaciones y actualizaciones de software

Las nuevas versiones de software están disponibles sin coste para las unidades de soporte.

Recursos de Autoservicio

Para obtener el máximo valor de tu inversión en la solución F5, explora los recursos que ofrece la Base de Conocimiento de AskF5™ y la comunidad online de DevCentral de F5.

Base de conocimientos de AskF5

Considera AskF5 como tu primera fuente de respuestas. Visita la web de AskF5 para descargar software, herramientas de licencias, guías de producto, notas de lanzamiento, soluciones a problemas conocidos,
y la información de cómo hacerlo. También puedes suscribirte para recibir alertas de seguridad por correo electrónico y feeds RSS específicos de productos.

F5 DevCentral

Únete a una comunidad online de desarrolladores de más de 300.000 usuarios de F5 en todo el mundo que colaboran y comparten innovaciones, incluyendo ejemplos de código, nuevas técnicas y otros consejos.

Servicios RMA Acelerados

Los servicios de RMA acelerados incluyen opciones para entrega en el siguiente día laborable, entrega en 4 horas y para que un técnico instale el producto por ti. Todos los niveles incluyen reemplazo avanzado.

Los clientes con soporte estándar o premium pueden actualizar a servicios RMA Acelerados. Las solicitudes de RMA solo pueden presentarse durante las horas soportadas, de acuerdo con el contrato de mantenimiento base de la unidad.

Wagner Pina

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Paquetes adicionales de mantenimiento

Los paquetes adicionales de mantenimiento ofrecen una oportunidad para mejorar proactivamente tu infraestructura de TI y alinear mejor la informática con los objetivos empresariales de forma continua.

Los clientes con niveles de soporte estándar o premium pueden adquirir paquetes adicionales.

Responsable de Prestación de Servicios

El complemento Service Delivery Manager proporciona un Service Delivery Manager (SDM) para facilitar la comunicación entre los propietarios de tu negocio y los recursos técnicos de F5
para identificar y anticipar problemas. Durante la escalada, tu SDM actúa como punto de contacto único y realiza llamadas para la gestión prioritaria de casos de Severidad 1 (sitio abajo) hasta que se resuelva el problema.

Premium Plus

El más alto nivel de soporte, Premium Plus proporciona un equipo dedicado de ingenieros de soporte de red F5 que se familiarizan con tu entorno empresarial y objetivos únicos, un SDM y una línea telefónica dedicada para tus llamadas. Las reuniones semanales de estado y las revisiones trimestrales en profundidad ofrecen la oportunidad de trabajar con tu equipo F5 para abordar los problemas actuales y ayudarte a alcanzar objetivos futuros. Para necesidades inmediatas, tus llamadas reciben el estatus de máxima prioridad.

Puedes adquirir un complemento Premium Plus a tus acuerdos de soporte Premium.

Comparación de niveles de soporte estándar y premium

Características del acuerdo de mantenimiento	Estándar	Prima
Disponibilidad de soporte 10x5 (lunes a viernes, 8:00–18:00, hora local)	✓	
Disponibilidad de soporte 24/7		✓
Acceso a la Base de Conocimientos de AskF5	✓	✓
Acceso al portal WebSupport	✓	✓
Respuesta a llamadas de despiste en un plazo de 30 minutos (solo teléfono)	✓	✓
Reemplazo adelantado de RMA*	✓	✓

*Actualización a servicios RMA acelerados disponibles

Wagner Pina

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

279

Comparación de paquetes adicionales

Características del paquete adicional	SDM	Premium Plus
Prioridad de la gestión de casos de gravedad 1	✓	✓
Colocación prioritaria en la cola telefónica de Soporte	✓	✓
Notificación del Gestor de Soporte Inmediato al crear el caso	✓	✓
Generación de casos y informes de estado programados regularmente	✓	✓
Revisión trimestral in situ	✓	✓
Máxima prioridad en la ruta de escalada de casos	✓	✓
Equipo senior dedicado de Soporte Técnico y familiarizado con tu entorno		✓

F5 está comprometida a ayudarte a mantener tu tecnología F5 en el máximo rendimiento. Si tu organización requiere un nivel de soporte que no está incluido en el soporte Standard o Premium, o en los Paquetes Adicionales de Mantenimiento, contacta con services@f5.com para informarte sobre servicios adicionales y consultoría personalizada.

Más información

Para saber más sobre los Servicios de Soporte Técnico F5, visita f5.com o contacta con services@f5.com. Para asistencia adicional con el desarrollo de iRules, contacte con F5 Professional Services en consulting@f5.com.

Wagner Peña

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Capítulo del manual : Configuración del HSM de red

Aplica a:

Mostrar versiones

Wagner Peña

Configuración del HSM de red

Descripción general: Configuración del HSM de red

F5 BIG-IP es compatible con los siguientes proveedores de HSM de red:

Amazon CloudHSM

- HSM Equinix SmartKey
- HSM de protección de datos a demanda (DPoD) SafeNet

Atos (Bull Trustway Proteccio) HSM

- SafeNet Luna SA

HSM nShield HSM

Estos HSM de red se pueden configurar instalando el software cliente del proveedor y añadiendo la ruta a la biblioteca PKCS #11 a la configuración de BIG-IP. Esto permite incorporar nuevos proveedores de HSM de red con mayor eficiencia. Además, el HSM de red añade compatibilidad con múltiples particiones en un HSM configurado y la capacidad de configurar las particiones y definir a qué partición pertenece una clave. Ahora, la configuración de la partición se realiza durante el proceso de instalación.

Para dar soporte a la funcionalidad de HSM de red, puede utilizar la nueva **Sistema Gestión de certificados Gestión de HSM** Puede configurar el HSM de red mediante la pantalla o los nuevos comandos TMSH. Si instala el HSM con el script de instalación F5 existente, la información se completará automáticamente al abrir la pantalla de administración del HSM. También puede instalar la biblioteca manualmente añadiendo su ubicación a la configuración.

Después de instalar el cliente Network HSM en el sistema BIG-IP, puede crear y operar con las claves dentro del HSM para usarlas con Access Policy Manager y Application Security Manager

Si va a instalar Network HSM en un sistema BIG-IP que se licenciará para el modo Appliance, debe instalar el software Network HSM antes de licenciar el sistema BIG-IP para el modo Appliance

Para obtener instrucciones específicas para la instalación y configuración del cliente HSM, siga los flujos de trabajo específicos del proveedor de HSM en esta guía que le enlazan a los sitios del proveedor donde se proporcionan los pasos en función de la versión que desee instalar.

Requisitos previos para configurar un HSM de red con un sistema BIG-IP

Antes de poder utilizar Network HSM con el sistema BIG-IP, debe asegurarse de que se cumplen estos requisitos:

- Usted ha creado el mundo de la seguridad de la red (arquitectura de seguridad).
- El sistema BIG-IP tiene licencia para "Interfaz externa y HSM de red".

No se puede ejecutar el sistema BIG-IP con HSM internos y externos al mismo tiempo

BIG-IP TMOS con HSM de red solo admite IPv4

Otra información administrativa a tener en cuenta durante la configuración:

- Los nombres de las particiones deben ser únicos.

  Solo se puede configurar un HSM de red a la vez.

- Debe identificar una partición al instalar un cliente (cuando utilice el instalador F5).

  Si modifica la ruta de instalación, el código del cliente o cualquier información de partición, deberá reiniciar el demonio pkcs11d.

  Si configura un HSM en la nube desde cero, debe reiniciar el demonio TMM.

- Ejecute la utilidad de prueba después de realizar cualquier cambio para asegurarse de que el HSM esté configurado correctamente.

  Si no especifica una partición al crear una clave, se utilizará la primera partición de la lista. El nombre de la partición se introducirá automáticamente como "auto".

-

  Si intenta eliminar una partición cuando hay claves definidas que utilizan esa partición, no se le permitirá hacerlo.

Para obtener información sobre las versiones de Network HSM compatibles con las versiones de BIG-IP TMOS, consulte la Matriz de interoperabilidad respectiva de cada proveedor para BIG-IP TMOS con el documento complementario de HSM disponible en AskF5

Versiones compatibles

Versiones compatibles con Network HSM:

- Amazon CloudHSM: Versión 2.0.4
- Equinix SmartKey: Versión 2.24.1051
- Atos Proteccio: Versión 1.08.18
- DPoD: Versión 1.1.0

Instalación y configuración del cliente HSM de red

Para configurar un HSM de red, debe tener acceso de red al HSM con el DNS configurado para resolverlo.

Resumen de tareas para Amazon CloudHSM y Equinix SmartKey HSM

- Configure su dispositivo HSM de red

  Instale el software cliente y cree un Usuario Criptográfico (CU).

- Configurar y activar el

  software Configure el BIG-IP

  - Agregue el servicio HSM (si lo hay) a los scripts de inicio de BIG-IP.
  - Agrega la ruta de la biblioteca
  - Configurar y configurar particiones
- Gestionar Particiones

Configuración de la instalación y configuración del cliente Amazon CloudHSM

Configura tu Amazon CloudHSM siguiendo la documentación en la sección Empezar de la guía CloudHSM.

Amazon CloudHSM solo está disponible para máquinas virtuales que se ejecutan en la nube de AWS.

Tu AWS BIG-IP VE es el cliente EC2 mencionado en la guía de inicio y debería estar en la misma VPC y zona de disponibilidad que el CloudHSM. Los temas iniciales incluyen información para ayudar a crear, inicializar y activar el clúster AWS CloudHSM.

Sigue las instrucciones del tema de AWS hasta seguir los pasos de tarea que se encuentran en la sección Instalación y Cliente (Linux)

Creación de un usuario criptográfico

Gestiona tus usuarios criptográficos (CU) o oficiales (CO) de HSM en tu clúster Amazon CloudHSM mediante:

- Creación de usuarios
- Listado de usuarios

  Cambio de contraseñas de usuario
- Eliminación de usuarios

Sigue los pasos necesarios en Gestión de Usuarios HSM en AWS CloudHSM

Instalación de los clientes

Instala los clientes iniciando sesión en el AWS BIG-IP VE como root y ejecuta:

Esta instalación del cliente debe realizarse después del proceso de actualización de BIG-IP

Wagner Peña 283

```
cd /compartido/
MKDIR NETHSM
CD NETHSM

curl -O https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-client-pk
cs11-3.2.1-1.el7.x86_64.rpm
curl -O https://s3.amazonaws.com/cloudhsmv2-software/CloudHsmClient/EL7/cloudhsm-clien
t-3.2.1-1.el7.x86_64.rpm

RPM -IVH cloudHSM-Client-PKCS11-3.2.1-1.el7.x86_64.rpm
RPM -IVH CloudHSM-Client-3.2.1-1.el7.x86_64.rpm
```

Configuración y activación del software

Para configurar y activar el software debes editar la configuración del cliente antes de poder usar el cliente CloudHSM para conectarte a tu clúster.

Sigue los pasos requeridos en Editar la configuración del cliente

El enlace te lleva a un recurso fuera de AskF5. Es posible que los documentos referidos hayan sido eliminados sin nuestro conocimiento.

Configurar el BIG-IP

Para configurar tu BIG-IP con tu HSM recién configurado y activado, puedes: Añadir

tu servicio HSM a los scripts de inicio de BIG-IP.

- Añade la ruta de la biblioteca y configura las particiones.

Añadir el servicio HSM a los scripts de inicio de BIG-IP
Para añadir tu servicio CloudHSM a los scripts de inicio de BIG-IP, ejecuta lo siguiente:

```
# systemctl enable cloudHSM-client.service
```

Añadir la ruta de la biblioteca y configurar las particiones
Para añadir tu biblioteca CloudHSM a la BIG-IP y configurar las particiones, realiza la pantalla de la interfaz o la CLI para realizar la tarea

1. En la pestaña Principal, haz clic **Sistema** **Gestión de Certificados HSM externo** .
   Se abre la pantalla del HSM externo.
2. Desde la lista **de vendedores**, selecciona **Auto**
3. En el campo **Ruta de Biblioteca PKCS11**, escribe lo siguiente:

```
/opt/cloudhsm/lib/libcloudhsm_pkcs11.so
```

4. En la **sección de Lista de** Particiones, añade los siguientes detalles:

a. En el campo Nombre, escribe **cavium** (con diferencia de mayúsculas y mayúsculas).

*Si escribes **auto** en el campo **Nombre**, se seleccionará la primera partición disponible*

b. En el campo Contraseña, escribe el nombre de *usuario < CU >:< contraseña >*

5. Haz clic en Añadir para añadir tantas particiones como sea necesario.
6. Para editar cualquier partición existente, selecciona la partición y haz clic **en Editar**
7. Para eliminar cualquier partición existente, selecciona la partición y haz clic **en Borrar**
8. Para probar cualquier partición existente, selecciona una partición y haz clic en **Probar**
9. Si has seleccionado **Prueba** , revisa la Salida del Examen para asegurarte de que tus datos son correctos.
    a. Si la prueba no pasa, intenta localizar el problema y activa el registro de depuración y vuelve a ejecutar la prueba para más detalles. Los registros están escribiendo en /var/log/ltm

Asegúrate de restablecer el registro de depuración a la configuración anterior antes de continuar.

10. Haz clic **en Actualizar**

Wagner Peña

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Si estás usando la CLI, haz lo siguiente:

1. Añade tu biblioteca CloudHSM a la BIG-IP introduciendo:

```
# TMSH Create SYS CRYPTO FIPS proveedor externo-HSM Auto
PKC S11-lib-path /opt/cloudhsm/lib/libcloudhsm_pkcs11.so
```

2. Configura la partición, introduciendo:

```
# tmsh crear sys crypto fips nethsm-partition <nombre de
partición> contraseña "<CU usuario nombre>:<contraseña>"
```

Para <nombre de partición>, usa "cavium" ya que es el nombre de partición predeterminado para AWS CloudHSM. También puedes usar "auto" para apuntar a la primera partición (que normalmente es la única partición para AWS CloudHSM).

3. Reinicia el dispositivo para iniciar el servicio y crear los enlaces.
4. Prueba tu salida utilizando la herramienta de pruebas de HSM de red e introduciendo:

```
# TMSH run sysCrypto nethsm-test --hsm partition name=<pa
nombre de la
```

Si no especificas hsm_partition_name entonces se elegirá la primera partición (que normalmente es la única partición para AWS CloudHSM)

Creando una clave en una partición

Para crear una clave en una partición, haz lo siguiente:

1. En la pestaña Principal, haz clic **Sistema** **Gestión de Certificados** **Gestión de Certificados de Tráfico** **Lista de certificados SSL** . Se abre la nueva pantalla del Certificado SSL.
2. Haz clic **en Crear** . Se abre la nueva pantalla del Certificado SSL.
3. En el campo **Nombre**, escribe el nombre del nuevo certificado SSL.
4. En el campo **Nombre Común**, escribe el nombre común del certificado. Por ejemplo, **nethsm_ecdsa**
5. Desde la lista de **particiones de NetHSM**, selecciona **Partición predeterminada**
6. Clic **Terminado**

Puedes elegir otras particiones cuando tengas varios tokens o ranuras configurados en tu HSM de red que usas para las claves

Comprobando la partición de la clave

Para comprobar la partición de la nueva clave, haz lo siguiente:

1. En la pestaña Principal, haz clic **Sistema** **Gestión de Certificados** **Gestión de Certificados de Tráfico** **Lista de certificados SSL** . Se abre la nueva pantalla del Certificado SSL.
2. Seleccione el nombre del certificado SSL recién creado.
3. Seleccione la pestaña **de clave** (si es necesario) para comprobar la partición de las propiedades de la clave (como nombre, tipo de clave, ID de clave, etc.).

Comprobando el estado del servicio

Para comprobar el estado del servicio, haz lo siguiente:

1. En la pestaña Principal, haz clic en **Sistema › Servicios › Lista de Servicios** . Se abre la pantalla de la Lista de Servicio
2. Localiza el nombre **del Servicio** (por ejemplo, pkcs11d) y consulta la información de Historial.
3. Haz clic **en Iniciar Para** , o **Reiniciar** según sea necesario

Configuración de la instalación y configuración del cliente Equinix SmartKey HSM

Crea y configura tu cuenta Equinix SmartKey HSM siguiendo la información de SmartKey para empezar.

Crea el grupo y la aplicación según se indica en las instrucciones SmartKey

Toma nota de la clave API después de crear la aplicación. La información de la clave API puede ser útil más adelante.

Instalación de los clientes

Instala los clientes siguiendo las instrucciones de la guía de desarrollador de SmartKey mientras inicies sesión en la IP BIG-como root.

Usa el cliente 2.9.804 en lugar del cliente vinculado en las instrucciones SmartKey.

Tras instalar el paquete RPM, el nombre del paquete RMP instalado puede cambiar de rpm -i smartkey-PKCS11-2.9.804-0.x86_64.rpm a rpm -q -l Fortanix-PKCS11-2.9.804-0.x86_64.rpm . Si intentas eliminar el paquete, búscalo usando las posibles opciones de nombre que se indican aquí.

Añadir la ruta de la biblioteca y configurar las particiones

Para añadir tu biblioteca SmartKey HSM a la BIG-IP y configurar las particiones, realiza la pantalla de la interfaz o la CLI para realizar la tarea.

1. En la pestaña Principal, haz clic en **Sistema › Gestión de Certificados › HSM externo** . Se abre la pantalla del HSM externo.
2. Desde la lista **de vendedores**, selecciona **Auto**
3. En el campo **Ruta de Biblioteca PKCS11**, escribe lo siguiente:

```
/opt/fortanix/pkcs11/fortanix_pkcs11.so
```

4. En la **sección de Lista de** Particiones, añade los siguientes detalles:
   a. En el campo **Nombre**, escribe **fortanix** (sensible a mayúsculas).

      *Si escribes **auto** en el campo **Nombre**, se seleccionará la primera partición disponible*

   b. En el campo Contraseña, escribe la clave API <

      El nombre de usuario y la contraseña se basan en el usuario criptográfico creado anteriormente.

5. Haz clic en Añadir para añadir tantas particiones como sea necesario.
6. Para editar cualquier partición existente, selecciona la partición y haz clic **en Editar**
7. Para eliminar cualquier partición existente, selecciona la partición y haz clic **en Borrar**
8. Para probar cualquier partición existente, selecciona una partición y haz clic en **Probar**
9. Si pulsaste **en Probar** , revisa la Salida del Test para asegurarte de que tus datos son correctos.
   a. Si la prueba no pasa, intenta localizar el problema y activa el registro de depuración y vuelve a ejecutar la prueba para más detalles. Los registros están escribiendo en /var/log/ltm

   Asegúrate de restablecer el registro de depuración a la configuración anterior antes de continuar.

10. Haz clic **en Actualizar**

Si estás usando la CLI, haz lo siguiente:

1. Añade tu biblioteca SmartKey HSM a la BIG-IP introduciendo:

```
# TMSH Create SYS CRYPTO FIPS proveedor externo HSM Auto
PKCS1 1-lib-path /opt/fortanix/pkcs11/fortanix_pkcs11.so
```

2. Configura la partición, introduciendo:

```
# tmsh crear sys crypto fips nethsm-partition <partition-na
me> contraseña "<API Key>"
```

Para <nombre de partición>, usa "fortanix" ya que es el nombre de partición predeterminado para Equinix SmartKey.

3. Reinicia el dispositivo para iniciar el servicio y crear los enlaces.
4. Prueba tu salida utilizando la herramienta de pruebas de HSM de red e introduciendo:

```
# TMSH run sys crypto nethsm-test --hsm partition name=<part
Nombre->
```

Si no especificas hsm_partition_name, entonces se elegirá la primera partición (que normalmente es la única partición para Equinix SmartKey)

Por defecto, smartkey-client realiza llamadas a la API REST al servidor SmartKey en https://www.smartkey.io. Para hacer llamadas a otro servidor SmartKey, establece la variable de entorno FORTANIX_API_ENDPOINT (FORTANIX_API_ENDPOINT=<smartkey-server-url>).

Configuración de la instalación y configuración del cliente HSM de SafeNet Data Protection on Demand (DPoD)

Para configurar tu HSM SafeNet DPoD, primero debes instalar el software en la IP BIG-IP y completar los pasos de configuración. Para información adicional sobre la configuración de SafeNet/Gemalto, siga la documentación de su sitio web que se indica a continuación.

Requisitos previos para configurar SafeNet DPoD HSM con el sistema BIG-IP

- Has obtenido una cuenta SafeNet DPoD con el archivo de configuración <nombre del servicio>.zip de HSM on Demand y la contraseña para la partición NetHSM.

  Has recibido tus nuevas llaves de registro.

- Has obtenido una licencia para BIG-IP 15.1.0

  Has licenciado correctamente el BIG-IP con el complemento NetHSM.

Configuración del BIG-IP para SafeNet DPoD

Para configurar el BIG-IP de SafeNet DPoD, realiza los siguientes pasos:

1. En la pestaña Principal, selecciona **Sistema** **Licencia**
2. Revisa la Resumen nformation y localiza el **HSM de Interfaz Externa y Red** en el campo **Módulos Activos** (por ejemplo, en Gestor de Tráfico Local) para confirmar

Ahora estás listo para crear una cuenta DPoD en SafeNet e instalar el archivo zip.

Instalación del archivo de DPoD.zip de SafeNet

Para instalar el archivo de DPoD.zip SafeNet, realiza los siguientes pasos:

1. Para descomprimir los archivos de SafeNet DPoD.zip después de crear un directorio (/shared/safenet/) y copiar los archivos de configuración al nuevo directorio, introduce los siguientes comandos:

```
                    [root@bigip:Activo:Independiente] safenet # descomprimir
                    configuración-f5_dpod
_test2.zip
     Archivo: setup-f5_dpod_test2.zip inflando:
     server-certificate.pem inflando:
     partition-ca-certificate.pem inflando:
     partition-certificate.pem inflando:
     Chrystoki.conf
     inflar: crystoki-template.ini
     inflar: cvclient-min.tar inflar:
     cvclient-min.zip inflar: EULA.zip

[root@bigip:Activo:Independiente] safenet # alquitrán -xvf cvclient-
    min.tar contenedor/
    Contenedor/64/
    Contenedor/64/Conte
    nedor
    LUNACM/64/Contenedo
    r
    CKDEMO/64/Contenedo
    r Multitoken/64/CMU
    etc/
    jsp/
    jsp/64/
    jsp/64/libLunaAPI.so
    jsp/LunaProvider.jar
    libs/
    libs/64/
    libs/64/libCryptoki2.so
    setenv
```

Wagner Peña

2. Para crear un **directorio lunasa** y copiar los archivos cliente DPoD en ese directorio, introduzca el siguiente comando:

```
                    # mkdir -p /compartido/safenet/lunasa
# [root@bigip:Activo:Independiente] safenet # cp -rf * /compartido/safenet/lunasa/
```

3. Para configurar el entorno y generar el archivo **de configuración Chrystoki.conf**, introduzca el siguiente comando:

```
                    # fuente: ./setenv
```

4. Para crear un directorio **de liberación** y mover las bibliotecas criptográficas al directorio creado, introduzca los siguiente comandos:

```
# mkdir /compartido/safenet/lunasa/lib
# mv /shared/safenet/lunasa/libs/64/libCryptoki2.so
/compartido/safenet/lunasa/lib
```

```
[root@bigip:Activo:Independiente] safenet # mv libs/64/libCryptoki2.so
/compartido/safene t/lunasa/lib/.
```

5. Para crear un archivo de contraseña que almacene la contraseña de la partición, introduzca el siguiente comando:

```
# tocar
# pOiu12zx > archivo
```

Este archivo se utiliza como contraseña cuando se llama a GemEngine. Por ejemplo, estamos usando ***pOiu12zx*** *como contraseña de partición.*

6. Abre y modifica el archivo **Chrystoki.conf**.

   a. Para modificar las **secciones Chrystoki2** y **Misc**, introduzca los siguientes comandos:

```
Chrystoki2 = {
LibUNIX64 = /shared/safenet/lunasa/lib/libCryptoki2.so;
}
Misc = {
  Apache = 0;
  PE1746Habilitado = 1;
  ToolsDir = /usr/bin;
  RSAKeyGenMechRemap = 1;
}
```

   b. Para crear una nueva **sección de GemEngine**, utiliza los siguientes valores:

Wagner Peña

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

```
                    GemEngine = {
EnableDsaGenKeyPair = 1;
EnableRsaGenKeyPair = 1;
DisablePublicCrypto = 1;
EnableRsaSignVerify = 1;
EnableLoadPubKey = 1;
EnableLoadPrivKey = 1;
DisableCheckFinalize = 1;
DisableEcdsa = 1;
DisableDsa = 0;
DisableRand = 0;
EngineInit="f5dpod":0:0:passfile=/shared/safenet/lunasa/passfile;
EnableLoginInit = 1;
LibPath64 = /compartido/safenet/lunasa/lib/libCryptoki2.so;
LibPath = /shared/safenet/lunasa/lib/libCryptoki2.so;
}
```


7. Para comprobar si los caminos están correctamente configurados y si la partición es accesible, ejecuta LunaCM introduciendo el siguiente comando:

```
# /compartido/safenet/lunasa/bin/64/lunacm
```

8. Para crear los enlaces blandos, introduzca los siguientes comandos:

```
                    # ln -sf /compartido/safenet/lunasa
/usr/lunasa # ln -sf /compartido/safenet/lunasa
/usr/safenet/lunaclient
# ln -sf /compartido/safenet/lunasa/Chrystoki.conf /etc/Chrystoki.conf
# ln -sf /shared/safenet/lunasa/lib/libCryptoki2.so /usr/lib/libCryptoki2_64.so
# ln -sf /shared/safenet/lunasa/lib/libCryptoki2.so /usr/lib/libCryptoki2.so
```

Puede que necesites volver a montar /usr antes de montar -o remontar, rw /usr

9. Reinicia los servicios para aplicar los cambios introduciendo el siguiente comando:

```
                    # Inicio BIGSTART
PKCS11D # Reinicio BIGSTART TMM
```

Ahora has instalado el archivo de DPoD.zip SafeNet y estás listo para configurar un HSM externo y una partición netHSM en la IP-BIG.

Para crear una partición HSM externa y de Red HSM en la BIG-IP, haz lo siguiente:

1. En la pestaña Principal, selecciona **Sistema** **Gestión de Certificados** **Gestión HSM**
2. En el campo **de ruta de biblioteca PKCS11**, selecciona la ruta **de biblioteca /shared/safenet/lunasa/libs/64/libCryptoki2.so**.
3. En el campo **Lista de particiones**, haz lo siguiente:
    a. En el campo **Nombre**, escribe un nombre (por ejemplo, **f5dpod**).
    b. En el campo **Contraseña**, escribe la contraseña del oficial de criptomonedas.
4. Haz clic **en Añadir**
5. Para probar la lista de particiones **Nombre** y **contraseña**, haz clic **en Probar** . Los resultados de la prueba aparecerán e la **Salida de la Prueba**
   campo

   Algunas pruebas pueden tardar hasta un minuto o más en mostrar resultados.

   *Si los resultados de tus pruebas muestran problemas, puedes activar el registro de depuración de PKCS11 con el siguiente comando: tmsh modify sys db log.pkcs11d.level value Debug . La información del registro aparecerá en **/var/log/ltm***

6. Haz clic **en Actualizar**
   Ahora has creado una partición HSM externa y de Red HSM en la BIG-IP. También

puedes configurar un HSM externo y una partición nethsm en el BIG-IP usando la CLI:

```
                tmsh crea sistemas criptográficos fips externo-proveedor hsm auto pkcs11-
lib-path /sh ared/safenet/lunasa/lib/lib/libCryptoki2.so contraseña pOiu12zx
create sys crypto fips nethsm-partition f5dpodTEST password pOiu12zx

[root@bigip:Active:Standalone] config # tmsh list sys crypto fips
sys crypto fips external-hsm {
    num-threads 20
    password $M$39$2g2pWUdT0f6INYhHJ1lZfQ==
    pkcs11-lib-path /shared/safenet/lunasa/lib/libCryptoki2.so
    proveedor auto
}
sys crypto fips nethsm-partition f5dpodTEST {
    password $M$Pk$b099uPx3zSycJWdEBrazhw==
}
```

Wagner Peña

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Iniciar sesión en LunaCM para inicializar el usuario de oficiales criptográficos (CO)

Para iniciar sesión en LunaCM e inicializar al usuario CO, introduzca los siguientes comandos:

```
                    [root@bigip19:Activo:Independiente] f5_dpod #
                    /compartido/safenet/lunasa/bin/6
4/lunacm
LunaCM v1.1.0-1044. Copyright (c) 2006-2017 SafeNet.
Ranura s

e   ID de ranura -          3
    > Etiqueta ->
    Número de serie ->      1334047160562
    Modelo ->               Cryptovisor7
    Versión del firmware -  7.1.3
    >                       1.1.0
t   Versión del firmware    Partición de usuario Luna con Firma SO (PW) con ranura de
    CV -> Configuración ->  token de usuario en modo clonación


    ID actual de la
```

Inicialización del rol de usuario cripto

Para inicializar el rol de usuario cripto, realiza los siguientes pasos.

1. Para introducir el ID de la ranura, introduce el siguiente comando:

```
lunacm:>conjunto de ranuras -ranura 3
```

El **ID actual de la ranura** : 3 (Firma de Clonación de Slot de Usuario Luna 7.1.3 (PW)).

El **resultado del comando** : Sin error.

2. Para introducir la información de la partición, introduzca el siguiente comando:

```
lunacm:>partition init -label f5dpodTEST
```

3. Escribe y luego vuelve a escribir la contraseña de **Partition SO**

   Ahora estás a punto de inicializar la partición. Todo el contenido de la partición será destruido.

4. Escribe **continuar** o **terminar** para detener la acción.
5. Si procedes, escribes y luego vuelves a escribir el nombre de dominio.

   *Si ni la opción **-domain** ni **la -defaultdomain** se especificaban, introducía una.*

El **resultado del comando** : Sin error.

6. Introduce el siguiente **comando Partition SO** y luego escribe la contraseña:

```
lunacm:>rol nombre de inicio de sesión -nombre
```

El **resultado del comando** : Sin error.

7. Introduce el siguiente comando y luego escribe, y vuelve a escribir, la nueva contraseña:

```
LUNACM:>rol INIT -nombre CO
```

El **resultado del comando** : Sin error.

8. Introduce el siguiente comando y luego escribe las contraseñas existentes y nuevas:

```
lunacm:>cambio de rolPW -nombre co
```

Wagner Peña

   a. Escribe la contraseña existente: ********
   b. Escribe la nueva contraseña: ********
   c. Vuelve a escribir la nueva contraseña: ********

Ahora has inicializado la partición.

Creación de un certificado y clave de HSM de red

Para crear un certificado HSM de red y una clave para asignar al servidor virtual, sigue los pasos siguientes.

Suposiciones:

Tienes un servidor HTTPS disponible.

1. En la pestaña Principal, selecciona **Sistema › Gestión de Certificados › Gestión de Certificados de Tráfico** y haz clic **Crear**
2. En el campo **Nombre**, escribe un nombre (por ejemplo, **my-fips**).
3. De la lista **de emisores**, selecciona **Self** para un certificado auto-firmado.
4. En el campo **Nombre Común**, escribe un nombre.
5. En la sección **de Propiedades de Clave**, desde la lista **de Tipo de Seguridad**, seleccione **NetHSM**

295

***NetHSM** solo es visible cuando NetHSM está licenciado*

6. Desde la lista de **particiones de NetHSM**, selecciona el nombre de partición que creaste antes (por ejemplo, **f5dpod**).
7. Clic **Terminado**

También puedes comprobar la clave en la partición introduciendo los siguientes comandos:

```
                    lunacm:>ro iniciar sesión

    -n co introducir contraseña: ********

Resultado del comando: Sin

error lunacm:>par con

El 'Oficial de Cripto' está conectado actualmente. Buscando objetos accesibles para
el 'Oficial de Criptografía'.

    Lista de objetos:

    Etiqueta:       rsa_19574 15ba2050
    Asa:            2156006992
    Tipo de objeto: Clave privada
    UID de objetos: 842B000000A0000012CBE0800

    Etiqueta:       ec_secp384r1_20117 28804c3f
    Asa:            746860604
    tipo de objeto: Clave
    privada
    UID de objetos: 822b00000a0000012cbe0800

    Etiqueta:       ec_secp384r1_20117 28804c3f
    Asa:            408279569
    tipo de objeto: Clave


    Número de objetos: 3


Resultado del comando:
Sin error
```


Ahora has creado un certificado y una clave de Red HSM.

Creación de un perfil SSL de cliente HSM de red

Para crear un perfil SSL de cliente HSM de red que utilice el certificado y la clave recién creados, haz lo siguiente:

1. En la pestaña Principal, selecciona **Tráfico local** **Perfiles** **SSL** **Cliente** y clic **Crear**

2. En el campo Nombre, escribe un nombre (por ejemplo, **my-fips-clientssl**).
3. Desde la lista **de Perfil de Padres**, selecciona **clientessl**
4. En el **campo Cadena de Llaves de** Certificados, seleccione la **casilla de verificación Personalizado** y haga clic **en Añadir** . Aparece la pantalla de Añadir Certificado SSL en el Lladro.
5. Desde las **listas de Clave** de Certificado y **Cadena**, selecciona **my-fips** para establecer los valores de tu certificado FIP
6. Haz clic **en Añadir**
7. Haz clic **en Terminado** para crear el nuevo perfil.
   Ahora has creado un perfil SSL de cliente HSM de red.

Asignación del nuevo perfil SSL del cliente a un servidor virtual

Para asignar tu nuevo perfil SSL de cliente a tu servidor virtual, haz lo siguiente:

1. En la pestaña Principal, selecciona **Tráfico Local › Servidores Virtuales › Lista de Servidores Virtuales** y haz clic **en Crear**
2. En el campo Nombre, escribe un nombre.
3. En el **campo Dirección de Destino**/Máscara, selecciona **<¿Host o Lista de Direcciones?>** y escribe la dirección.
   a. Especifica la información de la dirección IP de destino a la que envía el tráfico el servidor virtual. Especificar la dirección IP en formato CIDR: dirección/prefijo, donde la longitud del prefijo está en bits: por ejemplo, para IPv4: 10.0.0.1/32 o 10.0.0.0/24, y para IPv6: ffe1::0020/64 o 2001:ed8:77b5:2:10:10:100:42/64. El los valores predeterminados para DHCP son 255.255.255.255 (IPv4 por defecto) y ff02::1:2 (IPv6 por defecto). También puedes seleccionar Otro para especificar otra dirección de destino.
4. En el campo **Puerto de Servicio**, selecciona **<¿Puerto o Lista de puertos?>** y escribe la información del puerto antes de seleccionar una designación de puerto de la lista.
   a. Escribe un puerto de servicio o selecciona un tipo de la lista. Cuando seleccionas un tipo de la lista, el valor en **La caja de Service** Port cambia para reflejar el valor predeterminado asociado, que puedes cambiar.
5. En el **campo Perfil SSL (Cliente)**, selecciona **my-fips-clientssl** de la lista **Disponible** y muévelo a la **opción Selected** lista.
   a. Especifica el perfil SSL para gestionar el tráfico SSL del lado del cliente. Usa los botones Mover (<<) y (>>) para ajustar el uso del perfil.
6. Clic **Terminado**
   Ahora has asignado tu nuevo perfil SSL de cliente a tu servidor virtual.

Wagner Pena

Revisión del nuevo certificado

Para revisar el nuevo certificado al pasar tráfico a través de un navegador, haz lo siguiente:

1. Abre un navegador de tu elección y pasa el tráfico a través de tu dispositivo BIG-IP.
2. Consulta los detalles del certificado para el nombre del nombre común de tu certificado.

Configuración del BIG-IP para SafeNet DPoD al usar un par de alta disponibilidad

Para configurar tu BIG-IP para SafeNet DPoD usando un par de dispositivos de alta disponibilidad (HA), haz lo siguiente:

297

1. Sigue el proceso manual de instalación del archivo .zip en ambos dispositivos HA.

2. Crea el HSM externo en ambos dispositivos.

Este objeto no está sincronizado por configuración. Sin embargo, el objeto de partición nethsm sí se sincroniza.

Configuración de la instalación y configuración del cliente HSM de Atos (Bull Trustway Proteccio)

El sistema BIG-IP puede configurarse para utilizar el servicio HSM de la red Bull Trustway Proteccio, de Atos. Proteccio es un servicio HSM de red de terceros que no vende F5. Los clientes de Atos que poseen una licencia de Proteccio pueden configurar el HSM de red para que funcione en el sistema BIG-IP.

Para configurar tu HSM Atos Proteccio, consulta el material de soporte proporcionado por Bull Trustway Proteccio HSM en el sitio w de soporte en línea de Atos Technologies.

Utiliza la siguiente información para instalar y configurar tu HSM Atos Proteccio.

Montando el ISO Atos Proteccio

Para montar el ISO de Atos Proteccio en tu sistema de archivos local usando la CLI de BIG-IP, introduce el siguiente comando:

```
Montaje -o loop /compartido/rpms/Proteccio1.08.18_dec2017.iso /mnt/atos
```

Instalación de los clientes Atos

Para instalar el cliente Atos Proteccio, introduzca el siguiente comando:

```
cd /mnt/atos/Linux/
SH install.sh
```

Crear un directorio local en tu sistema

Para crear un directorio local en tu sistema para una comprobación de configuración, introduce los siguientes comandos:

```
                    cd /compartido/
mkdir proteccio
cd protecccio
cp /etc/proteccio/proteccio.rc ./
cat /shared/proteccio/proteccio.rc
chmod +w proteccio.rc
vi /shared/proteccio/proteccio.rc
[PROTECCIO]
IPaddr=193.251.82.208
SSL=1
SrvCert=proteccio.crt

[CLIENTE]
Modo=0
NivelRegistro=7
LogFile=my_log_file1.log
ClntKey=proteccio_client.key
ClntCert=proteccio_client.crt
```

Wagner Pena.

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Asegúrate de cambiar la dirección IP por la que proporciona Atos.

*Asegúrate de cambiar el valor SSL a **1***

Copia de los archivos de certificados (CRT)

Para añadir la ruta de la biblioteca y configurar las particiones, copia los archivos CRT a **/shared/proteccio/** e introduce el siguiente comando:

```
                    [root@localhost:Activo:Independiente] proteccio #
cliente19.crt cliente19.p12 cliente19.pem my_log_file1.log my_log_file.log proteccio_cli
ent.crt proteccio_client.key proteccio.crt proteccio.rc
```

Añadir la ruta de la biblioteca y configurar las particiones

Para añadir tu biblioteca HSM de Atos a la BIG-IP y configurar las particiones, realiza los pasos proporcionados en la pantalla de la interfaz o en la CLI.

1. En la pestaña Principal, haz clic en **Sistema › Gestión de Certificados › Gestión HSM › HSM Externo** . Se abre la pantalla del HSM externo.
2. Desde la lista **de vendedores**, selecciona **Auto**
3. En el campo **Ruta de Biblioteca PKCS11**, escribe lo siguiente:

   ```
   /usr/lib64/libnethsm.so
   ```

   Consulta la instalación de ATOS Virtual HSM y la guía de usuario para la ruta de la biblioteca NetHSM.

4. En la sección de Lista de Particiones, añade los siguientes detalles:

299

a. En el campo Nombre, tipifica **proteccio** (diferencia de mayúsculas y mayúsculas).

b. En el campo **Contraseña**, escribe la clave < **API** >

*Si escribes **auto** en el campo **Nombre**, se seleccionará la primera partición disponible.*

El nombre de usuario y la contraseña se basan en el usuario criptográfico creado anteriormente.

5. Haz clic en Añadir para añadir tantas particiones como sea necesario.
6. Para editar cualquier partición existente, selecciona la partición y haz clic **en Editar**
7. Para eliminar cualquier partición existente, selecciona la partición y haz clic **en Borrar**
8. Para probar cualquier partición existente, selecciona una partición y haz clic en **Probar**
9. Si pulsaste Test, revisa la salida de Test para asegurarte de que tus datos son correctos.

   Si la prueba no pasa, intenta localizar el problema y activa el registro de depuración y vuelve a ejecutar la prueba para más detalles. Los registros están escribiendo en **/var/log/ltm**

   Asegúrate de restablecer el registro de depuración a la configuración anterior antes de continuar.

10. Haz clic **en Actualizar**

Wagner Peña

expert IPX SRL RNC 130-850151 Santo Domingo, R.D.

Si estás usando la CLI, haz lo siguiente:

1. Para añadir tu biblioteca CloudHSM a la BIG-IP, introduce el siguiente comando:

```
# TMSH crea SYS CRYPTO FIPS proveedor externo HSM Auto PKCS1
1-lib-path/usr/lib64/libnethsm.so.
```

2. Para configurar la partición, introduzca el siguiente comando:

```
# TMSH Crear FIPS Cripto de SYS NETHSM-Partition <partition-
na ME> contraseña "<partition-password"
```

   *Para **<nombre de partición>** , utiliza el nombre de partición dado por ATOS (por ejemplo, **HSMV_6**). F5 recomienda no usar el nombre "auto" ya que la primera partición puede no estar siempre disponible.*

3. Reinicia el dispositivo para reiniciar el servicio y crea los enlaces.
4. Para probar tu salida, utiliza la herramienta de pruebas de HSM de red en **/shared/proteccio/** e introduce el siguiente

```
# TMSH run sys crypto nethsm-test --hsm partition name=<part
Nombre->
```

   comando:

   Si no especificas hsm_partition_name, entonces se elegirá la primera partición (que normalmente es la única partición para Atos)

300

5. Copia todos los archivos bajo **cp /compartido/proteccio/*** a **/etc/proteccio/**

6. Para reiniciar pkcs11d y comprobar su salud, introduce el siguiente comando:

```
                    reinicio de bigstart
pkcs11d estado de bigstart pkcs11d
```

7. Para realizar una prueba completa de validación, introduzca el siguiente comando:

```
                    Ejecuta TMSH el test de NETHSM de Cripto de TMSH
```

8. Para crear una clave desde pkcs11d para revisión, introduzca el siguiente comando:

```
                    tmsh crear clave criptográfica del sistema test_key tipo de
seguridad nethsm
Lista de claves criptográficas del sistema tmsh
```

Configuración del HSM externo y la partición nethsm en el sistema BIG-IP

Para configurar el HSM externo y la partición nethsm en el sistema BIG-IP, introduzca los siguientes comandos después de obtener la nueva partición del proveedor:

```
                TMSH crear sistema crypto FIPS external-HSM Vendor Auto PKCS11-lib-path
"/usr/lib64/libnethsm.so" contraseña kLG7j9p4
tmsh crear sistema crypto fips nethsm-partition 'HSMV1' contraseña kLG7j9p4

[root@bigip:Activo:Independiente] tmp # tmsh list sys crypto fips
sistema criptográfico fips hsm externo {
    número de hilos 20
    Contraseña $M$Zc$Mjpis3OHylCBsOReoHgMPQ==
    pkcs11-lib-path /usr/lib64/libnethsm.so
    vendedor auto
}
sys crypto fips nethsm-partition HSMV1 {
    Contraseña $M$1v$5T68lhIsqTPZNa0I36/OEQ==
}
```

Configuración e instalación del cliente SafeNet Luna SA HSM

Configure su HSM SafeNet Luna SA siguiendo la documentación de la guía de implementación del sistema BIG-IP y del HSM SafeNet Luna SA

Configuración e instalación del cliente Entrust nShield HSM

Configure su HSM SafeNet Luna SA siguiendo la documentación de la guía de implementación del sistema BIG-IP y nShield HSM

información adicional

Para garantizar una integración y compatibilidad perfectas, consulte la matriz de interoperabilidad para **SafeNet Luna SA**

HSM y **Confiar nShield HSM** abajo:

1. Matriz de interoperabilidad para BIG-IP TMOS con clientes SafeNet y HSM
2. Matriz de interoperabilidad para BIG-IP TMOS con clientes nShield y HSM

Contacta con el servicio
de asistencia

¿TIENES ALGUNA PREGUNTA? Soporte y ventas > **SÍGANOS**

Wagner Peña

expert IPX SRL RNC 130-850151 Santo Domingo, R.D.

Wagner Peña

Compresión de respuestas HTTP

Descripción general: Compresión de respuestas HTTP

Una función opcional del sistema BIG-IP es la capacidad del sistema para descargar las tareas de compresión HTTP del servidor de destino. Todas las tareas que necesita para configurar la compresión HTTP, así como el propio software de compresión, están centralizados en el sistema BIG-IP. La forma principal de habilitar la compresión HTTP es configurando un perfil de tipo de compresión HTTP y luego asignando el perfil a un servidor virtual. Esto hace que el sistema comprima el contenido HTTP para cualquier respuesta que coincida con los valores que especifique en la**URI de solicitud**o**Tipo de contenido**configuración del perfil de compresión HTTP

Si desea habilitar la compresión HTTP para conexiones específicas, puede escribir una iRule que especifique el comando HTTP:compress enable. Mediante la función de compresión HTTP del sistema BIG-IP, puede incluir o excluir ciertos tipos de URI o archivos que especifique. Esto es útil porque algunos tipos de URI o archivos ya pueden estar comprimidos. F5 Networks no recomienda usar recursos de CPU para comprimir datos que ya están comprimidos, ya que el costo de comprimir los datos suele superar los beneficios. Ejemplos de expresiones regulares que podría querer especificar para la exclusión son .\.pdf,*
.\.gif o .*\.html.*

Resumen de tareas para el equilibrio de carga a nodos IPv6

Cuando configure el equilibrio de carga de IPv4 a IPv6, debe crear un grupo para equilibrar el tráfico a nodos IPv6 y, a continuación, crear un servidor virtual IPv4 que procese el tráfico de la aplicación.

Creación de un perfil de compresión HTTP personalizado

Si necesita ajustar la configuración de compresión para optimizar la compresión para su entorno, puede modificar un perfil de compresión TTP personalizado.

En la pestaña Principal, haga clic**Aceleración › perfiles › Compresión HTTP**. Se abre la pantalla de la lista de perfiles de compresión HTTP.

2. Haga clic en**Crear**
   Se abre la pantalla Nuevo perfil de compresión HTTP.

3. En el**nombre**campoescriba un nombre único para el perfil.

Wagner Peña

IPX SRL RNC 130-850151 Santo Domingo, R.D.

4. De la**lista Perfil actual**seleccione uno de los siguientes perfiles:

ttpcompression

wan-optimized-compression

5. Seleccione la**Personalizado**casilla de verificación.

6. Modifique la configuración según sea necesario.

7. Haga clic en**finalizado**

El perfil de compresión HTTP modificado está disponible en la**Compresión HTTP**pantalla de lista.

Creación de un servidor virtual para la compresión HTTP

Puede crear un servidor virtual que utilice un perfil HTTP con un perfil de compresión HTTP para comprimir las respuestas HTTP.

En la pestaña Principal, haga clic**Tráfico local › Servidores virtuales** Se abre la pantalla Lista de servidores virtuales.

2. Haga clic en**Crear**
Se abre la pantalla Nuevo servidor virtual.

3. En el**nombre**campoEn el campo, escriba un nombre único para el servidor virtual.

4. Para la**Dirección/Máscara de destino**configuración, confirme que el**botón**más caro esté seleccionado y escriba la dirección IP en formato CIDR.

El formato admitido es dirección/prefijo, donde la longitud del prefijo está en bits. Por ejemplo, una dirección/prefijo IPv4 es 0.0.0.1o0.0.0.0/24y una dirección/prefijo IPv6 esfe1::0020/64o 2001:ed8:77b5:2:10:10:100:42/64Cuando se utiliza una dirección IPv4 sin especificar un prefijo, el sistema BIG-IP utiliza automáticamente un /32 prefijo.

La dirección IP que escriba debe estar disponible y no en la red de bucle invertido.

5. En el**Puerto de servicio**campocampo, escriba0o seleccione**TTP**de la lista.

6. Seleccione**http**en la**lista de perfiles HTTP**7. De la

lista de perfiles de compresión TTP**seleccione uno de los siguientes perfiles:**seleccione uno de los siguientes perfiles:

ttpcompression

wan-optimized-compression

8. En el área Recursos de la pantalla, de la lista

grupo predeterminado**seleccione el nombre del grupo correspondiente.**9. Haga clic en

finalizado**finalizado**

Después de crear un perfil de compresión HTTP personalizado y un servidor virtual, puede probar la configuración

Wagner Peña

Contactar con soporte

¿TIENE ALGUNA PREGUNTA?

Soporte y ventas

>SÍGANOS

ACERCA DE F5

Wagner Peña

EDUCACIÓN

Relaciones con los inversores

agentes

Acerca de AskF5

F5.com

SITIOS DE F5

Universidad F5

Capacitación en línea gratuita

TAREAS DE SOPORTE

DevCentral

Portal de soporte

Partner Central

F5 Labs

Lea las políticas de soporte

Información corporativa Sala de prensa de capacitación

Crear servicio Solicitud

Dejar comentarios [+]

Certificación

Privacidad Privacidad de California o No vender mi información personal

Políticas **!!??** **Preferencias de cookies**

Marcas comerciales

Compresión estrategia	Descripción
Latencia	Esta es la estrategia de compresión predeterminada. El sistema prioriza la latencia de los proveedores de compresión y retrasa la selección de un proveedor hasta que lleguen los datos. Esta estrategia ayuda a distribuir mejor la carga de trabajo asignada a cada proveedor. Dado que cada proveedor tiene diferentes capacidades de compresión (por ejemplo, un rendimiento potencial diferente), esta estrategia se centra en el rendimiento total del dispositivo manteniendo métricas sobre el nivel de rendimiento actual de todas las solicitudes combinadas. A medida que el dispositivo se acerca a su límite de trabajo teórico, el proveedor se vuelve menos favorable para la estrategia y el nuevo trabajo se asigna al proveedor menos ocupado. La estrategia de latencia proporciona un mejor mecanismo de limitación cuando hay una gran cantidad de solicitudes de compresión en la cola.
Velocidad	El sistema utiliza el proveedor de compresión de hardware en la mayor medida posible. Solo cuando el hardware está ocupado, el sistema utiliza un proveedor de compresión de software para comprimir las respuestas del servidor HTTP. La estrategia de Velocidad se utiliza mejor para la compresión masiva y para limitar la sobrecarga de la CPU.
Tamaño	El sistema realiza la mayor compresión posible en el software utilizando una relación de TMM y Descarga. Solo cuando el software está ocupado, el sistema utiliza el proveedor de compresión de hardware para comprimir las respuestas del servidor HTTP. La estrategia de Tamaño ofrece la mejor relación a expensas de la sobrecarga de la CPU.
Relación	El sistema utiliza un enfoque de round robin ponderado para decidir qué proveedor de compresión utilizar para comprimir los datos. La estrategia de Relación limita la sobrecarga de la CPU al tiempo que proporciona buenas relaciones de compresión.
Adaptativo	El sistema primero utiliza un proveedor de compresión de software para comprimir las respuestas del servidor HTTP. El sistema cambia a los proveedores de compresión de hardware según el nivel de compresión gzip que se haya configurado en el perfil de compresión HTTP y el proveedor de compresión de hardware que contiene el sistema. A medida que aumenta la carga en el sistema, este responde reduciendo el nivel de compresión gzip deseado (especificado en el perfil de compresión HTTP). El sistema utiliza el proveedor de compresión de hardware solo cuando dicho proveedor puede ofrecer el nivel de compresión gzip especificado o reducido sistemáticamente. La estrategia adaptativa le brinda el mayor control sobre cómo LTM®maneja la compresión.

Tabla de contenido << Capítulo anterior Capítulo siguiente >>

Wagner Peña

IPX SRL
RNC 130-850151
Santo Domingo, R.D.

¿TIENES ALGUNA PREGUNTA?

Soporte y ventas>

SÍGUENOS

Wagner Peña

IPX SRL
RNC 130-850151
Santo Domingo, R.D.

ACERCA DE F5	EDUCACIÓN	SITIOS DE F5	TAREAS DE SOPORTE
Información corporativa Sala de prensa de		F5.com	Leer las políticas de soporte
capacitación	Certificación	DevCentral	Crear servicio
Relaciones con los Inversores	Universidad F5	Portal de soporte	Solicitud
Agentes	Capacitación en línea gratuita	Partner Central	Dejar comentarios [+]
Acerca de AskF5		F5 Labs	

Marcas comerciales Políticas Privacidad Privacidad de California o No vender mi información personal

Capítulo del Manual Integración de ASM y APM con productos de seguridad de bases de datos

Aplica a:

Versiones del programa ⊞

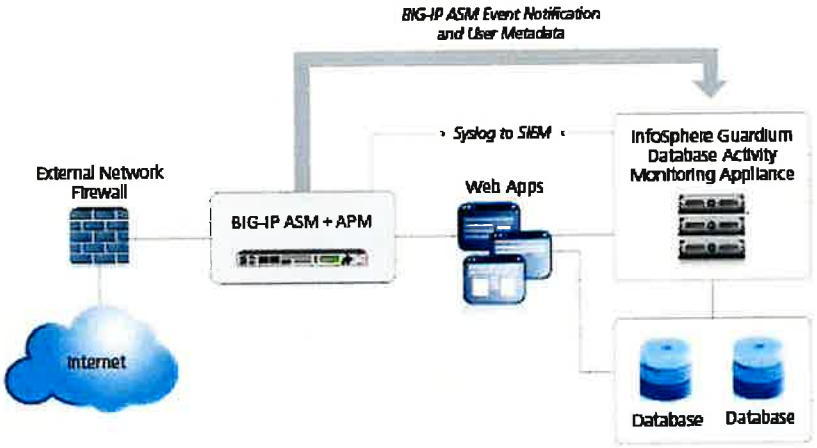
Índice | << Capítulo anterior | Próximo capítulo >>

Resumen: Integración de ASM y APM con productos de seguridad de bases de datos

Puedes desplegar el Gestor™ de Seguridad de Aplicaciones (ASM) y el Gestor® de Políticas de Acceso (APM®) con productos de seguridad de bases de datos, como IBM® InfoSphere® Guardium®, para aumentar la visibilidad de seguridad, recibir alertas sobre actividades sospechosas y prevenir ataques. Cuando se integra con la seguridad de la base de datos, ASM™ puede proporcionar información sobre cada solicitud HTTP y consulta de base de datos. Esto permite al sistema de seguridad de la base de datos correlacionar la transacción web con la consulta de la base de datos para realizar una evaluación de seguridad de la transacción. ASM también proporciona detalles a nivel de aplicación para mejorar el registro y la gestión de informes de seguridad del sistema de bases de datos.

Para integrar ASM con un producto de seguridad de bases de datos, el propio servidor de seguridad de bases de datos debe haber sido configurado y accesible en la red. En el sistema BIG-IP®, se especifica el nombre de host o la dirección IP del servidor de seguridad de la base de datos. Luego, se habilita la integración de seguridad de la base de datos para una o más políticas de seguridad configuradas para proteger los recursos de la aplicación web.

Al utilizar la seguridad de la base de datos, el Gestor de Seguridad de Aplicaciones supervisa el tráfico de aplicaciones web y envía información sobre los usuarios, las solicitudes y los eventos de informes al servidor de seguridad de la base de datos. La siguiente figura muestra un ejemplo de cómo ASM puede integrarse con el IBM InfoSphere Guardium Database Activity Monitoring Appliance.



Ejemplo de integración de ASM y APM con seguridad de bases de datos externas

La política de seguridad puede obtener nombres de usuario a partir de solicitudes usando páginas de inicio de sesión configuradas desde ASM, o puede recuperar los nombres de usuario desde el Gestor® de Políticas de Acceso (APM). Esta implementación describe cómo integrar ASM y APM™ con un servidor de seguridad de bases de datos externo. APM gestiona la autenticación de usuarios en este caso y proporciona la información que se envía al servidor de seguridad de la base de datos.

Requisitos previos para integrar ASM y APM con la seguridad de bases de datos

Para integrar un servidor de seguridad de bases de datos desde el Administrador™ de Seguridad de Aplicaciones (ASM™) de modo que la política de seguridad recupere los nombres de usuario desde el Gestor ® de Política de Acceso (APM®), necesitas realizar estas tareas básicas de configuración del sistema según las necesidades de tu configuración de red:

- Ejecuta la utilidad de configuración y crea una dirección IP de gestión.
  Licencia y provisión ASM, APM y Gestor™ de Tráfico Local (LTM®).
- Configurar una dirección DNS (**Sistema** **Configuración** **Dispositivo** **DNS**).
- Configurar un servidor NTP (**Sistema** **Configuración** **Dispositivo** **NTP**).
  Reiniciar ASM (en la línea de comandos, escribe `Reinicio TMSH /ASM de servicio de sistemas`).

Resumen de la tarea

Creación de una VLAN

Las VLANs representan una colección lógica de hosts que pueden compartir recursos de red, independientemente de su ubicación física en la red. Creas una VLAN para asociar interfaces físicas con esa VLAN.

1. En la pestaña Principal, haz clic **Red** **VLANs**
   Se abre la pantalla de la lista de VLANs.
2. Haz clic **en Crear**
   Se abre la nueva pantalla VLAN.
3. En el campo **Nombre**, escribe un nombre único para la VLAN.
4. En el campo **Etiqueta**, escribe una etiqueta numérica, entre 1 y 4094, para la VLAN, o deja el campo en blanco si quieres que el sistema BIG-IP asigne automáticamente una etiqueta VLAN.
   La etiqueta VLAN identifica el tráfico procedente de los hosts en la VLAN asociada.

Wagner Peña

311

5. Si quieres usar etiquetado Q-in-Q (doble), utiliza la **configuración Customer Tag** para realizar los dos siguientes pasos. Si no ves la configuración **de Etiquetas de Cliente**, tu plataforma de hardware no soporta etiquetado Q-in-Q y puedes saltarte este paso.
   a. Desde la lista **de etiquetas de cliente**, selecciona **Especificar**
   b. Escribe una etiqueta numérica, del 1 al 4094, para la VLAN.

   La etiqueta cliente especifica la etiqueta interna de cualquier trama que pase por la VLAN.

6. Para el escenario **de nterfaces**,
   a. Desde la lista **de Interface**, selecciona un número de interfaz.
   b. Desde la lista de **etiquetado**, selecciona **Sin etiquetar**
   Haz clic **en Añadir**

7. Para la configuración **de Cookies SYN de hardware**, selecciona o borra la casilla de verificación.
   Cuando activas esta configuración, el sistema BIG-IP activa la protección de cookies SYN por hardware para esta VLAN. Activar esta configuración hace que aparezcan ajustes adicionales. Estos ajustes aparecen solo en plataformas BIG-IP específicas.

8. Para la configuración **del umbral de Syncache**, conserva el valor por defecto o cámbialo para adaptarlo a tus necesidades.
   El valor **del umbral de Syncache** representa el número de paquetes de inundación SYN pendientes en la VLAN que activarán la función de protección de cookies hardware SYN.
   Cuando se activa la **configuración de Cookies SYN de hardware** , el sistema BIG-IP activa la protección de cookies SYN en cualquiera de estos casos, lo que ocurra primero:

   Se alcanza el número de conexiones TCP semiabiertas definidas en el Umbral Global de Comprobación de SYN de la configuración LTM® .
   - Se alcanza el número de paquetes de inundación SYN definidos en esta **configuración de umbral de Syncache**.

9. Para la **configuración del Límite de Tasa de Inundación SYN** , conserva el valor por defecto o cámbialo para adaptarlo a tus necesidades.
   El valor **del Límite de Tasa de Inundación SYN** representa el número máximo de paquetes de inundación SYN por segundo recibidos en esta VLAN antes de que el sistema BIG-IP active la protección de cookies hardware SYN para la VLAN.

10. Clic **Terminado**
    La pantalla se actualiza y muestra la nueva VLAN en la lista.

Creación de una dirección IP propia para una VLAN
Asegúrate de tener al menos una VLAN configurada antes de crear una dirección IP propia.

Las direcciones IP propias permiten al sistema BIG-IP®, y a otros dispositivos de la red, enrutar el tráfico de aplicaciones a través de la VLAN asociada.

1. En la pestaña Principal, haz clic **Red IPs propias**

2. Haz clic **en Crear**
   Se abre la pantalla de New Self IP.

3. En el campo **Nombre**, escribe un nombre único para la dirección IP propia.

4. En el campo **Dirección IP**, escribe una dirección IPv4 o IPv6.
   Esta dirección IP debe representar el espacio de direcciones de la VLAN que especifiques con la **VLAN/túnel** ajuste.

5. En el campo **Netmask**, escribe la máscara de red para la dirección IP especificada. Por ejemplo, puedes escribir `255.255.255.0`

6. Desde la lista **de VLAN/Túnel**, selecciona la VLAN a asociar con esta dirección IP propia.
   En la red interna, selecciona la VLAN interna o de alta disponibilidad asociada a un nterface o troncal interno
   En la red externa, selecciona la VLAN externa asociada a una interfaz o troncal externo.

7. Usa los valores por defecto para todos los ajustes restantes.

8. Clic **Terminado**
   La pantalla se actualiza y muestra la nueva dirección IP propia.

El sistema BIG-IP puede ahora enviar y recibir tráfico TCP/IP a través de la VLAN especificada.

Creación de un grupo de tráfico local para la seguridad de la aplicación

Puedes usar un pool de tráfico local con el sistema Application Security™ Manager para reenviar el tráfico al sistema correspondiente

Nota: *En lugar de hacerlo ahora, puedes crear opcionalmente un pool si estás creando un servidor virtual durante la creación de políticas de seguridad*

1. En la pestaña principal, haz clic en **Tráfico** local > **Pools**
   Se abre la pantalla de la lista de grupos.

2. Haz clic **en Crear**
   Se abre la nueva pantalla de billar.

3. En el campo Nombre, escribe un nombre único para el pool.

4. En el área de Recursos, para la configuración **de Nuevos Miembros**, añade al conjunto los servidores de aplicaciones que alojan la aplicación web:
   a. Escribe una dirección IP en el **campo Dirección**.
   b. En el campo **Puerto de Servicio**, escribe un número de puerto (por ejemplo, escribe `80` para el servicio HTTP) o selecciona un nombre de servicio de la lista.
   c. Haz clic **en Añadir**

5. Clic **Terminado**

La configuración del sistema BIG-IP® ahora incluye un pool de tráfico local que contiene los recursos que quieres proteger usando Application Security Manager™.

Creación de un servidor virtual para gestionar el tráfico HTTPS

Puedes crear un servidor virtual para gestionar el tráfico HTTPS.

1. En la pestaña Principal, haz clic **Tráfico local** **Servidores virtuales**
   Se abre la pantalla de la Lista de Servidores Virtuales.

2. Haz clic en el **botón Crear** .

Se abre la pantalla del Nuevo Servidor Virtual.

3. En el campo **Nombre**, escribe un nombre único para el servidor virtual.
4. En el campo **Puerto de Servicio**, escribe `443` o selecciona **HTTPS** de la lista.
5. Desde la lista de configuración**, selecciona** Avanzado
6. Desde la lista **de Perfiles HTTP**, selecciona **http**
7. Para la configuración **de Perfil SSL (Cliente)**, desde la **lista Disponible**, selecciona **clientssl** y, usando el botón Mover, mueve el nombre a la lista **Seleccionada**.
8. **Opcional:** Desde la lista **de Perfil SSL (Servidor)**, selecciona **serverssl**

   Nota: *Esta configuración garantiza que exista una conexión SSL entre el servidor virtual HTTP y el servidor HTTPS externo*
9. Desde la lista **de traducción de direcciones de origen**, selecciona **Auto Map**
10. Desde la lista **de Pool por defecto**, selecciona el pool configurado para la seguridad de aplicaciones.
11. Clic **Terminado**

El servidor virtual HTTPS aparece en la pantalla de la Lista de Servidores Virtuales.

Creación de una política de seguridad sencilla

Antes de poder crear una política de seguridad, debes realizar las tareas mínimas de configuración del sistema requeridas según las necesidades de tu entorno de red.

Puedes usar Application Security Manager™ para crear una política de seguridad robusta pero sencilla adaptada para proteger tu aplicación web. Esta es la forma más sencilla de crear una política de seguridad.

1. En la pestaña Principal, haz clic en **Seguridad** > **Seguridad de Aplicaciones** > Políticas > Lista de **Políticas de Seguridad**
   Se abre la pantalla de la Lista de Políticas.
2. Haz clic **en Crear nueva política**
   Solo ves este botón cuando no tienes ninguna política seleccionada.
3. En el campo **Nombre de la Póliza**, escribe un nombre para la póliza.
4. Tipo de política **de salida**, configurada en **Seguridad**
5. Para la **plantilla de política**, seleccione **Fundamental**
6. Para **Servidor Virtual**, haz clic **en Configurar nuevo servidor virtual** para especificar dónde dirigir las solicitudes de aplicación.
   a. ¿ **Para qué tipo de protocolo utiliza tu aplicación?**, selecciona **HTTP HTTPS**, o ambos.
   b. En el campo **Nombre del Servidor** Virtual, escribe un nombre único.
   c. En el campo **Destino del Servidor Virtual HTTP**, escribe la dirección en formato IPv4 (`10.0.0.1`) o IPv6 (`2001:ed8:77b5:2:10:10:100:42/64`) y especifica el puerto de servicio.
      Consejo: Si quieres que se dirijan varias direcciones IP aquí, usa la configuración **de Red**.
   d. En la configuración HTTP Pool Member, especifica las direcciones de los servidores de aplicaciones del backend.

Desde la lista **de Perfiles de Registro**, selecciona un perfil como **Registrar solicitudes ilegales** para determinar qué eventos se registran en el sistema.

7. En la esquina superior derecha, haz clic **en Avanzado**
   Puedes usar valores predeterminados para la configuración Avanzada, pero es buena idea echarles un vistazo.
   - Si seleccionaste **Fundamental** **Comprensivo** para la **Modo de aprendizaje de plantilla de políticas** se establece en **El modo automático** y **de aplicación** está configurado en **Bloqueo**
     Consejo: Si necesitas cambiar estos valores, establece el lenguaje de la aplicación en un valor distinto a **Auto Detect**
     Si conoces el **lenguaje de aplicaciones**, elimícelo o usa **Unicode (utf-8)**
   - Para añadir protecciones específicas (imponer firmas de ataque adicionales) a la política, para **Tecnologías de Servidor**, selecciona las tecnologías que se aplican a los servidores de aplicaciones de backend. Puedes configurar direcciones IP de confianza que quieras que la política de seguridad considere seguras.

8. Haz clic **en Crear política** para crear la política de seguridad.

ASM™ crea una política de seguridad que empieza a proteger tu aplicación de inmediato. El modo de aplicación de la política de seguridad está configurado en Bloqueo. El tráfico que se considera un ataque, como el tráfico que no cumple con el protocolo HTTP, tiene cargas útiles deformadas, utiliza técnicas de evasión, realiza web scraping, contiene información sensible o valores ilegales, es bloqueado. Se reportan otras posibles infracciones pero no se bloquean.
El sistema examina el tráfico hacia la aplicación web haciendo sugerencias para construir más específicamente la política de seguridad. El Constructor de Políticas aprende selectivamente nuevas entidades como tipos de archivos, parámetros y cookies utilizadas en las peticiones a la aplicación. Cuando ASM procesa suficiente tráfico, añade automáticamente las entidades a la política de seguridad y las hace cumplir.

El sistema aplica un conjunto básico de firmas de ataque a la política de seguridad y las coloca en staging (por defecto, durante 7 días). Si especificas tecnologías de servidor, se incluyen firmas de ataque adicionales. ASM informa de ataques comunes descubiertos en comparación con las firmas, pero no bloquea estos ataques hasta que termina el periodo de preparación y se hacen cumplir. Eso te da la oportunidad de estar seguro de que estos ataques son reales y no solicitudes legítimas.

Consejo: Este es un buen punto para enviar algo de tráfico y comprobar que puedes acceder a la aplicación protegida por la política de seguridad y comprobar que el tráfico se está procesando correctamente por el sistema BIG-IP®. Envía el tráfico a la dirección de destino del servidor virtual.

Creación de un perfil de acceso

Creas un perfil de acceso para proporcionar la configuración de la política de acceso de un servidor virtual que establece una sesión segura.

1. En la pestaña Principal, haz clic **Acceso** **Perfiles / Políticas**
   Se abre la pantalla de Perfiles de Acceso (Políticas por Sesión).

2. Haz clic **en Crear**
   Se abre la pantalla de Nuevo Perfil.

3. En el campo **Nombre**, escribe un nombre para el perfil de acceso.

   Nota: *Un nombre de perfil de acceso debe ser único entre todos los perfiles de acceso y cualquier nombre de política por solicitud*

4. Desde la lista **de Tipos de perfil**, selecciona **SSL-VPN**
   Pantalla de ajustes adicionales.

Wagner Pina

expert IPX SRL RNC 130-850151 Santo Domingo, R.D.

315

5. Desde la lista de Ámbito de Perfil, **conserva el valor por defecto o selecciona otro.**
   Perfil: Da al usuario acceso solo a recursos que están detrás del mismo perfil de acceso. Este es el valor por defecto.
   Servidor Virtual: Da al usuario acceso solo a recursos que están detrás del mismo servidor virtual.
   Global: Da al usuario acceso a recursos detrás de cualquier perfil de acceso que tenga alcance global.

6. Para configurar los ajustes de tiempo de espera y de sesión, selecciona la **casilla de Personalizado** .

7. En el campo **Tiempo de Espera de** Inactividad, escribe el número de segundos que deben pasar antes de que la política de acceso expire. Escribe 0 para poner que no haya tiempo muerto.
   Si no hay actividad (definida por el **umbral de actualización** de sesión y la ventana de actualización de sesión en la configuración de acceso a la red) entre el cliente y el servidor dentro del tiempo umbral especificado, el sistema cierra la sesión actual.

8. En el campo **de Tiempo de Espera de la Política de Acceso**, escribe el número de segundos que deberían pasar antes de que el perfil de acceso expire debido a la inactividad.
   Escribe 0 para poner que no haya tiempo muerto.

9. En el campo **Tiempo Máximo de Sesión**, escribe el número máximo de segundos que puede existir la sesión.
   Escribe 0 para poner que no haya tiempo muerto.

10. En el campo **Max Concurrent Users**, escribe el número máximo de usuarios que pueden usar este perfil de acceso al mismo tiempo.
    Tipo 0 para establecer sin máximo

11. En el campo **Sesiones Máximas por Usuario**, escribe el número máximo de sesiones concurrentes que un usuario puede iniciar.
    Tipo 0 para no poner máximo.

    Nota: *Solo un usuario en los roles de administrador, editor de aplicaciones, gestor o administrador de recursos tiene acceso a este campo*

12. En el campo **Sesiones en Progreso Por IP de Cliente**, escribe el número máximo de sesiones concurrentes que pueden estar en curso para una dirección IP de cliente.
    Al establecer este valor, ten en cuenta si los usuarios proceden de una dirección de cliente con NAT o proxiada y, de ser así, considera aumentar el valor en consecuencia. El valor por defecto es 128.

    Nota: *Solo un usuario en los roles de administrador, editor de aplicaciones, gestor o administrador de recursos tiene acceso a este campo*

    Nota: *F5 no recomienda poner este valor a 0 (ilimitado).*

13. Seleccione la casilla **Restringir a IP de Cliente Único** para restringir la sesión actual a una sola dirección IP. Esta configuración asocia el ID de sesión con la dirección IP.

    Nota: *Solo un usuario en los roles de administrador, editor de aplicaciones, gestor o administrador de recursos tiene acceso a este campo*

    Tras una solicitud a la sesión, si la dirección IP ha cambiado, la solicitud se redirige a una página de cierre de sesión, se elimina el ID de sesión y se escribe una entrada de registro que indica que se ha detectado un intento de secuestro de sesión. Si

Wagner Peña

expert IPX SRL RNC 130-850151 Santo Domingo, R.D.

316

Tal redirección no es posible, la solicitud se deniega y ocurren los mismos eventos.

14. Para configurar los URIs de cierre de sesión, en el área de Configuraciones, escribe cada URI de cierre de sesión en el campo URI y luego haz clic
    Agregar

15. En el campo **Tiempo de Cierre de Sesión** del URI, escribe el retraso en segundos antes de que ocurra la salida para los URIs personalizados definidos en la **lista Inclusión de URI de Salida**.

16. Para configurar SSO:
    - Para que los usuarios inicien sesión en varios dominios usando una sola configuración SSO, hay que saltarse la configuración en el área SSO Across Authentication Domains (modo Dominio Único). Solo puedes configurar SSO para varios dominios después de terminar la configuración inicial del perfil de acceso.
    - Para que los usuarios inicien sesión en un solo dominio usando una configuración SSO, configura la configuración en el área SSO Across Authentication Domains (modo Dominio Único), o puedes configurar la configuración SSO después de terminar la configuración inicial del perfil de acceso.

17. En el campo **Cookie de dominio**, especifica una cookie de dominio, si la conexión de control de acceso a la aplicación utiliza una cookie.

18. En la opción **de Opciones de cookies**, especifica si usar una cookie segura.
    Si la política requiere una cookie segura, seleccione la casilla **de verificación Segura** para añadir la palabra clave segura a la cookie de sesión.
    Si configuras un escenario de acceso LTM que utiliza un servidor virtual HTTPS para autenticar al usuario y luego envía al usuario a un servidor virtual HTTP existente para usar aplicaciones, marca esta casilla.

19. Si la política de acceso requiere una cookie persistente, en la opción **de Opciones de cookies**, seleccione la **casilla de verificación Persistente.**
    Esto establece cookies si la sesión no tiene webtop. Cuando la sesión se establece por primera vez, las cookies de sesión no se marcan como persistentes; Pero cuando la primera respuesta se envía al cliente tras completar con éxito la política de acceso, las cookies se marcan como persistentes. Las cookies persistentes se actualizan para el tiempo de caducidad cada 60 segundos. El tiempo muerto es igual al tiempo muerto de inactividad de la sesión. Si el tiempo de espera de inactividad de la sesión se sobrescribe en la política de acceso, el valor sobrescrito se utilizará para establecer la expiración persistente de la cookie.

20. Desde la lista **de Configuraciones** SSO, selecciona una configuración SSO.

21. En el área de Configuración de idioma, añade y elimina idiomas aceptados, y establece el idioma predeterminado.
    Un navegador utiliza el lenguaje aceptado de mayor prioridad. Si ningún idioma del navegador coincide con la lista de idiomas aceptados, el navegador utiliza el idioma por defecto.

22. Clic **Terminado**

El perfil de acceso se muestra en la Lista de Perfiles de Acceso. Se asigna la configuración predeterminada de registro al perfil de acceso.

Para añadir una configuración SSO para varios dominios, haz clic en **SSO / Auth Domains** en la barra de menú. Para proporcionar funcionalidad con un perfil de acceso, debes configurar la política de acceso. La política de acceso predeterminada para un perfil niega todo el tráfico y no contiene acciones. Haz clic **en Editar** en la columna **de Política de acceso** para editar la política de acceso.

Configuración de una política de acceso

Configuras una política de acceso para proporcionar autenticación, comprobaciones de endpoints y recursos para un perfil de acceso.

317

Este procedimiento configura una política de acceso sencilla que añade una página de inicio de sesión, obtiene las credenciales de usuario, las envía a un tipo de autenticación de tu elección, luego permite usuarios autenticados y denega a otros.

1. En la pestaña Principal, haz clic en **Acceder** > **Perfiles / Políticas**
   Se abre la pantalla de Perfiles de Acceso (Políticas por Sesión).

2. Haz clic en el nombre del perfil de acceso que quieres editar.

3. En la barra de menú, haz clic en Política **de acceso**

4. Para la configuración **del Editor de Políticas Visuales**, haz clic en **la política de acceso Editar para el Perfil *policy_name*** enlace. El editor visual de políticas abre la política de acceso en una ventana o pestaña separada.

5. Haz clic en el **icono (+)** en cualquier parte de la política de acceso para añadir un nuevo elemento.

   Nota: *Solo un subconjunto aplicable de elementos de política de acceso está disponible para su selección en el editor visual de políticas para cualquier tipo de perfil de acceso.*

   Se abre una ventana emergente que muestra acciones predefinidas en pestañas como Propósito General, Autenticación, etc.

6. En la pestaña Inicio de sesión, selecciona **Página de inicio** de sesión y haz clic en el **botón Añadir objeto**. Se abre la pantalla de propiedades del Agente de Página de Inicio de Sesión.

7. Haz clic **en Guardar**
   La pantalla de Política de Acceso se reabre.

8. En la rama de reglas, haz clic en el signo **más (+)** entre **Página de inicio** de sesión y **Rechazar**

9. Configura la autenticación y las comprobaciones del lado del cliente necesarias para el acceso a la aplicación en tu empresa, y haz clic **en Añadir elemento**

10. Cambia la rama de reglas Exitosa de **Denegar** a **Permitir** y haz clic en el **botón de guardar** .

11. Si es necesario, configura acciones adicionales en las ramas de reglas exitosas y de respaldo de este elemento de política de acceso, y guarda los cambios.

12. En la parte superior de la pantalla, haz clic en el **enlace Aplicar Política de Acceso** para solicitar y activar tus cambios en esta política de acceso.

13. Haz clic en **el botón Cerrar** para cerrar el editor visual de políticas.

Para aplicar esta política de acceso al tráfico de red, añade el perfil de acceso a un servidor virtual.

Nota: *Para asegurarte de que el registro está configurado para cumplir con tus requisitos, verifica la configuración del registro para el perfil de acceso.*

Añadir el perfil de acceso al servidor virtual
Antes de poder realizar esta tarea, necesitas crear un perfil de acceso usando Access Policy Manager®

Asocias el perfil de acceso con el servidor virtual creado para la aplicación web que el Application Security Manager™ está protegiendo.

1. En la pestaña Principal, haz clic **Tráfico local** **Servidores virtuales**

Se abre la pantalla de la Lista de Servidores Virtuales.

2. Haz clic en el nombre del servidor virtual que gestiona los recursos de red de la aplicación web que estás asegurando.
3. En el área de Política de Acceso, desde la **lista de Perfiles de Acceso**, selecciona el perfil de acceso que configuraste antes.
4. Haz clic **en Actualizar**

Tu política de acceso ahora está asociada al servidor virtual.

Configuración de un servidor de seguridad de bases de datos

Para integrar el Gestor™ de Seguridad de Aplicaciones (ASM) con un producto de seguridad de bases de datos de terceros, necesitas configurar el servidor de seguridad de la base de datos en ASM™. Puedes configurar un servidor de seguridad de base de datos por sistema.

1. En la pestaña Principal, haz clic en **Seguridad** > **Opciones** > **Seguridad de Aplicaciones** > **Servicios Integrados** > **Seguridad de Bases de Datos**
   Se abre la pantalla de configuración de seguridad de la base de datos.
2. En el campo **Nombre de Host del Servidor/Dirección IP**, escribe el nombre de host o la dirección IP del servidor de seguridad de la base de datos

   Nota: *Si se utiliza SSL para establecer una sesión segura entre el sistema BIG-IP ®y el servidor de seguridad de la base de datos, escriba la dirección IP de un servidor virtual configurado para la conexión segura. El servidor virtual utiliza cualquier dirección IP abierta como destino, el puerto IBM Guardium (16016, por defecto) para el puerto de servicio,* `serverssl` *o un perfil personalizado para la configuración* ***de Perfil SSL (Servidor),*** *y especifica un pool por defecto (que contiene un miembro, el servidor de seguridad de la base de datos, usando su dirección IP y puerto de servicio, normalmente 16016)*
3. Para **el número de puerto del servidor**, escribe el número de puerto del servidor de base de datos. El valor por defecto es 16016, el puerto utilizado por IBM® InfoSphere® Guardium.®
4. Si quieres que el sistema espere una respuesta ACK del servidor de seguridad de la base de datos antes de enviar la solicitud al servidor de aplicaciones, desde la **lista de Tiempo de Espera de** Solicitudes, selecciona **Habilitado** y escribe el número de milisegundos que queda esperando la respuesta.
   El valor por defecto es 5 milisegundos.
   Cuando esta configuración está activada, el sistema reenvía la solicitud al servidor de aplicaciones tan pronto como el servidor de seguridad de la base de datos envía un ACK, o cuando ha pasado el tiempo de espera. Si dejas esta configuración desactivada, el sistema reenvía la solicitud al servidor de aplicaciones inmediatamente.
5. Haz clic **en Guardar**
   El sistema guarda los ajustes de configuración.

El Gestor de Seguridad de Aplicaciones ahora está configurado para conectarse al servidor de seguridad de la base de datos.

Para que ASM pueda reenviar los datos de las solicitudes al servidor de seguridad de la base de datos, a continuación necesitas habilitar la integración de la seguridad de la base de datos en una o más políticas de seguridad.

Habilitar la integración de la seguridad de bases de datos con ASM y APM

Antes de poder habilitar la integración de seguridad de bases de datos, necesitas haber creado una política de seguridad para proteger tu

aplicación web. Para que la política recupere los nombres de usuario de quienes hacen solicitudes, necesitas haber configurado el Gestor® de Políticas de Acceso (APM®) en el sistema BIG-IP®.

Se habilita la integración de la seguridad de la base de datos en una política de seguridad para que el Gestor™ de Seguridad de Aplicaciones (ASM) reenvíe la información de las solicitudes a un servidor de bases de datos de terceros.

1. En la pestaña principal, haz clic en **Seguridad** > **Seguridad de Aplicaciones** > **Servicios Integrados** > **Seguridad de Bases de Datos**
   Se abre la pantalla de Seguridad de la Base de Datos.

2. En la lista **de políticas de seguridad editadas actuales** cerca de la parte superior de la pantalla, verifica que la política de seguridad mostrada sea la que quieres trabajar.

3. Seleccione la **casilla** de verificación Integración de Seguridad de la Base de Datos.

4. Para **la fuente de usuario**, selecciona **Usar nombres de usuario APM e ID de sesión**
   El sistema utiliza nombres de usuario y ID de sesión del Gestor de Políticas de Acceso (APM) para determinar la fuente del usuario. Solo puedes elegir esta opción si tienes APM licenciado y provisionado.

5. Haz clic **en Guardar**
   El sistema guarda los ajustes de configuración.

El Gestor de Seguridad de Aplicaciones se conecta al servidor de seguridad de la base de datos y puede reenviar los datos de las solicitudes a él.

Resultado de la implementación

Has configurado un sistema BIG-IP® para usar el Administrador™ de Seguridad de Aplicaciones (ASM) para asegurar el tráfico de aplicaciones, y el Gestor™ de Políticas de Acceso (APM) para comprobar las credenciales de usuario.

El tráfico del cliente se enruta al servidor virtual de la aplicación web. Al principio, el tráfico se gestiona mediante el módulo APM. APM® verifica las credenciales de usuario y permite que quienes tienen credenciales válidas utilicen aplicaciones web. APM también envía los nombres de usuario y los IDs de sesión de usuarios válidos a ASM™. Después de eso, ASM comprueba las violaciones de seguridad y reenvía el tráfico que cumple con los requisitos de la política de seguridad al servidor backend.

El servidor de seguridad de la base de datos incluye la información de aplicaciones y usuarios proporcionada por ASM y APM, por lo que puede verse en registros e informes sobre ese sistema. El servidor de seguridad de la base de datos puede realizar una evaluación de seguridad más profunda de la solicitud web.

Si quieres revisar informes y registros de eventos que asocian el nombre de usuario con la información de sesión en el BIG-
Puedes configurar el seguimiento de sesiones (activando la conciencia de sesión). Cuando la conciencia de sesión está activada, puedes ver los nombres de usuario en la pantalla Registros de eventos: Aplicación: Solicitudes en Detalles Generales sección de solicitudes específicas. ADEMÁS, la pantalla de Informe: Aplicación: Gráficos muestra los usuarios que enviaron las solicitudes ilegales.

Índice | << Capítulo anterior | Próximo capítulo >>

Wagner Pena

Contacta con el soporte

320

¿TIENES ALGUNA PREGUNTA?
Soporte y > de ventas

SÍGUENOS

Wagner Peña

SOBRE F5	EDUCACIÓN	SITIOS F5	TAREAS DE APOYO
Formación en Información Corporativa		F5.com	Leer políticas de soporte
Carreras en	Certificación	Portal de	Crear solicitud
Relaciones con	F5 University	soporte	de servicio
Inversores en	Formación online gratuita	DevCentral	Deja comentarios [+]
Redacción		Partner Central	
Acerca de AskF5		F5 Labs	

321

Wagner Pena

Capítulo del Manual Introducción a iRules

Wagner Peña

Índice | Próximo capítulo >>

¿Qué es un iRule?

Un ***iRule*** es una función potente y flexible dentro del Gestor de Tráfico Local BIG-IP que puedes utilizar para gestionar tu tráfico de red. Utilizando una sintaxis basada en el estándar industrial Tools Command Language (Tcl), la función iRules no solo te permite seleccionar pools basándote en datos de cabecera, sino que también te permite dirigir el tráfico buscando en cualquier tipo de datos de contenido que definas. Por ello, la función iRules mejora significativamente tu capacidad para personalizar el cambio de contenido según tus necesidades exactas.

Importante: Para información completa y detallada sobre la sintaxis de iRules, consulte el sitio web de DevCentral de F5 Networks, http://devcentral.f5.com. Ten en cuenta que las iRules deben ajustarse a las reglas estándar de gramática Tcl; por lo tanto, para más información sobre la sintaxis Tcl, véase http://tmml.sourceforge.net/doc/tcl/index.html
Un iRule es un script que escribes si quieres que las conexiones individuales se dirijan a un pool distinto al pool por defecto definido para un servidor virtual. iRules te permite especificar de forma más directa los destinos a los que quieres que se dirija el tráfico. Usando iRules, puedes enviar tráfico no solo a los pools, sino también a miembros individuales del pool, puertos o URIs. Las iRules que creas pueden ser simples o sofisticadas, dependiendo de tus necesidades de cambio de contenido.

cuando CLIENT_ACCEPTED { si { [IP::addr [IP::client_addr] es igual a 10.10.10.10] } { pool my_pool } }
Esta iRule se activa cuando se ha aceptado una conexión del lado del cliente, haciendo que el Gestor de Tráfico Local envíe el paquete al pool `my_pool` , si la dirección del cliente coincide `con 10.10.10.10`

Usando una función llamada ***Motor de Inspección Universal***, puedes escribir un iRule que busca ya sea en el encabezado de un paquete o en el contenido real del paquete, y luego dirige el paquete en función del resultado de esa búsqueda. Los iRules también pueden dirigir paquetes basándose en el resultado de un intento de autenticación del cliente.

iRules puede dirigir el tráfico no solo a pools específicos, sino también a miembros individuales del pool, incluyendo números de puerto y rutas URI, ya sea para implementar persistencia o para cumplir requisitos específicos de balanceo de carga.

La sintaxis que usas para escribir iRules se basa en el estándar de programación Tool Command Language (Tcl). Por tanto, puedes usar muchos de los comandos estándar de Tcl, además de un conjunto robusto de extensiones que ofrece Local Traffic Manager para ayudarte a aumentar aún más la eficiencia del balanceo de carga.

Importante: Al referenciar un objeto dentro de un iRule, debes incluir el nombre completo del camino del objeto.

Comandos iRule

Un ***comando iRule*** dentro de un iRule hace que el Gestor de Tráfico Local tome alguna acción, como consultar datos, manipular datos o especificar un destino de tráfico. Los tipos de comandos que puedes incluir dentro de iRules son

Comandos de instrucción

Estos comandos provocan acciones como seleccionar un destino de tráfico o asignar una dirección de traducción SNAT. Un ejemplo de comando de instrucción es `pool <name>`, que dirige el tráfico al pool de balanceo de carga nombrado.

Comandos que consultan o manipulan datos

Algunos comandos buscan datos de cabecera y contenido, mientras que otros realizan manipulación de datos, como insertar cabeceras en peticiones HTTP. Un ejemplo de comando de consulta es `IP::remote_addr`, que busca y devuelve la dirección IP remota de una conexión. Un ejemplo de comando de manipulación de datos es `HTTP::header emove <name>`, que elimina la última aparición del encabezado nombrado de una solicitud o respuesta.

Comandos de utilidad

Estos comandos son funciones útiles para analizar y manipular contenido. Un ejemplo de comando de utilidad es `decode_uri <cadena>`, que decodifica la cadena nombrada usando codificación HTTP URI y devuelve el resultado.

Declaraciones de eventos

iRules están impulsados por eventos, lo que significa que Local Traffic Manager activa una iRule basada en un evento que especifiques en la iRule. Una ***declaración de evento*** es la especificación de un evento dentro de un iRule que hace que el Administrador de Tráfico Local active ese iRule cada vez que ocurre ese evento. Ejemplos de declaraciones de eventos que pueden desencadenar un iRule son `HTTP_REQUEST`, que activa un iRule cada vez que el sistema recibe una solicitud HTTP, y `CLIENT_ACCCEPTED`, que activa un iRule cuando un cliente ha establecido una conexión.

cuando HTTP_REQUEST { si { [HTTP::uri] contiene "aol" } { pool aol_pool } else { pool all_pool } }

Operadores

Un operador iRule compara dos operandos en una expresión.

Por ejemplo, puedes usar el operador contains para comparar un operando variable con una constante. Se hace creando una instrucción if que representa lo siguiente: "Si el URI HTTP contiene aol, envía a la aol_pool pool."

Creando una iRule

Creas una iRule para personalizar la forma en que el sistema BIG-IP procesa el tráfico.

1. En la pestaña Principal, haz clic **Tráfico local** **Reglas**
2. Haz clic **en Crear**
3. En el campo Nombre, escribe un nombre, como `my_irule` El nombre completo de la ruta de iRule no puede superar los 255 caracteres.
4. En el campo Definición, escribe la sintaxis de iRule usando la sintaxis del Lenguaje de Comandos de Herramientas (Tcl). Para información completa y detallada sobre la sintaxis de iRules, consulte el sitio web de DevCentral de F5 Networks http:// devcentral.f5.com
5. Clic **Terminado**

Índice | Próximo capítulo >>

Wagner Pena

Contacta con el soporte

¿TIENES ALGUNA PREGUNTA?

Soporte y > de ventas

SÍGUENOS

Wagner Pina

SOBRE F5	*EDUCACIÓN*	*SITIOS F5*	*TAREAS DE APOYO*
Formación en Información Corporativa		*F5.com*	*Leer políticas de soporte*
Carreras en	Certificación	Portal de	Crear solicitud
Relaciones con	F5 University	soporte	de servicio
Inversores en	Formación online gratuita	DevCentral	Deja comentarios [+]
Redacción		Partner Central	
Acerca de AskF5		F5 Labs	

325

Wagner Pitre

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

326

más información sobre el incidente de seguridad en F5, las acciones que estamos tomando para abordarlo,

y nuestros esfuerzos continuos para proteger a nuestros clientes, haga clicantes de

Solución de soporte

42275060: Existen varios métodos de balanceo de carga. ¿Cuál es el mejor para su entorno?

Fecha de publicación: 9 de noviembre de 2021 Fecha de actualización: 26 de junio de 2025

Contenido recomendado por IA

Se aplica a:

Wagner Peña

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

descripción

Ir ta determinar qué método de balanceo de carga de BIG-IP LTM funcionará mejor para su aplicación y desea saber cuál elegir. Los factores a considerar son los miembros del grupo y la capacidad de cada uno para gestionar la carga dirigida a él y a la red. Existen muchos métodos de balanceo de carga y algunos tienen varios submétodos.

De forma predeterminada, BIG-IP utilizará Round Robin, que funcionará bien para la mayoría de las implementaciones.

medio ambiente

Cada entorno tiene sus propias particularidades, pero a nivel básico se aplicará lo siguiente:

LTM de BIG-IP
El servidor virtual que transporta el tráfico, los miembros del grupo y el método de equilibrio de carga
Los productos, las configuraciones y las características varían, pero girarán en torno a las necesidades de la aplicación y del entorno de red que ejecuta el tráfico.

Con esto en mente, aquí hay una descripción general de cada método:

Partido redondo: El sistema pasa cada nueva solicitud de conexión al siguiente servidor en la fila, distribuyendo las conexiones uniformemente entre las máquinas que se están balanceando. Este método funciona bien en la mayoría de las configuraciones, especialmente si los equipos que se están balanceando tienen una velocidad de procesamiento y memoria prácticamente iguales.

Relación (miembros): La cantidad de conexiones que recibe cada máquina a lo largo del tiempo es proporcional a un peso de relación que usted define para cada máquina dentro del grupo.

Menos conexiones (miembro): El sistema transfiere una nueva conexión al nodo con el menor número de conexiones actuales en el pool. Este método funciona mejor en entornos donde los servidores u otros equipos que se están balanceando tienen capacidades similares. Se trata de un método de balanceo de carga dinámico que distribuye las conexiones según diversos aspectos del análisis del rendimiento del servidor en tiempo real, como el número actual de conexiones por nodo o el tiempo de respuesta más rápido del nodo.

Observado (miembro): El sistema clasifica los nodos según el número de conexiones. Los nodos con un mejor equilibrio de menor número de conexiones reciben una mayor proporción de conexiones. Este método difiere del método de menor número de conexiones (miembro) en que este último mide las conexiones solo en el momento del balanceo de carga, mientras que el método observado rastrea el número de conexiones de Capa 4 a cada nodo a lo largo del tiempo y crea una proporción para el balanceo de carga. Este método de balanceo de carga dinámico funciona bien en cualquier entorno, pero puede ser especialmente útil en entornos donde el rendimiento de los nodos varía significativamente.

Predictivo (miembro): Utiliza el método de clasificación empleado por los métodos Observados (miembro), con la diferencia de que el sistema analiza la tendencia de la clasificación a lo largo del tiempo, determinando si el rendimiento de un nodo mejora o empeora. Los nodos del grupo con mejor clasificación de rendimiento, que actualmente mejoran en lugar de empeorar, reciben una mayor proporción de conexiones. Este método de balanceo de carga dinámico funciona bien en cualquier entorno.

Relación (nodo): La cantidad de conexiones que recibe cada máquina a lo largo del tiempo es proporcional a un peso razonado que usted define para cada máquina en todos los grupos de los que el servidor es miembro.

Menos conexiones (nodo): El sistema transfiere una nueva conexión al nodo con el menor número de conexiones actuales de todos los grupos a los que pertenece. Este método funciona mejor en entornos donde los servidores u otros equipos que se balancean tienen capacidades similares. Se trata de un método de balanceo de carga dinámico que distribuye las conexiones en función de diversos aspectos del análisis del rendimiento del servidor en tiempo real, como el número de conexiones actuales por nodo o el tiempo de respuesta más rápido del nodo.

Más rápido (nodo): El sistema transfiere una nueva conexión basándose en la respuesta más rápida de todos los grupos a los que pertenece un servidor. Este método puede ser especialmente útil en entornos donde los nodos están distribuidos en diferentes redes lógicas.

Observado (nodo): El sistema clasifica los nodos según el número de conexiones. Los nodos con un mejor equilibrio de menor número de conexiones reciben una mayor proporción de conexiones. Este método difiere del método de menor número de conexiones (nodo) en que este último mide las conexiones solo en el momento del balanceo de carga, mientras que el método observado rastrea el número de conexiones de capa 4 a cada nodo a lo largo del tiempo y crea una proporción para el balanceo de carga. Este método de balanceo de carga dinámico funciona bien en cualquier entorno, pero puede ser especialmente útil en entornos donde el rendimiento de los nodos varía significativamente.

Predictivo (nodo): Utiliza el método de clasificación empleado por los métodos Observados (miembro), con la diferencia de que el sistema analiza la tendencia de la clasificación a lo largo del tiempo, determinando si el rendimiento de un nodo mejora o empeora. Los nodos del grupo con mejor clasificación de rendimiento, que actualmente mejoran en lugar de empeorar, reciben una mayor proporción de conexiones. Este método de balanceo de carga dinámico funciona bien en cualquier entorno.

Relación dinámica (nodo): Este método es similar al modo Ratio (nodo), salvo que las ponderaciones se basan en la monitorización continua de los servidores y, por lo tanto, cambian constantemente. Se trata de un método de balanceo de carga dinámico que distribuye las conexiones en función de diversos aspectos del análisis del rendimiento del servidor en tiempo real, como el número de conexiones actuales por nodo o el tiempo de respuesta más rápido del nodo.

Más rápido (aplicación): Aprueba una nueva conexión según la respuesta más rápida de todos los nodos activos en un grupo. Este método puede ser especialmente útil en entornos donde los nodos están distribuidos en diferentes redes lógicas.

Menos sesiones: El sistema transfiere una nueva conexión al nodo con el menor número de sesiones persistentes. Este método funciona mejor en entornos donde los servidores u otros equipos que se equilibran tienen capacidades similares. Se trata de un método de equilibrio de carga dinámico que distribuye las conexiones en función de diversos aspectos del análisis del rendimiento del servidor en tiempo real, como el número de sesiones activas. Para usar este método de equilibrio de carga, el servidor virtual debe consultar un perfil de persistencia que registre las conexiones persistentes.

Relación dinámica (miembro): Este método es similar al modo Ratio (nodo), salvo que las ponderaciones se basan en la monitorización continua de los servidores y, por lo tanto, cambian constantemente. Se trata de un método de balanceo de carga dinámico que distribuye las conexiones en función de diversos aspectos del análisis del rendimiento del servidor en tiempo real, como el número de conexiones actuales por nodo o el tiempo de respuesta más rápido del nodo.

Conexiones mínimas ponderadas (miembro): El sistema utiliza el valor especificado en "Límite de conexión" para establecer un algoritmo proporcional para cada miembro del grupo. El sistema basa la decisión de balanceo de carga en esa proporción y en el número de conexiones actuales a ese miembro del grupo. Por ejemplo, el miembro_a tiene 20 conexiones y su límite de conexión es 100, por lo que está al 20 % de su capacidad. De igual manera, el miembro_b tiene 20 conexiones y su límite de conexión es 200, por lo que está al 10 % de su capacidad. En este caso, el sistema selecciona al miembro_b. Este algoritmo requiere que todos los miembros del grupo tengan especificado un límite de conexión distinto de cero.

Conexiones mínimas ponderadas (nodo): El sistema utiliza el valor especificado en el Límite de Conexión del nodo y el número de conexiones actuales a dicho nodo para establecer un algoritmo proporcional. Este algoritmo requiere que todos los nodos utilizados por los miembros del grupo tengan un límite de conexión distinto de cero.

Wagner Peña

Ratio (sesión): El sistema selecciona al miembro del grupo según la proporción de sesiones activas de cada uno. Tenga en cuenta que las sesiones pendientes se consideran activas.

Relación de conexiones mínimas (miembro): El sistema selecciona al miembro del grupo según la relación del número de conexiones que cada miembro del grupo tiene activas.

Relación de conexiones mínimas (nodo): El sistema selecciona el nodo según la relación del número de conexiones que cada nodo tiene activas.

Acciones recomendadas

Al considerar cuál utilizar...

Pregunte ¿cuál es la aplicación y sus requisitos?

Algunos protocolos y aplicaciones tienen necesidades y requisitos específicos, y existen artículos de MyF5 que los abordan.

¿Qué recursos tienen los miembros de mi grupo?

¿Varían esos recursos? ¿Cuántos miembros hay en el grupo? ¿Cuánto tráfico se procesará?

Los artículos de las dos secciones siguientes le ayudarán a comenzar a determinar el método de equilibrio de carga adecuado.

información adicional

Hay maneras de abordar algunas preguntas e inquietudes sobre recursos y capacidades. Estas incluyen...

Activación de grupo prioritario: Acció**n7065: Confi gramoorina gramoLos BIG-IP yUtilizar servidores alternativos cuando los miembros del grupo no estén disponibles**

en caso de interrupción del servicio: **15095: Descripción general de la función Acción en caso de interrupción del servicio**

Monitores de salud: consulte **Capítulo anual: Implementación del monitoreo de la salud y el desempeño**para la versión en uso.

Contenido eufórico

K9125: Descripción general de D yBalanceo de carga de relación dinámica gramo

K02024845: BIG-IP LTM-DNS de pageraciones gramoGuía | Capítulo 2: Balanceo de carga BIG-IP LTM gramo K10430: Causas del equilibrio desigual de la carga gramo K01052782: Descripción general del equilibrio de carga de Ratio gramomodos

K11870: Equilibrio de carga de relación gramoEl método requiere más CPU que el equilibrio de carga Round Robin. gramoMétodo K14129: Visualización gramola d yrelación dinámica wei gramoaltura de un nodo (11.x - 16.x)

K6406: Descripción general del equilibrio de carga de los miembros del grupo de conexiones menos frecuentes, más rápidas, observadas y predictivas gramo K8968: Habilitación gramoLa persistencia de un servidor virtual permite regresar gramoclientes a b ypequilibrio de carga de culo gramo K24595255: Creatina gramoun servidor virtual SFTP con equilibrio de carga K96316382: Equilibrio de carga gramoLDAPS en BIG-IP ytallos K9347: Confi gramoorina gramopaso a través gramoEquilibrio de carga FTPS gramo K7170: Confi gramoorina gramoBalanceo de carga PPTP gramo

K13403: Confi gramoorina gramoEquilibrio de carga L3 nPath gramoy monitoreo gramo

K13575: Confi gramoorina gramoun servidor virtual BIG-IP con mensajes gramoequilibrio de carga basado en e gramoperfil

K00725997: El servidor virtual OneConnect ma ypreservar el pagSelección de herramientas en múltiples pagSolicitudes HTTP K14358: Descripción general del multiprocesamiento en clúster gramo(11.3.0 y posteriores)

Wagner Pena

Contenido recomendado por IA

Aviso de seguridad -**000156572: Trimestral ySeguridad yNotificación (octubre de 2025))** Política -**5903: Software BIG-IP su pagpolicía portuaria y** Conocimiento -**000135931: Contactar con el soporte de F5**

Política -**4309: Vida útil del producto de hardware F5c ycle sup pagpolicía de ort y**

Los ingenieros de soporte de F5 que trabajan directamente con los clientes escriben artículos de conocimiento y soluciones de soporte que le brindan acceso inmediato a sugerencias de mitigación, soluciones alternativas o resolución de problemas.

¿Fue útil esta información?

Sí o

¿Cómo podemos mejorar este contenido?

¿Podemos comunicarnos con usted directamente con respecto a estos comentarios?

Sí o

Protegido por reCAPTCHA: privacidad & Términos

Asegure y brinde experiencias digitales extraordinarias

La cartera de capacidades de automatización, seguridad, rendimiento y conocimiento de 5 permite a nuestros clientes crear, proteger y operar aplicaciones adaptables que reducen costos, Mejorar las operaciones y proteger mejor a los usuarios.ganar más ›

LO QUE OFRECEMOS

FUENTES ELECTRÓNICAS

APOYO

ARTISTAS

COMPAÑÍA

CONECTA CON NOSOTROS

CONTACTAR CON SOPORTE

Wagner Pina

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Capítulo del Manual Creación del Thales HSM

Aplica a:

Versiones del programa

Wagner Peña

Índice | Próximo capítulo >>

Creación del Thales HSM

Resumen: Creación del Thales HSM

El Thales nShield Connect es un HSM externo disponible para su uso con sistemas BIG-IP®. Como es basada en red, puedes usar la solución Thales nShield Connect con todas las plataformas BIG-IP, incluyendo chasis VIPRION® Series y BIG-IP Virtual Edition (VE).

La arquitectura Thales nShield Connect incluye un componente llamado Sistema de Archivos Remoto (RFS) que almacena y gestiona los archivos clave cifrados. El RFS puede instalarse en el sistema BIG-IP o en otro servidor de tu red

El sistema BIG-IP es cliente del RFS, y todos los sistemas BIG-IP inscritos con el RFS pueden acceder a las claves cifradas desde esta ubicación central.

Solo los conjuntos de cifrado basados en RSA utilizan el HSM de red.

Después de instalar el cliente Thales nShield Connect en el sistema BIG-IP, las claves almacenadas en el HSM de Thales y los certificados correspondientes están disponibles para su uso con el Gestor® de Políticas de Acceso y el Gestor™ de Seguridad de Aplicaciones.

Para más información sobre el uso de Thales nShield Connect, consulte la página web de Thales: (https://www.thales-esecurity.com).

Nota: *Si vas a instalar Thales nShield Connect en un sistema BIG-IP que tendrá licencia para el modo Appliance, debes instalar el software Thales nShield Connect antes de licenciar el sistema BIG-IP para el modo Appliance.*

Requisitos previos para configurar Thales nShield Connect con sistemas BIG-IP

Antes de que puedas usar Thales nShield, conecta con el BIG-IP® Debes asegurarte de que estos requisitos estén en vigor:

- El dispositivo Thales nShield Connect está instalado en tu red.
  La dirección IP del cliente BIG-IP visible para el HSM de Thales está en la lista de clientes permitidos en el dispositivo Thales nShield Connect. Si estás implementando Thales nShield Connect con un sistema VIPRION®, necesitas añadir las direcciones IP de gestión del clúster y la dirección IP miembro del clúster para cada blade instalado en el chasis a la lista de permisos. Esto se aplica al uso de la red de gestión. Si usas una interfaz TMM con una dirección IP flotante, solo se requiere esa dirección IP.
  El servidor RFS está instalado. Esto podría ser un servidor externo en tu red o en el sistema local BIG-IP.
- El dispositivo Thales nShield Connect, el RFS y el sistema BIG-IP pueden iniciar conexiones entre sí a través del puerto 9004 (por defecto).
  Habéis creado el Mundo de la Seguridad de Thales (arquitectura de seguridad).
- El sistema BIG-IP está licenciado para "Interfaz Externa y HSM de Red."

Importante: *No puedes ejecutar el sistema BIG-IP con HSM internos y externos al mismo tiempo*

Nota: *BIG-IP TMOS con Thales HSM solo soporta IPv4.*

Además, antes de comenzar el proceso de instalación, asegúrate de poder localizar estos elementos en el DVD de instalación que viene con la unidad de hardware de Thales:

El software Thales Security World para Linux 64 bits

- El nShield_Connect_and_netHSM_User_Guide.pdf

Nota: *Para las versiones de cliente y HSM de Thales compatibles con información sobre versiones BIG-IP TMOS, consulte el documento suplementario de la Matriz de Interoperabilidad para BIG-IP TMOS con Thales y HSM disponible en AskF5.*

Instalación de componentes Thales nShield Connect en el sistema BIG-IP

Antes de poder configurar los componentes Thales nShield Connect en un sistema BIG-IP, debes obtener el CD ISO de Linux de 64 bits de Thales y copiar archivos del CD a ubicaciones específicas del sistema BIG-IP usando copia segura (SCP). F5 Networks ha probado estos pasos de integración con Thales Security World Software para Linux 64bit. Para preguntas sobre componentes de Thales, consulta con tu representante de Thales.

Puedes instalar archivos desde el CD ISO de 64 bits de Linux de Thales al sistema BIG-IP.

1. Inicia sesión en la interfaz de línea de comandos del sistema usando una cuenta con privilegios de administrador.
2. Crea un directorio bajo /shared llamado thales_install/amd64/nfast
   ```
   mkdir -p /compartido/thales_install/amd64/nfast
   ```
3. En el nuevo directorio, crea subdirectorios llamados ctls hwcrhk hwsp y pkcs11
4. Copia los archivos del CD y colócalos en los directorios especificados:

Archivo para copiar del CD	Ubicación para colocar archivo en BIG-IP
/Linux/LIBC6_3/AMD64/NoFast/CTLS/Aug.	/compartido/thales_install/amd64/nfast/ctls/agg.tar
/linux/libc6_3/amd64/nfast/hwcrhk/user.tar	/shared/thales_install/amd64/nfast/hwcrhk/user.tar
/linux/libc6_3/amd64/nfast/hwsp/agg.tar	/compartido/thales_install/amd64/nfast/hwsp/agg.tar
/linux/libc6_3/amd64/nfast/pkcs11/user.tar	/compartido/thales_install/amd64/nfast/pkcs11/user.tar

Antes de configurar el Sistema de Archivos Remoto (RFS) en el sistema BIG-IP, asegúrate de que el Thales nShield se conecte

Wagner Pena

Configuración del RFS en el sistema BIG-IP (opcional)

El dispositivo está instalado en tu red.

Nota: *Configurar el RFS en el sistema BIG-IP es opcional. Si el RFS se ejecuta en otro servidor de tu red, no necesitas realizar esta tarea.*

Si el RFS no está funcionando en otro servidor de tu red, necesitas configurar el RFS en el sistema BIG-IP.

1. Inicia sesión en la interfaz de línea de comandos del sistema BIG-IP usando una cuenta con privilegios de administrador.
2. Ejecuta el script para configurar el RFS.
   `nethsm-thales-rfs-install.sh --hsm_ip_addr=<`***`Thales_nShield Conectar dirección IP del dispositivo`***`> --rfs_interface=nombre` ***`de la interfaz <local`***
   Este ejemplo configura el RFS para que funcione en el sistema BIG-IP, donde la dirección IP del Thales nShield
   El dispositivo Connect tiene una dirección IP 192.27.13.59
   `nethsm-thales-rfs-install.sh --hsm_ip_addr=192.168.13.59 --rfs_interface=eth0`

   La opción de interfaz RFS es la interfaz que utiliza el BIG-IP para conectarse al HSM.

Después de configurar el RFS, debes configurar un Mundo de Seguridad antes de intentar conectarte a la IP BIG-como cliente

Configuración del cliente Thales nShield Connect en el sistema BIG-IP

Antes de configurar el cliente de Thales, asegúrate de que el cliente Thales nShield Connect esté instalado en el sistema BIG-IP y que el Mundo de la Seguridad esté configurado. Además, asegúrate de que el RFS esté instalado y configurado tanto en un servidor remoto como en el sistema BIG-IP de tu red.

Nota: *Si el cliente Thales nShield Connect estaba instalado en un sistema BIG-IP antes de que el RFS se instalara en la red, entonces debes reinstalar el cliente en el sistema BIG-IP*

Nota: *La dirección IP del sistema BIG-IP puede no ser la misma que la dirección IP del paquete saliente, como cuando un cortafuegos modifica la dirección IP*

Para usar el dispositivo Thales nShield Connect con el sistema BIG-IP, primero debes configurar el cliente de Thales en el sistema BIG-IP. Para que la inscripción funcione correctamente, la dirección IP del sistema BIG-IP debe ser cliente del HSM en red. En el caso del sistema VIPRION y la conexión a través de las interfaces de administración, cada blade y la dirección IP del chasis deben añadirse como un cliente. Configuras la dirección IP usando el panel frontal del dispositivo nShield Connect o empujando la configuración del cliente. Para detalles sobre cómo añadir, editar y visualizar clientes, consulta la documentación de Thales

Si configuras el cliente de Thales en un sistema VIPRION, ejecutas el script de configuración solo en la hoja primaria, y luego el sistema propaga la configuración a las blades activas adicionales.

1. Inicia sesión en la interfaz de línea de comandos del sistema BIG-IP usando una cuenta con privilegios de administrador.
2. Verifica que la interfaz F5 que vas a usar para comunicarte con el nShield Connect haya sido introducida en el panel frontal del HSM; es decir, el Thales nShield Connect debe permitir conexiones desde la IP fuente F5

Wagner Peña

dirección.

3. Configura el cliente Thales nShield Connect usando una de estas opciones:

   Opción 1: Configurar el cliente cuando el RFS esté remoto.

   ```
   nethsm-thales-install.sh
   --hsm_ip_addr=<nShield_Connect_device_IP_address>
   --rfs_ip_addr=<remote_RFS_server_IP_address>
   --rfs_username=<remote_RFS_server_username_for_SSH_login>
   ```

   El siguiente ejemplo establece el cliente donde el dispositivo Thales nShield Connect tiene una dirección IP `192.168.13.59` , el RFS remoto tiene una dirección IP `192.168.13.58` , el nombre de usuario para un inicio de sesión SSH en el RFS es root, y la interfaz cliente de Thales es la interfaz de gestión:

   ```
   nethsm-thales-install.sh --hsm_ip_addr=192.168.13.59 --rfs_ip_addr=192.168.12.58 -
   -rfs_username=raíz
   ```

   - Opción 2: Configurar el cliente cuando el RFS esté configurado en el sistema local BIG-IP:

     ```
     nethsm-thales-install.sh
     --hsm_ip_addr=<nShield_Connect_device_IP_address>
     --rfs_interface=<local_RFS_server_interface>
     ```

     El siguiente ejemplo configura el cliente donde el dispositivo Thales nShield Connect tiene una dirección IP `172.168.13.59` y el RFS se instala en el sistema BIG-IP usando la interfaz eth0:

     ```
     nethsm-thales-install.sh --hsm_ip_addr=172.168.13.59 --rfs_interface=eth0
     ```

     Además, el RFS instalado en el sistema BIG-IP puede usar la interfaz TMM (concretamente una VLAN):

     ```
     nethsm-thales-install.sh --hsm_ip_addr=10.20.20.1 --rfs_interface=<VLAN_name>
     ```

4. Recarga la variable de entorno PATH.
   Si vas a instalar el Thales nShield Connect en un sistema VIPRION, necesitas recargar la variable de entorno PATH en cualquier blade con sesiones ya abiertas: `source ~/.bash_profile`

5. Puedes usar el número predeterminado de hilos proporcionado, o especificar el número de hilos usando la opción num-threads. Esto también puede ajustarse más adelante usando tmsh

Configurar el cliente Thales nShield Connect en una hoja recién añadida o activada (opcional)

Después de configurar el cliente Thales nShield Connect en la hoja principal de un sistema VIPRION, el sistema propaga la configuración a las palas activas adicionales. Si posteriormente añades una hoja secundaria, activas una hoja desactivada o enciendes una hoja apagada, necesitas ejecutar un script en la nueva hoja secundaria.

1. Inicia sesión en la interfaz de línea de comandos del sistema usando una cuenta con privilegios de administrador.

2. Ejecuta este script en cualquier blade secundario nuevo o reactivado:
   `thales-sync.sh`

3. Si haces que el nuevo blade sea un blade principal antes de ejecutar el script de sincronización, necesitas ejecutar el procedimiento habitual de configuración del cliente solo en el nuevo blade principal.
   `nethsm-thales-install.sh`

Wagner Pena

Configuración del cliente Thales nShield Connect para múltiples HSM en un grupo HA

Antes de comenzar esta tarea, necesitas configurar el cliente Thales nShield Connect en el sistema BIG-IP. Puedes realizar estos pasos adicionales para configurar el cliente Thales nShield Connect para varios HSM.

1. Inicia sesión en la interfaz de línea de comandos del sistema usando una cuenta con privilegios de administrador.

2. Inscribe a cada HSM adicional en el grupo de Educación Alta.
   `/opt/nfast/bin/nethsmenroll --fuerza` ***`<HSM_ip_address>`*** `$(anonkneti` ***`<HSM_ip_address>`***
   Realiza este paso para cada uno de los HSM adicionales en el grupo HA. Para que la inscripción funcione correctamente, la dirección IP del sistema BIG-IP debe ser cliente de cada HSM en red. Configuras la dirección IP usando el panel frontal del dispositivo nShield Connect o empujando la configuración del cliente. Para detalles sobre cómo añadir, editar y visualizar clientes, consulta la documentación de Thales.

3. Actualiza los permisos.
   ```
   chmod 755 -R /opt/nfast/bin
   chown -R nfast:nfast /opt/nfast/kmdata/
   chmod 700 -R /opt/nfast/kmdata/tmp/nfpriv_root
   chown -R raíz:raíz /opt/nfast/kmdata/tmp/nfpriv_root
   ```

4. Verifica la instalación.
   `/opt/nfast/bin/consulta`
   Este comando muestra todos los módulos instalados que tienen el estado `Operativo` Nota: en este ejemplo, tres HSM están operativos.
   ```
   Servidor

   Modo de                 CB9E-745E-F901 A1D0-2DBE-AD98 5286-D07F-7601
   número de               operacional
   ```

5. Reiniciar el servicio pksc11
   `servicio de reinicio de tmsh pkcs11d`

6. Reinicia el servicio TMM.
   `TMSH Reiniciar el servicio de sistemas TMM`

7. Espera a que el TMM esté activo.

8. Verifica la instalación.
   `/opt/nfast/bin/consulta`

Configuración de opciones para una recuperación más rápida en un HSM de Thales en configuración HA
Thales recomienda que en una configuración de producción, salvo que haya una razón sólida para modificar estos ajustes, lo mejor sea usar los valores por defecto.

Cuando un HSM de Thales se desconecta en una configuración de HSM HA, el cambio al otro HSM ocurrirá tras el tiempo de fallo por conmutación. En otras palabras, los handshakes SSL fallarán entre el momento en que el HSM se cae y cuando ocurre el tiempo de fallo (90 segundos por defecto). Utiliza estos ajustes para configurar un tiempo de recuperación más rápido en caso de una interrupción en una configuración de HSM de HA.

Wagner Peña

expert IPX SRL RNC 130-850151 Santo Domingo, R.D.

1. Puedes reducir la configuración correspondiente editando la configuración de Thales en /opt/nfast/kmdata/config/config. La guía de usuario de Thales tiene una explicación detallada de lo que hace cada configuración.

2. Si quieres ajustes moderados de recuperación, usa la configuración de ejemplo que aparece a continuación.

```
[server_settings]
connect_retry=3
connect_keepalive=4
connect_broken=10
connect_command_block=15
```

3. Si quieres configuraciones muy ajustadas, usa la configuración de ejemplo que aparece a continuación.

   Importante: *Estos ajustes pueden hacer que un módulo se marque como fallido cuando hay un pequeño fallo de red del que puede recuperarse.*

```
[server_settings]
connect_retry=1
connect_keepalive=10
connect_broken=1
connect_command_block=0
```

Configuración para una recuperación más rápida en un HSM Thales en configuración HA
Estos son los ajustes de Thales que te ayudarán a limitar el tiempo en que fallarán las conexiones SSL. Thales recomienda que en una configuración de producción, salvo que haya una razón sólida para modificar estos ajustes, lo mejor sea usar los valores por defecto.

Nombre del escenario	Descripción Configuración	Predeterminado Configuración	moderado tado	Muy apre
connect_retry	Este campo especifica el número de segundos que hay que esperar antes de intentar de nuevo una conexión remota a un HSM de red cliente.	10	3	
connect_broken	Este campo especifica el número de segundos de inactividad permitidos antes de que se declare roto una conexión a un HSM de red cliente.	90	10	
connect_keepalive	Este campo especifica el número de segundos entre paquetes keepalive para conexiones remotas a un HSM de red cliente.	10	4	10
connect_command_block	Cuando un NetHSM ha fallado, este campo especifica el número de segundos que el servidor duro debe esperar antes de fallar los comandos dirigidos a ese netHSM con un mensaje de NetworkError. Para que los comandos tengan posibilidades de éxito después de que un netHSM haya fallado, este valor debería ser mayor que el de connect_retry. Si está configurado en 0, los comandos a un netHSM fallan con ErrorNetworkError inmediatamente, tan pronto como falla el NetHSM.	35	15	0

Índice | Próximo capítulo >>

Contacta con el soporte

¿TIENES ALGUNA PREGUNTA?

Soporte y > de ventas

SÍGUENOS

Wagner Pastor

SOBRE F5	EDUCACIÓN	SITIOS F5	TAREAS DE APOYO
Formación en Información Corporativa		F5.com	Leer políticas de soporte
Carreras en	Certificación	Portal de	Crear solicitud
Relaciones con	F5 University	soporte	de servicio
Inversores en	Formación online gratuita	DevCentral	Deja comentarios [+]
Redacción		Partner Central	
Acerca de AskF5		F5 Labs	

Wagner Peña

IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Capítulo del manual : Uso de la gestión de luces apagadas

Aplica a:

Mostrar versiones

Índice | << Capítulo anterior | Capítulo siguiente >>

7

Uso de la gestión de luces apagadas

Presentamos la gestión de apagado de luces

Acceso al menú de comandos

Presentamos la gestión de apagado de luces

Las plataformas más recientes de F5 Networks incluyen un sistema de gestión remota . Este sistema permite gestionar de forma remota ciertos aspectos del funcionamiento de la plataforma y del sistema BIG-IP® en caso de que el software de gestión de tráfico quede inhabilitado.

El sistema de gestión de apagado de luces consta de los siguientes elementos.

- Procesador de control de tarjeta de conmutación (SCCP):
  El hardware que proporciona el control de hardware sobre toda la unidad.
- Shell de consola del host (hostconsh).
  El shell que proporciona acceso al menú de comandos.
- Menú de comandos.
  El menú que contiene las opciones para la gestión del modo de apagado de luces.
- Sistema operativo de gestión de tráfico (TMOS).
  El software que configura para gestionar el tráfico de su sitio web.
- Comandos de gestión fuera de banda.
  Estos comandos permiten controlar diversos aspectos del sistema mediante una serie de pulsaciones de teclas.

El menú de comandos funciona independientemente del sistema operativo de gestión de tráfico a través del puerto de gestión, la consola del puerto serie y de forma remota a través de los puertos de gestión de tráfico.

Puede utilizar el menú de comandos para reiniciar la unidad, incluso si el sistema de gestión de tráfico BIG-IP se ha bloqueado.

Puede configurar remotamente una unidad para que arranque desde la red para reinstalar el software desde una imagen ISO.

Puedes obtener acceso a la consola del propio sistema de gestión de tráfico BIG-IP, de modo que puedas configurarlo desde la interfaz de línea de comandos.

341

El sistema de gestión de apagado automático y el sistema de gestión de tráfico BIG-IP funcionan de forma independiente dentro de la unidad de hardware. La figura 7.1 muestra la relación entre el sistema de gestión de apagado automático y el sistema de gestión de tráfico.

El sistema de gestión de apagado de luces es accesible a través de la interfaz de gestión (número 1 en la figura 7.1) y el puerto de consola (número 2 en la figura 7.1). Esta funcionalidad es independiente del sistema de gestión de tráfico (número 3 en la figura 7.1).

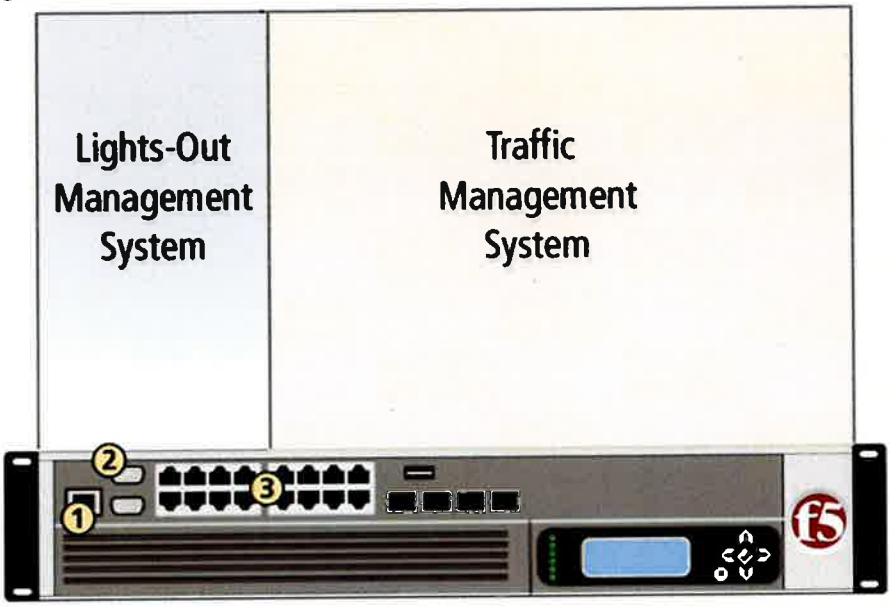


Figura 7.1 Interfaces del sistema de gestión de apagado de luces y del sistema de gestión de tráfico

Acceso al menú de comandos

Puede acceder al menú de comandos a través de la consola del host (hostconsh) mediante la consola serie del panel frontal, o de forma remota mediante SSH. La siguiente sección describe cómo acceder al menú de comandos tanto a través de la consola serie como con un cliente SSH a la interfaz de administración.

Opciones para acceder al menú de comandos

Existen dos métodos para acceder al menú de comandos: desde la consola serie o desde un cliente SSH a la interfaz de administración.

Para acceder al menú de comandos desde la consola serie

Desde la consola serie conectada al puerto CONSOLE, escriba la siguiente secuencia de teclas.

Esc (

Se abre el menú de comandos.

Para obtener detalles sobre cada opción del menú de comandos, consulte Uso del menú de comandos .

Para acceder al menú de comandos mediante SSH

Antes de poder acceder al menú de comandos mediante SSH, también debe tener configurada una dirección IP para la administración remota sin supervisión. Para obtener más información, consulte Configuración del acceso SSH remoto sin supervisión .

1. Abra el cliente SSH en una estación de trabajo de administración conectada al puerto MGMT en la plataforma 4300.
2. Escriba el siguiente comando, donde <IP addr> es la dirección IP que configuró para el sistema de apagado automático. Se abrirá la consola del host.

consola ssh@<dirección IP>

3. Para abrir el menú de comandos, escriba la siguiente secuencia de teclas.

Esc (

Para obtener detalles sobre cada opción del menú de comandos, consulte Uso del menú de comandos .

Configuración del acceso SSH remoto sin necesidad de iluminación

Puede usar el menú de comandos para configurar el acceso SSH remoto al sistema BIG-IP. Para configurar el acceso remoto, ejecute la utilidad de configuración de red SCCP para configurar una dirección IP, una máscara de red y una puerta de enlace para el sistema remoto. La conexión remota con el cliente SSH solo se puede realizar a través de la red de administración conectada al puerto de administración (MGMT).

Para configurar el acceso remoto SSH en modo apagado

1. Inicie sesión en el sistema a través de la consola serie.
2. Escriba la siguiente secuencia de teclas.

Esc (

3. Después de que se abra el menú de comandos, escriba N. Esto inicia la utilidad de configuración de red para SCCP.
4. Agregue una dirección IP, una máscara de red y una puerta de enlace en la red de administración.

Utilizando comandos de gestión fuera de banda

La consola del host implementa un subconjunto del protocolo de administración fuera de banda estándar de Microsoft® . Estos comandos permiten administrar el procesador del host mediante una serie de combinaciones de teclas. La tabla 7.1 muestra las combinaciones de teclas disponibles.

Tabla 7.1 Combinaciones de teclas de gestión fuera de banda

Combinación de teclas	Resultado
Esc + R + Esc + r + Esc + R	Puede usar esta secuencia durante el modo de transferencia directa para reiniciar la plataforma. No recomendamos usar este método para reiniciar la plataforma.
Esc (	Abre el menú de comandos.

Utilizando el menú de comandos

El menú de comandos proporciona las opciones de gestión de apagado del sistema (ver Figura 7.2).

Figura 7.2 Vista de la consola del menú de comandos del procesador host

```
1 --- Conectar con la consola del subsistema host
2 --- Seleccione el modo de arranque del subsistema host: arrancar desde la unidad local
3 --- Seleccione el modo de arranque del subsistema host: arranque de red desde SCCP
4 --- Seleccione el modo de arranque del subsistema host: arranque de red desde un servidor
externo
5 --- Reiniciar el subsistema host (envía el comando de reinicio)
6 --- Detener el subsistema del host (envía el comando de detención)
7 --- Restablecer el subsistema host (emite un reinicio de hardware; ¡ÚSELO CON
PRECAUCIÓN!)
8 --- Reiniciar el subsistema SCCP (emite un reinicio del hardware; ¡ÚSELO CON
PRECAUCIÓN!)
9 --- Detener el subsistema SCCP (provoca el apagado del hardware - ¡ÚSELO CON
PRECAUCIÓN!)
B --- Configurador de velocidad de transmisión SCCP
L --- Inicio de sesión SCCP
N --- Configurador de red SCCP
```

Cada una de estas opciones se describe en la Tabla 7.2 . Tenga en cuenta que algunos de estos comandos no están destinados al uso por parte de los usuarios finales. La Tabla 7.2 también especifica qué comandos no se recomiendan para su uso.

Tabla 7.2 Opciones del menú de comandos

Opción	Descripción
1	Sale del menú de comandos y regresa al modo de emulación de terminal.
2	Configura el sistema operativo de gestión de tráfico BIG-IP® (TMOS) para que arranque desde el disco duro local o la tarjeta CompactFlash.
3	Configura el subsistema host para que arranque desde el procesador del subsistema host. Esta opción solo se utiliza para pruebas de fábrica.
4	Configura SCCP para que arranque el procesador host desde un servidor externo conectado a la interfaz de red de administración. Esta opción permite iniciar el proceso de instalación PXE de forma remota.
5	Reinicia el subsistema host. En este caso, se reinicia el sistema operativo de gestión de tráfico BIG-IP® (TMOS) .

6	Detiene el subsistema host. En este caso, se detiene el sistema operativo de gestión de tráfico BIG-IP® (TMOS) .
7	Reinicia el subsistema host. En este caso, el sistema se reinicia mediante un reinicio por hardware.
8	Reinicia el procesador de control de la tarjeta de conmutación (SCCP). Esto reinicia toda la unidad.
9	Detiene el procesador de control de la tarjeta de conmutación (SCCP). Esto apaga toda la unidad.
B	Ejecuta la utilidad de configuración de velocidad de transmisión del procesador de control de la tarjeta de conmutación (SCCP) . Esta utilidad permite configurar la velocidad y los parámetros de la comunicación serie del SCCP. Esta opción solo está disponible a través de la consola serie del panel frontal.
L	Muestra una solicitud de inicio de sesión para el subsistema del procesador de control de la tarjeta de conmutación (SCCP). Este subsistema no puede ser configurado por los usuarios finales. Esta opción solo está disponible a través de la consola serie del panel frontal.
norte	Ejecuta la utilidad de configuración de red del procesador de control de la tarjeta de conmutación (SCCP) . Esta utilidad permite reconfigurar la dirección IP, la máscara de red y la puerta de enlace predeterminada que utiliza el SCCP. Si modifica estos ajustes, se desconectará su sesión. Esta opción solo está disponible a través de la consola serie del panel frontal.

Importante: No recomendamos utilizar la opción de reinicio (opción 7) en circunstancias normales. No permite un apagado correcto de la plataforma 4300.

Índice | << Capítulo anterior | Capítulo siguiente >>

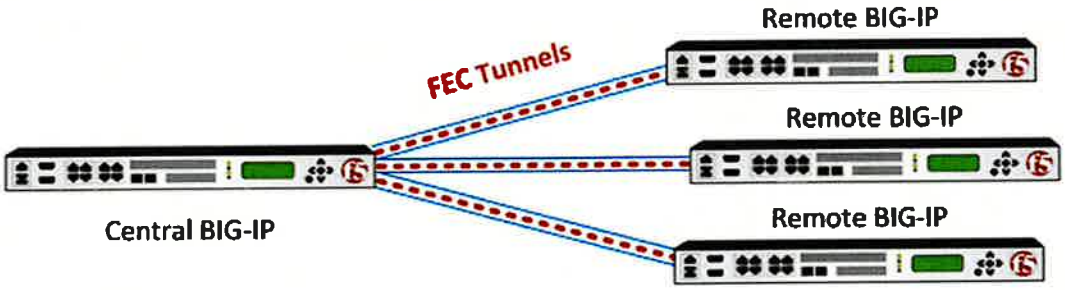
Contacta con el servicio de asistencia

¿TIENES ALGUNA PREGUNTA? Soporte y ventas > **SÍGANOS**

346

Wagner Pena

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.



Además de configurar la corrección de errores hacia adelante (FEC) entre dos sistemas BIG-IP, puede configurarla entre un cliente perimetral y un sistema BIG-IP que tenga licencia de Access Policy Manager®licenciado. Consulte la documentación de Access Policy Manager (APM®) para obtener información sobre la configuración de la implementación del acceso del cliente.

Nota:*Antes de poder configurar la corrección de errores hacia adelante (FEC), debe tener licenciado y aprovisionado Application Acceleration Manager (AAM™).*

Acerca de la corrección de errores hacia adelante (FEC)

Corrección de errores hacia adelante (FEC)es una técnica de aceleración para todo tipo de tráfico, incluido el tráfico TCP y UDP en redes con pérdidas. FEC controla los errores de transmisión de datos en canales de comunicación poco fiables o ruidosos. Con EC, el remitente codifica los mensajes con un código de corrección de errores (ECC) adicional. La redundancia permite al receptor detectar un número limitado de errores que podrían ocurrir en cualquier parte del mensaje y, a menudo, corregir estos errores sin retransmisión.

La pérdida de paquetes se produce cuando uno o más paquetes que viajan a través de una red no llegan a su destino. La pérdida de paquetes puede ser causada por una serie de factores que inevitablemente dan lugar a problemas de rendimiento muy notables, en particular con protocolos en tiempo real, tecnologías de transmisión, voz sobre IP, juegos en línea y videoconferencias. Algunos Los protocolos de transporte de red, como TCP, proporcionan una entrega confiable de paquetes. En caso de pérdida de paquetes, el receptor puede solicitar la retransmisión o el emisor reenvía automáticamente cualquier segmento que no haya sido confirmado. Aunque TCP puede recuperarse de la pérdida de paquetes, la retransmisión de paquetes faltantes provoca una disminución del rendimiento general de la conexión. La corrección de errores se produce sin necesidad de un canal inverso para solicitar la retransmisión de datos, pero a costa de un ancho de banda fijo y mayor del canal directo. Por lo tanto, la FEC es más útil en situaciones donde las retransmisiones son costosas o imposibles.

Resumen de tareas

El BIG-IP®El sistema gestiona la corrección de errores hacia adelante según los parámetros del perfil FEC que seleccione al crear un túnel FEC. Si el perfil FEC proporcionado por el sistema no satisface las necesidades de su red, puede personalizarlo. Por ejemplo, si sabe que la mayor parte del tráfico no es compresible, puede desactivar la compresión LZO. El perfil FEC proporcionado por el sistema tiene habilitada la configuración adaptativa, lo que significa que ajusta el número de paquetes de origen y reparación según las condiciones del tráfico de red. Esta función es particularmente útil en condiciones inestables. Si las condiciones de su red son estables, puede ajustar el perfil FEC en consecuencia.

Nota:*Si utiliza iSession™ con FEC, desactive la compresión en la conexión iSession o en el perfil FEC que seleccione para el túnel FEC.*

Lista de tareas

Personalización de un perfil FEC

Puede personalizar los parámetros de mitigación de pérdida de paquetes FEC para ajustarlos a las condiciones de su red.

. En la pestaña Principal, haga clic en**red>Túneles>perfiles>EC>Crear** Se abre la pantalla Nuevo perfil FEC.

. en el**nombre**campoescriba un nombre único para el perfil.

. de la**lista Perfil predeterminado**seleccione un perfil. Hay un perfil predeterminado,**ec**disponible.

348

. Seleccione la**Personalizado**casilla de verificación.

. Modifique la configuración, según sea necesario.

. Haga clic en**finalizado**

Este perfil FEC ahora está disponible para aplicarse a un túnel FEC.

Para aplicar este perfil FEC al tráfico entre BIG-IP®sistemas, debe seleccionarlo de la**Tipo de encapsulación**lista en la pantalla de Inicio rápido de aceleración, la pantalla de punto final local de optimización simétrica o la pantalla Nuevo túnel.

Creación de un túnel FEC para recibir tráfico

Puede configurar un túnel FEC en un dispositivo BIG-IP para recibir solicitudes de conexión FEC desde un dispositivo BIG-IP remoto.

. En la pestaña Principal, haga clic en**red>Túneles>Lista de túneles>Crear** Se abre la pantalla Nuevo túnel.

. en el**nombre**campocampo, escriba un nombre único para el túnel.

. de la**Tipo de encapsulación**lista, seleccione**fec**
Esta configuración le indica al sistema qué perfil de túnel usar. El perfil proporcionado por el sistema**fec**está configurado para un comportamiento adaptativo para la cantidad de paquetes de origen y reparación. Si crea un nuevo perfil FEC con configuraciones personalizadas, el perfil aparecerá en esta lista, donde podrá seleccionarlo.

. en el**Dirección local**campocampo, escriba la dirección IP del punto final local
Si está utilizando una conexión iSession, use la misma dirección IP que usó para el extremo local de iSession. De lo contrario, use cualquier dirección IP propia en el sistema BIG-IP.

. o la**Dirección remota**lista, conserve la selección predeterminada,**Cualquiera**

. Haga clic en**finalizado**

Ahora tiene un túnel configurado para recibir tráfico FEC de cualquier sistema BIG-IP que tenga un túnel FEC configurado con la dirección IP del sistema local especificada como la**Dirección remota**

Si también desea iniciar tráfico a través de un túnel FEC desde el sistema BIG-IP local, debe crear un túnel FEC con la dirección IP específica de un sistema BIG-IP remoto que esté configurado para recibir tráfico FEC.

Creación de un túnel FEC para iniciar tráfico

Puede configurar un túnel FEC entre dispositivos BIG-IP®para usar la corrección de errores hacia adelante para mitigar la pérdida de datos durante la transmisión.

. En la pestaña Principal, haga clic en**red>Túneles>Lista de túneles>Crear** Se abre la pantalla Nuevo túnel.

. en el**nombre**campocampo, escriba un nombre único para el túnel.

. de la**Tipo de encapsulación**lista, seleccione**fec**
Esta configuración le indica al sistema qué perfil de túnel usar. El perfil proporcionado por el sistema**fec**El perfil está configurado para

un comportamiento adaptativo para la cantidad de paquetes de origen y reparación. Si crea un nuevo perfil FEC con configuración personalizada, el perfil aparecerá en esta lista, donde podrá seleccionarlo.

. en el**Dirección local**campocampo, escriba la dirección IP del punto final local
Si está utilizando una conexión iSession, use la misma dirección IP que usó para el extremo local de iSession. De lo contrario, use cualquier dirección IP propia en el sistema BIG-IP.

. de la**Dirección remota**lista, seleccione**Especifique**y escriba la dirección IP del dispositivo BIG-IP en el otro extremo del túnel.

. Haga clic en**finalizado**

Ahora tiene un túnel que puede transmitir tráfico FEC al sistema BIG-IP especificado por la dirección IP remota, siempre que el otro sistema BIG-IP tenga un túnel FEC abierto para recibir transmisiones FEC.

Si también desea recibir tráfico a través de un túnel FEC desde el otro sistema BIG-IP, debe crear un túnel FEC con una dirección IP no definida

Visualización de estadísticas del túnel FEC

Puede ver las estadísticas a nivel de paquete para los túneles FEC que ha creado.

. Acceda a la utilidad de línea de comandos tmsh.

. En el símbolo del sistema, escriba**tmsh show /net tunnels fec-stat all-properties.**
La siguiente lista es un ejemplo de los resultados de este comando.

et::FEC Tunnel

ame	Profile	Out pkts Raw	Out bits Raw	Out pkts Rdnt	Out bits Rdnt
0.10.10.2	fec_1	51.5K	30.1M	19.3K	28.2M

In pkts Raw	In bits Raw	In pkts Rdnt	In bits Rdnt	In pkts Rdnt Lost
97.4K	1.1G	152.4K	1.7G	864

In pkts Raw Lost	Rmt In Rdnt Pkts	Rmt In Raw Pkts	Rmt In Rdnt Lost	Rmt In Pérdida de datos sin procesar
613	18.2K	48.6K	28	63

Tabla de contenido << Capítulo anterior Capítulo siguiente >>

Soporte de contacto

¿TIENES ALGUNA PREGUNTA?

Soporte y ventas>

SÍGUENOS

RECURSOS DOCUMENTOS TÉCNICOS

La escalabilidad DNS inteligente de F5

Arquitectura de referencia

Introducción

El Sistema de Nombres de Dominio (DNS) se creó en 1983 para permitir que las personas identificaran fácilmente todos los ordenadores, servicios y recursos conectados a Internet por nombre, en lugar de por dirección de Protocolo de Internet (IP), una cadena de información binaria imposible de memorizar.

Un servidor DNS traduce los nombres de dominio que escribe en un navegador a una dirección IP, lo que permite que su dispositivo encuentre el servicio o sitio que busca en Internet.

Podría decirse que la principal tecnología que permite Internet, el DNS es También es uno de los componentes más importantes en la infraestructura de red. Además de entregar contenido y aplicaciones, NS también administra una arquitectura distribuida y redundante para garantizar una alta disponibilidad y un tiempo de respuesta rápido para el usuario; por lo tanto, es fundamental contar con una infraestructura DNS disponible, inteligente, segura y escalable. Si el DNS falla, la mayoría de las aplicaciones web dejarán de funcionar correctamente, lo que afectará a su negocio y a su marca.

La arquitectura de referencia de escalabilidad DNS inteligente de extremo a extremo de 5 permite a las organizaciones construir una base DNS sólida que maximiza los recursos y aumenta la administración de servicios, al tiempo que se mantiene lo suficientemente ágil como para admitir arquitecturas de red, dispositivos y aplicaciones existentes y futuras.

Los servicios NS son fundamentales para la disponibilidad

Cuando un usuario solicita una página web, esa solicitud se pasa a un servidor DNS local, que a su vez se comunica con los servidores DNS principales. Todo funciona bien hasta que un aumento repentino del tráfico o un atacante inunda el servidor con solicitudes de consulta DNS. Si su servidor DNS principal se sobrecarga, dejará de responder, lo que puede hacer que su sitio web no esté disponible

353

Las fallas de DNS representan el 41 por ciento del tiempo de inactividad de la infraestructura web, por lo que es esencial mantener su DNS disponible. Según una encuesta de Aberdeen Group, las organizaciones pierden un promedio de $138,000 por cada hora que sus centros de datos están inactivos. El tiempo de inactividad afecta negativamente a los clientes, puede generar pérdida de ingresos e incluso puede afectar a los empleados que intentan acceder a los recursos corporativos, como el correo electrónico.

Por eso, la importancia de una base sólida de DNS no puede ser exagerada. Sin ella, es posible que sus clientes no puedan acceder a su contenido y aplicaciones cuando lo deseen, y si no pueden obtener lo que quieren de usted, probablemente irán a otro lugar.

Problemas de remo

Hay muchas razones por las que los requisitos de DNS están creciendo tan rápidamente. En los últimos cinco años, el número de usuarios de Internet ha crecido un 82 por ciento; el número de sitios web ha crecido de aproximadamente 580 millones a 1.240 millones y el número de consultas DNS ha crecido en más del 100 por ciento.

Además, el número de conexiones móviles en uso creció en 2.2 millones y casi el 60 por ciento de los usuarios de la web dicen que esperan que un sitio web se cargue en su teléfono móvil en tres segundos o menos

Las organizaciones están experimentando un rápido crecimiento en términos de aplicaciones, así como en el volumen de tráfico que accede a ellas. Además, las propias aplicaciones web están creciendo y volviéndose cada vez más complejas. Cada icono, URL y fragmento de contenido incrustado en una página web requiere una consulta DNS. Cargar sitios complejos puede requerir cientos de consultas DNS, e incluso las aplicaciones sencillas para teléfonos inteligentes pueden requerir numerosas consultas DNS solo para cargarse.

En los últimos cinco años, el volumen de consultas DNS para direcciones .com y .net se ha duplicado con creces, aumentando a una carga de consulta diaria promedio de 124 mil millones en el primer trimestre de 2016. En el mismo

354

En ese período, se agregaron más de 10 millones de nombres de dominio a Internet. Se espera que el crecimiento futuro ocurra a un ritmo aún más rápido a medida que se implementen más soluciones en la nube.

Problemas de seguridad

Si bien el DNS es la columna vertebral de Internet (responde a todas las consultas y resuelve todos los números para que puedas encontrar tus sitios favoritos), también es uno de los puntos más vulnerables de tu red. Debido al papel crucial que desempeña, el DNS es un objetivo de alto valor para los atacantes.

Los ataques DDoS al DNS pueden inundar tus servidores DNS hasta el punto de falla o secuestrar y redirigir las solicitudes a un servidor malicioso. Para prevenir esto, se debe integrar en la red una arquitectura DNS distribuida, segura y de alto rendimiento, junto con capacidades de descarga de DNS

Generalmente, las organizaciones tienen un conjunto de servidores DNS, cada uno capaz de manejar hasta 150,000 consultas DNS por segundo. Los servidores DNS de alto rendimiento pueden manejar alrededor de 200,000 consultas por segundo. Los ciberdelincuentes pueden superar fácilmente esas tasas, como lo demuestran las interrupciones del DNS que afectaron a Dyn, The New York Times, LinkedIn, Network Solutions y Twitter.

Para abordar los picos de DNS y los ataques DDoS de DNS, las empresas agregan más servidores DNS, que realmente no son necesarios durante las operaciones comerciales normales. Esta costosa solución también suele requerir intervención anual para realizar cambios. Además, los servidores DNS tradicionales requieren mantenimiento y parches frecuentes, principalmente para nuevas vulnerabilidades.

La solución tradicional

Al buscar soluciones DNS, muchas organizaciones eligen BIND (Berkeley Internet Naming Daemon), el solucionador DNS original de Internet. Instalado en aproximadamente el 80 por ciento de los servidores DNS del mundo, BIND es un proyecto de código abierto mantenido por Internet Systems Consortium (ISC). ISC es una organización sin fines de lucro organización con una rama de consultoría con fines de lucro llamada DNS-CO,

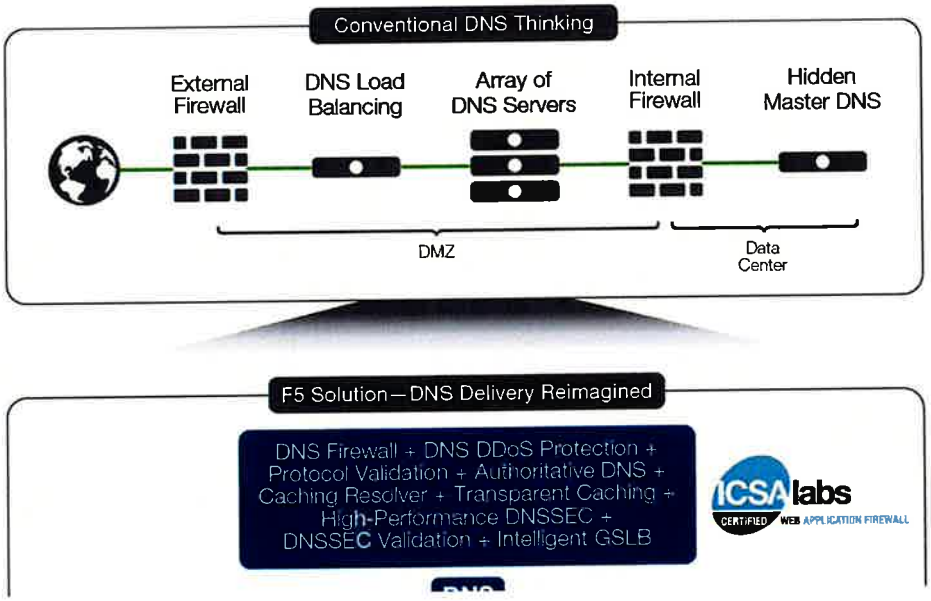
que ofrece 4 niveles diferentes de suscripción y servicios de soporte.

A pesar de su popularidad, BIND requiere un mantenimiento significativo varias veces al año, principalmente debido a vulnerabilidades, parches y actualizaciones. Se puede descargar gratuitamente, pero necesita servidores (un costo adicional, incluidos los contratos de soporte) y un sistema operativo. Además, BIND normalmente escala a solo 50,000 respuestas por segundo (RPS), lo que lo hace vulnerable a picos de DNS legítimos y maliciosos.

Soluciones para un panorama cambiante

La arquitectura de referencia F5 Intelligent DNS Scale proporciona una forma más inteligente de responder y escalar a las consultas DNS y tiene en cuenta una variedad de condiciones y situaciones de red para distribuir las solicitudes de aplicaciones de usuario y los servicios de aplicaciones según las políticas comerciales, las condiciones del centro de datos, las condiciones de la red y el rendimiento de las aplicaciones.

En lugar de preocuparse por las interrupciones de DNS y comprar infraestructura DNS adicional para combatir los picos, puede instalar un dispositivo BIG-IP 5 en la DMZ de su red y dejar que maneje las solicitudes en nombre de su servidor DNS principal.



Escalado bajo demanda

IG-IP DNS hiperescala a 100 millones de RPS, lo que significa que incluso grandes picos de solicitudes DNS (incluidas las maliciosas) no interrumpirán su contenido ni afectarán la disponibilidad de aplicaciones críticas.

Sus administradores de red pueden estar más tranquilos, sabiendo que su sitio responderá a todas las consultas DNS y permanecerá disponible incluso durante un ataque. Su marca está protegida y su empresa puede evitar una noticia vergonzosa en primera plana.

Mejore la disponibilidad con BIG-IP DNS

La arquitectura de referencia F5 Intelligent DNS Scale ayuda a garantizar que sus aplicaciones y contenido estén disponibles continuamente para sus usuarios. Una de las piezas más importantes de esta arquitectura es la función de respuesta de consulta DNS Express, diseñada específicamente para BIG-IP DNS, que administra las consultas DNS autorizadas transfiriendo zonas del servidor DNS primario a su propia RAM.

BIG-IP DNS solo tiene que abrir el paquete de consulta DNS una vez, siempre que la solicitud sea para una dirección que se encuentre en la zona que se transfirió a DNS Express, lo que simplifica el proceso y mejora significativamente el rendimiento y los tiempos de respuesta de su arquitectura NS.

Con DNS Express, el núcleo individual de cada dispositivo BIG-IP puede responder aproximadamente de 125,000 a 200,000 solicitudes por segundo, escalando a más de 50 millones de consultas RPS, más de 12 veces la capacidad de un servidor DNS primario típico.

La plataforma BIG-IP: su firewall en la DMZ

Cada dispositivo BIG-IP cuenta con la certificación de ICSA Labs como firewall de red

Al evaluar de forma inteligente la reputación de los hosts de Internet, el dispositivo IG-IP puede evitar que los atacantes desconecten su DNS con un ataque DDoS, roben datos, comprometan los recursos corporativos o interrumpan su negocio de cualquier otra forma.

Además, DNSSEC puede proteger su infraestructura DNS, incluidas las implementaciones en la nube, de ataques de envenenamiento de caché y secuestros de dominio. Con la compatibilidad con DNSSEC, puede firmar digitalmente y respaldar su consulta DNS con respuestas cifradas, lo que permite al solucionador determinar la autenticidad de la respuesta y evitar el secuestro de DNS y el envenenamiento de caché. El servicio de inteligencia IP de F5 mejora su seguridad general al denegar el acceso a direcciones IP que se sabe que están infectadas con malware, en contacto con puntos de distribución de malware y con mala reputación.

Servicios NS en el borde de la red

La arquitectura de referencia de escalado de DNS inteligente de F5 también ayuda a mantener su contenido y aplicaciones disponibles al responder a las consultas NS desde el borde de la red, en lugar de desde lo profundo de su infraestructura crítica. Cuando descarga las respuestas DNS a la plataforma BIG-IP, las solicitudes no llegan al backend de su red, lo que aumenta en gran medida su capacidad de escalar y responder a los picos de DNS, además de proteger su infraestructura DNS

Wagner Patria

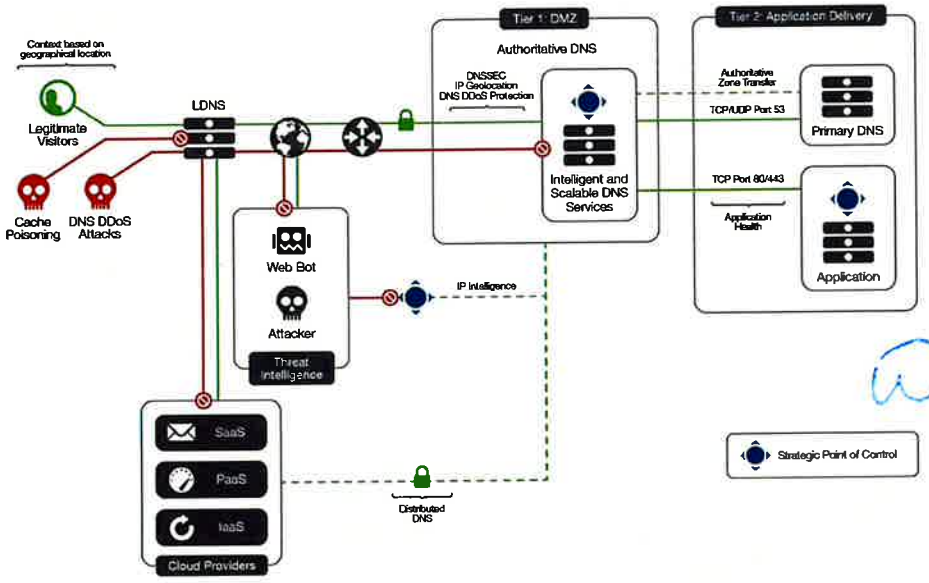
Al aumentar la velocidad, la disponibilidad, la escalabilidad y la seguridad de su infraestructura DNS, la arquitectura de referencia F5 Intelligent DNS Scale garantiza que sus clientes y sus empleados puedan acceder a sus servicios críticos de web, aplicaciones y bases de datos siempre que los necesiten.

DNS distribuido

Esto también se aplica a las implementaciones en la nube o a las infraestructuras donde el DNS está distribuido. Las organizaciones pueden replicar su infraestructura DNS de alto rendimiento en casi cualquier entorno. Ellas

Puede tener DNS en la nube para recuperación ante desastres/continuidad del negocio, o incluso un servicio de DNS en la nube con zonas DNSSEC firmadas. La compatibilidad mejorada con AXFR de los servicios DNS de F5 ofrece transferencias de zona desde un dispositivo IG-IP a cualquier servicio DNS, lo que permite a las organizaciones replicar DNS en entornos físicos, virtuales y en la nube. El servicio de replicación NS se puede enviar a otros dispositivos BIG-IP u otros servidores DNS generales en centros de datos o nubes que estén más cerca de los usuarios.

Además, las organizaciones pueden enviar a los usuarios a un sitio que les brinde la mejor experiencia. Los servicios DNS de BIG-IP utilizan una variedad de métodos de equilibrio de carga y monitoreo inteligente para cada aplicación y usuario específicos. El tráfico se enruta de acuerdo con su negocio políticas, así como con las condiciones actuales de la red y del usuario. Los servicios NS de BIG-IP incluyen una base de datos de geolocalización precisa y granular, lo que le brinda control de la distribución del tráfico según la ubicación del usuario.



IG-IP DNS y servicios DNS

IG-IP DNS es una solución DNS global que proporciona servicios de nombres en el límite de sus redes de acceso y entrega de servicios. Al emplear servicios de ubicación geográfica, puede dirigir a los usuarios al centro de datos de entrega de servicios más cercano según su ubicación física.

IG-IP DNS proporciona los siguientes servicios de nombres:

Servicios NS en el límite de la red para todos los servicios internos y externos

Servicios de geolocalización para una precisión milimétrica en la entrega de aplicaciones o servicios según la ubicación del usuario móvil.

El servicio IP Intelligence protege las infraestructuras al detectar y detener el acceso desde direcciones IP asociadas con actividad maliciosa.

Un único punto de control para la gestión de todos los servicios de nombres globales y locales.

Soluciones adicionales de servicios inteligentes de BIG-IP, como la entrega global de aplicaciones, la aplicación de políticas, la traducción NAT64 y DNS64, los monitores de estado y el lenguaje de scripting F5, Rules.

Compatibilidad con servicios DNS globales

Integración con DNS iRules para decisiones DNS granulares y la entrega del mismo servicio.

Compatibilidad con protocolos específicos del proveedor de servicios, como las solicitudes NUM para transacciones SIP.

Servicios IG-IP LTM y DNS

Dentro del centro de datos, BIG-IP Local Traffic Manager (LTM) puede garantizar que sus aplicaciones y contenido permanezcan altamente disponibles mediante la creación de una arquitectura tolerante a fallos desde el borde móvil hasta el servicio. Además de proporcionar alta disponibilidad, IG-IP LTM también admite aplicaciones específicas del proveedor de servicios, como el equilibrio de carga de las solicitudes ENUM para transacciones SIP.

Las soluciones IG-IP LTM para servicios de nombres incluyen:

360

Integración con BIG-IP DNS para extender los servicios de nombres enriquecidos al centro de datos local y la red de servicios.

Compatibilidad con el equilibrio de carga tanto para DNS local como para NS recursivo.

Compatibilidad con protocolos específicos del proveedor de servicios, como las solicitudes NUM para transacciones SIP.

Monitores de estado transparentes para evaluar el estado del servicio antes de enviar usuarios al servicio. BIG-IP LTM puede transmitir información de estado a BIG-IP DNS para llevar el conocimiento de la aplicación al borde de la SDN.

Integración con iRules para decisiones de DNS granulares y entrega de servicios de nombres.

Implementación de una infraestructura completa de entrega de servicios

La arquitectura de referencia de escalado de DNS inteligente de F5 se ajusta para Aplicaciones de alta disponibilidad y gran volumen, que admiten simultáneamente millones de solicitudes de usuario por segundo. Funcionan junto con otras funciones de entrega de servicios de BIG-IP, como el lenguaje de scripting iRules, la aplicación transparente y otros servicios relacionados con IP para crear una infraestructura completa de entrega de servicios: la red de entrega de servicios F5. La escalabilidad y la flexibilidad sin problemas se logran aprovechando la plataforma inteligente de entrega de servicios común a todos los dispositivos BIG-IP.

Conclusión

y utilizando la arquitectura de referencia F5 Intelligent DNS Scale, las organizaciones pueden:

aumentar la velocidad, la disponibilidad, la escalabilidad y la seguridad de su infraestructura DNS.

361

reducir la complejidad y el costo al eliminar servidores DNS adicionales innecesarios.

disfrutar de la tranquilidad de saber que su sitio responderá a todas las solicitudes DNS.

La arquitectura de referencia F5 Intelligent DNS Scale es una solución integral Una solución de entrega de DNS que mejora el rendimiento web al reducir la latencia del DNS, protege sus propiedades web y la reputación de su marca al mitigar los ataques DDoS de DNS, reduce los costos del centro de datos al consolidar la infraestructura de DNS. Lo más importante es que dirige a sus clientes a los componentes con mejor rendimiento para una entrega óptima de aplicaciones y servicios.

La arquitectura de referencia F5 Intelligent DNS Scale también ofrece la tranquilidad de saber que sus aplicaciones web responderán a todas las consultas DNS, manteniendo su contenido y aplicaciones disponibles para sus usuarios donde y cuando quieran acceder a ellos.

PUBLICADO EL 24 DE ENERO DE 2018

CONECTE CON F5

362

5 LABS

Lo último en inteligencia de amenazas de aplicaciones.

inteligencia

Ir a F5 Labs

EVCENTRAL

la comunidad F5 para debates

foros y artículos de expertos.

ir a DevCentral

SALA DE PRENSA DE F5

noticias, blogs de F5 y más.

ir a la sala de prensa

363

Entregar y proteger cada aplicación

Las soluciones de entrega y seguridad de aplicaciones de F5 están diseñadas para garantizar que cada aplicación y API implementada en cualquier lugar sea rápida, esté disponible y sea segura.Aprenda cómo podemos asociarnos para ofrecer experiencias excepcionales en todo momento.

QUÉ OFRECEMOS

RECURSOS

SOPORTE

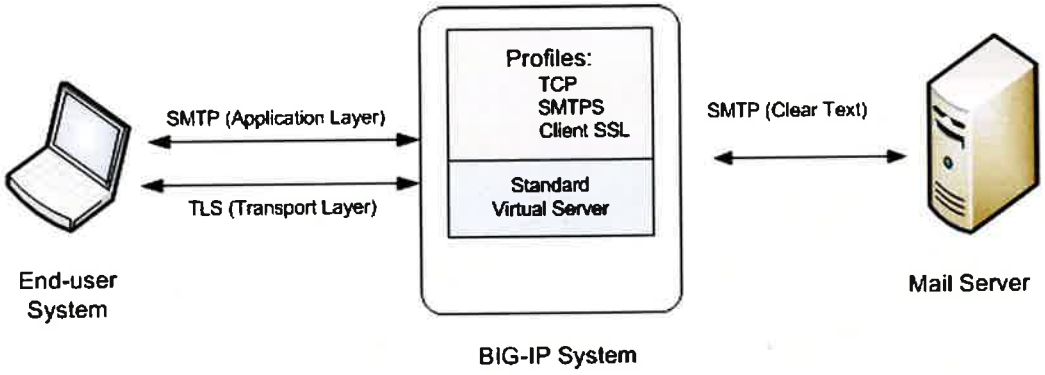
SOCIOS

EMPRESA

CONÉCTESE CON NOSOTROS

365


expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.



Ejemplo de configuración de BIG-IP para tráfico SMTP con activación de STARTTLS

Resumen de tareas

Para configurar el BIG-IP®sistema para procesar el tráfico del Protocolo Simple de Transferencia de Correo (SMTP) con funcionalidad SSL, realice algunas tareas básicas.

Lista de tareas

Creación de un perfil SMTP

Esta tarea especifica que se debe requerir la autenticación y el cifrado STARTTLS para todo el tráfico del Protocolo Simple de Transferencia de Correo (SMTP) del lado del cliente. Cuando se requiere STARTTLS para el tráfico SMTP, el BIG-IP®sistema actualiza efectivamente las conexiones SMTP para incluir SSL, en el mismo puerto SMTP.

. En la pestaña Principal, haga clic en**Tráfico local>perfiles>Servicios>SMTPS** Se abre la pantalla de la lista de perfiles SMTPS.

. Haga clic en**Crear**
Se abre la pantalla Nuevo perfil SMTPS.

. en el**nombre**campoescriba un nombre único para el perfil.

. Seleccione la**Personalizado**casilla de verificación.

. de la**Modo de activación STARTTLS**lista, seleccione**Requerir**

. Haga clic en**finalizado**

El sistema BIG-IP ahora debe activar STARTTLS para todo el tráfico SMTP del lado del cliente.

Creación de un perfil SSL de cliente

Se crea un perfil SSL de cliente cuando se desea que el sistema BIG-IP®autentique y descifre/cifre el tráfico de la aplicación del lado del cliente.

. En la pestaña Principal, haga clic en**Tráfico local>perfiles>SSL>cliente** Se abre la pantalla de la lista de perfiles de cliente.

. Haga clic en**Crear**
Se abre la pantalla Nuevo perfil SSL de cliente.

. Configure todos los ajustes del perfil según sea necesario.

. Haga clic en**finalizado**

Después de crear el perfil SSL de cliente y asignarlo a un servidor virtual, el sistema BIG-IP puede aplicar seguridad SSL al tipo de tráfico de aplicación para el que el servidor virtual está configurado para escuchar

Creación de un servidor virtual y un grupo de equilibrio de carga

Esta tarea se utiliza para crear un servidor virtual, así como un grupo predeterminado de servidores del Protocolo Simple de Transferencia de Correo (SMTP). El servidor virtual escucha y aplica seguridad SSL al tráfico de aplicaciones SMTP del lado del cliente. Luego, el servidor virtual reenvía el tráfico SMTP al grupo de servidores especificado.

Nota:*Al usar esta tarea, se asigna un perfil SMTPS al servidor virtual en lugar de un perfil SMTP. También se debe asignar un perfil SSL de cliente.*

. En la pestaña Principal, haga clic en**Tráfico local**>**Servidores virtuales** Se abre la pantalla Lista de servidores virtuales.

. Haga clic en el**Crear**botón.
Se abre la pantalla Nuevo servidor virtual.

. en el**nombre**campocampo, escriba un nombre único para el servidor virtual.

. o la**destino**configuración, seleccione el tipo y escriba una dirección, o una dirección y una máscara, según corresponda a su red.

. en el**Puerto de servicio**campocampo, escriba**5**o seleccione**SMTP**de la lista.

. de la**configuración**lista, seleccione**básico**

. o la**Perfil SSL (Cliente)**configuración, en el**Disponible**cuadro, seleccione un nombre de perfil y, mediante el botón Mover, mueva el nombre al**Seleccionado**cuadro

. de la**Perfil MTPS**En la lista, seleccione el perfil SMTPS que creó anteriormente.

En el área Recursos de la pantalla, para la**configuración de Grupo predeterminado**haga clic en el**crear (+)**botón. Se abre la pantalla Nuevo grupo.

0. En el**nombre**campocampo, escriba un nombre único para el grupo.

1. En el área Recursos, para la configuración de**Nuevos miembros**seleccione el tipo de nuevo miembro que está agregando y, a continuación, escriba la información correspondiente en el**Código Nombre Dirección**y**Puerto de servicio**campocampos y haga clic en**Agregar**para agregar tantos miembros del grupo como necesite.

2. Haga clic en**finalizado**para crear el grupo.
La pantalla se actualiza y vuelve a abrir la pantalla Nuevo servidor virtual. El nombre del nuevo grupo aparece en la configuración de Grupo predeterminadolista.

3. Haga clic en**finalizado**

Después de realizar esta tarea, el servidor virtual aplica los perfiles personalizados de SMTPS y SSL de cliente al SMTP entrante

tráfico.

Resultado de la implementación

Después de crear un perfil SMTPS y un perfil SSL de cliente y asignarlos a un servidor virtual, el sistema BIG-IP escucha el tráfico SMTP del lado del cliente en el puerto 25. A continuación, el sistema BIG-IP activa el método STARTTLS para ese tráfico, para proporcionar seguridad SSL en ese mismo puerto, antes de reenviar el tráfico al grupo de servidores especificado.

Tabla de contenido << Capítulo anterior Capítulo siguiente >>

Contactar con soporte

Información corporativa Sala de prensa de capacitación
Relaciones con los Inversores
Agentes
Acerca de AskF5

Certificación
Universidad F5
Formación online gratuita

F5.com
DevCentral
Portal de soporte
Partner Central
F5 Labs

Leer las políticas de soporte
Crear servicio
Solicitud
Dejar comentarios [+]

Administración remota de cuentas de usuario

Acerca de las cuentas de usuario remotas

Cada sistema BIG-IP requiere una o más cuentas de usuario administrativas. En lugar de almacenar estas cuentas de usuario de BIG-IP localmente en el sistema BIG-IP, puede almacenarlas en un servidor de autenticación remoto, ya sea LDAP, Active Directory, RADIUS o TACACS+. En este caso, crea todas sus cuentas de usuario estándar de BIG-IP (incluidos los nombres de usuario y las contraseñas) en el servidor remoto, utilizando el mecanismo proporcionado por el proveedor de ese servidor. El servidor remoto entonces realiza toda la autenticación de esas cuentas de usuario

Para implementar el control de acceso para las cuentas de usuario de BIG-IP almacenadas remotamente, puede usar la utilidad de configuración de BIG-IP o tmsh. Primero, especifique la información para el tipo de servidor de autenticación remoto y luego configure estas propiedades de control de acceso:

propiedades:

- Rol de usuario
- Acceso a particiones
- Acceso a terminales

Para garantizar una administración sencilla del control de acceso para las cuentas remotas, el sistema BIG-IP crea automáticamente una única cuenta de usuario llamadaOtros usuarios externosEsta cuenta de usuario representa todas las cuentas de usuario de BIG-IP almacenadas remotamente que cumplen con las propiedades de control de acceso definidas en el sistema BIG-IP.

Especificación de la información del servidor LDAP o Active Directory

antes de comenzar:

- Verifique que las cuentas de usuario del sistema BIG-IP se hayan creado en el servidor de autenticación remoto.
- Verifique que los grupos de usuarios apropiados, si los hay, estén definidos en el servidor de autenticación remoto.
- Si desea verificar el certificado del servidor de autenticación, importe uno o más certificados SSL

Puede configurar el sistema BIG-IP para usar un servidor LDAP o Microsoft Windows Active Directory para autenticar las cuentas de usuario del sistema BIG-IP, es decir, el tráfico que pasa por la interfaz de administración (MGMT).

los valores que especifique en este procedimiento para el ***Rol,Acceso a la partición****, y* ***acceso al terminal*** *configuración no se aplica al control de acceso basado en grupos. Estos valores representan los valores predeterminados que el sistema BIG-IP aplica a cualquier cuenta de usuario que no forme parte de un grupo de usuarios almacenado de forma remota. Además, para la* Otros usuarios externos *cuenta de usuario, puede modificar el* ***Rol,Acceso a la partición,*** *y* ***Acceso al terminal*** *configuración solo cuando su partición actual en el sistema BIG-IP esté configurada en*

común *Si intenta modificar esta configuración cuando su partición actual no sea* *Común,* *El sistema muestra un mensaje de error.*

. En la pestaña Principal, haga clic en **Sistema › Usuarios › Autenticación**

2. En la barra de menú, haga clic en **Autenticación**.

3. Haga clic en **Cambiar**

4. En la **lista Directorio de usuarios** seleccione **Remoto - LDAP** o **remoto - Active Directory**

5. En el **host** ficampo, escriba la dirección IP del servidor remoto.

   El dominio de ruta al que pertenece esta dirección debe ser el dominio de ruta

6. Para la **configuración de** puerto, conserve el número de puerto predeterminado (389) o escriba un nuevo número de puerto.

   Este número representa el número de puerto que el sistema BIG-IP utiliza para acceder al servidor remoto.

7. En el **Árbol de directorio remoto** fiEn el campo, escriba la ubicación del archivo (árbol) de la base de datos de autenticación de usuarios en el servidor LDAP o Active Directory.

   Como mínimo, debe especificar un componente de dominio (es decir, dc=[valor]).

8. Para la configuración de **Ámbito** conserve el valor predeterminado (ub) o seleccione un nuevo valor.

   Esta configuración especifica el nivel de la base de datos del servidor remoto en el que el sistema BIG-IP debe buscar la autenticación de usuario.

9. Para la configuración de **Ind**, especifique un ID de inicio de sesión de usuario para el servidor remoto:

   a. en el **DN** fiEn el campo, escriba el nombre distinguido para el ID de usuario remoto.

   . en el **Contraseña** ficampo, escriba la contraseña para el ID de usuario remoto.

   c. en el **Confirmar** ficampo, vuelva a escribir la contraseña que escribió en el **contraseña** ficampo.

Plantilla de usuario **escriba una cadena que contenga una variable que represente el nombre distinguido del** fiusuario, en el formato s

Este campo solo puede contener una s y no puede contener ningún otro especificador de formato.

Por ejemplo, puede especificar una plantilla de usuario como s@siterequest.com o uxml:Id=%s,ou=people,dc=siterequest,dc=com

El resultado es que cuando un usuario intenta iniciar sesión, el sistema reemplaza s con el nombre de usuario especificado en el cuadro de diálogo Autenticación básica y pasa ese nombre como nombre distinguido para la operación de enlace. El sistema también pasa la contraseña asociada como contraseña para la operación de enlace.

1. Para la

Comprobar atributo de miembro en el grupo **configuración, seleccione la casilla de verificación si desea que el sistema compruebe el atributo de miembro del usuario en el grupo LDAP o AD remoto.** 2. Para habilitar la autenticación basada en SSL, en la

SSL **SSL** lista, seleccione **habilitado** de 18

a. de la**Lista de certificados CA SSL**. de la

. de la**Lista de claves de cliente SSL**seleccione el nombre de la clave SSL del cliente.

utilice esta configuración solo cuando el servidor remoto requiera que el cliente presente un certificado.

c. de la**Lista de certificados de cliente SSL**seleccione el nombre del certificado SSL del cliente.

utilice esta configuración solo si el servidor remoto requiere que el cliente presente un certificado.

3. En el**Atributo LDAP de inicio**fiEn este campo, escriba el nombre de la cuenta del servidor LDAP.

El valor de esta opción suele ser el ID de usuario. Sin embargo, si el servidor es un servidor de Microsoft Windows Active Directory, el valor debe ser el nombre de la cuenta.AMAccountName ((distingue entre mayúsculas y minúsculas). El valor predeterminado es ninguno.

4. En la**Campo Nombre del certificado del cliente**lista:

a. seleccione un nombre alternativo del sujeto o el nombre del sujeto (**Nombre común**).

. si selecciona el nombre alternativo del sujeto**Otro nombre**, entonces en el**OID**ficampo, escriba un identificador de objeto (OID).

El OID indica el formato y la semántica del nombre alternativo del sujeto.

5. For the **volver a Local**En la configuración, seleccione la casilla de verificación cuando desee permitir que la autenticación remota recurra a la autenticación local cuando el servidor remoto no esté disponible.

6. De la**lista de**rol, seleccione el rol de usuario que desea que el sistema BIG-IP asigne de forma predeterminada a todas las cuentas de usuario del sistema BIG-IP autenticadas en el servidor remoto.

7. De la lista de**acceso a la partición**seleccione la partición administrativa predeterminada a la que pueden acceder todas las cuentas de usuario del sistema BIG-IP autenticadas de forma remota.

8. De la lista de**acceso al terminal**seleccione una de estas opciones como opción de acceso al terminal predeterminada para las cuentas de usuario autenticadas de forma remota:

deshabilitado	Elija esta opción cuando no desee que las cuentas de usuario almacenadas de forma remota tengan acceso al terminal del sistema BIG-IP.
tmsh	Elija esta opción cuando desee que las cuentas de usuario almacenadas de forma remota solo tengan acceso tmsh al sistema BIG-IP.

9. Haga clic en**finalizado**

Ahora puede autenticar las cuentas de usuario administrativas almacenadas en un servidor LDAP o Active Directory remoto. Si no necesita configurar el control de acceso para los grupos de usuarios almacenados remotamente, sus tareas de configuración están completas.

Especificación de la información del servidor LDAP del certificado de cliente

Verifique que las cuentas de usuario necesarias para el sistema BIG-IP existan en el servidor de autenticación remoto.

o para autenticar las cuentas de usuario del sistema BIG-IP (es decir, el tráfico que pasa por la interfaz de administración [MGMT]), puede configurar el sistema BIG-IP para autenticar los certificados emitidos por el estado del certificado en línea de una autoridad de certificación. respondedor del protocolo (OCSP).

los valores que especifique en este procedimiento para el ***Rol, Acceso a la partición, y acceso al terminal*** *La configuración no se aplica a la autorización basada en grupos. Estos valores representan los valores predeterminados o las cuentas de usuario configuradas localmente (que anulan el rol predeterminado) que el sistema BIG-IP aplica a cualquier cuenta de usuario que no forme parte de un grupo de roles remoto.*

. En la pestaña Principal, haga clic en **Sistema › Usuarios › Autenticación**

2. En la barra de menú, haga clic en **Autenticación**.

3. Haga clic en **Cambiar**

4. En la **lista Directorio de usuarios** seleccione **Remoto - ClientCert LDAP**

5. En el **host** ficampo, escriba la dirección IP del servidor remoto.

   El dominio de ruta al que pertenece esta dirección debe ser el dominio de ruta

6. Para la **configuración de** puerto, conserve el número de puerto predeterminado (389) o escriba un nuevo número de puerto.

   Este número representa el número de puerto que el sistema BIG-IP utiliza para acceder al servidor remoto.

7. En el **Árbol de directorio remoto** ficampo, escriba la ubicación del archivo (árbol) de la base de datos de autenticación de usuario en el servidor de certificados de cliente.

   Como mínimo, debe especificar un componente de dominio (es decir, dc=[valor]).

8. Para la configuración de **Ámbito** conserve el valor predeterminado (ub) o seleccione un nuevo valor.

   Esta configuración especifica el nivel de la base de datos del servidor remoto en el que el sistema BIG-IP debe buscar la autenticación de usuario.

9. Para la configuración de **Ind**, especifique un ID de inicio de sesión de usuario para el servidor remoto:

   a. en el **DN** fiEn el campo, escriba el nombre distinguido para el ID de usuario remoto.

   . en el **Contraseña** ficampo, escriba la contraseña para el ID de usuario remoto.

   c. en el **Confirmar** ficampo, vuelva a escribir la contraseña que escribió en el **contraseña** ficampo.

0. Para habilitar la autenticación basada en SSL, desde la **SSL** lista, seleccione **habilitado** y, si es necesario, configure estos ajustes:

   a. de la **Lista de certificados CA SSL** seleccione el nombre de un certificado de cadena; es decir, la CA de terceros o el certificado autofirmado que normalmente reside en el servidor de autenticación remoto.

   . de la **Lista de claves de cliente SSL** seleccione el nombre de la clave SSL del cliente.

   utilice esta configuración solo cuando el servidor remoto requiera que el cliente presente un certificado.

   c. de la **Lista de certificados de cliente SSL** seleccione el nombre del certificado SSL del cliente.

   utilice esta configuración solo si el servidor remoto requiere que el cliente presente un certificado.

1. En el **campo de certificados CA** fiescriba la ruta de carpeta absoluta de *Objeto de archivo apache-ssl-cert* para la autoridad de certificación (CA).

Wagner Pérez

La ruta absoluta de la carpeta es*/Common/<ruta de la carpeta>/<nombre del certificado>*Para determinar la ruta absoluta de la carpeta del *objeto de archivo apache-ssl-cert*, haga clic en**sistema › Administración de archivos › Lista de certificados de Apache**y anote la partición y la ruta del certificado de destino.

Los certificados de Apache solo se pueden almacenar dentro de /Common.

2. En el**Nombre de inicio de sesión**ficampo, escriba un prefijo de búsqueda LDAP que contenga el nombre distinguido (DN) del certificado de usuario, comoN

   Esto especifica el atributo LDAP que se utilizará como nombre de inicio de sesión. El valor predeterminado es deshabilitado.

3. En el**Atributo LDAP de inicio**fiEn este campo, escriba el nombre de la cuenta del servidor LDAP.

   El valor de esta opción suele ser el ID de usuario. Sin embargo, si el servidor es un servidor de Microsoft Windows Active Directory, el valor debe ser el nombre de la cuenta.AMAccountName ((distingue entre mayúsculas y minúsculas). El valor predeterminado es ninguno.

4. En el**Filtro de inicio**ficampo, escriba el atributo LDAP que contiene el nombre corto del usuario.

   Esto especifica el filtro que se aplicará al nombre común (CN) del certificado de cliente y, por lo general, este es el ID de usuario o AMAccountNameEl filtro es una expresión regular que se utiliza para extraer la información necesaria del CN del certificado de cliente que se compara con los resultados de la búsqueda LDAP. El valor predeterminado es deshabilitado.

5. Para la **profundidad**conserve el valor predeterminado (0)o escriba un nuevo valor para la profundidad de verificación.

6. De la **Campo Nombre del certificado del cliente**lista:

   a. seleccione un nombre alternativo del sujeto o el nombre del sujeto (**Nombre común**).

   . si selecciona el nombre alternativo del sujeto**Otro nombre**, entonces en el**OID**ficampo, escriba un identificador de objeto (OID).

   El OID indica el formato y la semántica del nombre alternativo del sujeto.

7. De la lista de**Anulación de CSP**seleccione**Activado**o**off**para especificar si el sistema utiliza un respondedor OCSP específico para anular el certificado de CA para autenticar/autorizar las operaciones de inicio de sesión.

8. Si la**Anulación de OCSP**está configurada ennentonces en el**Respondedor CSP**ficampo, conserve el valor predeterminado o escriba el nombre del servidor o la URL que autentica/autoriza las operaciones de inicio de sesión.

   El valor predeterminado eslocalhost.localdomain

9. De la**lista de**rol, seleccione el rol de usuario que desea que el sistema BIG-IP asigne de forma predeterminada a todas las cuentas de usuario del sistema BIG-IP autenticadas en el servidor remoto.

0. De la lista de**acceso a la partición**seleccione la partición administrativa predeterminada a la que pueden acceder todas las cuentas de usuario del sistema BIG-IP autenticadas de forma remota.

   de las cuentas de usuario del sistema.

1. De la lista de**acceso al terminal**seleccione una de estas opciones como opción de acceso al terminal predeterminada para las cuentas de usuario autenticadas de forma remota:

deshabilitado	Elija esta opción cuando no desee que las cuentas de usuario almacenadas de forma remota tengan acceso al terminal del sistema BIG-IP.
tmsh	Elija esta opción cuando desee que las cuentas de usuario almacenadas de forma remota solo tengan acceso tmsh al sistema BIG-IP.

Wagner Patricio

2. Haga clic en**finalizado**

Ahora puede autenticar el tráfico administrativo para las cuentas de usuario almacenadas en un servidor de certificados de cliente remoto. Si no necesita configurar la autorización de usuario basada en grupos, sus tareas de configuración están completas.

Especificación de la información del servidor RADIUS

antes de comenzar:

Verifique que las cuentas de usuario del sistema BIG-IP se hayan creado en el servidor de autenticación remoto.

Verifique que los grupos de usuarios apropiados, si los hay, estén definidos en el servidor de autenticación remoto.

Puede configurar el sistema BIG-IP para usar un servidor RADIUS para autenticar las cuentas de usuario del sistema BIG-IP, es decir, el tráfico que pasa por la interfaz de administración (MGMT).

*los valores que especifique en este procedimiento para el**Rol,Acceso a la partición**, y**acceso al terminal**La configuración no se aplica a la autorización basada en grupos. Estos valores representan los valores predeterminados que el sistema BIG-IP aplica a cualquier cuenta de usuario que no forme parte de un grupo de roles definido en el servidor de autenticación remoto. Además, para lacuenta de usuario Otros usuarios externos, puede modificar la**Rol,Acceso a la partición**, y**acceso al terminal**configuración solo cuando su partición actual en el sistema BIG-IP esté configurada enComún.Si intenta modificar esta configuración cuando su partición actual no sea común,El sistema muestra un mensaje de error.*

. En la pestaña Principal, haga clic en**Sistema › Usuarios › Autenticación**

2. En la barra de menú, haga clic en**Autenticación**.

3. Haga clic en**Cambiar**

4. Desde la **lista Directorio de usuarios**seleccione**Remoto - RADIUS**

5. Para la **primario**configuración:

a. en el**Host**ficampo, escriba el nombre del servidor RADIUS primario.

El dominio de ruta con el que está asociado este host debe ser el dominio de ruta0

. en el**Secreto**ficampo, escriba la contraseña para acceder al servidor RADIUS primario.

c. en el**Confirmar**ficampo, vuelva a escribir el secreto de RADIUS.

6. Si configura la**Configuración del servidor**en**primario y secundario**, entonces, para el**Secundario**configuración:

a. en el**Host**ficampo, escriba el nombre del servidor RADIUS secundario.

El dominio de ruta con el que está asociado este host debe ser el dominio de ruta0

. en el**Secreto**ficampo, escriba la contraseña para acceder al servidor RADIUS secundario.

c. en el**Confirmar**ficampo, vuelva a escribir el secreto de RADIUS.

7. Para el**volver a Local**En la configuración, seleccione la casilla de verificación cuando desee permitir que la autenticación remota recurra a la autenticación local cuando el servidor remoto no esté disponible.

8. De la lista de**lista de**rol, seleccione el rol de usuario que desea que el sistema BIG-IP asigne de forma predeterminada a todas las cuentas de usuario del sistema BIG-IP autenticadas en el servidor remoto.

9. De la**acceso a la partición**seleccione la partición administrativa predeterminada a la que pueden acceder todas las cuentas de usuario del sistema BIG-IP autenticadas de forma remota.

de las cuentas de usuario del sistema.

0. De la lista de**acceso al terminal**seleccione una de estas opciones como opción de acceso al terminal predeterminada para las cuentas de usuario autenticadas de forma remota:

cuentas de usuario autenticadas:

deshabilitado	Elija esta opción cuando no desee que las cuentas de usuario almacenadas de forma remota tengan acceso al terminal del sistema BIG-IP.
tmsh	Elija esta opción cuando desee que las cuentas de usuario almacenadas de forma remota solo tengan acceso tmsh al sistema BIG-IP.

1. Haga clic en**finalizado**

Ahora puede autenticar el tráfico administrativo para las cuentas de usuario del sistema BIG-IP que se almacenan en un servidor RADIUS remoto. Si no necesita configurar el control de acceso para los grupos de usuarios almacenados remotamente, sus tareas de configuración están completas.

Especificación de la información del servidor TACACS+

antes de comenzar:

Verifique que las cuentas de usuario del sistema BIG-IP se hayan creado en el servidor de autenticación remoto.

Verifique que los grupos de usuarios apropiados, si los hay, estén definidos en el servidor de autenticación remoto.

Puede configurar el sistema BIG-IP para usar un servidor TACACS+ para autenticar las cuentas de usuario del sistema BIG-IP, es decir, el tráfico que pasa por la interfaz de administración (MGMT).

*los valores que especifique en este procedimiento para el**Rol**,**Acceso a la partición**, y**acceso al terminal**La configuración no se aplica a la autorización basada en grupos. Estos valores representan los valores predeterminados que el sistema BIG-IP aplica a cualquier cuenta de usuario que no forme parte de un grupo de roles remotos. Además, para lacuenta de usuario Otros usuarios externospuede modificar la**Rol**, **Acceso a la partición**, y**Acceso al terminal**configuración solo cuando su partición actual en el sistema BIG-IP esté configurada encomún. Si intenta modificar esta configuración cuando su partición actual no seacomún,El sistema muestra un mensaje de error.*

. En la pestaña Principal, haga clic en**Sistema › Usuarios › Autenticación**

2. En la barra de menú, haga clic en**Autenticación**.

3. Haga clic en**Cambiar**

4. En la**lista Directorio de usuarios**seleccione**Remoto - TACACS+**

5. Para la**volver a Local**En la configuración, seleccione la casilla de verificación cuando desee permitir que la autenticación remota recurra a la autenticación local cuando el servidor remoto no esté disponible.

6. Para la**Servidores**escriba una dirección IP para el servidor TACACS+ remoto.

El dominio de ruta al que pertenece esta dirección debe ser el dominio de ruta

7. Haga clic en**Agregar**

La dirección IP del servidor TACACS+ remoto aparece en la**Servidores**lista.

8. En el**Secreto**fiescriba la contraseña para acceder al servidor TACACS+.

No incluya el símbolo # en el secreto. Si lo hace, la autenticación de las cuentas de usuario locales (comooot

ydmin)fallará.

9. En el campo**Confirmar secreto**fivuelva a escribir el secreto de TACACS+.

0. De la lista de**cifrado**lista, seleccione una opción de cifrado:

habilitado	especifica que el sistema cifra los paquetes TACACS+
deshabilitado	Especifica que el sistema envía paquetes TACACS+ sin cifrar.

1. En el**Nombre del servicio**fiescriba el nombre del servicio que el usuario solicita autenticarse para usar (generalmentepp).

   Especificar el servicio hace que el servidor TACACS+ se comporte de manera diferente para diferentes tipos de solicitudes de autenticación. Ejemplos de nombres de servicio que puede especificar son:pp lip rap hell ty-daemon sistema de conexiónyfirewall

2. En el**Nombre del protocolo**ficampo, escriba el nombre del protocolo asociado con el valor especificado en el**Nombre del servicio**fi campo.

   Este valor suele serpEjemplos de nombres de protocolo que puede especificar son: p cp px talk ines sicpy at xremote tn3270 telnet login ad vpdn tp ttp deccp desconocido

3. Desde el**lista de**rol, seleccione el rol de usuario que desea que el sistema BIG-IP asigne de forma predeterminada a todas las cuentas de usuario del sistema BIG-IP autenticadas en el servidor remoto.

4. En la**acceso a la partición**seleccione la partición administrativa predeterminada a la que pueden acceder todas las cuentas de usuario del sistema BIG-IP autenticadas de forma remota.

5. En la lista**acceso al terminal**seleccione una de estas opciones como opción de acceso al terminal predeterminada para las cuentas de usuario autenticadas de forma remota:

deshabilitado	Elija esta opción cuando no desee que las cuentas de usuario almacenadas de forma remota tengan acceso al terminal del sistema BIG-IP.
tmsh	Elija esta opción cuando desee que las cuentas de usuario almacenadas de forma remota solo tengan acceso tmsh al sistema BIG-IP.

6. Haga clic en**finalizado**

Ahora puede autenticar el tráfico administrativo para las cuentas de usuario del sistema BIG-IP que se almacenan en un servidor TACACS+ remoto. Si no necesita configurar el control de acceso para los grupos de usuarios almacenados de forma remota, sus tareas de configuración están completas.

Cambiar el control de acceso predeterminado para las cuentas remotas

Realice esta tarea para cambiar el rol de usuario, el acceso a la partición y el acceso al terminal que desea que el sistema BIG-IP asigne de forma predeterminada a todos los usuarios remotos que sean miembros de la cuenta de usuariocuenta de usuario Otros usuarios externos,

. En la pestaña Principal, haga clic en**Sistema › Usuarios › Autenticación**

2. Haga clic en**Cambiar**

3. Desde el**lista Directorio de usuarios**seleccione**Remoto - Active Directory remoto - LDAP,emote - RADIUS**o

Remoto - TACACS+

4. En la**lista de**lista, seleccione un rol de usuario.

   El sistema BIG-IP asigna este rol de usuario a cualquier cuenta remota que no forme parte de un grupo de usuarios remotos al que haya asignado explícitamente un rol de usuario.

5. En la lista**acceso a la partición**lista, seleccione un nombre de partición.

   Todas las cuentas de usuario remotas que sean miembros de la cuenta BIG-IPOtros usuarios externospueden tener acceso a todas las particiones o a la misma partición individual. Los miembros individuales de esta cuenta no pueden tener acceso a particiones diferentes.

6. De la**acceso al terminal**seleccione**Habilitado**o**Deshabilitado**

7. Haga clic en**actualizar**

Después de realizar esta tarea, la mayoría de las cuentas de usuario de BIG-IP almacenadas en un servidor de autenticación remoto tendrán el rol de usuario especificado, así como acceso a la partición y a la consola. Las cuentas remotas que forman parte de un grupo de roles no están sujetas a esta configuración de autenticación.

Acerca de los grupos de usuarios remotos

En el sistema BIG-IP, puede asignar propiedades de control de acceso (rol de usuario, partición y acceso a terminal) a cualquier grupo de cuentas de usuario de BIG-IP definidas en un servidor de autenticación remoto. Puede asignar estas propiedades utilizando la utilidad de configuración de BIG-IP o el Shell de administración de tráfico (tmsh) para especificar la cadena de atributos remotos y el orden de línea adecuados para cada grupo de usuarios de BIG-IP, junto con los valores de control de acceso que desea asignar al grupo.

Puede configurar el control de acceso para grupos remotos de cuentas de usuario de BIG-IP de las siguientes maneras:

Especificando en el sistema BIG-IP la cadena de atributos correspondiente y el rol, el acceso a partición y el acceso a terminal que desea asignar al grupo.

Especificando en el sistema BIG-IP la cadena de atributos correspondiente y luego utilizando la sustitución de variables (solo tmsh).

Tenga en cuenta que el control de acceso para estas cuentas de usuario basadas en grupos es independiente del control de acceso asignado a las cuentas representadas por la cuenta de usuario de BIG-IP denominadacuenta de usuario Otros usuarios externos,

Ejemplos de configuración

Debido a que algunos tipos de servidores remotos permiten que un usuario sea miembro de varios grupos de usuarios, la configuración de roles de usuario y particiones para los grupos de usuarios de BIG-IP® en esos servidores puede generar conflictos. Por ejemplo, dos grupos de usuarios remotos separados podrían especificar roles diferentes en la misma partición administrativa. Para un usuario que es miembro de ambos grupos, esta configuración infringe la regla de BIG-IP de que un usuario no puede tener dos roles para una misma partición.

En caso de tales conflictos, el sistema BIG-IP debe elegir uno de los roles en conflicto para el usuario al iniciar sesión. La forma principal en que el sistema BIG-IP realiza esta elección es mediante el orden de línea. El orden de línea que especifique dentro de cada configuración de rol remoto afecta la forma en que el sistema resuelve los conflictos.

Por el contrario, dentro de un solo grupo de usuarios remotos, no se producen conflictos porque el sistema BIG-IP impide que los administradores asignen más de un rol a la misma partición.

Ejemplo 1: Entradas de rol-partición en conflicto dentro de un grupo

El siguiente ejemplo muestra que dos roles de usuario, Invitado y Administrador de certificados, están asociados a la misma partición,A

para el mismo grupo de usuarios remotos,igIPAdminGroup

Esta configuración no es válida porque ningún usuario puede tener más de un rol para una partición específica. Si un administrador

Si se intenta implementar esta configuración, el sistema BIG-IP la deniega y muestra un mensaje de error.

```
BigIPAdminGroup
        attribute memberOF=CN=BigIPAdminGroup        OU=BIP,DC=dean,DC=local
        console tmsh
        line-order      30
        role guest
        user-partition      A

        attribute memberOF=CN=BigIPAdminGroup OU=BIP,DC=dean,DC=local console
        tmsh
        line-order 30
        role manager
        user-partition B

        attribute memberOF=CN=BigIPAdminGroup OU=BIP,DC=dean,DC=local console
        tmsh
        line-order 30
        role certificate manager user-
        partition A
```

Ejemplo 2: Entradas de role-partition en conflicto en varios grupos

En el siguiente ejemplo, el servidor remoto contiene dos grupos de usuarios BIG-IP igIPNetworkGroup yigIPAdminGroup,y el sistema BIG-IP tiene tres particiones,AByC.

Supongamos que el usuariosmithes miembro de ambos grupos. La configuración a continuación muestra que al iniciar sesión en el sistema BIG-IP, al usuariojsmithse le asignará claramente el rol de Operador para la partición y de Administrador para la partición. Pero para la

particiónAhay un conflicto, porque un usuario solo puede tener un rol por partición en el sistema, y esta configuración intenta asignar los roles de Administrador e Invitado para esa partición.

Para resolver el conflicto, el sistema BIG-IP utiliza el orden de línea para determinar cuál de los roles en conflicto asignar asmith para la particiónAEn este caso, el sistema elegirá Administrador, el rol con el número de orden de línea más bajo (20).

Grupo de red BigIP

atributo memberOF=CN= BigIPNetworkGroup OU=BIP,DC=dean,DC=local consola
tmsh
orden de línea 20
role manager
partición de usuario A

atributo memberOF=CN=BigIPNetworkGroup,OU=BIP,DC=dean,DC=local consola tmsh

orden de línea 10
rol operador
user-partition B

atributo memberOF=CN=BigIPNetworkGroup,OU=BIP,DC=dean,DC=local consola tmsh

orden de línea 40
role manager
partición de usuario C

BigIPAdminGroup

attribute memberOF=CN=BigIPAdminGroup OU=BIP,DC=dean,DC=local
console tmsh
line-order 30
role guest
partición de usuario A

Ejemplo 3: Entradas de partición de rol en conflicto debido al acceso universal

En el siguiente ejemplo, suponga que el usuariosmithes miembro de tres grupos de usuarios remotos: igIPGuestGroup igIPOperatorGroupyigIPAdminGroupy el sistema BIG-IP tiene tres particiones,A y

En esta configuración, el rol especificado paraigIPAdminGroupcrea un conflicto, porque algunas entradas especifican un rol particular para cada partición, mientras queigIPAdminGroupespecifica un rol de Administrador para las tres particiones. Para resolver el conflicto, el sistema BIG-IP utiliza el orden de línea configurado.

Debido a que el orden de línea paraigIPAdminGroupes 9 y, por lo tanto, no es el número de orden de línea más bajo, el sistema BIG-IP ignorará el rol de Administrador parasmith,dejándola con el rol de Invitada en las particionesAyC,y Operadora en la particiónB

BigIPGuestGroup
atributo memberOF=CN=BigIPGuestGroup,OU=BIP,DC=dean,DC=local consola tmsh

line-order 2
role guest
user-partition A

BigIPOperatorGroup
atributo memberOF=CN=BigIPOperatorGroup,OU=BIP,DC=dean,DC=local
consola tmsh
orden de línea 10
rol operador
user-partition B

BigIPAdminGroup
atributo memberOF=CN=BigIPAdminGroup,OU=BIP,DC=dean,DC=local consola
tmsh
orden de línea 9
rol administrador
partición de usuario Todas

BigIPGuestGroup
atributo memberOF=CN=BigIPGuestGroup,OU=BIP,DC=dean,DC=local consola tmsh

line-order 3
role guest
user-partition C

Configurando el control de acceso para grupos de usuarios remotos

Esta tarea se realiza para asignar un rol de usuario, una partición administrativa correspondiente y un tipo de acceso a terminal a un grupo de cuentas de usuario almacenadas remotamente. Para un grupo de usuarios determinado, puede asignar tantas combinaciones de rol y partición como necesite, siempre que cada rol esté asociado a una partición diferente. Si la partición que asocia con un rol esTodasesta entrada podría o no tener efecto, dependiendo de si laTodasdesignación entra en conflicto con otras combinaciones de rol y partición para ese grupo de usuarios. En caso de conflicto, se debe tener en cuenta el orden de las líneas en la configuración. Para asignar varios roles-

Para cada combinación de particiones de un grupo de usuarios, repita esta tarea para cada combinación, especificando la misma cadena de atributos para cada tarea.

. En la pestaña Principal, haga clic en **sistema › usuarios**

2. En la barra de menú, haga clic en **Grupos de roles remotos**

3. Haga clic en**Crear**

4. En el**Nombre del grupo**fiescriba el nombre del grupo definido en el servidor de autenticación remota. Un ejemplo de nombre de grupo es**BigIPOperatorsGroup**

5. En el**Orden de línea**ficampo, escriba un número.

Este valor especifica el orden de esta configuración de control de acceso en el archivo*/config/bigip/auth/remoterole*para el grupo con nombre. Los servidores LDAP y Active Directory leen este archivo línea por línea. El orden de la información es importante; por lo tanto, F5 Networks recomienda que especifique un valor de000para el número de la primera línea. Esto le permite, en el futuro, insertar líneas antes de la primera línea.

382

6. En el**campo Cadena de atributo**fiescriba un atributo.

Un ejemplo de cadena de atributo es memberOF=cn=BigIPOperatorsGroup,cn=users,dc=dev,dc=net

El sistema BIG-IP intenta hacer coincidir este atributo con un atributo en el servidor de autenticación remoto. Al encontrar una coincidencia, el sistema BIG-IP aplica la configuración de control de acceso definida aquí a los usuarios de ese grupo. Si no se encuentra una coincidencia, el sistema aplica la configuración de control de acceso predeterminada a todas las cuentas de usuario almacenadas remotamente (excluyendo cualquier cuenta de usuario para la que se haya configurado individualmente la configuración de control de acceso).

7. De la lista de**lista Acceso remoto**seleccione un valor.

habilitado	Elija este valor si desea habilitar el acceso remoto para el grupo de usuarios definido.
deshabilitado	Elija este valor si desea deshabilitar el acceso remoto para el grupo de usuarios definido. Tenga en cuenta que si configura varias instancias de este grupo de roles remotos (una instancia para cada par rol-partición para la cadena de atributos), elegir un valor de **Deshabilitado**deshabilita el acceso remoto para todos los miembros del grupo de usuarios, independientemente de la instancia del grupo de roles remotos.

8. De la lista de**Lista de roles asignados**seleccione un rol de usuario para el grupo de usuarios remotos.

9. De la**acceso a la partición**En la lista, seleccione un valor de partición administrativa.

Todas	Elija este valor para dar a los usuarios del grupo definido acceso a sus objetos autorizados en todas las particiones del sistema BIG-IP.
partición *nombre_de_partición*	Elija un nombre de partición específico para dar a los usuarios del grupo definido acceso solo a esa partición.
Común	Elija este valor para dar a los usuarios del grupo definido acceso a la partición**Común**solamente.

0. De la lista de**acceso al terminal**lista, seleccione el tipo de acceso a la línea de comandos que desea otorgar a los usuarios del grupo, si alguno.

1. Haga clic en**finalizado**o**repetir**

Después de realizar esta tarea, el grupo de usuarios que especificó tendrá el rol asignado, el acceso a la partición y el acceso a la terminal asignados.

Acerca de la sustitución de variables

Como alternativa al uso de BIG-IP Utilidad de configuración para especificar valores explícitos para las propiedades de control de acceso para Para grupos de usuarios remotos, puede configurar el servidor remoto para que devuelva un atributo específico del proveedor con variables para rol, acceso a particiones y acceso a la consola. Luego, puede asignar valores a esas variables (numéricos o alfabéticos) y usar el comando `tmsh remoterole` para realizar la sustitución de variables para esas propiedades de control de acceso.

o, por ejemplo, suponga que configura un servidor de autenticación RADIUS remoto para que devuelva el atributo específico del proveedor F5-TM-User-Info-1 =C1,junto con tres variables y sus valores:

F5-LTM-User-Role =00 (variable)

F5-LTM-User-Partition =App_C (variable)

F5-LTM-User-Console = (variable)

Un valor de rol de usuario de400significa eloperadorrol de usuario.

El comando remoterole puede usar el atributo 5-LTM-User-Info-1 para la coincidencia. El comando puede leer los valores de ole, partición de usuario y consola de las tres variables, en lugar de que usted los especifique explícitamente. Para ello, debe especificar cada una de las tres variables en la línea de comandos, precedidas por la cadena % como argumentos.

A continuación se muestra un ejemplo de uso del comando remoterole. Este comando de ejemplo coincide con el atributo específico del proveedor 5-LTM-User-Info-1 y luego, usando las variables anteriores, asigna un rol de usuario de (operador (400)),acceso a particiónApp_Cy acceso a tmsh) a cualquier cuenta de usuario que forme parte del Centro de datos 1 (DC1):

```
tmsh auth remote-role role-info add { DC1 { attribute "F5-LTM-User-Info-1=DC1" console %F5-LTM-User-Console" role
"%F5-LTM-User-Role" user partition
 "%F5-LTM-User-Partition" line order 1 } }
```

Valores para variables de rol remoto

Esta tabla enumera los valores para la variable BIG-IP5-LTM-User-Roleque se utiliza para definir un rol para un grupo de usuarios almacenado remotamente. Por ejemplo, un valor de00para la variable5-LTM-User-Roleindica el rol de usuario administrador.

Rol de usuario	Valor
Administrador	0
Administrador de recursos	20
Administrador de recursos	40
Auditor	80
Administrador de og	90
administrador	00
Editor de aplicaciones	300
operador	400
Administrador de firewall	450
Administrador de protección de ruido	480
Administrador de certificados	500
Administrador de certificados	510
solicitante	700
Administrador de seguridad de aplicaciones	800
Editor de seguridad de aplicaciones	810

384

Rol de usuario	Valor
Editor de políticas de aplicaciones	50
o-Acceso	00

Acerca del acceso a la terminal para grupos de usuarios remotos

Si utiliza el comando remotorole de Traffic Management Shell (tmsh) para configurar el acceso a la consola para una cuenta de usuario dentro de un grupo de usuarios remotos, el comportamiento del sistema BIG-IP difiere según el valor de la opción de consola:

Si una cadena de atributos para un grupo de usuarios remotos tiene uno o más pares rol-partición asignados a ese atributo, y establece el valor de la opción de consola en**tmsh**Luego, tras una autenticación exitosa, el sistema BIG-IP otorga a todos los usuarios de ese grupo de usuarios acceso tmsh al sistema BIG-IP

Si establece el valor de la opción de consola en deshabilitar (o no configura la opción de consola) para todas las combinaciones de rol y partición asignadas a la misma cadena de atributos, el sistema BIG-IP deniega el acceso tmsh al sistema BIG-IP a todos los usuarios de ese grupo de usuarios, incluso con una autenticación correcta. Tenga en cuenta que esto no afecta al acceso de los usuarios a la utilidad de configuración de BIG-IP.

Guardar la configuración de control de acceso en un archivo

Puede guardar la configuración en ejecución del sistema, incluyendo toda la configuración para la autenticación y autorización de usuarios remotos, en un archivo de texto plano con un nombre específico y la extensión.*scf*

. En el sistema BIG-IP, acceda a un símbolo del sistema.

2. En el símbolo del sistema, abra el Shell de administración de tráfico escribiendo el comando tmsh

3. Escribays save***nombre_archivo***

ys save myConfiguration053107crea el archivoyConfiguration053107.scfen el directorio. ar/local/scf

sys save /config/myConfiguration crea el archivoyConfiguration.scfen el*/config*directorio.

Ahora puede importar este archivo a otros dispositivos BIG-IP en la red.

Importación de datos de configuración de BIG-IP a otros sistemas BIG-IP

Puede usar el comando tmsh ys load para importar un único archivo de configuración (SCF), incluidos los datos de control de acceso, a otros dispositivos BIG-IP en la red.

Esta tarea es opcional.

1. En el sistema BIG-IP en el que creó el SCF, acceda a un símbolo del sistema de la línea de comandos.

2. Copie el SCF que creó anteriormente a una ubicación en su red a la que pueda acceder desde el sistema que desea configurar.

3. Edite el SCF para reflejar el enrutamiento de administración y las contraseñas especiales del sistema BIG-IP que desea configurar:

a. Abra el SCF en un editor.

. Donde sea necesario, cambie los valores de la dirección IP de administración, la máscara de red, la administración

Cambie la ruta predeterminada, las direcciones IP propias, las direcciones IP del servidor virtual, las rutas, las rutas predeterminadas y los campos de nombre de host a los valores del nuevo sistema.

c. Si es necesario, cambie las contraseñas de lasootyadmincuentas usando el comando ser ***nombre*** contraseña ninguna nueva contraseña***contraseña***

Al configurar una unidad que forma parte de una configuración de sistema redundante y que utiliza el SCF de la unidad par, no modifique lasootyadmincuentas. Estas cuentas deben ser idénticas en ambas unidades del sistema redundante.

Conserve el SCF editado.

4. En el sistema BIG-IP que desea configurar, abra el Shell de administración de tráfico escribiendo el comando tmsh

5. Escribays load***cf_filename***

ys load myConfiguration053107.scfguarda una copia de seguridad de la configuración en ejecución en el*/directorio var/local/scf* directorio y, a continuación, restablece la configuración en ejecución con la configuración contenida en el SCF que está cargando.

Acerca de la visualización de cuentas de usuario remotas

Al usar la utilidad de configuración de BIG-IP, puede mostrar una lista de las cuentas de usuario remotas a las que les asignó explícitamente un rol de usuario no predeterminado. Si una cuenta de usuario remota tiene asignado el rol predeterminado, no podrá verla en la lista de cuentas de usuario.

Cualquier usuario que tenga acceso a una partición en la que residen las cuentas remotas puede ver una lista de cuentas de usuario remotas.

Mostrar una lista de cuentas de usuario remotas

Esta tarea se realiza para mostrar una lista de cuentas de usuario almacenadas remotamente.

. En la pestaña Principal, haga clic en**sistema › usuarios**

2. En la barra de menú, haga clic en**Autenticación**.

3. Verifique que la configuración de**Directorio de usuarios**especifique un tipo de servidor de autenticación remota (Active Directory, LDAP o RADIUS).

4. En la barra de menú, haga clic en**Lista de usuarios**

5. Vea la lista de cuentas de usuario. Las cuentas de usuario remotas a las que se les asigna el rol de usuario predeterminado aparecen como**Otros usuarios externos**

Visualización de las propiedades de control de acceso

. En la pestaña Principal, haga clic en**sistema ›** usuarios

2. En la barra de menú, haga clic en**Autenticación**.

3. Verifique que la configuración de**Directorio de usuarios**especifique un tipo de servidor de autenticación remota (Active Directory, LDAP o RADIUS).

4. En la barra de menú, haga clic en**Lista de usuarios**

5. Vea la lista de cuentas de usuario. Las cuentas de usuario remotas a las que se les asigna el rol de usuario predeterminado aparecen como**Otros usuarios externos**

386

6. En la lista de cuentas de usuario, busque la cuenta de usuario que desea ver y haga clic en el nombre de la cuenta. Esto muestra las propiedades de esa cuenta de usuario.

Contactar con soporte

¿TIENE ALGUNA PREGUNTA?

Soporte y ventas>

SÍGANOS

Wagner Pastre

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

388

Para obtener más información sobre el incidente de seguridad en F5, las medidas que estamos tomando para abordarlo, y nuestros esfuerzos continuos para proteger a nuestros clientes, haga clicaquí

Conocimiento

14783: Descripción general del perfil SSL del cliente (11.x - 21.x)

Fecha de publicación: 17 de octubre de 2018 Fecha de actualización: 7 de noviembre de 2025

Contenido recomendado por IA

Se aplica a:

Tema

Este artículo se aplica a BIG-IP 11.x a 21.x. Para obtener información sobre otras versiones, consulte el siguiente artículo:

K10167: Descripción general del SSL del cliente pperfil (9.x - 10.x)

Este artículo analiza la configuración del perfil SSL del cliente. Puede encontrar el perfil SSL del cliente en la utilidad de configuración yendo a**Tráfico local>Perfiles>SL>Cliente**

Descripción

El perfil SSL de cliente de BIG-IP permite que el sistema BIG-IP acepte y finalice las solicitudes de cliente que se envían mediante un protocolo totalmente encapsulado en SSL. También proporciona una serie de ajustes configurables para administrar las conexiones SSL del lado del cliente. Normalmente, solo necesita configurar algunos de los ajustes disponibles y mantener los ajustes restantes en sus valores predeterminados, a menos que el soporte de F5 le indique lo contrario. Las siguientes tablas enumeran y describen la configuración del perfil SSL de cliente de BIG-IP.

Propiedades generales pConfiguración de

propiedades gconfiguración

Proxy de reenvío SSL y_

Autenticación de cliente

Eliminación restringida de certificado de cliente gación

Lo ggen g

Nota: *Dependiendo de su versión de BIG-IP, es posible que algunas secciones o ajustes no estén disponibles en su sistema.*

Propiedades generales

Ajuste	descripción
nombre	El ajuste del nombre es obligatorio. Para crear un perfil SSL de cliente, debe especificar un nombre único para el perfil
principal perfil	Esta configuración especifica un perfil existente para usar como perfil principal. Un perfil hereda la configuración de su perfil principal, a menos que la anule seleccionando la casilla de verificación personalizada y modificando el valor. El valor predeterminado es el perfil clientssl.

Configuración

Esta tabla describe la configuración SSL más utilizada para un perfil SSL de cliente, incluyendo, por ejemplo, el certificado y la clave que se enviarán a los clientes SSL para el intercambio de certificados

Ajuste	descripción
código	Establece el estado del perfil en habilitado (predeterminado) o deshabilitado (desmarcando la casilla). La configuración de código se introdujo en BIG-IP 11.5.0.

Clave de certificado Cadena	La cadena de claves de certificado es obligatoria y especifica uno o más certificados y claves para asociar con el perfil SSL. Al hacer clic en Agregar, el sistema presenta un cuadro de diálogo donde puede especificar la siguiente configuración para la cadena de claves de certificado. **Certificado**De forma predeterminada, el perfil SSL de cliente utiliza un certificado autofirmado, llamado**default.crt** Sin embargo, casi siempre se personaliza para hacer referencia a un certificado específico del sitio al que se aplica el perfil. El certificado SSL debe estar en formato de correo electrónico con privacidad mejorada (PEM) y debe importarlo al sistema BIG-IP con la clave correspondiente antes de que un perfil SSL pueda hacer referencia al certificado y la clave. Para obtener información sobre cómo importar un certificado y una clave SSL mediante la utilidad de configuración, consulte**K14620: Mana gen gCertificados SSL para sistemas BIG-IP yusando gla configuración gutilidad de configuración y**Para obtener información sobre cómo importar un certificado y una clave SSL mediante la consola TMOS (**tmsh**), consulte**14031: Im p ortin gel certificado y la clave SSL yusando gla consola TMOS** Para obtener información sobre cómo verificar el formato del certificado, consulte**13349: Verif yen gCertificado y clave SSL ypares desde la línea de comandos (11.x - 13.x)** **Clave**Eley**configuración es obligatoria. De forma predeterminada, el perfil SSL del cliente utiliza la clave integrada, denominada **default.key**, que coincide con**default.crt**. Debe elegir la clave que coincida con el certificado configurado y la clave debe estar en formato PEM. Después de importar el certificado SSL y la clave correspondiente al sistema BIG-IP, elija la clave apropiada de la**ey**configuración. **Cadena**: Esta configuración es opcional. Se utiliza la**Cadena**Configuración para especificar un paquete o cadena de certificados que el cliente puede usar para establecer una relación de confianza con un servidor que presenta un certificado firmado por una Autoridad de Certificación (CA) de confianza. El valor predeterminado para la**Cadena**configuración es**Ninguno**lo que indica que no se presenta ningún certificado de cadena al cliente con el certificado SSL del servidor. Esta configuración enumera el nombre de todos los certificados SSL instalados en el almacén de certificados SSL del sistema BIG-IP. Si usa certificados firmados por una CA intermedia, F5 recomienda que cree e instale un paquete que contenga los certificados de todas las CA en la cadena entre el certificado configurado en el perfil SSL y una CA externa cuyo certificado sea de confianza para la base de clientes esperada. Luego puede seleccionar el nuevo paquete de certificados en la**Cadena**configuración. Para obtener información sobre cómo crear e instalar un paquete de certificados personalizado, consulte**13302: Configuración gurin gel sistema BIG-IP ypara usar un certificado de cadena SSL (11.x - 16.x)** ***Nota**: Independientemente de la**Cadena**configuración, si configura las**Autoridades de Certificación de Confianza**Configuración, el sistema presenta el paquete de certificados contenido en el archivo configurado**Autoridades de Certificación de Confianza**archivole.* **Contraseña**Esta configuración es opcional. Solo es necesaria si la clave está protegida con contraseña. No hay un valor predeterminado para esta configuración. Si su clave está protegida con contraseña, introduzca la contraseña requerida.
OCSP Stapling parámetros	Le permite seleccionar un perfil de OCSP Stapling (Protocolo de estado de certificado en línea) SSL que contiene varios parámetros de OCSP Stapling. El valor predeterminado es uno, lo que significa que el OCSP Stapling no está habilitado. La opción Parámetros de OCSP Stapling se introdujo en BIG-IP 11.6.0.
Notificar certificado Estado a servidor virtual Servidor	Introducida en BIG-IP 13.0.0, esta opción especifica si se debe propagar el estado de los certificados asociados con este perfil SSL de cliente a los servidores virtuales que utilizan este perfil SSL de cliente. Deshabilitado por defecto. ***Nota**: Esta opción se utiliza para comunicar el estado de revocación del certificado SSL al servidor virtual. Normalmente se implementa junto con una configuración de OCSP Stapling.*

Cifrados	Los cifrados La configuración es opcional. De forma predeterminada, el perfil SSL del cliente utiliza la cadena de cifrado PREDETERMINADA. En la mayoría de los casos, las casos, la cadena de cifrado PREDETERMINADA es apropiada, pero puede personalizarla según sea necesario para cumplir con los necesidades de seguridad y rendimiento de su sitio. Para obtener información sobre cómo configurar el cifrado SSL para un perfil SSL, consulte**17370: Configurar gurin gla fuerza del cifrado gpara perfiles SSL (12.x - 13.x)** .
Opciones	Cuando está habilitado (Lista de opciones), hace referencia a la configuración de la Lista de opciones, que las opciones y soluciones alternativas SSL estándar de la industria utilizan para manejar el procesamiento SSL. La configuración predeterminada es Todas las opciones deshabilitadas..
Lista de opciones	La configuración de la Lista de opciones permite seleccionar entre un conjunto de opciones y soluciones alternativas SSL estándar de la industria para manejar el procesamiento SSL.
ata 0-RTT	Con la protección contra repetición y datos anticipados habilitada, puede iniciar una conexión de servidor para datos anticipados y recibir los beneficios de los datos anticipados entregados al servidor. En lugar de que los clientes retengan los datos anticipados hasta que se complete el protocolo de enlace (cliente finalizado, protocolo de enlace completado) y luego los entreguen al proxy/servidor, si los datos anticipados están configurados y se aceptan, pueden activar la conexión/protocolo de enlace del servidor y entregar los datos anticipados en ese momento (primer vuelo). Las opciones son las siguientes: **Deshabilitar**Esta es la configuración predeterminada y especifica que los datos iniciales con (o sin) protección contra repetición están deshabilitados. **Habilitar con protección contra repetición**Esta es la configuración recomendada y especifica que las aplicaciones pueden enviar datos en la primera sesión TCP después de que se complete el protocolo de enlace TCP, en lugar de que el cliente retenga los datos iniciales hasta que se complete el protocolo de enlace (el cliente finaliza, el protocolo de enlace se completa) y luego los reenvíe al proxy/servidor. BIG-IP proporciona protección opcional contra la repetición de datos iniciales mediante la protección contra repetición. Esto permite el uso de datos iniciales sin requisitos adicionales impuestos al servidor backend. **Habilitar sin protección contra repetición**Esta configuración no se recomienda y especifica que los datos iniciales sin protección contra repetición pueden dejar un servidor TLS expuesto a la repetición de datos por parte de un cliente TLS malicioso.
Proxy SSL	La configuración SSL roxy se introduce en BIG-IP 11.0.0. De forma predeterminada, la configuración SSL roxy está deshabilitada (borrada). Cuando se habilita, el cliente puede autenticarse directamente con el servidor y el servidor puede autenticarse con el cliente, basándose en el certificado de cliente presentado. En una configuración típica, con el sistema BIG-IP en el medio, el cliente y el servidor no pueden comunicarse directamente para autenticarse entre sí. La configuración SSL roxy requiere tanto un perfil SSL de cliente como un perfil SSL de servidor, y debe habilitar la configuración en ambos perfiles. Para obtener información sobre la configuración SSL roxy, consulte los siguientes recursos: **13385: Descripción general del proxy yfunción SSL** El**Implementación de Proxy SSL en un único sistema BIG-IP**capítulo del anual. ***Implementaciones de IG-IP LTM*** ***Nota**: Para obtener información sobre cómo localizar los manuales de productos de F5, consulte* ***98133564: Consejos para búsqueda gAskF5 y encontrar gdocumentación del producto*** .
Proxy SSL passthrough	Permite que Proxy SSL pase el tráfico cuando el conjunto de cifrado negociado entre el cliente y el servidor no es compatible. Deshabilitado de forma predeterminada. Si lo habilita, también debe habilitar esta opción en el perfil SSL del servidor. La opción Proxy SSL Passthrough se introdujo en BIG-IP 11.6.0.

odSSL métodos	Métodos odSSL habilita o deshabilita la emulación del método ModSSL. Habilite esta opción cuando los métodos de OpenSSL sean inadecuados. Por ejemplo, habilítela cuando desee utilizar la compresión SSL sobre TLSv1. Deshabilitado (borrado) de forma predeterminada.
Tamaño de caché	La configuración Tamaño de caché especifica el número máximo de sesiones SSL permitidas en la caché de sesiones SSL. El valor predeterminado para Tamaño de caché es de 262144 sesiones. Para obtener información sobre la configuración de Tamaño de caché SSL, consulte**6767: Descripción general de la configuración del perfil de caché de sesiones SSL de BIG-IP** gs
Tiempo de espera de caché	La configuración de Tiempo de espera de caché especifica la cantidad de segundos que el sistema permite que las sesiones SSL permanezcan en la caché de sesiones SSL antes de eliminarlas. El valor predeterminado para Tiempo de espera de caché es de 3600 segundos. El rango de valores configurables para Tiempo de espera de caché está entre 0 y 86400 segundos inclusive. ***Nota**: Los períodos de tiempo de espera de caché más largos pueden aumentar el riesgo de secuestro de sesiones SSL.*
Tiempo de espera de alerta	La configuración de Tiempo de espera de alerta especifica la duración durante la cual el sistema intenta cerrar una conexión SSL transmitiendo una alerta o iniciando un cierre incorrecto antes de restablecer la conexión. El valor predeterminado para BIG-IP 12.0.0 HF1 y versiones posteriores, así como para BIG-IP 12.1.0 y versiones posteriores, es indefinido. El valor predeterminado para BIG-IP 11.2.0 - 12.0.0 es de 10 segundos. El valor predeterminado para BIG-IP 11.0.0 - 11.1.0 es de 0 segundos. Seleccione Indefinido para especificar que la conexión no debe restablecerse después de transmitir una alerta o iniciar un cierre incorrecto. A partir de BIG-IP 15.0.0, 14.1.0, 14.0.0.3, 13.1.1.2 y 12.1.3.7, el sistema BIG-IP envía un RST una vez que**Tiempo de espera de alerta**Se ha alcanzado el valor, lo que provoca la interrupción forzosa de la conexión y reduce la cantidad de datos transferidos entre el sistema par y el sistema BIG-IP. A partir de BIG-IP 15.1.0, 15.0.1.3 y 14.1.3.1, la**Tiempo de espera de alerta**configuración admite el**Inmediato**valor, que hace que el sistema BIG-IP reinicie los flujos del lado del cliente y del servidor después de 1/1000 de segundo
andshake Tiempo de espera	La configuración de tiempo de espera de andshake especifica la cantidad de segundos que el sistema intenta establecer una conexión SSL antes de finalizar la operación. El valor predeterminado para BIG-IP 11.2.0 y versiones posteriores es de 10 segundos. El valor predeterminado para BIG-IP 11.0.0 - 11.1.0 es de 0 segundos. Seleccionar indefinido especifica que el sistema continúa intentando establecer una conexión por tiempo ilimitado.
negociación	Puede configurar la opción de renegociación para controlar si el servidor virtual permite la negociación de sesión intermedia. Cuando está habilitada (predeterminado), la negociación permite que el sistema BIG-IP procese las solicitudes de negociación SSL intermedias. Cuando está deshabilitada, el sistema finaliza la conexión o ignora la solicitud, según la configuración del sistema.
negociación período	La configuración del período de negociación indica el tiempo que transcurre antes de que el sistema renegocie la sesión SSL después de la conexión inicial. Si se establece en Indefinido (predeterminado), el sistema no renegocia la sesión SSL.
negociación Tamaño	Indica la cantidad de datos de la aplicación en megabytes que el sistema debe recibir desde el momento de la conexión inicial antes de renegociar la sesión SSL. Si se establece en indefinido (predeterminado), el sistema no negocia la sesión SSL.
negociar Registro ax demora	Indica el número de registros SSL permitidos durante la renegociación SSL antes de que el sistema finalice la conexión. Si se establece en indefinido, el sistema permite un número ilimitado. Indefinido es la configuración predeterminada en BIG-IP 11.4.0 y versiones posteriores

Seguro negociación	Los perfiles SSL de BIG-IP admiten la extensión de indicación de renegociación TLS, que permite especificar el método de renegociación segura para las conexiones SSL. El valor predeterminado para el perfil SSL de cliente es requerir. Los valores para la configuración de Renegociación segura en el perfil SSL de cliente son los siguientes: **Solicitar**: Especifica que el sistema solicita la renegociación segura de las conexiones SSL. **Requerir**: Especifica que el sistema requiere la renegociación segura de las conexiones SSL. En este modo, el sistema permite los protocolos de enlace SSL iniciales de los clientes, pero finaliza las renegociaciones de los clientes que no admiten la renegociación segura. **Requerir estricto**Especifica que el sistema requiere una renegociación segura y estricta de las conexiones SSL. En este modo, el sistema deniega los protocolos de enlace SSL iniciales de los clientes que no admiten la negociación segura.
ax renegociaciones	Especifica el número máximo de intentos de renegociación SSL por conexión que el sistema puede recibir en un minuto antes de renegociar una sesión SSL. Por ejemplo, un cliente con tres conexiones puede Permite un número máximo de intentos de renegociación SSL igual a tres veces el valor de renegociación ax configurado. Después de que el sistema recibe este número de registros de renegociación SSL, cierra la conexión. Esta configuración se aplica solo a los perfiles de cliente. El valor predeterminado es . La opción de renegociación ax se introdujo en BIG-IP 11.6.0.
Agregado ax negociación	Especifica el número máximo de registros de renegociación SSL agregados que el sistema puede recibir antes de renegociar una sesión SSL. Después de que el sistema recibe este número de registros de renegociación SSL agregados, cierra la conexión. Esta configuración se aplica solo a los perfiles de cliente. El valor predeterminado es indefinido. La opción de renegociación agregada ax se introdujo en BIG-IP 12.0.0
Nombre del servidor	A partir de BIG-IP 11.1.0, los perfiles SSL de BIG-IP admiten la extensión TLS Server Named Indication (SNI), lo que permite al sistema BIG-IP seleccionar el perfil SSL apropiado en función de la información TLS SNI proporcionado por el cliente. La configuración del nombre del servidor especifica el nombre de host DNS completo del servidor o una cadena comodín que contiene el carácter asterisco (*) para que coincida con varios nombres, utilizada en la conexión TLS SNI. No hay un valor predeterminado para esta configuración. Para obtener información sobre la configuración de la función TLS SNI en el sistema BIG-IP, consulte**13452: Configuración gurin gun servidor virtual para servir varios sitios HTTPS sin gFunción de indicación de nombre de servidor TLS**
SSL predeterminado perfil para SNI	Cuando está habilitada, esta configuración indica que el sistema debe usar el perfil como perfil SSL predeterminado cuando no haya ninguna coincidencia con el nombre del servidor o cuando el cliente no admita la extensión TLS SNI. De forma predeterminada, esta configuración está deshabilitada (borrada). Para obtener información sobre la configuración de la función TLS SNI en el sistema BIG-IP, consulte**K13452: Configuración gurin gun servidor virtual para servir varios psitios HTTPS usando gFunción de indicación de nombre de servidor TLS** .
par requerido Compatibilidad con SNI	Cuando está habilitada, esta configuración requiere que el cliente sea compatible con la extensión TLS SNI; de lo contrario, el sistema BIG-IP desconecta la conexión del cliente con una alerta fatal. Deshabilitado (borrado) de forma predeterminada.

Wagner Pastor

expert IPX SRL RNC 130-850151 Santo Domingo, R.D.

nclean Cierre	El protocolo SSL realiza un cierre limpio de una conexión TLS/SSL activa enviando una alerta de notificación de cierre al sistema par. La configuración de Cierre limpio permite que el sistema BIG-IP realice un cierre no limpio de las conexiones SSL cerrando la conexión TCP subyacente sin enviar las alertas de cierre SSL. alertas de notificación. De forma predeterminada, esta configuración está habilitada (seleccionada) y es útil para ciertos navegadores que manejan las alertas de cierre SSL de manera diferente. Por ejemplo, algunas versiones de Internet Explorer requieren alertas de cierre SSL del servidor, mientras que otras versiones no, y el perfil SSL no siempre puede detectar este requisito. **importante**Si deshabilita (borra) la**Cierre no limpio**casilla de verificación, algunos navegadores pueden mostrar páginas en blanco o errores al conectarse al servidor virtual
Reanudación estricta	La configuración de Reanudación estricta habilita o deshabilita la reanudación de sesiones SSL después de un cierre incorrecto. Deshabilitado (borrado) de forma predeterminada.
Ticket de sesión	A partir de BIG-IP 11.4.0, los perfiles SSL de BIG-IP admiten el mecanismo de reanudación de sesiones TLS sin estado, como se describe en**Internet En gineerin gGrupo de trabajo (RFC 5077)**Este mecanismo permite que el sistema BIG-IP encapsule el estado de la sesión TLS como un ticket para el cliente y le permite reanudar posteriormente una sesión TLS utilizando el mismo ticket. Deshabilitado (borrado) de forma predeterminada. ***Nota:*** *Este enlace lo lleva a un recurso externo a AskF5, y es posible que el documento se elimine sin nuestro conocimiento.* ***Nota:****El****Ticket de sesión****opción es visible en BIG-IP 11.3.0, pero no funciona hasta BIG-IP 11.4.0.*
Ticket de sesión Tiempo de espera	Especifica el tiempo de espera para el ticket de sesión. El valor predeterminado es de segundos, lo que significa que el sistema utiliza el tiempo de espera de la caché. La opción Tiempo de espera del ticket de sesión se introduce en BIG-IP 12.0.0.
Sesión irroring	Habilita o deshabilita la duplicación de los datos de ID de sesión SSL a un par de alta disponibilidad. La configuración predeterminada está deshabilitada, lo que impide que el sistema duplique los datos de ID de sesión SSL.
Alerta genérica	Cuando está habilitada (predeterminado), esta configuración hace que el sistema envíe todas las alertas SSL utilizando un mensaje genérico de error de protocolo de enlace. Cuando la configuración está deshabilitada, el sistema envía mensajes de alerta SSL más específicos. La configuración de Alerta genérica se introduce en BIG-IP 11.5.0.
on-SSL Conexiones	Habilita o deshabilita la aceptación de conexiones no SSL. Deshabilitado (borrado) de forma predeterminada.
Permitir tamaño de registro dinámico tamaño de registro	Una mejora del rendimiento de TLS que evita el almacenamiento en búfer y la demora en la entrega de fragmentos de registro TLS. El sistema IG-IP ajusta dinámicamente el tamaño de los registros TLS según el estado de la conexión. Está deshabilitado de forma predeterminada. La opción Permitir tamaño de registro dinámico se introduce en BIG-IP 12.1.0.
máximo tamaño de registro	Indica el tamaño máximo de registro del perfil. Habilítelo cuando desee permitir el ajuste dinámico del tamaño de registro. El rango es de 128 a 16384. La configuración predeterminada es 16384.

Wagner Pastor

expert IPX SRL RNC 130-850151 Santo Domingo, R.D.

Hash de firma SSL	Especifica el algoritmo hash que el sistema BIG-IP utiliza para firmar los intercambios de claves del servidor con Diffie-ellman (DHE), incluidos los cifrados de curva elíptica (ECDHE), y para los mensajes de verificación de certificados. Las opciones posibles son SHA1, SHA256, SHA384 y Cualquiera. Cuando selecciona Cualquiera, autoriza al sistema a elegir cualquiera de los algoritmos hash. El sistema BIG-IP respeta la extensión signature_algorithms del cliente, tal como se define en TLS 1.2. Cuando sea posible, el sistema BIG-IP prefiere SHA256 en la firma del protocolo de enlace según el contenido de la extensión signature_algorithms. El sistema BIG-IP actualiza además el algoritmo hash de HA256 a HA384 cuando se utiliza P-384 Esta mejora adicional solo se aplica a BIG-IP 12.0.0 y versiones posteriores. El sistema BIG-IP intenta evitar el uso de SHA1 en el protocolo de enlace TLS, excepto cuando se utilizan firmas en certificados X.509 (estas firmas son creadas por la Autoridad de Certificación X.509). El sistema BIG-IP solo utiliza la firma de protocolo de enlace HA1 cuando se utiliza una clave SA y falta la extensión signature_algorithms o signature_algorithms está presente y solo enumera HA1.
eer No-negociar Tiempo de espera	Indica el número de segundos que el sistema espera antes de restablecer la conexión con sistemas pares que no renegocian sesiones SSL. El valor predeterminado es 10. La opción Tiempo de espera eer No-renegotiate se introdujo en BIG-IP 11.6.0
Máximo de protocolos de enlace activos protocolos de enlace	La configuración de Máximo de protocolos de enlace activos limita el número de protocolos de enlace SSL simultáneos. Cuando el número de protocolos de enlace SSL activos alcanza el límite especificado, el sistema finaliza el protocolo de enlace SSL más reciente. protocolo de enlace. La configuración predeterminada es indefinida, lo que significa que no hay límite. La opción Máximo de protocolos de enlace activos se introduce en BIG-IP 12.1.0.

Proxy de reenvío SSL

El**Función de proxy de reenvío SSL**configuración se introduce en BIG-IP 11.3.0. Para obtener información sobre el uso de la**función de proxy de reenvío SSL,**consulte el**capítulo sobre la implementación del proxy de reenvío SSL en un único sistema BIG-IP.**capítulo del***Implementaciones de BIG-IP LTM*f

Nota*98133564: Consejos para buscar****AskF5 y encontrar gAskF5 y encontrar gdocumentación del producto***

Ajuste	descripción
Reenvío SSL función de proxy	La configuración de proxy de reenvío SSL está deshabilitada (borrada) de forma predeterminada. Cuando está habilitada, el sistema cifra todo el tráfico entre un cliente y el sistema BIG-IP utilizando un segundo certificado de servidor único generado dinámicamente por el sistema BIG-IP, y cifra todo el tráfico entre el sistema BIG-IP y el servidor utilizando el certificado proporcionado por el servidor. La configuración de la función de proxy de reenvío SSL requiere un perfil SSL de cliente y un perfil SSL de servidor, y debe habilitarla en ambos perfiles. *Nota: El sistema BIG-IP utiliza el certificado proporcionado por el servidor (incluido el certificado comodín) para crear el segundo certificado de servidor único*

Certificado de CA Cadena de claves	Especifica el certificado de CA que el sistema utilizará cuando la configuración de la función de proxy reenviado SSL esté habilitada. Al hacer clic en Agregar, el sistema presenta un cuadro de diálogo donde puede especificar la siguiente configuración para la cadena de claves del certificado de CA: **Certificado**Especifica el certificado de CA que el sistema utilizará cuando la**función de proxy reenviado SSL** esté habilitada. El valor predeterminado para esta configuración es**efault.crt** **Clave**Especifica la clave asociada con el certificado de CA que el sistema utilizará cuando la**Función de proxy de reenvío SSL**esté habilitada. El valor predeterminado para esta configuración es**efault.key Chain**Especifica un paquete o cadena de certificados que se utilizará para establecer una relación de confianza con un servidor que presenta un certificado firmado por una autoridad de certificación (CA) no confiable. **Contraseña**Especifica la contraseña de la clave asociada con el certificado de CA que el sistema utilizará cuando la**función de proxy reenviado SSL**esté habilitada. El valor predeterminado para esta configuración es **Ninguno**
de Confianza ifespan	Especifica la duración, en días, del certificado de CA que el sistema utiliza cuando la configuración de proxy de reenvío SSL está habilitada. El valor predeterminado es de 30 días
de Confianza extensiones / de Confianza Lista de extensiones	Especifica las extensiones del certificado de CA que el sistema utilizará cuando la configuración de la función de proxy de reenvío SL esté habilitada. Para activar una extensión, seleccione Lista de extensiones en la configuración Extensiones de certificado y, a continuación, seleccione las extensiones que el sistema utilizará en el certificado de la función de proxy de reenvío SL en Extensiones disponibles en la configuración Lista de extensiones de certificado. Seleccione Habilitar para moverlas a Habilitadas. extensiones.
Certificado en caché y Dirección-Puerto	A partir de BIG-IP 11.4.0, puede usar la configuración de la función de proxy de reenvío SL para buscar certificados por dirección IP y número de puerto cuando esta configuración esté habilitada. Deshabilitado (borrado) de forma predeterminada.
Reenvío SSL Omisión de proxy	Compara el tráfico SSL con las listas de permitidos (omisión) y las listas de denegación (interceptación) de la aplicación, según la IP de origen, la IP de destino o el nombre de host. La función de omisión de proxy de reenvío SL se introdujo en BIG-IP 11.6.0
omisión en alerta de handshake	***Nota:*** *A partir de BIG-IP 16.x y 17.x, esta configuración se elimina de la utilidad de configuración. Todavía puede verla a través de tmsh* ***(tmos)*** *utilidad, pero no es funcional y no tiene impacto en los perfiles SSL del cliente. Se aplican solo a la configuración del perfil SSL del servidor proxy de reenvío SSL asociado. Para obtener más información, consulte****D 1270849****.* A partir de BIG-IP 13.0.0, esta opción habilita o deshabilita la omisión del proxy de reenvío SSL al recibir un **handshake_failure rotocol_versiononsupported_extension**mensaje de alerta durante el handshake SSL del lado del servidor. Cuando esto ocurre, el tráfico SSL omite el sistema BIG-IP sin descifrado ni cifrado. Deshabilitado de forma predeterminada.
omisión en el cliente Fallo del certificado	***Nota:*** *A partir de BIG-IP 16.x y 17.x, esta configuración se elimina de la utilidad de configuración. Todavía puede verla a través de tmsh* ***(tmos)*** *utilidad, pero no es funcional y no tiene impacto en los perfiles SSL del cliente. Se aplican solo a la configuración del perfil server-ssl del proxy de reenvío SSL asociado. Para obtener más información, consulte****D 1270849*** *.* A partir de BIG-IP 13.0.0, esta opción habilita o deshabilita la omisión del proxy de reenvío SSL cuando no se puede obtener el certificado de cliente que solicita el servidor. Cuando esto ocurre, el tráfico SSL omite el sistema BIG-IP sin descifrado ni cifrado. Deshabilitado de forma predeterminada.

Verificado andshake	Cuando está habilitada, la función de protocolo de enlace verificado especifica que, en el modo de proxy de reenvío SSL, el sistema siempre debe realizar un protocolo de enlace TLS con el servidor primero antes de realizar el protocolo de enlace del cliente. Cuando está deshabilitada, el sistema realiza el protocolo de enlace del servidor primero solo si no ha falsificado y almacenado en caché previamente el certificado del servidor. Después de que el certificado del servidor esté listo, el sistema siempre realiza un protocolo de enlace con el cliente primero. El valor predeterminado es Deshabilitado. La función de protocolo de enlace verificado se introduce en BIG-IP 14.0.0.
Extensiones de saludo	Seleccione Todas las extensiones deshabilitadas o Lista de extensiones de la lista. Si selecciona Lista de extensiones, la Lista de extensiones de saludo aparece con la opción de habilitar o deshabilitar la negociación del protocolo de capa de aplicación (ALPN) de la lista Extensiones disponibles para especificar las extensiones de saludo recibidas del cliente que se incluirán en la extensión de saludo enviada al servidor por el proxy de reenvío SSL. El valor predeterminado es Todas extensiones deshabilitadas.

Autenticación de cliente

El**Autenticación de cliente**La sección del perfil SSL de cliente es específica para la autenticación de certificados de cliente. Algunas aplicaciones requieren que los clientes establezcan su identidad ante el servidor antes de continuar con la sesión SSL. La autenticación de certificados de cliente utiliza la siguiente secuencia de eventos:

. El cliente solicita una conexión SSL.
. El servidor SSL presenta su certificado SSL y cualquier paquete de certificados de cadena configurado al cliente.
. El cliente SSL utiliza los certificados de CA almacenados en su almacén de certificados de dispositivo de confianza y la cadena de certificados proporcionada, si es necesario, para autenticar el servidor.
. El servidor SSL solicita un certificado de cliente, anunciando una lista de CA preferidas si está configurado para hacerlo.
. El cliente SSL presenta su certificado SSL
El servidor SSL utiliza su paquete de certificados de CA configurado y de confianza para autenticar al cliente.

Ajuste	descripción

Cliente de Confianza	La configuración del certificado de cliente es obligatoria. Habilita y deshabilita la autenticación mediante certificado de cliente. Las opciones posibles para la configuración del certificado de cliente son: **Ignorar**: La**Hace que la conexión ignore el estado desconocido y continúe.**configuración es la configuración predeterminada. Deshabilita la autenticación mediante certificado de cliente. El sistema BIG-IP ignora cualquier certificado presentado y no autentica al cliente antes de establecer la sesión SSL. **solicitar**: La**solicitar**La configuración habilita la autenticación opcional mediante certificado de cliente. El sistema BIG-IP solicita un certificado de cliente e intenta verificarlo. Sin embargo, se establece una sesión SSL independientemente de si una CA de confianza presenta un certificado de cliente válido. La**solicitar**configuración se utiliza a menudo junto con iRules para proporcionar acceso selectivo en función del certificado presentado. Por ejemplo, esta opción es Es útil si desea permitir que los clientes que presenten un certificado de la CA de confianza configurada obtengan acceso a la aplicación, mientras que los clientes que no proporcionen el certificado requerido se redirigen a una página que detalla los requisitos de acceso. Sin embargo, si no utiliza iRules para imponer un resultado diferente, según los detalles del certificado, no hay ningún beneficio funcional en usar la**solicitar**configuración en lugar de la predeterminada**Ignorar**configuración. **requerir**: La**requerir**La configuración impone la autenticación de certificado de cliente. El sistema BIG-IP solicita un certificado de cliente e intenta verificarlo. El sistema establece una sesión SSL solo si una CA de confianza presenta un certificado de cliente válido. Utilice la**requerir**configuración para restringir el acceso solo a los clientes que presenten un certificado válido de una CA de confianza. ***nota**: La**Automático**La configuración se eliminó en BIG-IP 11.0.0.*
frecuencia	La configuración de frecuencia especifica la frecuencia de autenticación del cliente para una sesión SSL. El valor predeterminado para esta configuración es una vez
retener de Confianza	A partir de BIG-IP 11.4.0, puede configurar el perfil SSL de BIG-IP para que no almacene un certificado de cliente en una sesión SSL. Almacenar un certificado de cliente en una sesión SSL normalmente solo es necesario en implementaciones de BIG-IP APM. Cuando esta configuración está deshabilitada, el certificado de cliente no se almacena en una sesión SSL. Habilitado (seleccionado) de forma predeterminada.
de Confianza Cadena Recorrido profundidad	La configuración de Profundidad de recorrido de la cadena de certificados especifica el número máximo de certificados que se recorrerán en una cadena de certificados de cliente. El valor predeterminado es

La configuración de Autoridades de certificación de confianza solo es necesaria si el sistema BIG-IP realiza la autenticación de certificados de cliente. Esta configuración especifica el almacén de Autoridades de certificación de confianza del sistema BIG-IP (las CA en las que el sistema BIG-IP confía cuando verifica un certificado de cliente que se presenta durante la autenticación de certificados de cliente). El valor predeterminado para la configuración de Autoridades de certificación de confianza es uno que indica que o Las CA son de confianza. El valor único solo es apropiado si no desea permitir la autenticación de certificados de cliente. El servidor SSL no necesita confiar en ninguna CA, a menos que el servidor realice la autenticación de certificados de cliente. Si el modo de certificado de cliente de BIG-IP está configurado en "requerido" pero las entidades de certificación de confianza están configuradas en "Ninguna", los clientes no pueden establecer sesiones SSL con el servidor virtual. Esta configuración enumera el nombre de todos los certificados SSL instalados en el sistema BIG-IP.

El**paquete a**certificado puede ser apropiado para su uso como un paquete de certificados de entidades de certificación de confianza. Sin embargo, si este paquete se especifica como el almacén de certificados de entidades de certificación de confianza, cualquier certificado de cliente válido que esté firmado por una de las CA raíz populares incluidas en el paquete predeterminado**a-bundle.crt**se autentica. Esto proporciona cierto nivel de identificación, pero muy poco control de acceso, ya que casi cualquier certificado de cliente válido podría autenticarse. Sin embargo, al configurar la autenticación de certificados de cliente, es más común aceptar certificados de cliente de una o unas pocas PKI o CA privadas

Si desea confiar solo en los certificados firmados por una CA específica o un conjunto de CA, F5 recomienda que cree e instale un paquete que contenga certificados de CA confiables. El nuevo paquete de certificados se puede seleccionar en la**configuración de Autoridades de Certificación de Confianza**Para obtener información sobre cómo crear un paquete de certificados personalizado, consulte

13302: Configuración gurin gel sistema BIG-IP ypara usar un certificado de cadena SSL (11.x - 13.x)

Autoridades de Certificación de Confianza

Para admitir varias jerarquías de PKI, este paquete puede contener certificados de CA de varias PKI diferentes

A partir de BIG-IP 11.6.0, el paquete puede incluir solo el certificado raíz o los certificados de firma de CA intermedios que firmaron el certificado del cliente. Antes de BIG-IP 11.6.0, el paquete debe incluir toda la cadena de certificados de CA necesaria para establecer una cadena de confianza, como se describe en la**cadena**configuración.

El archivo no necesita contener certificados de CA de la PKI que firmó el certificado SSL del servidor, a menos que el sistema BIG-IP deba validar los certificados SSL del cliente de esa PKI. Sin embargo, en la práctica, la autenticación de certificados de cliente se usa con mayor fre

Autoridades de certificación de confianza**configuración a menudo solo contiene un certificado o una cadena de la PKI que firmó el certificado del servidor** Puede usar el opensslcomando para verificar el certificado del cliente con el paquete de Autoridad de Certificación de Confianzaantes de importarlo al sistema BIG-IP. Por ejemplo, el siguiente comando verifica el certificado del cliente,comando para verificar el certificado del cliente con el paquete de Autoridad de Certificación de Confianzaclient.crt, con el paquete de Autoridad de Certificación de Confianza:openssl verify -purpose sslclient -CAfile /ruta/al/paquete-de-ca-de-confianza.crt /ruta/al/client.crt

Si el sistema puede establecer la cadena de confianza para el certificado del servidor usando la cadena especificada, el comando devuelve una salida similar al siguiente ejemplo:

client.crt: OK

importante

importanteA partir de BIG-IP 11.5.0, el sistema ya no presenta el paquete de certificados contenido en la entidad de certificación de confianza asociada.**Autoridades de Certificación de Confianza**archivocuando la opción de**Certificado de cliente**está configurada en**solicitaro requerir**

Wagner Pastor

	La configuración de Autoridades de Certificación Anunciadas es opcional. Puede usarla para especificar las CA que el sistema BIG-IP anuncia como de confianza al solicitar un certificado de cliente para la autenticación de certificados de cliente. Si la configuración de Certificado está configurada en requerir o solicitar, puede configurar la configuración de Autoridades de Certificación Anunciadas para enviar a los clientes una lista de CA en las que el servidor probablemente confíe. El valor predeterminado para la configuración de Autoridades de Certificación Anunciadas es uno, lo que indica que no se anuncia ninguna CA. Cuando se establece en uno, no se envía ninguna lista de CA de confianza a un cliente con la solicitud de certificado. Esta configuración enumera el nombre de todos los certificados SSL instalados en el sistema BIG-IP. Si desea anunciar solo una CA específica o un conjunto de CA, F5 recomienda que cree e instale un paquete que contenga los certificados de la CA que se va a anunciar. Luego puede seleccionar el nuevo paquete de certificados en la configuración de Autoridades de Certificación Anunciadas. Para obtener información sobre cómo crear un paquete de certificados personalizado, consulte**13302: Configuración gurin gel BIG-IP para usar un certificado de cadena SSL (11.x - 16.x)**
Anunciado de Confianza Para admitir varias jerarquías de PKI, este paquete puede contener certificados CA de varias PKI diferentes.	Puede configurar la**Autoridades de certificación anunciadas**para enviar una lista de CA distintas de la especificada para las Autoridades de certificación de confianza. Esto permite un mayor control sobre la información de configuración compartida con clientes desconocidos. Es posible que no desee revelar la lista completa de CA de confianza a un cliente que no presente automáticamente un certificado de cliente válido de una CA de confianza. Aunque puede configurar las dos opciones de forma diferente, en la mayoría de los casos, debe configurar la**Autoridades de certificación anunciadas**opción para usar el mismo paquete de certificados que la**Autoridades de Certificación de Confianza**configuración. **importante**Evite especificar un paquete que contenga muchos certificados al configurar las**Anunciado Autoridades de certificación**configuración. Esto minimiza la cantidad de certificados que deben intercambiarse durante un protocolo de enlace SSL cliente. El tamaño máximo permitido por el sistema BIG-IP para los mensajes de protocolo de enlace SSL nativo es de 14,304 bytes. Aunque los protocolos de enlace típicos no generan una longitud de mensaje excesiva, si el protocolo de enlace SSL está negociando un cifrado nativo y la longitud total de todos los mensajes en el protocolo de enlace supera este umbral de bytes, el protocolo de enlace falla.
CRL	Le permite configurar un objeto validador de CRL para comprobar dinámicamente los archivos CRL en función de las URL de CRL en los certificados SSL recibidos. La opción RL se introduce en BIG-IP 15.1.0.
Permitir	La configuración del archivo de lista de revocación de certificados (CRL) le permite especificar una CRL que el sistema BIG-IP debe Se utiliza para comprobar el estado de revocación de un certificado antes de autenticar a un cliente. Si desea utilizar una CRL, debe importarla al sistema BIG-IP. El nombre del archivo CRL se puede seleccionar en la lista desplegable de configuración de Archivo CRL. Para obtener información sobre cómo importar un archivo CRL SSL, consulte**14620: Mana gen gCertificados SSL para sistemas BIG-IP yusando gla configuración gutilidad de configuración y**Archivo CRL
CRL caducada Indica al sistema que utilice el archivo CRL especificado, incluso si ha caducado. Deshabilitado de forma predeterminada. La opción Permitir CRL caducada se introdujo en BIG-IP 12.0.0.	Delegación restringida de certificado de cliente

A partir de BIG-IP 13.1.0, puede usar la función de Delegación Restringida de Certificado de Cliente (C3D). Para obtener información, consulte

72668381: Descripción general de la función de Delegación Restringida de Certificado de Cliente SSL

función de ación gy el Administración del tráfico SSL**capítulo del**Sistema IG-IP: Administración SL***manual.***f**

Not

Nota**98133564: Consejos para buscar**AskF5 y encontrar** **gAskF5 y encontrar** **gdocumentación del producto

Ajuste	descripción
restringida delegación habilita o deshabilita la función C3D. El uso de la delegación restringida evita que los usuarios tengan que proporcionar credenciales dos veces para ciertas acciones de autenticación.	especifica el nombre del perfil SSL del cliente del archivo de certificado que se utiliza como certificado de cliente cuando el cliente no envía uno durante el protocolo de enlace SSL. Puede hacer clic en el icono + para abrir la pantalla de creación de
certificado Especifica el objeto OCSP de C3D que el SSL del sistema BIG-IP utilizará para conectarse al respondedor OCSP y comprobar el estado del certificado del cliente.	nuevo objeto OCSP. Reserva de cliente
Especifica la acción que realiza el sistema cuando el objeto OCSP devuelve un estado desconocido:	Puede seleccionar crear nuevo(para abrir elcrear nuevo OCSP**objeto.**CSP
Control de respuesta Registro	descartar ((Ignorar **Hace que la conexión ignore el estado desconocido y continúe.**OCSP desconocido

La

Elregistro se introduce en BIG-IP 16.1.0 y le permite especificar un destino de registro para los mensajes de registro SSL mediante un publicador de registros.

Descripción

Ajuste	Descripción
Especifica el publicador de registros definido para que el [illegible] que son iguales o superiores al nivel de registro especificado. El valor predeterminado es Advertencia. En orden descendente de urgencia, las opciones disponibles son: Alerta de emergencia, Alerta crítica, Adver	
eventos El perfil registra los eventos de autenticación de cliente SSL que son iguales o superiores al nivel de registro especificado. El valor predeterminado es alerta. En orden descendente de urgencia, las opciones disponibles son: Alerta de emergencia, Error crítico, Advertencia, Aviso, Informativo y Depuración. La opción R	Negociación SSL
Autenticación Authentication El perfil registra los eventos de autenticación de cliente SSL que son iguales o superiores al nivel de registro especificado. El valor predeterminado es alerta. En orden descendente de urgencia, las opciones disponibles son: Alerta de emergencia, Error crítico, Advertencia, Aviso, Informativo y Depuración. La opción R	Registro de cliente SSL
og SSL Reenvío Eventos de proxy	El perfil registra los eventos de proxy de reenvío SSL que son iguales o superiores al nivel de registro especificado. El valor predeterminado es Advertencia. En orden descendente de urgencia, las opciones disponibles son: emergencia, alerta, error crítico, advertencia, aviso, informativo y depuración. La opción Registrar eventos de proxy de reenvío SSL se introdujo en BIG-IP 17.1.0.

og SSL C3D Eventos	El perfil registra los eventos de delegación restringida de certificado de cliente SSL (C3D) que son iguales o superiores al nivel de registro especificado. El valor predeterminado es Advertencia. En orden descendente de urgencia, las opciones disponibles son: emergencia, alerta, crítico, error, advertencia, aviso, informativo y depuración. La opción Registrar eventos C3D SSL se introdujo en BIG-IP 17.1.0.

recomendaciones

Ninguno

Contenido relacionado

K10251520: BIG-IP su ppuerto para TLS 1.3
K8802: Uso de gCifrados SSL con perfiles SSL de cliente y servidor de BIG-IP K12390: La opción 'Preferencia del servidor de cifrado' en el perfil SSL de cliente no tiene efecto K14499: Uso de g OpenSSL para crear certificados de CA y de cliente (11.x - 16.x) K17379: Administración gen g Certificados y claves SSL de BIG-IP ys K14806: Descripción general del perfil SSL de servidor (11.x - 16.x) K75106155: Configuración gurin gOCSP staplin g(13.x - 15.x) K72355246: Requisitos del perfil SSL para servidores virtuales

Wagner Pastor

Contenido recomendado por IA

Aviso de seguridad -000156572: Trimestral ySeguridad yNotificación (octubre de 2025) Política -4309: Ciclo de vida del producto de hardware F5 ySoporte de línea pPolítica de soporte y Aviso de seguridad -
000157334: Vulnerabilidad de BIND yCVE-2025-40778
Aviso de seguridad - 000157862: Vulnerabilidad de Apache Tomcat yCVE-2025-55754

Los ingenieros de soporte de F5 que trabajan directamente con los clientes escriben artículos de Soluciones de soporte y Conocimiento, que le brindan acceso inmediato a sugerencias de mitigación, soluciones alternativas o solución de problemas.

↑ Volver a la página principal e

¿Le resultó útil esta información?

○ ○

Sí o

¿Cómo podemos mejorar este contenido?

¿Podemos ponernos en contacto con usted directamente con respecto a estos comentarios?

○ ○

Wagner Pina

Proteja y ofrezca experiencias digitales extraordinarias

La cartera de capacidades de automatización, seguridad, rendimiento y análisis de F5 permite a nuestros clientes crear, proteger y operar aplicaciones adaptativas que reducen costos, mejoran las operaciones y protegen mejor a los usuarios.obtener más información ›

QUÉ OFRECEMOS

RECURSOS

SOPORTE

SOCIOS

EMPRESA

CONÉCTESE CON NOSOTROS

CONTACTAR CON SOPORTE

más información sobre el incidente de seguridad en F5 y las medidas que estamos tomando para solucionarlo,

y nuestros esfuerzos continuos para proteger a nuestros clientes, haga clicantes de

Conocimiento

15434: Descripción general del perfil de compresión HTTP

Fecha de publicación: 3 de enero de 2015 Fecha de actualización: 21 de febrero de 2023

Contenido recomendado por IA

Aplica a:

Tema

Este artículo se aplica a BIG-IP LTM 11.x a 15.x. Para obtener información sobre otras versiones, consulte el siguiente artículo:

3393: Descripción general de com pagajuste de resolución gramos para el perfil HTTP

Cuando configura un perfil de compresión HTTP y lo asigna a un servidor virtual, el sistema BIG-IP lee el**Codificación de aceptación** El sistema BIG-IP analiza la cabecera de una solicitud del cliente y determina qué método de codificación de contenido prefiere el cliente. A continuación, elimina la cabecera. **Codificación de aceptación**El encabezado de la solicitud se pasa al servidor. Al recibir la respuesta del servidor, el sistema BIG-IP inserta el encabezado. **codificación de contenido**encabezado, especificando ya sea el**gzip**o**desinflar**, en función del método de compresión que el cliente especifique en el **Codificación de aceptación**encabezamiento.

Nota*En BIG-IP 11.x, la función de compresión del perfil HTTP se trasladó a un perfil independiente: Compresión HTTP. Antes de BIG-IP 11.x, l configuración de la compresión se gestionaba mediante el perfil HTTP.*

Descripción

Configuración	Valor	Descripción
lectivo impresión	habilitado o deshabilitado	Cuando está activada, la compresión HTTP se realiza únicamente cuando una iRule configurada contiene el comando OMPRESS::enable. Cuando está desactivada, la compresión se realiza según la configuración de compresión especificada en el perfil de compresión HTTP. ***Nota****La compresión de datos solo comprime las respuestas del servidor HTTP y no las solicitudes del cliente.*

Rhode Island Compresión	Lista de RI o no desfigurado	Especifica si se debe comprimir el contenido HTTP para las respuestas que coincidan con los valores incluidos en la lista URI.
Lista de RI	Lista nclude: Enumera los URI definidos cuyos El contenido TTP El sistema considera para compresión operaciones. Lista de exclusión: Enumera los URI definidos cuyos El contenido TTP El sistema sí lo considera para compresión operaciones. ***beneficios según objetivos****La lista de exclusión debe ser un subconjunto de las RI de la lista de inclusión.*	Especifica los URI que desea que el sistema BIG-IP incluya o excluya de las operaciones de opresión. ***beneficios según objetivos****La cadena que especificas en el****Lista de URI****La configuración puede ser una cadena de patrón o una expresión regular. Los tipos de lista distinguen entre mayúsculas y minúsculas en las cadenas de patrón. Por ejemplo, el sistema trata la cadena de patrón****www.f5.com/test** *de forma diferente a la cadena de patrón****www.f5.com/PRUEBA*** *Puedes anular este comportamiento mediante Utilice el comando de expresión regular de Linux apropiado. Por ejemplo, para especificar una coincidencia que no distinga entre mayúsculas y minúsculas para la ruta URI****/prueba****, utilice lo siguiente en su lista de inclusión: (?i)/ test.* ***beneficios según objetivos****En BIG-IP 11.0.0 a 11.1.0, si elimina todo****URI / contenido** *tipos de los****URI / Lista de contenido****caja en la****Compresión TTP****perfil, el sistema BIG-IP Comprime todo el contenido HTTP. Para deshabilitar la compresión para un servidor virtual usando n****Compresión TTP****En los perfiles de las versiones 11.0.0 a 11.1.0, debe desvincular el perfil del servidor virtual. En BIG-IP 11.2.0 y versiones posteriores, si elimina todos los perfiles, estos se desvincularán del servidor virtual.****URI / contenido****tipos de los****RI / lista de contenido****cajas en el****Compresión TTP** *En el perfil, el sistema BIG-IP no comprime ningún contenido HTTP. Para mayor claridad, tanto la lista de URI como la lista de contenido deben estar habilitadas.*
Contenido Compresión	Lista de contenidos	Especifica si el sistema comprime el tipo de contenido HTTP que se encuentra en el encabezado content-Type de una respuesta.
Lista de contenido	Lista nclude: Enumera los tipos de contenido definidos que el sistema comprime. Lista de exclusión: Enumera los tipos de contenido definidos. lo cual hace el sistema o comprimir.	Especifica el tipo de contenido para su inclusión o exclusión. ***beneficios según objetivos****La cadena que especificas en el****Lista de contenido****La configuración puede ser una cadena de patrón o una expresión regular. Los tipos de lista distinguen entre mayúsculas y minúsculas en las cadenas de patrón. Por ejemplo, el sistema trata la cadena de patrón****aplicación/pdf** *de forma diferente a la cadena de patrón****Aplicación/PDF****Puedes anular este comportamiento utilizando el comando de expresión regular de Linux apropiado.*
referido método	Cierre o desinfle	Especifica el método de compresión preferido para este perfil.
inimum Contenido longitud	número de bytes	Especifica la longitud mínima de una respuesta del servidor que el sistema considera para su opresión.
Compresión naño de la prenda	número de bytes	Especifica el número máximo de bytes comprimidos que el sistema almacena en búfer antes de decidir si mantiene una conexión Keep-Alive y reescribe el encabezado Ontentength.

gzip Compresión nivel	Un preajuste o un valor entre 1 y 9.	Especifica el nivel de compresión que el sistema utiliza cuando gzip es el método de compresión preferido. El valor mínimo es 1 y el máximo es 9. Puede seleccionar los valores 1, 6 o 9 de la lista; sin embargo, al hacer clic allí podrá introducir cualquier valor entre 1 y 9. Un número menor proporciona una relación de compresión menor pero más rápida. Un número mayor Proporciona una mayor relación de compresión, pero requiere más procesamiento, lo que hace que la compresión sea más lenta. ***beneficios según objetivos****Utilizar la configuración del nivel de compresión gzip cuando el método preferido esté configurado para****desinflar****puede modificar el nivel de compresión para****inflar****Sin embargo, la configuración de nivel no se corresponde directamente con los niveles de compresión gzip. Modificar el nivel de compresión gzip solo incrementa la compresión para****desinflar****usando niveles 1 -* *Configurar el nivel de compresión gzip a un valor superior a 5 generalmente utiliza el mismo máximo.****inflar****Se alcanza el nivel de compresión cuando se utiliza* *Nivel de impresión 5.* ***beneficios según objetivos:****Las diferentes plataformas tendrán diferentes niveles de compresión dependiendo del hardware específico utilizado para la compresión.*
Memoria gzip nivel	1 - 256 kilobytes	Su valor especifica la cantidad de memoria que la biblioteca de compresión (**zlib**) ses para sus búferes de compresión internos. El valor predeterminado (8 kilobytes) es la configuración óptima para la mayoría de los casos. Sin embargo, los sitios que sirven principalmente archivos más grandes pueden beneficiarse al aumentar este valor. Debe tener en cuenta el Tamaño promedio de los archivos que el sistema comprime cuando se modifica esta configuración. ***beneficios según objetivos****Aumentar el****nivel de memoria gzip****El aumento de este valor puede incrementar la velocidad del proceso de impresión, pero esto conlleva un mayor uso de memoria o conexión.*
Ventana gzip Tamaño	1 - 128 kilobytes	Esta configuración determina la cantidad de memoria que el sistema utiliza para el búfer del historial de compresión. Este valor es similar al Nivel de Memoria de zip, pero zlib lo interpreta de forma diferente. Al igual que con el Nivel de Memoria de zip, los sitios que sirven principalmente archivos grandes pueden beneficiarse al aumentar este valor. Debe tener en cuenta el tamaño promedio de los archivos que se comprimen al modificar esta configuración.
Variar encabezado	habilitado o deshabilitado	Cuando está habilitado, especifica que el sistema inserta la codificación Vary: Accept-Encoding. El encabezado `Vary` se incluye en las respuestas comprimidas del servidor, independientemente del tipo de contenido configurado. Si el encabezado `Vary` ya existe en la respuesta, el sistema añade el valor `Accept-Encoding` a dicho encabezado.
TTP/1.0 legados	habilitado o deshabilitado	Cuando está habilitado, especifica que el sistema puede comprimir las respuestas a HTTP/1.0. Las solicitudes del cliente se rechazan si el servidor responde con un encabezado Connection: Close y el contenido de la respuesta no es mayor que el valor de la configuración de tamaño de búfer de compresión.

Aceptar ncoding	habilitado o deshabilitado	Cuando está habilitada, especifica que el sistema conserva la cabecera Accept-Encoding en la solicitud HTTP, lo que permite que el servidor de destino realice la compresión, en lugar de que lo haga el sistema. El comportamiento normal es que el sistema elimine la cabecera Accept-Encoding. Cabecera ncoding de la solicitud HTTP.
remero Soluciones alternativas	habilitado o deshabilitado	Cuando está habilitado, especifica que el sistema BIG-IP utiliza soluciones alternativas integradas para Varios problemas comunes del navegador que ocurren al comprimir contenido. Específicamente, el sistema verifica las siguientes condiciones y, si las encuentra, impide la compresión de las respuestas del servidor: El navegador del cliente es Netscape versión 4.0x. El navegador del cliente es Netscape versión 4.10 y superior.**Contenttype**La cabecera de la respuesta del servidor no está configurada para**texto/html**o**texto plano** El navegador del cliente es Microsoft Internet Explorer (cualquier versión), el**ontentype** La cabecera de la respuesta del servidor se establece en:**texto/css**o**aplicación/xjavascript**y la conexión del cliente utiliza SSL. El navegador del cliente es Microsoft Internet Explorer (cualquier versión), el**ontentype**La cabecera de la respuesta del servidor se establece en:**texto/css**o**aplicación/xjavascript**y el **Control de caché**La cabecera de la respuesta del servidor está configurada para **o-cache**. *Nota: La opción de soluciones alternativas para el navegador no está incluida en BIG-IP 13.x ni en versiones posteriores.*
orro de CPU	habilitado o deshabilitado	Cuando está habilitado, especifica que el sistema monitoriza el porcentaje de uso de la CPU y Ajusta automáticamente las tasas de compresión cuando el uso de la CPU alcanza el umbral alto de ahorro de CPU o el umbral bajo de ahorro de CPU.
Ahorro de CPU alto Límite	porcentaje	Especifica la cantidad de uso de CPU que provoca que el sistema cambie la cantidad de contenido que comprime y el nivel de compresión que aplica. Por ejemplo, cuando se alcanza el porcentaje de uso de CPU configurado: Cada conexión se evalúa individualmente para determinar si hay impresión en ese momento. El nivel de compresión se cambia al valor más bajo (más rápido).
Ahorro de CPU Ay Límite	porcentaje	Especifica la cantidad de uso de CPU que hace que el sistema vuelva a los valores de compresión definidos por el servidor.

recomendaciones

Ninguno

Contenido eufórico

El**Acerca de los perfiles de compresión HTTP**sección de la***Gestión del tráfico local de BIG-IP: Referencia de perfiles*** más tarde) anual (11.6.0 y

El**Acerca de los perfiles de compresión HTTP**sección de la***Administrador de tráfico local BIG-IP: Conceptos***anual (11.5.0 - 11.5.4) El **Compresión de respuestas HTTP**sección de la***BIG-IP Local Traffic Manager: Implementaciones***anual para su versión de

Nota*Para obtener información sobre cómo localizar los manuales de productos F5, consulte* ***pag*** ***98133564: Consejos para la búsqueda*** ***gramoAskF5 y encontrar*** ***gramo***

Documentación del producto

K14994: Nombre del perfil HTTP gramoconsideraciones cuando u pág.radin gramoDe BIG-IP 10.x a 11.x

Contenido recomendado por IA

Aviso de seguridad - **000156572: Trimestral ySeguridad yNotificación (octubre de 2025))** .

Política - **4309: Ciclo de vida del producto de hardware F5 ycle sup pagpolicía de ort y** .

Política - **5903: Software BIG-IP su pagpolicía portuaria y** .

Conocimiento - **7727: Activación de licencia ma yserá necesario antes de una actualización de software. gramomercado para BIG-IP**

Los ingenieros de soporte de F5 que trabajan directamente con los clientes escriben artículos de Soluciones de Soporte y de Conocimiento, que le brindan acceso inmediato a sugerencias de mitigación, soluciones alternativas o resolución de problemas.

Volver a pag .

¿Fue útil esta información?

Sí o

¿Cómo podemos mejorar este contenido?

¿Podemos ponernos en contacto con usted directamente en relación con estos comentarios?

Sí o

Protegido por reCAPTCHA: privacidad & Términos

Garantizar y ofrecer experiencias digitales extraordinarias

La cartera de capacidades de automatización, seguridad, rendimiento y análisis de 5 permite a nuestros clientes crear, proteger y operar aplicaciones adaptativas que reducen los costos.

mejorar las operaciones y proteger mejor a los usuarios. Más información

LO QUE OFRECEMOS

RECURSOS ELECTRÓNICOS

APOYO

ARTISTAS

COMPAÑÍA

CONÉCTATE CON NOSOTROS

CONTACTAR CON SOPORTE

Wagner Pastor

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

más información sobre el incidente de seguridad en F5 y las medidas que estamos tomando para solucionarlo,

y nuestros esfuerzos continuos para proteger a nuestros clientes, haga clicantes de

Solución de soporte

26898044: Métodos de persistencia disponibles en F5 BIG-IP

Fecha de publicación: 7 de noviembre de 2022 Fecha de actualización: 21 de febrero de 2023

Contenido recomendado por IA

Aplica a:

descripción

Cuando sea necesario mantener una sesión de usuario redirigida a un miembro específico del grupo, es necesario definir y asignar un método de persistencia.

medio ambiente

Big-IP
LTM

Causa

Las solicitudes de los usuarios dentro de una misma sesión se distribuirán equitativamente entre todos los miembros del grupo, si no se ha definido ningún método de persistencia y no se ha asignado al servidor virtual correspondiente.

acciones recomendadas

Seleccione el método de persistencia más conveniente y asígnelo al servidor virtual.

Dependiendo del tipo de sesión, existen varios métodos de persistencia entre los que elegir.

E son los métodos de persistencia compatibles con las unidades BIG-IP de F5 Networks:

persistencia de cookies

asociados a la persistencia simple, ya que el ID de sesión es único.

persistencia de afinidad de dirección de destino

También conocida como persistencia sticky, la persistencia por afinidad de dirección de destino admite los protocolos TCP y UDP, y dirige las solicitudes de sesion al mismo servidor basándose únicamente en la dirección IP de destino de un paquete.

persistencia hash

La persistencia hash permite crear un hash de persistencia basado en un perfil de persistencia hash existente. Su uso es similar al de la persistencia universal, con la diferencia de que, en el caso de la persistencia hash, la clave de persistencia resultante es un hash de los datos, en lugar de los datos en sí. Se puede crear un valor hash a partir de la IP de origen, la IP de destino y el puerto de destino. Si bien no es necesariamente único para cada sesión, esta técnica permite una distribución más uniforme de la carga entre los servidores.

No se puede asociar la persistencia hash con un servidor virtual que gestione tráfico Fast L4; el uso de la persistencia hash para tráfico Fast L4 está prohibido.

persistencia del huésped

La persistencia de host permite que el sistema BIG-IP utilice la cabecera HTTP Host incluida en una solicitud HTTP para determinar qué miembro del pool seleccionar. También puede activar la persistencia de host desde una iRule.

Persistencia del protocolo de escritorio remoto de Microsoft

La persistencia del Protocolo de Escritorio Remoto de Microsoft (MSRDP) realiza un seguimiento de las sesiones entre clientes y servidores que ejecutan el servicio de Protocolo de Escritorio Remoto de Microsoft (RDP).

persistencia SIP

La persistencia SIP es un tipo de persistencia específica de la aplicación que se utiliza en servidores que reciben mensajes del Protocolo de Inicio de Sesión (SIP) enviados a través de UDP, SCTP o TCP. Esta técnica de persistencia se suele utilizar con aplicaciones con estado que dependen de que el cliente esté conectado a la misma instancia de la aplicación durante toda la sesión.

persistencia de afinidad de dirección de origen

También conocida como persistencia simple, la persistencia por afinidad de dirección de origen admite los protocolos TCP y UDP, y dirige las solicitudes de sesión al mismo servidor basándose únicamente en la dirección IP de origen de un paquete.

persistencia SSL

Dado que las sesiones SSL deben establecerse y están estrechamente vinculadas a la conexión entre cliente y servidor, si no se mantiene la sesión segura mediante SSL, se produce una renegociación de la misma. El sistema BIG-IP utiliza el ID de sesión SSL para garantizar que la sesión se enrute correctamente a la instancia de la aplicación a la que se conectó inicialmente. Incluso si la dirección IP del cliente cambia, el sistema BIG-IP sigue reconociendo la conexión como persistente gracias al ID de sesión.

persistencia universal

que el sistema BIG-IP pueda inspeccionar y extraer cualquier dato de una solicitud o respuesta. Con la persistencia universal, puede escribir una expresión que defina los datos que el sistema BIG-IP conservará en un paquete.

información adicional

La información anterior es un extracto de la sección "perfiles de persistencia de sesión" del manual de configuración. Se recomienda encarecidamente leer dicho documento para comprender completamente todos los tipos de persistencia.

Capítulo del manual:Perfiles de persistencia de sesión

Contenido recomendado por IA

Aviso de seguridad - **000156572: Trimestral ySeguridad yNotificación (octubre de 2025))**

Política - **4309: Ciclo de vida del producto de hardware F5 ycle sup pagpolicía de ort y**

Política - **5903: Software BIG-IP su pagpolicía portuaria y**

Conocimiento - **7727: Activación de licencia ma yserá necesario antes de una actualización de software. gramomercado para BIG-IP**

Los ingenieros de soporte de F5 que trabajan directamente con los clientes escriben artículos de Soluciones de Soporte y de Conocimiento, que le brindan acceso inmediato a sugerencias de mitigación, soluciones alternativas o resolución de problemas.

olver a pag

¿Fue útil esta información?

Sí o

¿Cómo podemos mejorar este contenido?

¿Podemos ponernos en contacto con usted directamente en relación con estos comentarios?

Sí o

tegido por reCAPTCHA: privacidad & Términos

Garantizar y ofrecer experiencias digitales extraordinarias

La cartera de capacidades de automatización, seguridad, rendimiento y análisis de 5 permite a nuestros clientes crear, proteger y operar aplicaciones adaptativas que reducen los costos. Mejorar las operaciones y proteger mejor a los usuarios.gana más ›

LO QUE OFRECEMOS

RECURSOS ELECTRÓNICOS

APOYO

ARTISTAS

COMPAÑÍA

CONÉCTATE CON NOSOTROS

Wagner Peña

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

CONTACTAR CON SOPORTE

más información sobre el incidente de seguridad en F5 y las medidas que estamos tomando para solucionarlo,

y nuestros esfuerzos continuos para proteger a nuestros clientes, haga clicantes de

Conocimiento

44525501: Descripción general del plano de datos y el carril de control de BIG-IP

Fecha de publicación: 9 de mayo de 2022 Fecha de actualización: 15 de octubre de 2024

Contenido recomendado por IA

Aplica a:

Wagner Peña

expert IPX SRL RNC 130-850151 Santo Domingo, R.D.

Tema

Lstemas tradicionales de tráfico y computación suelen dividir el procesamiento en dos componentes discretos: el plano de datos y el plano de control.

Descripción

plano de datos

El procesamiento del plano de datos se ocupa del proceso básico de obtención de datos, ya sean entradas del sistema o solicitudes de los usuarios, y de la devolución de datos (salidas, archivos o respuestas). Este procesamiento se relaciona con la conectividad básica que gestiona el flujo de tráfico hacia y desde lc destinos. En el caso del sistema BIG-IP, el plano de datos es responsable de casi todo el procesamiento del tráfico de red en tiempo de ejecución, incluido el tráfico balanceado por el Microkernel de Gestión de Tráfico (TMM). El TMM se ejecuta como un proceso de usuario en tiempo real dentro del sistema operativc BIG-IP (TMOS). Por ejemplo, el plano de datos procesa el tráfico para lo siguiente:

Objetos de gestión de tráfico, por ejemplo, servidores virtuales, SNAT y NAT;
módulos del sistema BIG-IP, por ejemplo, BIG-IP APM y BIG-IP ASM.
Tráfico con balanceo de carga entre blades VIPRION procesado por la instancia TMM apropiada ***Nota****El sistema operativo anfitrión basado en Linux no participa en el procesamiento de las tareas TMM.*

r de control

El plano de control gestiona las tareas relacionadas con la administración para procesar el tráfico de administración en función del contexto y las políticas. Por ejemplo, el plano de control procesa el tráfico de administración (no TMM) para lo siguiente:

Procesos BIG-IP, por ejemplo, MCPD y crond.

tráfico de gestión de clústeres y blades de VIPRION

iControl REST

SSH, ya sea a través de la dirección IP de administración o una dirección IP propia que exponga los puertos HTTPS o SSH (443 o 22).

La utilidad de configuración de BIG-IP, Traffic Management Shell (**tmsh**), y TMCTL

Nota*Esto también se aplica a la Edición Virtual y a las instancias invitadas.*

información adicional

Los monitores y comprobaciones de estado de BIG-IP pueden procesar tráfico del plano de control y del plano de datos, según su configuración. Por ejemplo, al configurar la cadena de envío/recepción o los campos de nombre de usuario/contraseña de su monitor, el miembro del grupo puede devolver datos de la aplicación que podrían contener información confidencial. Además, tenga en cuenta lo siguiente:**Monitores In-TMM** y**monitores externos** que también puede procesar datos de la aplicación.

Contenido eufórico

K15003: Las tareas del plano de datos y del plano de control utilizan un plano separado. gramonúcleos ical cuando el BIG-IP s yLa CPU Stem utiliza Intel H yper-Threadin gramo Tecnología gy

Wagner Peña

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Contenido recomendado por IA

Aviso de seguridad - **000156572: Trimestral ySeguridad yNotificación (octubre de 2025))**

Política - **4309: Ciclo de vida del producto de hardware F5 ycle sup pagpolicía de ort y**

Política - **5903: Software BIG-IP su pagpolicía portuaria y**

Conocimiento - **7727: Activación de licencia ma yserá necesario antes de una actualización de software. gramomercado para BIG-IP**

Los ingenieros de soporte de F5 que trabajan directamente con los clientes escriben artículos de Soluciones de Soporte y de Conocimiento, que le brindan acceso inmediato a sugerencias de mitigación, soluciones alternativas o resolución de problemas.

↑ **Volver a pag**

¿Fue útil esta información?

○ ○

Sí o

¿Cómo podemos mejorar este contenido?

¿Podemos ponernos en contacto con usted directamente en relación con estos comentarios?

○ ○

Sí o

Garantizar y ofrecer experiencias digitales extraordinarias

La cartera de capacidades de automatización, seguridad, rendimiento y análisis de 5 permite a nuestros clientes crear, proteger y operar aplicaciones adaptativas que reducen los costos. Mejorar las operaciones y proteger mejor a los usuarios.gana más ›

LO QUE OFRECEMOS

RECURSOS ELECTRÓNICOS

APOYO

ARTISTAS

COMPAÑÍA

CONÉCTATE CON NOSOTROS

Wagner Peña

IPX SRL
RNC 130-850151
Santo Domingo, R.D.

CONTACTAR CON SOPORTE

más información sobre el incidente de seguridad en F5, las acciones que estamos tomando para abordarlo,

y nuestros esfuerzos continuos para proteger a nuestros clientes, haga clicantes de

Conocimiento

7820: Descripción general de las funciones de SNAT

Fecha de publicación: 22 de septiembre de 2015 Fecha de actualización: 13 de octubre de 2025

Contenido recomendado por IA

Se aplica a:

Tema

Descripción general

Una Traducción Segura de Direcciones de Red (SNAT) es un objeto que asigna la dirección IP del cliente de origen en una solicitud a una dirección de traducción definida en el dispositivo BIG-IP. Cuando el sistema BIG-IP recibe una solicitud de un cliente, y si la dirección IP del cliente en la solicitud está definida en la lista de direcciones de origen de la SNAT, el sistema BIG-IP traduce la dirección IP de origen del paquete entrante a la dirección SNAT.

Un SNAT puede usarse por sí solo para transferir tráfico no destinado a un servidor virtual. Por ejemplo, puede usar un objeto SNAT para transferir cierto tráfico (como solicitudes DNS) desde una red interna a una red externa donde reside su servidor DNS.

Una SNAT también se puede usar junto con un servidor virtual y la dirección de destino de una NAT (mostrada como dirección NAT en la utilidad de configuración) para traducir la dirección IP de origen de una conexión entrante. (Si no se configura una SNAT, no se realiza la traducción de la dirección de origen). En este caso, los objetos SNAT coinciden con el tráfico después de que este ya haya coincidido con un servidor virtual o NAT y, por lo tanto, traducen la dirección de origen al salir al servidor, a menos que dicho tráfico ya esté sujeto a SNAT aplicadas al servidor virtual.

418

Por ejemplo, cuando el sistema BIG-IP recibe una nueva conexión desde la dirección IP de origen**192.168.20.1**a la dirección IP de destino **192.168.10.1**El servidor virtual o el oyente NAT en**192.168.10.1**acepta la conexión y, al salir al lado del servidor, el oyente SNAT**92.168.20.0/24**procesa la conexión y traduce la dirección de origen a la**Traducción**dirección que es

objeto SNAT. Siguiendo con el ejemplo, el sistema traduce**192.168.20.1**a**172.16.20.1**Como resultado de este comportamiento, puede configurar un único objeto SNAT para traducir el tráfico de todos los servidores virtuales destinados al siguiente salto en el lado del servidor, en lugar de configurar el**Traducción de la dirección de origen**Propiedad en cada servidor virtual. En este caso, si desea omitir el SNAT de un servidor virtual específico (que tiene un grupo configurado) y permitir la dirección del cliente en el servidor, puede deshabilitar la configuración del grupo asociado.**Permitir SNAT**

También puede usar una SNAT para garantizar que el tráfico de respuesta se devuelva a través del sistema BIG-IP sin necesidad de que otro tráfico saliente sir balanceo de carga se enrute también a través del sistema BIG-IP, y sin necesidad de realizar cambios en la configuración del enrutador o del servidor. SNAT también es un componente crítico en las configuraciones de un solo brazo, ya que impide que el servidor responda directamente al cliente.

Un SNAT funciona de la siguiente manera:

El sistema BIG-IP recibe una solicitud directamente de un cliente o del tráfico del servidor virtual y verifica si esa dirección IP de origen está definida en la lista de direcciones de origen para el SNAT.
Si la dirección IP del cliente está definida en la lista de direcciones de origen para el SNAT, el sistema BIG-IP traduce la dirección IP de origen a la dirección de traducción definida en el SNAT.
Luego, el sistema BIG-IP envía la solicitud del cliente al miembro del grupo o a otro destino.

Tipos de SNAT

Las SNAT estándar y las SNAT inteligentes se ilustran en las siguientes secciones:

SNAT estándar

Los siguientes tres ejemplos ilustran tres tipos de SNAT estándar:

Un SNAT en el que se especifica una dirección de traducción específica

Una forma de crear una SNAT es asignar directamente una o más direcciones IP originales a una dirección de traducción específica que usted elija. Para la dirección de origen de la SNAT, puede especificar direcciones de host, direcciones de red o un comodín que coincida con todas las direcciones. Por ejemplo, el siguiente**tmsh**El comando traduce la dirección de las conexiones que se originan en la dirección 10.10.10.1 a la dirección de traducción 172.16.0.1:

reate /ltm snat /Common/test_snat origins agregar { 10.10.10.1/32 } traducción 172.16.0.1

Nota*Asegúrese de especificar el ID del dominio de ruta en la dirección de origen y de traducción al traducir direcciones para dominios de ruta específicos. Por ejemplo:**10.10.10.1%5/32*

Nota:*Para obtener más información sobre SNAT y grupos de SNAT, consulte**K47945399: Crear SNAT básicos y grupos de SNAT*.

Automático SNAT

De las opciones SNAT disponibles, la opción automática SNAT suele ser la preferida porque es fácil de configurar y mantener, y ayuda a conservar direcciones IP al usar las direcciones IP existentes del sistema BIG-IP.

Cuando el sistema BIG-IP procesa conexiones desde las direcciones IP de origen que coinciden con una definición de mapa automático SNAT, elige una

conmutación por error sin interrupciones. Si se configuran varias direcciones IP propias flotantes en la VLAN, el sistema BIG-IP traduce la dirección de las conexiones de cliente alternando entre un conjunto de todas las IP propias flotantes en la VLAN.

Nota**Es posible que la función de asignación automática de SNAT no utilice la dirección de traducción deseada si no hay una IP propia flotante disponible en la VLAN de salida, o s[illegible]ección IP propia flotante era originalmente una dirección IP propia estática. Para obtener más información, consulte**K7336: El mapa automático SNAT y la selección automática de dirección IP

Por ejemplo, lo siguiente**tmsh**El comando traduce la dirección de las conexiones que se originan en la dirección 10.10.10.1 a una de las direcciones IP propias del sistema:

reate /ltm snat /Common/test_snat orígenes de asignación automática agregar { 10.10.10.1/32 }

La siguiente**tmsh**El comando traduce direcciones del rango de red 10.10.0.0/16:

reate /ltm snat /Common/test_snat orígenes de asignación automática agregar { 10.10.0.0/16 }

Grupos SNAT

Un grupo SNAT representa un conjunto de direcciones de traducción que se configuran en el sistema BIG-IP. La dirección IP original se asigna a todo el grupo de traducción, denominado grupo SNAT. Por ejemplo, el siguiente ejemplo**tmsh**El comando contiene las direcciones de traducción 172.16.0.1 y 172.16.0.2:

[illegible]ear /ltm snatpool /Common/my_snatpool miembros agregar { 172.16.0.1 172.16.0.2 }

Después de crear el grupo SNAT, debe asociarlo con un objeto SNAT. Por ejemplo, el siguiente**tmsh**El comando traduce la dirección d las conexiones que se originan en la dirección 10.10.10.1 a una de las direcciones IP del grupo SNAT:

crear /ltm snat /Common/test_snatpool orígenes agregar { 10.10.10.1/32 { } } snatpool y_snatpool

importanteAl utilizar un grupo SNAT con direcciones IP de la VLAN de salida (la VLAN por la que sale el paquete en el sistema BIG-IP) y redes VLAN que no son de salida, la dirección de red de la VLAN de salida tiene mayor prioridad. Por ejemplo, la VLAN de salida **externo**como una IP propia de 172.16.0.254/24 y direcciones de miembros del grupo SNAT de 172.16.0.1/24 y 10.1.1.1/24. El sistema BIG-IP hace referencia a la dirección del miembro del grupo SNAT de VLAN de salida 172.16.0.1 y continúa usando la misma dirección hasta que no esté disponible.

***Nota**:El sistema BIG-IP equilibra la carga de las conexiones del grupo SNAT entre los miembros mediante el**conexiones del este**algoritmo.*

*I[illegible]:Para obtener más información sobre SNAT y grupos de SNAT, consulte**K47945399: Crear SNAT básicos y grupos de SNAT** .*

SNAT inteligentes **420**

Una SNAT inteligente consiste en la asignación de una o más direcciones IP de cliente originales a una dirección de traducción. Sin embargo, este tipo de asignación de SNAT se implementa dentro de una iRule. Una SNAT inteligente permite al sistema BIG-IP basar la selección de una dirección de traducción.

paquete, como un puerto de servidor o una cookie HTTP.

Para configurar un SNAT inteligente, debe completar las siguientes tareas:

eterminar el tipo de paquete de datos que el sistema BIG-IP utiliza como base para seleccionar una dirección de traducción, como el puerto del servidor.

Cree el SNAT o los grupos de SNAT que el sistema BIG-IP utiliza para seleccionar una dirección de traducción. Asigne la iRule como recurso al servidor virtual.

Los siguientes dos ejemplos ilustran la asignación de direcciones IP de clientes originales a una dirección de traducción utilizando una iRule:

Ejemplo 1

Si desea que el sistema BIG-IP base la selección de una dirección de traducción en el puerto de destino, primero debe crear un grupo de datos que contenga los puertos de destino y, a continuación, crear la iRule que aplica la dirección de traducción SNAT a las conexiones que utilizan un puerto especificado en el grupo de datos. Después de crear el grupo de datos y la SNAT, debe asignar la iRule como recurso al servidor virtual. A continuación:**tmsh**El comando crea un grupo de datos llamado**puertos**que contiene los puertos 80, 81 y 8080:

crear /ltm grupo de datos internos Puertos tipo cadena registros agregar { 80 81 8080 }

Después de crear el grupo de datos, cree la iRule que aplica la dirección de traducción SNAT a las conexiones que utilizan los puertos del grupo de datos Puertos. Los siguientes ejemplos de iRule aplican la dirección de traducción SNAT 172.16.0.1 a las conexiones que utilizan los puertos del grupo de datos P s:

. Crea la iRule usando**tmsh**e ingresando el siguiente comando:

crear la regla /ltm Ports_Snat_iRule

. Coloque una estrofa similar a la siguiente entre las llaves de apertura y cierre:

cuando CLIENTE_ACEPTADO {
f { [coincidencia de clase [TCP::local_port] es igual a Puertos]} { nat
172.16.0.1

. Después de que el sistema confirme los cambios, presione ESC para salir del modo interactivo y luego ingrese:**wq**

. SeleccionaryPara guardar los cambios.

Aplique la iRule al servidor virtual utilizando la siguiente sintaxis de comando:

odify /ltm reglas virtuales ftp_vs { Port_Snat_iRule }

Guarde la configuración ingresando el siguiente comando:

ave /sys config particiones todas

Ejemplo 2

Si desea que el sistema BIG-IP base su selección de una dirección de traducción en la dirección IP de origen/cliente y el puerto de destino, y luego reenvíe el tráfico sin cambios que no coincida con estos criterios, primero deberá crear dos grupos de datos que contengan las direcciones IP de origen/cliente y los puertos de destino respectivamente, y luego crear la iRule que aplicaría la dirección de traducción SNAT.

crear /ltm grupo de datos Tipo de host Registros IP agregar { 10.10.10.1 10.10.10.2 10.10.10.3 }

L uientetmshEl comando crea un grupo de datos llamadoPuertos, que contiene los puertos 80 y 8080:

crear /ltm grupo de datos Puertos tipo cadena registros agregar { 80 8080 }

Después de crear los grupos de datos, cree la iRule que aplica la dirección de traducción SNAT a las conexiones que utilizan direcciones IP y puertos de los grupos de datos Hosts y Puertos, y reenvía todas las demás conexiones. El siguiente ejemplo de iRule aplica la dirección de traducción SNAT de 172.16.0.1 a las conexiones que utilizan direcciones IP y puertos de los grupos de datos Hosts y Puertos, y reenvía todas las demás conexiones:

Para crear la iRule usando tmsh, ingrese el siguiente comando:

crear regla /ltm Hosts_Ports_Snat_iRule

. Coloque una estrofa similar a la siguiente entre las llaves de apertura y cierre:

cuando CLIENTE_ACEPTADO {

f { [coincidencia de clase [IP::client_addr] es igual a Hosts]} { f
{ [coincidencia de clase [TCP::local_port] es igual a Puertos]} { nat
172.16.0.1
demás {

hacia adelante

. Después de que el sistema confirme los cambios, presione ESC para salir del modo interactivo y luego ingrese:**wq**

. SeleccionaryPara guardar los cambios.

Aplique la iRule al servidor virtual utilizando la siguiente sintaxis de comando:

odify /ltm reglas virtuales ftp_vs { Hosts_Ports_Snat_iRule }

Guarde la configuración ingresando el siguiente comando:

ave /sys config particiones todas

Agotamiento del puerto SNAT

El agotamiento de puertos o las colisiones pueden ocurrir bajo condiciones de uso intensivo o patrones de tráfico de clientes especiales. Como resultado, las conexiones que no se pueden traduci debido a la falta de puertos disponibles en una dirección de traducción determinada pueden ser descartadas.

Cuando se configura una SNAT en el sistema BIG-IP (ya sea de forma independiente o junto con un servidor virtual), la dirección de origen de cada conexión se traduce a una dirección SNAT configurada y el puerto de origen se asigna a un puerto disponible para esa dirección. De forma p terminada, el sistema BIG-IP intenta conservar el puerto de origen, pero si este ya está en uso en la dirección de traducción seleccionada, el sistema también traduce el puerto de origen.

Nota*A partir de BIG-IP 10.0.0, es posible controlar, por servidor virtual, si el sistema debe conservar el puerto de origen del cliente. Para más información, consulte****11003: Confi gramoorina gramofuente pagPreservación de ort para servidores virtuales***

que utilizan un entero sin signo de 16 bits (de 0 a 65535) para especificar los puertos de origen y destino. Sin embargo, cada dirección SNAT puede procesar potencialmente más de 65535 conexiones simultáneas, siempre que cada par de sockets sea único. Un par de sockets se define mediante una estructura de 4 tuplas que consta de los siguientes elementos:

irección IP de origen

Puerto de origen

Dirección IP de destino

Puerto de destino

Wagner Pena

Por ejemplo, una dirección SNAT determinada puede seguir utilizando el mismo puerto de origen siempre que el socket remoto sea único, lo que permite que la dirección SNAT procese más de 65535 conexiones simultáneas.

Por ejemplo:

Dirección SNAT y puerto Socket remoto

0.1.1.1:1234 ----------> 10.1.1.200:80
0.1.1.1:1234 ----------> 10.1.1.201:80
0.1.1.1:1234 ----------> 10.1.1.200:8080
0.1.1.1:1234 ----------> 10.1.1.201:8080

Nota*Cuando se utiliza SNAT junto con un servidor virtual que equilibra la carga de las conexiones a un pool, el socket remoto es la dirección IP y el puerto del miembro del pool seleccionado. Por lo tanto, suponiendo que una dirección SNAT esté configurada en un solo servidor virtual, esta puede procesar aproximadamente 65535 conexiones simultáneas para cada miembro del pool (cada socket remoto único).*

Si bien la singularidad de los sockets remotos depende completamente de su configuración y tráfico específicos, para simplificar, considere 65535 conexiones simultáneas como la capacidad máxima para cualquier dirección SNAT. Si cree que más de 65535 conexiones podrían requerir traducción, debería configurar más direcciones SNAT (por ejemplo, mediante un pool SNAT).

Es posible que pueda determinar cuándo se produce el agotamiento del puerto SNAT revisando los archivos de registro del sistema. Cuando se produce un agotamiento del puerto, se registran en el sistema mensajes de error similares a los siguientes ejemplos.**/var/log/ltm**file:

01010201:2: Agotamiento del puerto Inet del 10.1.21.26 al 172.28.21.71:53 (proto 17) 01010201:2: Agotamiento del puerto Inet del 10.10.10.211 al 172.28.21.123:80 (proto 6)

Nota*:Los mensajes de error anteriores no son específicos del agotamiento del puerto SNAT y pueden registrarse siempre que el microkernel de administración de tráfico (TMM) detecte el agotamiento del puerto de un objeto de administración de tráfico.*

A partir de BIG-IP 12.0.0, el sistema emite una alerta temprana cuando detecta que el grupo de puertos de servicio disponibles está a punto de agotarse. Para obtener más información sobre cómo configurar el umbral del mensaje de agotamiento de puertos, consulte**K63275550: Modificación yen gramoLos BIG-IP yAdvertencia de agotamiento del puerto efímero del tallo gramo**.

P e monitorear la cantidad de conexiones simultáneas que pasan por SNAT ejecutando el comando**tmsh mostrar /ltm snat**comando, o en la utilidad de configuración, elija uno de los siguientes métodos:

BIG-IP 12.0.0 y posteriores

- Inicie sesión en la utilidad de configuración.
- Ir a**Estadísticas > Estadísticas del módulo > Tráfico local**.

BIG-IP 11.0 y anteriores

Ir a**Descripción general**>**Estadística**>**Tráfico local**>**Tipo de estadísticas**y seleccionar**SNAT**

Para obtener información sobre cómo mitigar el agotamiento del puerto SNAT, consulte**pecado gramo**Grupos SNAT o mapas automáticos SNAT para evitar colisiones de puertos en el SNAT se utilizan y se aplican las siguientes prácticas recomendadas.

Usos y mejores prácticas de SNAT

Al planificar el tráfico SNAT, debe considerar los siguientes factores:

Número de conexiones simultáneas

Reutilización de conexiones

Tiempo de espera inactivo de TCP/UDP

Para maximizar la disponibilidad de los puertos SNAT efímeros, limite el tiempo que un puerto TCP/UDP permanece inactivo reduciendo el tiempo de espera d SNAT al mínimo posible para el tráfico que admite. Por ejemplo, el tráfico HTTP no requiere un tiempo de espera prolongado, ya que utiliza conexiones activas de corta duración. Un tiempo de espera de TCP inactivo de 60 segundos es más que suficiente para el tráfico HTTP general. Si la SNAT admite tráfico FTP, el tiempo de espera debe tener en cuenta el flujo de datos tanto por el canal de control como por el de datos: el canal de control puede quedar inactivo mientras se envían datos por el canal de datos, por lo que el tiempo de espera de SNAT debe reflejar el tiempo de transferencia de la descarga de datos más larga pr ta. En general, un tiempo de espera de TCP inactivo de 120 a 300 segundos es más que suficiente para el tráfico FTP.

Uso juicioso

Habilite SNAT solo cuando sea necesario, para preservar las direcciones IP y los puertos de origen disponibles.

Permitir que los hosts internos accedan a dispositivos externos a través del sistema BIG-IP

Si tiene hosts internos configurados para enrutar al sistema BIG-IP y estos hosts requieren acceso a dispositivos externos a través de este, puede crear un objeto SNAT. Por ejemplo, puede crear un objeto SNAT en el sistema BIG-IP para transferir cierto tráfico administrativo, como DNS o SNMP, desde una red interna a una red externa. El objeto SNAT traduce la dirección IP de origen del paquete a la dirección SNAT para que el dispositivo externo enrute el paquete de respuesta de vuelta al sistema BIG-IP.

Conexión a un servidor virtual con un miembro del grupo que está en la misma subred IP que el cliente

Si desea equilibrar la carga de las solicitudes a los nodos que se encuentran en la misma red que los clientes, debe configurar un SNAT en el sistema BIG-IP para que las conexiones y las respuestas se transmitan a través de él. Esto se conoce comúnmente como configuración de un solo brazo.

l e grupos SNAT o mapas automáticos SNAT para evitar colisiones de puertos

Las SNAT tienen un límite de 65535 puertos. Las conexiones SNAT pueden fallar si un gran número de solicitudes de clientes las atraviesan. Para mitigar las colisiones de puertos, cree grupos de SNAT o utilice la asignación automática de SNAT con un número adecuado de direcciones IP propias en la VLAN para soportar el nivel esperado de conexiones simultáneas mediante SNAT.

Una SNAT reduce la aceleración de velocidad de paquetes ASIC (PVA) en sistemas equipados con un chip PVA. Cuando una SNAT se asocia a un servidor virtual, este se reduce a aceleración PVA parcial.

L IAT no conservan la dirección del cliente

Cuando el sistema BIG-IP traduce la dirección IP de origen del paquete entrante a la dirección SNAT, el servidor web considera que la solicitud proviene de la dirección SNAT, no de la dirección IP original del cliente. Si el servidor web debe registrar las conexiones utilizando la dirección IP original del cliente, la traducción de direcciones SNAT lo impide.

Los SNAT solo reenvían tráfico TCP y UDP

De forma predeterminada, las SNAT solo reenvían tráfico TCP y UDP. Se descarta cualquier otro tráfico IP, como el Protocolo de mensajes de control de Internet (ICMP). Puede configurar las SNAT para que reenvíen cualquier paquete IP modificando la configuración de reenvío de paquetes SNAT. Para obtener más información, consulte **K3760: Confi gramoorina gramoSNAT para reenviar un yprotocolos IP** .

Sistemas BIG-IP redundantes y automáticos SNAT

Si decide usar la asignación automática de SNAT en un par BIG-IP de alta disponibilidad (HA), asegúrese de que exista al menos una dirección IP flotante propia en cada VLAN de salida. Esto garantiza que el tráfico se traduzca a la misma dirección de traducción (la dirección IP flotante propia), independientemente de la unidad activa.

Tiempo de espera inactivo del mapa automático SNAT

Lc etos de automapa SNAT tienen un valor de tiempo de espera de inactividad no configurable. Si necesita implementar un SNAT con un tiempo de espera de inactividad configurable, cree un SNAT con una dirección IP de traducción definida o un grupo de SNAT y, a continuación, configure el tiempo de espera de inactividad deseado para las direcciones de traducción. Puede especificar un valor de tiempo de espera en segundos o usar la palabra clave**Indefinido**. Para obtener más información, consulte **K6017: El valor del tiempo de espera inactivo del mapa automático BIG-IP SNAT no está configurado gramosostenible**

Contenido eufórico

El***Administrador de tráfico local IG-IP: Implementaciones***manual ***Nota****:Para obtener información sobre cómo localizar los manuales de productos F5, consulte* ***pag*** ***98133564: Consejos para la búsqueda gramoAskF5 y encontrando gramo documentación del producto***

K4832: Descripción general de la aceleración de PVA

K4816: Uso gramoEl encabezado HTTP X-Forwarded-For para preservar el origen gramoDirección IP final del cliente para el tráfico que se está enviando gramotraducido b yun SNAT

K9038: El orden de precedencia para el tráfico local bjoyentes ect K05528125: equilibrio de carga del grupo SNAT gramocomportamiento

Contenido recomendado por IA

Aviso de seguridad -**000156572: Trimestral ySeguridad yNotificación (octubre de 2025)**) Política -**5903: Software BIG-IP su pagpolicía portuaria** y Conocimiento -**000135931: Contactar con el soporte de F5**

Política -**4309: Vida útil del producto de hardware F5c ycle sup pagpolicía de ort y**

Los ingenieros de soporte de F5 que trabajan directamente con los clientes escriben artículos de conocimiento y soluciones de soporte que le brindan acceso inmediato a sugerencias de mitigación, soluciones alternativas o resolución de problemas.

↑ Regresar a A pag

Wagner Pastor

expert IPX SRL RNC 130-850151 Santo Domingo, R.D.

Asegure y brinde experiencias digitales extraordinarias

La cartera de capacidades de automatización, seguridad, rendimiento y conocimiento de 5 permite a nuestros clientes crear, proteger y operar aplicaciones adaptables que reducen costos, Mejorar las operaciones y proteger mejor a los usuarios.ganar más ›

LO QUE OFRECEMOS

FUENTES ELECTRÓNICAS

APOYO

ARTISTAS

COMPAÑÍA

CONECTA CON NOSOTROS

CONTACTAR CON SOPORTE

más información sobre el incidente de seguridad en F5, las acciones que estamos tomando para abordarlo,

y nuestros esfuerzos continuos para proteger a nuestros clientes, haga clicantes de

Guía de operaciones

41572395: Traducción de direcciones de red (NAT) | Guía de operaciones de BIG-IP AFM

Fecha de publicación: 9 de octubre de 2018 Fecha de actualización: 9 de febrero de 2023

Contenido recomendado por IA

Se aplica a:

Capítulo 4: Traducción de direcciones de red (NAT)

Tabla de contenido |<< Capítulo anterior |Siguiente cha pagter >>

Una Traducción de Direcciones de Red (NAT) es la asignación de una dirección IP a otra. Esta asignación puede ser una traducción de origen, destino o ambos. Una NAT puede ser de salida o de entrada.

Contenido

Secciones del capítulo

Wagner Pina

Cifras

Importante: Las reglas de enrutamiento y firewall de BIG-IP AFM deben configurarse para admitir las configuraciones NAT y/o PAT configuradas.

NAT de salida

La NAT de salida traduce una dirección de origen interna a una dirección pública. También se puede usar para traducir la dirección IP de un nodo interno a una dirección IP enrutable por Internet.

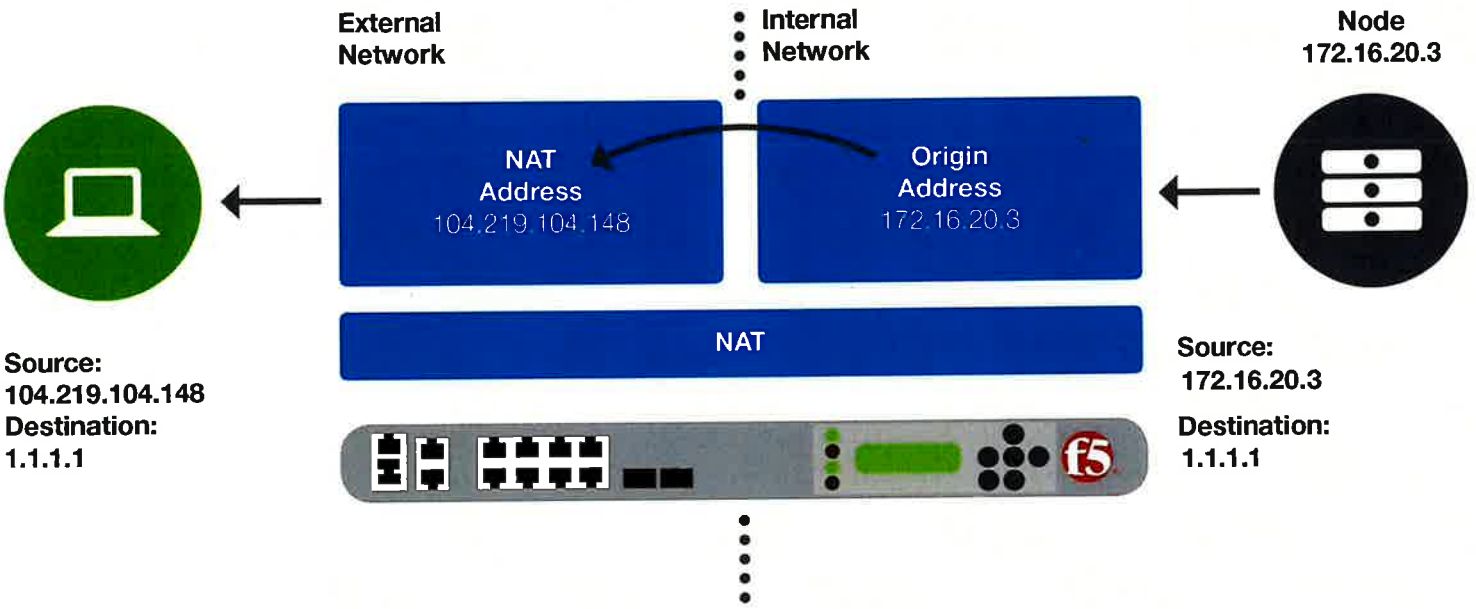


Figura 4.1 NAT de salida

Creación del perfil de salida NAT de origen

. Inicie sesión en la utilidad de configuración de BIG-IP AFM.

. Ir a**Traducción de direcciones de red de seguridad**.

. Seleccionar**Traducción de la fuente**

. Seleccionar**Crear**.

. Ingrese un nombre para el perfil de traducción.

. En el**Tipo**menú, seleccionar**NAT estática**.

. En el**Direcciones**En el cuadro, introduzca la dirección IP que se utilizará como dirección de origen traducida. ***Nota:****En el ejemplo****Figura 4.1****La dirección es 104.219.104.148.*

. Colocar**Eco CMP, ARP proxy**y**Anuncio de ruta**a**habilitado**

. Colocar**Interfaces de gress**a **"habilitado en...**

-. Seleccione la casilla de verificación de interfaz o VLAN que se utiliza para acceder al recurso de destino que requiere la traducción de la dirección de en.

-. Seleccionar**Ahorrar**

-. Seleccionar**Entregar**.

Creación de la política NAT de salida

. Ir a**Seguridad>Traducción de direcciones de red>Políticas**.

. Seleccionar**Crear**.

. Introduzca un nombre de política.

. Seleccionar**Agregar regla**

grese un nombre para la regla NAT.

. Colocar**Tatea****Activado**

. Seleccione el protocolo que desea permitir desde el**Protocolo** enu o salir en**Cualquier**(por defecto).

. En el**Fuente**En el cuadro, introduzca la dirección IP de origen.

Nota:*En el ejemplo****Figura 4.1****Esta dirección es 172.16.20.3.*

-. Dejar**destino**en la configuración predeterminada para lo siguiente:**Dirección: Cualquiera**, **orts: Cualquiera**, con **Roxy ARP**y **salida** **Anuncio**empezar a**deshabilitado**

-. Desde el**Destino traducido**enu, seleccione el nombre del perfil de traducción creado en el procedimiento anterior.

Nota:*En el ejemplo****Figura 4.1****Esta dirección es 104.219.104.148.*

- Seleccione el perfil de registro deseado de la**Perfil de og**menú.

-. Seleccionar**una Edición**

-. Seleccionar**Confirmar cambios en el sistema**.

Nota:*En este punto puede aplicar la política NAT al servidor virtual apropiado o como Traducción de direcciones de red global.*

Asignación de la política NAT

. Inicie sesión en la utilidad de configuración de BIG-IP AFM.

. Ir a**Tráfico local>Servidores virtuales>Lista de servidores virtuales**.

. Seleccione el nombre del servidor virtual a modificar.

eleccionar**Políticas de seguridad**.

. En el**Traducción de direcciones de red**Sección, seleccione la política NAT creada en el paso anterior de la lista.

Nota:*Alternativamente, puede asignar la nueva política NAT a la****Traducción de direcciones de red NAT de firewall global****Con esa configuración, la política se aplica a todos los servidores virtuales.*

NAT de enlace nbound

La NAT entrante traduce una dirección de destino pública a una dirección interna. Cuando un cliente externo envía tráfico a la dirección IP pública definida en una NAT, el sistema BIG-IP traduce esa dirección de destino a la dirección IP del nodo interno.

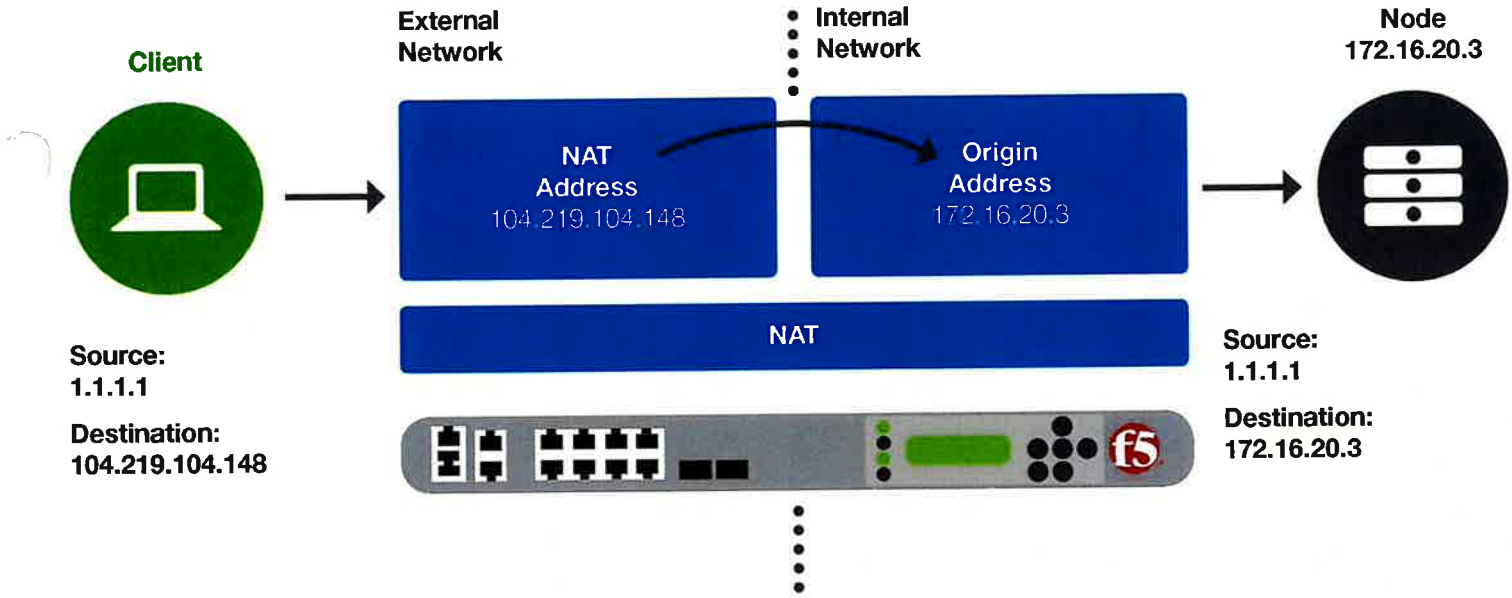


Figura 4.2 NAT entrante

Creación de un NAT entrante para permitir la traducción de una dirección IP a otra mediante la utilidad de configuración

Creación del perfil de entrada NAT de origen

. Inicie sesión en la utilidad de configuración de BIG-IP AFM.

. Ir a **Seguridad>Traducción de direcciones de red**.

. Seleccionar **destino Traducción**.

. Seleccionar **Crear**.

. Ingrese un nombre para el perfil de traducción.

. Para **tipo**, seleccionar **NAT estática**.

. En el **Direcciones** En este cuadro, ingrese la dirección IP o el rango de direcciones IP que se utilizarán como direcciones de destino traducidas.

Nota: *En el ejemplo* ***Figura 4.2*** *La dirección es 172.16.20.3.*

. Seleccionar **Ahorrar**

Creación de la política NAT de entrada

. Inicie sesión en la utilidad de configuración de BIG-IP AFM.

. Ir a **Seguridad>Traducción de direcciones de red** **Políticas**.

. Seleccionar **Crear**.

. Introduzca un nombre de política.

. Seleccionar **Agregar regla**

. Ingrese la regla NAT **Nombre**.

. Colocar **Tate** a **Activado**

. Para **rotocol** Seleccione el protocolo que se permitirá o déjelo en **Cualquier** (por defecto).

. Para **fuente**, ingrese las direcciones IP de origen que se traducirán o **Cualquier** (por defecto). **destino**

-. Para Introduzca la dirección IP de destino traducida a la dirección IP del destino interno.

Nota: *En el ejemplo* ***Figura 4.2*** *La dirección es 104.219.104.148.*

-. Para **Destino traducido**, seleccione el nombre del perfil de traducción creado en el procedimiento anterior (172.16.20.3). **og**

-. Para **Perfil**, Seleccione el perfil de registro.

-. Seleccionar**Confirmar cambios en el sistema**.

Aplicación de la política NAT

. Inicie sesión en la utilidad de configuración de BIG-IP AFM.

. Ir a**Servidores virtuales de tráfico local Lista de servidores virtuales**.

. Seleccione el nombre del servidor virtual a modificar.

. Seleccionar**Seguridad**.

. En el **Traducción de direcciones de red**Sección, seleccione la política NAT creada en el paso anterior.

. Seleccionar **actualización**

Nota:*Alternativamente, puede asignar la nueva política NAT a la****Cortafuegos global NAT*** *configuración,* ***Traducción de direcciones de red****. Con eso la política se aplica a todos los servidores virtuales.*

PAT dinámico

NAT, por diseño, es una operación uno a uno, mientras que la traducción de direcciones de puerto (PAT) se puede utilizar para asignar muchas direcciones IP a una dirección IP con el fin de ocultar las redes IP de origen.

Modos y mapeo dinámicos de PAT

En la configuración de red cliente-servidor más común, el mecanismo de traducción de direcciones BIG-IP garantiza que las respuestas del servidor regresen al cliente a través del sistema BIG-IP.

Modo determinista

Modo NAPT

Mapeo del modo de asignación de bloques de puertos gramo

Modo determinista

El modo de traducción de direcciones proporciona una traducción que elimina el registro de cada asignación de direcciones, a la vez que permite el seguimiento de las direcciones de los clientes internos utilizando únicamente una dirección y un puerto externos, y una dirección y un puerto de destino. El modo determinista permite la identificación única de la dirección del cliente interno basándose en: la dirección y el puerto externos (la dirección y el puerto visibles para el servidor de destino), la dirección y el puerto de destino (el servicio al que accede el cliente) y la hora. Este modo reduce significativamente la carga de registro al asignar la dirección IP interna de un suscriptor a una dirección y un puerto de Internet externos.

Modo NAPT

Proporciona traducción estándar de direcciones y puertos, lo que permite que varios clientes de una red privada accedan a redes remotas utilizando la única dirección IP asignada a su router. Para los paquetes salientes, NAPT traduce la dirección IP de origen y el identificador de transporte de origen. Para los paquetes entrantes, NAPT traduce la dirección IP de destino, el identificador de transporte de destino y las sumas de comprobación de las cabeceras de IP y transporte. Este modo es beneficioso para los usuarios de acceso remoto.

Modo de asignación de bloques de puertos

Registra la asignación y liberación de bloques de puertos para solicitudes de traducción de suscriptores, en lugar de registrar cada traducción por separado.

manteniendo al mismo tiempo los requisitos de mapeo legal e inverso.

Cartografía

.grupación de direcciones emparejadaspermite que todas las sesiones asociadas con una dirección IP interna se asignen a la misma dirección IP externa durante la duración de la sesión.

Mapeo independiente de puntos finales Asigna la misma dirección externa y puerto para todas las conexiones desde el host si utiliza el mismo puerto interno.

Ningunono asigna ningún modo de mapeo a las asignaciones de puertos dinámicos.

Clientes y servidores en la misma subred

Para equilibrar la carga de las solicitudes a los nodos de servidor que se encuentran en la misma subred que los nodos de cliente, cree una SNAT para que las respuestas del servidor se envíen a través del sistema BIG-IP en lugar de directamente del nodo de servidor al nodo de cliente. De lo contrario, pueden surgir problemas, como que el cliente (172.16.1.30) rechace la respuesta porque el origen de la respuesta (172.16.20.1) no coincide con el destino de la solicitud (172.16.1.100).

El sistema BIG-IP no es la puerta de enlace predeterminada del nodo servidor

A veces, la ruta predeterminada de un servidor no se puede definir como una ruta a través del sistema BIG-IP. Esto puede causar problemas, como que el cliente rechace la respuesta porque el origen de la respuesta no coincide con el destino de la solicitud.

L. .olución es crear una SNAT. El sistema BIG-IP traduce la dirección IP de origen del nodo cliente en la solicitud a la dirección SNAT, lo que hace que e. ..do servidor utilice esa dirección SNAT como dirección de destino al enviar la respuesta. Esto, a su vez, obliga a que la respuesta regrese al nodo cliente a través del sistema BIG-IP en lugar de a través de la puerta de enlace predeterminada del servidor.

PAT dinámica saliente (NAPT explícita)

***Nota**:Comportamiento similar al SNAT de traducción de dirección de origen BIG-IP LTM.*

La PAT estática de salida traduce una dirección de origen interna a una única dirección traducida (pública), solo tráfico de respuesta entrante.

Creación del perfil PAT dinámico

. Inicie sesión en la utilidad de configuración de BIG-IP AFM.

. Ir a**Seguridad>Traducción de direcciones de red**.

. Seleccionar**Traducción de la fuente**

. Seleccionar**Crear**.

. Ingrese un nombre para el perfil de traducción.

. Para**tipo,**seleccionar**PAT dinámico**.

. Para**Direcciones:**Introduzca la dirección IP que se utilizará para traducir todo el tráfico según lo definido por la política.

. Para**puertos:**, ingrese el puerto o rango de puertos esperado que utilizará la dirección IP traducida al acceder a los recursos.

. Colocar**Eco CMP, Proxy ARP,**y **Anuncio de salida**a**Activado**

-. Colocar **Interfaces de gress**a "**habilitado en...**

-. Para **Interfaces de gress,**Seleccione la interfaz de destino adecuada o las casillas de verificación VLAN).

-. Seleccionar **PAT dinámico**

Nota:*Configuración****xplicit****Sólo permitirá la comunicación bidireccional para las conexiones establecidas inicialmente.*

-. Seleccionar**Ahorrar**

C ción de la política PAT dinámica de salida

. Inicie sesión en la utilidad de configuración de BIG-IP AFM.

. Ir a**Seguridad** **Traducción de direcciones de red** **Políticas**.

. Seleccionar**Crear**.

. Introducir una política ame.

. Seleccionar**Agregar regla**

. Introduzca la regla PAT ame.

. Colocar **TateaActivado**

. Para **rotocol**Seleccione el protocolo que se permitirá o déjelo como está**Cualquier**por defecto).

. Para **fuente,**Agregue las direcciones IP o el rango de red que utilizarán el perfil PAT dinámico para la traducción.

-. Dejar **destino**en la configuración predeterminada.

-. Para**Fuente traducida,**Seleccione el nombre del perfil de traducción creado en el procedimiento anterior.

-. Dejar**Destino traducido**a la configuración predeterminada de**uno**.

-. Para**og Perfil,**Seleccione el perfil de registro.

-. Seleccionar**una Edición**

-. Seleccionar**Confirmar cambios en el sistema**.

Aplicación de la política PAT dinámica

. nicie sesión en la utilidad de configuración de BIG-IP AFM.

. Ir a**Tráfico local>Servidores Virtuales Lista de Servidores Virtuales**.

. Seleccione el nombre del servidor virtual a modificar.

. Seleccionar**Seguridad**.

. Para**Traducción de direcciones de red**Seleccione la política NAT creada en el paso anterior.

. Seleccionar**actualización**

Nota:*Alternativamente, puede asignar la nueva política NAT a la****Cortafuegos global NAT*** *configuración,* ***Traducción de direcciones de red****. Con eso la política se aplica a todos los servidores virtuales.*

agotamiento por esfuerzo

Cada dirección NAT tiene solo 65 535 puertos disponibles. Esto se debe a un límite de los protocolos TCP y UDP, que utilizan un entero sin signo de 16 bits para los puertos de origen.

El agotamiento de puertos o las colisiones pueden ocurrir bajo condiciones de uso intensivo o patrones de tráfico de clientes con una distribución inusual. Por razones de rendimiento, el sistema BIG-IP no busca exhaustivamente un puerto de origen disponible. El agotamiento de puertos puede ocurrir mucho antes de que se utilicen los 65 535 puerto Como resultado, las conexiones que no se pueden traducir debido a la falta de puertos disponibles en una dirección de traducción determinada pueden ser descartadas.

Para determinar cuándo se produce el agotamiento del puerto NAT, revise los archivos de registro del sistema. Cuando se produce el agotamiento del puerto, el sistema BIG-IP registra mensajes en el.../**var/log/ltm**file.

El siguiente es un ejemplo de un mensaje de registro de agotamiento de puerto:

10.10.20.21 a 23.73.217.114:80 (proto 6)

Mapeo de puertos

Cuando se configura una NAT en el sistema BIG-IP (de forma independiente o junto con un servidor virtual), la dirección de origen de cada conexión se traduce a una dirección NAT configurada y el puerto de origen se asigna a un puerto disponible para esa dirección NAT. De forma predeterminada, el sistema BIG-IP intenta conservar el puerto de origen, pero si este ya está en uso en la dirección de traducción seleccionada, el sistema traduce el puerto de origen.

Mitigación del agotamiento de los puertos

Para mitigar el agotamiento de puertos, utilice un rango de direcciones IP de traducción NAT. Si ya utiliza un rango de direcciones IP NAT, añadir un rango adicional al perfil de origen o destino NAT puede aumentar el total de puertos disponibles para el NAT.

Estadísticas NAT y PAT

Monitoreo de la cantidad de conexiones simultáneas que pasan a través de NAT mediante la utilidad de configuración

Ir a **Seguridad** **Informes** **Traducción de direcciones de red>Traducción de la fuente**

Ir a **Seguridad** **Informes** **Destino de traducción de direcciones de red>Traducción**

Monitoreo del número de conexiones simultáneas que pasan por NAT usando tmsh

Introduzca el siguiente comando:

msh show /seguridad nat

-5903: Software BIG-IP su pagpolicía portuaria y Conocimiento -000135931: Contactar con el soporte de F5

Política -4309: Vida útil del producto de hardware F5c ycle sup pagpolicía de ort y

Regresar a A pag

Wagner Pastra

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Asegure y brinde experiencias digitales extraordinarias

La cartera de capacidades de automatización, seguridad, rendimiento y conocimiento de 5 permite a nuestros clientes crear, proteger y operar aplicaciones adaptables que reducen costos, Mejorar las operaciones y proteger mejor a los usuarios.ganar más ›

LO QUE OFRECEMOS

FUENTES ELECTRÓNICAS

APOYO

ARTISTAS

COMPAÑÍA

CONECTA CON NOSOTROS

CONTACTAR CON SOPORTE

Wagner Peña

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Capítulo del manual : Monitoreo de la salud y el rendimiento

Aplica a:

Mostrar versiones

Wagner Pena

Índice | << Capítulo anterior | Capítulo siguiente >>

Monitoreo de salud y rendimiento

Introducción al monitoreo de la salud y el rendimiento

BIG-IP® Local Traffic Manager™ puede supervisar el estado o el rendimiento de los miembros del grupo o de los nodos. Local Traffic Manager admite los siguientes métodos de supervisión:

Monitoreo simple

La monitorización simple simplemente determina si el estado de un nodo es`arriba`o`abajo`Los monitores simples no supervisan los miembros del grupo (y, por lo tanto, los protocolos, servicios o aplicaciones individuales en un nodo), sino solo el nodo en sí. El sistema incluye dos tipos de monitores simples: ICMP y TCP_ECHO.

Monitoreo activo

La supervisión activa comprueba el estado de un miembro del grupo o nodo de forma continua, a intervalos regulares. Si un miembro del grupo o nodo supervisado no responde dentro del tiempo de espera especificado, o si su estado indica una degradación del rendimiento, Local Traffic Manager puede redirigir el tráfico a otro miembro del grupo o nodo. Existen varios tipos de monitores activos. Cada tipo comprueba el estado de un protocolo, servicio o aplicación específicos. Por ejemplo, un tipo de monitor es HTTP. Un monitor HTTP permite supervisar la disponibilidad del servicio HTTP en un grupo, miembro del grupo o nodo. Un monitor WMI permite supervisar el rendimiento de un nodo que ejecuta el software de Instrumental de administración de Windows (WMI). Los monitores activos se dividen en dos categorías: monitores de verificación de contenido extendida (ECV) y monitores de verificación de aplicaciones extendida (EAV).

Nota: *Si configura un monitor de rendimiento, como un monitor SNMP DCA o WMI, también debe configurar un monitor de estado. La configuración de un monitor de estado garantiza que Local Traffic Manager informe con precisión sobre el estado de disponibilidad de los nodos.*

Monitoreo pasivo

La monitorización pasiva se produce como parte de una solicitud del cliente. Este tipo de monitorización comprueba el estado de un miembro del grupo basándose en un número determinado de intentos de conexión o de solicitud de datos que se producen dentro de un período de tiempo específico. Si, tras el número de intentos

437

especificado dentro del intervalo definido, el sistema no puede conectarse al servidor ni recibir una respuesta, o si recibe una respuesta incorrecta, el sistema marca al miembro del grupo como inactivo.`abajo`Solo existe un tipo de monitor pasivo, llamado monitor ***en banda*** .

Comparación de métodos de monitoreo

En la breve descripción, describa concisamente el propósito y la intención de la información contenida en este tema. Este elemento es un requisito de F5® .

Método de monitoreo	Beneficios	Restricciones
Simple	• Funciona bien cuando solo necesitas determinar el estado activo o inactivo de un nodo.	• Solo puede comprobar el estado de un nodo, no de un miembro del grupo.
Activo	• Puede consultar las respuestas específicas. • Puede funcionar con o sin tráfico de clientes.	• Crea tráfico de red adicional más allá de la solicitud del cliente y la respuesta del servidor. • Puede tardar en marcar a un miembro del grupo como inactivo
Pasivo	• No genera tráfico de red adicional más allá de la solicitud del cliente y la respuesta del servidor. • Se puede marcar rápidamente un miembro del grupo como inactivo, siempre que haya cierta cantidad de tráfico de red.	• No se pueden comprobar las respuestas específicas. • Puede que tarde en marcar a un miembro del grupo como activo.

Acerca de la configuración del monitor

Cada monitor consta de ajustes con valores. Estos ajustes y sus valores varían según el tipo de monitor. En algunos casos, Local Traffic Manager™ asigna valores predeterminados. Este ejemplo muestra que un monitor de tipo ICMP tiene estos ajustes y valores predeterminados.

La configuración especifica que un monitor de tipo ICMP está configurado para comprobar el estado de una dirección IP cada cinco segundos y que el tiempo de espera expirará cada 16 segundos. La dirección IP de destino que comprueba el monitor se especifica mediante la configuración de Dirección de alias, con el valor `* All Addresses` . Por lo tanto, en el ejemplo, se comprueban todas las direcciones IP con las que está asociado el monitor.

```
Nombre my_icmp
Tipo ICMP
Intervalo 5
Tiempo de espera 16
Transparente No
Dirección alternativa * Todas las direcciones
```

Descripción general de la implementación del monitor

Los monitores se implementan mediante la utilidad de configuración de BIG-IP o una utilidad de línea de comandos. El proceso de implementación varía según si se utiliza un monitor preconfigurado o se crea uno personalizado. Un ***monitor preconfigurado*** es uno existente que Local Traffic Manager™ proporciona con su configuración ya establecida. Un ***monitor personalizado*** es uno que se crea a partir de uno de los tipos de monitor permitidos.

Si desea implementar un monitor preconfigurado, solo necesita asociarlo a un grupo, un miembro del grupo o un nodo, y luego configurar el servidor virtual para que haga referencia al grupo correspondiente. Si desea implementar un monitor personalizado, primero debe crearlo. Luego, puede asociarlo a un grupo, un miembro del

438

grupo o un nodo, y configurar el servidor virtual para que haga referencia al grupo.

Monitores preconfigurados

Para ciertos tipos de monitores, Local Traffic Manager™ incluye monitores preconfigurados. No es posible modificar la configuración de estos monitores, ya que están diseñados para usarse tal cual. Su función es evitar que tenga que crear un monitor manualmente. Utilice un monitor preconfigurado cuando los valores de la configuración se ajusten a sus necesidades.

Los nombres de los monitores preconfigurados que incluye Local Traffic Manager son:

- **gateway_icmp**
- **http**
- **https**
- **https_443**
- **icmp**
- **inband**
- **real_server**
- **snmp_dca**
- **tcp**
- **tcp_echo**

Un ejemplo de monitor preconfigurado es el **icmp** monitor mostrado. Este ejemplo muestra el **icmp** monitor con valores configurados para sus ajustes **de Intervalo** , **Tiempo de espera** y **Dirección de alias 5** . Observe que el valor de Intervalo es , el valor de Tiempo de espera es **16** , el valor de Transparencia es **No** y el valor de Dirección de alias es *** All Addresses** .

Si los valores de Intervalo, Tiempo de espera, Transparencia y Dirección de alias satisfacen sus necesidades, simplemente asigne el **icmp** monitor preconfigurado directamente a un grupo, miembro de grupo o nodo, mediante las pantallas Grupos o Nodos de la utilidad de configuración de BIG-IP. En este caso, no es necesario utilizar las pantallas Monitores, a menos que desee consultar los valores de la configuración del monitor preconfigurado.

```
Nombre icmp
Tipo ICMP
Intervalo 5
Tiempo de espera 16
Transparente No
Dirección alternativa * Todas las direcciones
```

Importante: *Todos los monitores preconfigurados residen en la partición* **Common** *.*

Monitores personalizados

Se crea un monitor personalizado cuando los valores definidos en un monitor preconfigurado no satisfacen sus necesidades, o cuando no existe un monitor preconfigurado para el tipo de monitor que está creando.

Al crear un monitor personalizado, utilice la utilidad de configuración de BIG-IP o una utilidad de línea de comandos para: asignarle un nombre único, especificar su tipo y, si ya existe un monitor de ese tipo, importar su configuración y valores. Posteriormente, podrá modificar los valores de la configuración importada.

Debe basar cada monitor personalizado en un tipo de monitor. Al crear un monitor, la utilidad de configuración de BIG-IP muestra una lista de tipos de monitor. Para especificar un tipo de monitor, simplemente elija el que corresponda al servicio que desea comprobar. Por ejemplo, si desea crear un monitor que compruebe el estado

del servicio HTTP en un grupo, seleccione HTTP como tipo de monitor.

Si desea comprobar más de un servicio en un grupo o miembro del grupo (por ejemplo, HTTP y HTTPS), puede asociar más de un monitor a ese grupo o miembro del grupo.

La comprobación de servicios no es el único motivo para implementar un monitor. Si solo desea verificar que la dirección IP de destino esté activa, o que la ruta a través de un nodo transparente esté activa, utilice uno de los monitores simples. **icmp** O **tcp_echo** bien, si solo desea verificar TCP, utilice el monitor **tcp** .

Importar la configuración desde un monitor preconfigurado

Si existe un monitor preconfigurado que corresponda al tipo de monitor personalizado que está creando, puede importar su configuración y valores al monitor personalizado. Luego, podrá modificar dichos valores según sus necesidades. Por ejemplo, si crea un monitor personalizado llamado «A» **my_icmp** , este puede heredar la configuración y los valores del monitor preconfigurado «A» **icmp** . Esta capacidad de importar valores de configuración existentes resulta útil cuando desea conservar algunos valores de configuración para su nuevo monitor, pero modificar otros.

El ejemplo muestra un monitor personalizado de tipo ICMP llamado **my_icmp** , basado en el monitor preconfigurado **icmp** . Observe que el valor de Intervalo se ha cambiado a **10** y el valor de Tiempo de espera a **20** . El resto de la configuración conserva los valores definidos en el monitor preconfigurado.

```
Nombre my_icmp
Tipo ICMP
Intervalo 10
Tiempo de espera 20
Transparente No
Dirección alternativa * Todas las direcciones
```

Importar la configuración desde un monitor personalizado

Puede importar la configuración de otro monitor personalizado en lugar de la de un monitor preconfigurado. Esto resulta útil cuando prefiere usar los valores de configuración definidos en otro monitor personalizado o cuando no existe un monitor preconfigurado para el tipo de monitor que está creando. Por ejemplo, si crea un monitor personalizado llamado **my_oracle_server2** , puede importar la configuración de un monitor existente de tipo Oracle **my_oracle_server1** . En este caso, dado que Local Traffic Manager™ no proporciona un monitor de tipo Oracle preconfigurado, un monitor personalizado es el único tipo de monitor desde el que puede importar valores de configuración.

Seleccionar un monitor es sencillo. Al igual que **icmp** otros monitores, cada uno tiene una configuración de Tipo basada en el tipo de servicio que comprueba (por ejemplo, `service` **http** , **https** `service`, ` service` **ftp** , **pop3** `service`, `service`), y toma ese tipo como nombre. (Existen excepciones, como los monitores específicos de puerto **external** , que ejecutan un programa proporcionado por el usuario).

Destinos de monitoreo

De forma predeterminada, el valor de la configuración **de Dirección de alias** en los monitores se establece en un comodín *** Addresses** , al igual que el valor de la configuración **de Puerto de servicio de alias * Ports** . Este valor hace que la instancia de monitor creada para un grupo, miembro del grupo o nodo tome la dirección o la dirección y el puerto de dicho nodo como destino. Sin embargo, puede reemplazar uno o ambos comodines co

un valor de destino explícito creando un monitor personalizado. Un valor explícito para la configuración de **Dirección de alias** o **Puerto de servicio de alias** (o ambas) se utiliza para forzar el destino de la instancia a una dirección o puerto específicos, que podrían no ser los del grupo, miembro del grupo o nodo.

Los tipos de monitor ECV HTTP, HTTPS y TCP incluyen las configuraciones **Cadena de envío** y **Cadena de recepción** para la cadena de envío y la expresión de recepción, respectivamente.

El valor más común **para Send String** `GET /` es , que recupera una página HTML predeterminada de un sitio web. Para recuperar una página específica de un sitio web, puede introducir un valor **de Send String** que sea una ruta de acceso completa:

```
"GET /www/support/customer_info_form.html"
```

El valor **de la cadena de recepción** es la cadena de texto que el monitor busca en el recurso devuelto. Los valores más comunes **de la cadena de recepción** contienen una cadena de texto incluida en una página HTML específica de su sitio. Esta cadena de texto puede ser texto sin formato, etiquetas HTML o nombres de imágenes.

El valor de ejemplo **"Recibir cadena"** que se muestra a continuación busca una etiqueta HTML estándar:

```
"<ENCABEZADO>"
```

También puede usar el valor nulo predeterminado **para la cadena de recepción** `[""]` . En este caso, cualquier contenido recuperado se considera una coincidencia. Si ambos campos, **Cadena de envío** y **Cadena de recepción** , se dejan vacíos, solo se realiza una comprobación de conexión básica.

Para los monitores HTTP y FTP, puede usar los valores especiales `--host` **`GET`** o **`hurl`** `--host` en lugar de los valores `--host` **`Send String`** y ` **`Receive String`** --host`. En el caso específico de los monitores FTP, el valor `GET` debe especificar la ruta completa al archivo que se va a recuperar.

Modos transparente e inverso

El comportamiento normal y predeterminado de un monitor es hacer ping al grupo de destino, al miembro del grupo o al nodo mediante una ruta no especificada y marcar el nodo.**`arriba`**Si la prueba es exitosa. Sin embargo, con ciertos tipos de monitores, puede especificar una ruta a través de la cual el monitor envía pings al servidor de destino. Esto se configura especificando la opción Transparente o Inversa dentro de un monitor personalizado.

Configuración transparente

A veces es necesario hacer ping al destino con alias a través de un grupo transparente, un miembro del grupo o un nodo. Cuando crea un monitor personalizado y configura elAl configurar la transparencia en Sí, Local Traffic Manager™ fuerza al monitor a realizar pings a través del grupo, miembro del grupo o nodo con el que está asociado (normalmente un firewall) al grupo, miembro del grupo o nodo de destino. (Es decir, si hay dos firewalls en un grupo de balanceo de carga, el grupo, miembro del grupo o nodo de destino siempre se contacta a través del grupo, miembro del grupo o nodo especificado, no a través del grupo, miembro del grupo o nodo seleccionado por el método de balanceo de carga). De esta manera, se prueba el grupo, miembro del grupo o nodo transparente: si no hay respuesta, se marca como no disponible.**`abajo`**.

Algunos ejemplos comunes son la comprobación de un router o de un servidor de correo o FTP a través de un firewall. Por ejemplo, puede que desee comprobar la dirección del router **`10.10.10.53:80`** a través de un firewall transparente **`10.10.10.101:80`** . Para ello, cree un monitor denominado ` <nombre_del_monitor>` **`http_trans`** en el que especifique **`10.10.10.53:80`** `<dirección_del_monitor>` como dirección de destino y

configure la opción «Transparente» en «Sí». A continuación, asocie el monitor **`http_trans`** con el grupo, miembro o nodo transparente.

Esto hace que el monitor verifique la dirección **`10.10.10 53:80`** a través de **`10.10.10.101:80`** . (En otras palabras, el sistema BIG-IP® enruta la verificación de **`10.10.10.53:80`** a través de **`10.10.10.101:80`** .) Si no se recibe la respuesta correcta de **`10.10.10.53:80`** , entonces **`10.10.10.101:80`** se marca como .**`abajo`**.

Configuración inversa

Con la opción Inversa activada, el monitor marca el grupo, el miembro del grupo o el nodo como inactivo cuando la prueba se realiza correctamente. Por ejemplo, si el contenido de la página de inicio de su sitio web es dinámico y cambia con frecuencia, puede configurar una comprobación inversa del servicio ECV que busque la cadena "`Error`". Si se encuentra una coincidencia con esta cadena, significa que el servidor web estaba**`abajo`**.

Monitores que incluyen la configuración Transparente o Inversa

Esta tabla muestra los monitores que contienen la configuración Transparente o ambas configuraciones, Inversa y Transparente.

Tipo de monitor	Ajustes
TCP	Transparente e inverso
HTTP	Transparente e inverso
HTTPS	Transparente e inverso
Eco TCP	Transparente
TCP semiabierto	Transparente
ICMP	Transparente

La función de reanudación manual

Por defecto, cuando un monitor detecta que un recurso (es decir, un nodo o un miembro de un grupo) no está disponible, el sistema BIG-IP® marca el recurso como**`abajo`**y dirige el tráfico al siguiente recurso apropiado según lo dicte el método de balanceo de carga activo. Cuando el monitor determina que el recurso está disponible de nuevo, el sistema BIG-IP marca el recurso como**`arriba`**y considera inmediatamente que el recurso está disponible para las solicitudes de conexión de balanceo de carga. Si bien este proceso es adecuado para la mayoría de los recursos, existen situaciones en las que se desea designar manualmente un recurso como disponible, en lugar de permitir que el sistema BIG-IP lo haga automáticamente. Puede designar manualmente un recurso como disponible configurando la opción Reanudación manual del monitor.

Por ejemplo, considere un monitor asignado a un recurso para verificar la disponibilidad del archivo HTML index.html de un sitio web. Durante la jornada laboral, decide reiniciar el sistema que aloja el sitio web. El monitor detecta el reinicio e informa al sistema BIG-IP que el recurso ya no está disponible. Al reiniciarse el sistema, el monitor detecta que el archivo index.html está disponible y comienza a enviar solicitudes de conexión al sitio web. Sin embargo, es posible que el resto del sitio web no esté listo para recibir dichas solicitudes. En consecuencia, el sistema BIG-IP envía solicitudes de conexión al sitio web antes de que este pueda responder correctamente.

Para evitar este problema, puede configurar la opción de Reanudación Manual del monitor. Al activar la opción Reanudación Manual, se asegura de que el sistema BIG-IP considere el recurso como no disponible hasta que lo habilite manualmente.

Reanudación de las conexiones
Si tiene un recurso (como un miembro de un grupo o un nodo) que un monitor ha marcado como`abajo`Si el recurso vuelve a estar disponible posteriormente, deberá volver a habilitarlo manualmente si la opción **«Reanudación manual»** del monitor está configurada en «Sí». Al volver a habilitar manualmente el recurso, el sistema BIG-IP® reanudará el envío de conexiones a dicho recurso.

El procedimiento para volver a habilitar manualmente un recurso varía dependiendo de si el recurso es un grupo, un miembro de un grupo o un nodo.

Wagner Peña

La función Tiempo hasta Arriba

Por defecto, el sistema BIG-IP® marca un miembro del grupo o un nodo como activo inmediatamente después de recibir la primera respuesta correcta a un comando ping .

La función «Tiempo hasta la activación» permite ajustar el comportamiento predeterminado. Esta función permite que el sistema retrase el marcado de un miembro del grupo o nodo como activo durante un número determinado de segundos tras la recepción de la primera respuesta correcta. El objetivo de esta función es garantizar que el monitor marque al miembro del grupo o nodo como activo solo después de que este haya respondido correctamente al sistema BIG-IP de forma consistente durante el período de tiempo definido. Con esta función, se asegura que un miembro del grupo o nodo que esté disponible solo momentáneamente, tras enviar una respuesta correcta, no se marque como activo.

Un valor de Tiempo Hasta Activación (TUT) de 0 `0` provoca el comportamiento predeterminado. Cuando el valor de TUT es distinto de 0, el sistema BIG-IP marca un miembro del pool o un nodo como activo solo cuando todas las respuestas de los miembros del pool o del nodo durante el período de TUT son correctas.

expert IPX SRL RNC 130-850151 Santo Domingo, R.D.

Balanceo de carga de relación dinámica

Puede configurar el equilibrio de carga de relación dinámica para grupos que constan de servidores RealNetworks® RealServer ™, servidores Microsoft® Windows® equipados con Windows Management Instrumentation (WMI) o cualquier servidor equipado con un agente SNMP · como el agente SNMP de UC Davis o el agente SNMP de Windows® 2000 Server.

Para implementar el balanceo de carga de relación dinámica en este tipo de servidores, BIG-IP® Local Traffic Manager™ proporciona un archivo de complemento de monitorización especial y un monitor de rendimiento para cada tipo de servidor. La excepción son los servidores equipados con un agente SNMP. En este caso, Local Traffic Manager solo proporciona el monitor; no se requiere ningún archivo de complemento especial para un servidor que ejecute un agente SNMP.

Debe instalar el complemento de monitorización en cada servidor que se vaya a monitorizar y crear un monitor de rendimiento que resida en el sistema BIG-IP. Una vez creado el monitor, este se comunica directamente con el complemento del servidor.

Complementos de monitor y plantillas de monitor correspondientes
Para cada tipo de servidor, esta tabla muestra el complemento de monitorización necesario y los tipos de monitorización de rendimiento correspondientes.

443

Tipo de servidor	Complemento de monitor	Tipo de monitor
Servidor Windows RealServer	F5RealMon.dll	Servidor real
Servidor UNIX RealServer	f5realmon.so	Servidor real
Servidor Windows con WMI	f5isapi.dll o F5Isapi64.dll o F5.IsHandler.dll	WMI
Servidor Windows 2000 Server	Agente SNMP	SNMP DCA y SNMP DCA Base
Servidor UNIX	Agente SNMP de UC Davis	SNMP DCA y SNMP DCA Base

Monitorizar la asociación con pools y nodos

Debe asociar un monitor al servidor o servidores que se van a monitorizar. El servidor o servidores pueden ser un grupo, un miembro de un grupo o un nodo, según el tipo de monitor. Puede asociar un monitor a un servidor de cualquiera de las siguientes maneras:

Asociación de monitor a piscina
Este tipo de asociación vincula un monitor con un grupo de balanceo de carga completo. En este caso, el monitor verifica todos los miembros del grupo. Por ejemplo, puede crear una instancia del monitor **`http`** para cada miembro del grupo **`my_pool`** , lo que garantiza que se verifiquen todos los miembros del mismo.

Asociación de miembros de Monitor-to-Pool
Este tipo de asociación vincula un monitor con un miembro específico del grupo, es decir, una dirección IP y un servicio. En este caso, el monitor solo verifica ese miembro del grupo y no los demás. Por ejemplo, puede crear una instancia del monitor **`http`** para el miembro **`10.10.10.10:80`** del grupo **`my_pool`** .

Asociación de monitor a nodo
Este tipo de asociación vincula un monitor con un nodo específico. En este caso, el monitor solo verifica el nodo en sí, y no los servicios que se ejecutan en él. Por ejemplo, puede crear una instancia del monitor **`icmp`** para el nodo <nombre_nodo> **`10.10.10.10`** . En este caso, el monitor solo verifica el nodo específico, y no los servicios que se ejecutan en él. Puede designar un monitor como el monitor predeterminado que desea que Local Traffic Manager asocie con uno o más nodos. En este caso, cualquier nodo al que no le haya asignado un monitor específicamente heredará el monitor predeterminado.
Algunos tipos de monitores están diseñados para asociarse únicamente con nodos, y no con grupos ni miembros de grupos. Otros tipos de monitores están diseñados para asociarse únicamente con grupos y miembros de grupos, y no con nodos.

Los monitores de nodo especifican una dirección de destino en formato de dirección IP sin puerto de servicio (por ejemplo, **`10.10.10.2`**). En cambio, los monitores que se pueden asociar con nodos, grupos y miembros de grupo especifican una dirección de destino en formato de dirección IP y puerto de servicio (por ejemplo, **`10.10.10.2:80`**). Por lo tanto, al usar la utilidad de configuración de BIG-IP para asociar un monitor con un grupo, un miembro de grupo o un nodo, la utilidad muestra únicamente los monitores preconfigurados diseñados para asociarse con ese servidor.

Por ejemplo, no se puede asociar el monitor **`icmp`** con un grupo o sus miembros, ya que el **`icmp`** monitor está diseñado para comprobar el estado de un nodo en sí mismo y no de ningún servicio que se ejecute en ese nodo.

Al asociar un monitor a un servidor, Local Traffic Manager™ crea automáticamente una ***instancia*** de dicho monitor para ese servidor. De esta forma, una asociación de monitor crea una instancia del mismo para cada

444

Instancias de monitor

servidor que especifique. Esto significa que puede tener varias instancias del mismo monitor ejecutándose en sus servidores.

Debido a que las instancias de monitores no son objetos particionados, un usuario puede habilitar o deshabilitar una instancia de un monitor sin tener permiso para administrar el grupo o el miembro del grupo asociado.

Por ejemplo, un usuario con el rol de Administrador, que solo tiene acceso a la partición **AppA** , puede habilitar o deshabilitar instancias de monitorización para un grupo que reside en dicha partición **Common** . Sin embargo, este usuario no puede realizar operaciones en el grupo ni en los miembros del grupo asociados al monitor. Si bien este es el funcionamiento correcto, el usuario podría no esperar este comportamiento. Para evitarlo, asegúrese de que todos los grupos y sus miembros asociados a las instancias de monitorización residan en la misma partición.

Índice | << Capítulo anterior | Capítulo siguiente >>

Wagner Peña

Solución de soporte

65271370: Métodos SSL más comunes para LTM: descarga SSL, paso a través de SSL y proxy SSL completo

Fecha de publicación: 7 de mayo de 2020 Fecha de actualización: 20 de enero de 2025

Contenido recomendado por IA

Se aplica a:

Wagner Peña

IPX SRL RNC 130-850151 Santo Domingo, R.D.

descripción

IP está diseñado para manejar el tráfico SSL en escenarios de equilibrio de carga y cumplir con la mayoría de los requisitos de seguridad de manera efectiva. Las 3 configuraciones SSL comunes que se pueden configurar en el dispositivo LTM son:

Descarga de SSL
Paso de SSL
Proxy SSL completo / Reencriptación SSL / Puente SSL / Terminaciones SSL

entorno de escritorio

Objetos y configuraciones de configuración: perfiles SSL de servidor virtual, SSL de cliente y servidor
BIG-IP, LTM

Causa

Ninguna

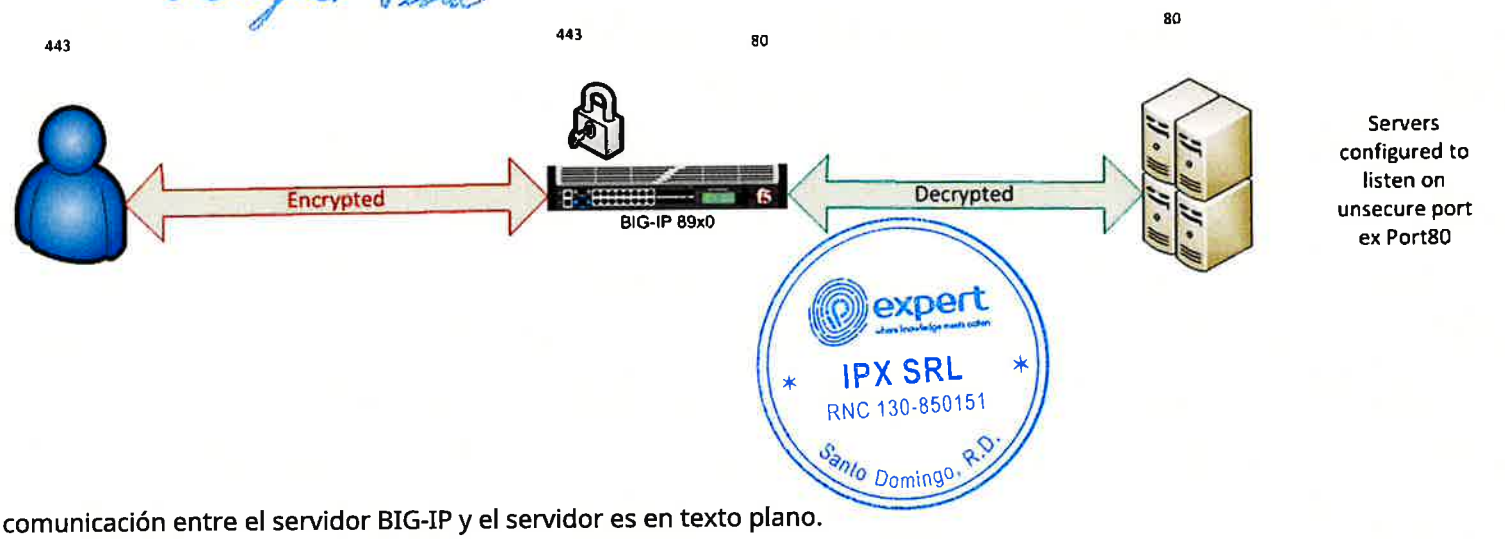
Acciones recomendadas

Para obtener información sobre cómo configurar estos diferentes modos SSL, consulte la lista de artículos en la sección **Contenido relacionado**en la parte inferior de este artículo.

Información adicional

La configuración típica de la infraestructura de balanceo de carga sería Cliente--->BIG-IP VIP ---->Los servidores que alojan aplicaciones, es decir, el tráfico de cliente, se dirigirán a un balanceador de carga como BIG-IP que, a cambio (usando un algoritmo complejo), envía el tráfico a[illegible] servidor apropiado.

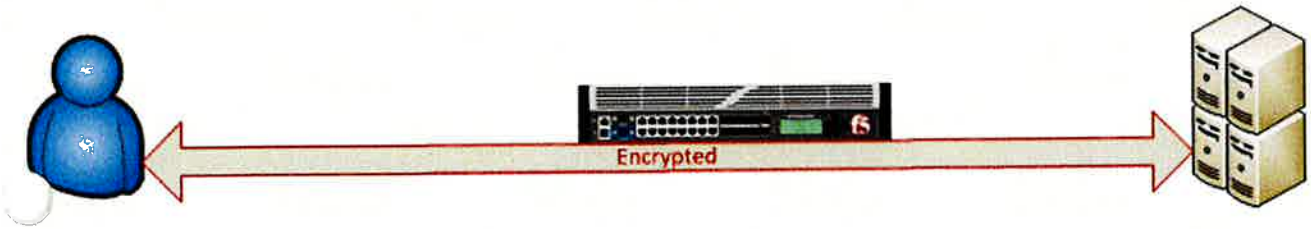
Descarga deSSL: en este método, el tráfico de clientes a BIG-IP se envía cifrado. En lugar de que el servidor descifre y vuelva a cifrar el tráfico, BIG-IP manejaría esa parte. Por lo tanto, el tráfico del cliente es descifrado por el BIG-IP y el tráfico descifrado se envía al servidor. La comunicación de retorno desde el servidor al cliente es encriptada por el BIG-IP y enviada de vuelta al cliente. De esta forma, se ahorra al servidor una carga adicional de cifrado y descifrado. Todos los recursos del servidor ahora se pueden utilizar completamente para servir al contenido de la aplicación o para cualquier otro propósito para el que estén diseñados.



Nota:

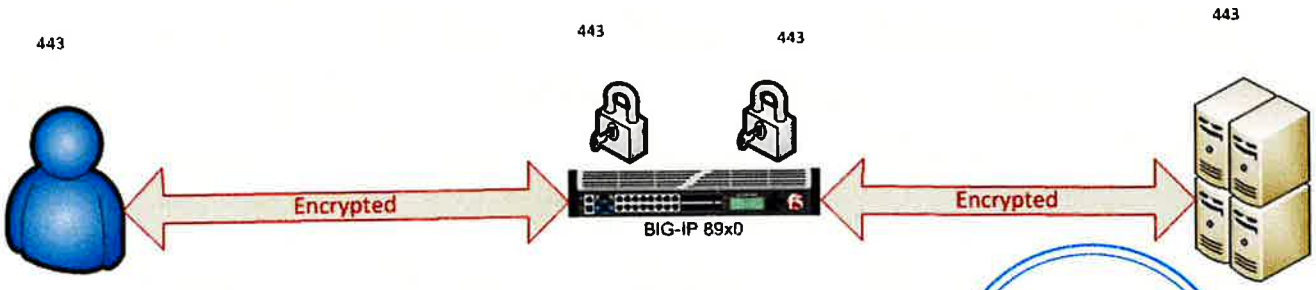
La comunicación entre el servidor BIG-IP y el servidor es en texto plano.
Los servidores están configurados para escuchar en puertos no seguros del Puerto 80
Dado que BIG-IP descifra el tráfico HTTP, ahora tiene la capacidad de leer el contenido (encabezado, txt, cookies, etc.) y se pueden aplicar todas las opciones de persistencia. (Dirección de origen, Dirección de destino, Cookies, SSL, SIP, Universal, MSRDP)

SSL Pass through-Como su nombre indica, BIG-IP solo pasará el tráfico del cliente a los servidores que se abstengan de cualquier carga de trabajo relacionada con SSL. En lugar de reenviar problemas SSL y conexiones a los servidores directamente, solo pasará el tráfico del cliente a los servidores. Por lo general, esta configuración se utiliza si las aplicaciones que se sirven son anti-proxy SSL o no pueden consumir tráfico descifrado.



Dado que solo pasa por LTM, no puede leer los encabezados, lo que introduce limitaciones en la persistencia. Solo se puede utilizar la información no SSL del paquete para mantener la persistencia, como la dirección IP de origen y la dirección IP de destino.

Proxy SSL completo-Este método se conoce por varios nombres, como reencriptación SSL, puenteo SSL y terminaciones SSL. En este método, BIG-IP vuelve a encriptar el tráfico antes de enviarlo a los servidores. El cliente envía tráfico encriptado a BIG-IP, BIG-IP lo desencripta y, antes de enviarlo a los servidores o miembros del grupo, lo vuelve a encriptar. Este método se utiliza generalmente para satisfacer el requisito de que el tráfico también esté encriptado entre LTM y los servidores. Este requisito puede implementarse para mayor seguridad o para evitar intrusiones desde dentro de la red. Cuando se utiliza este método, los servidores también tendrán que desencriptar y encriptar el tráfico.



Nota –

La comunicación entre el servidor LTM y el servidor es segura

Los servidores están configurados para escuchar en puertos seguros, por ejemplo, el puerto 443.

Dado que el LTM descifra inicialmente el tráfico HTTP, aún tiene la capacidad de leer el contenido (encabezado, txt, cookies, etc.) y se pueden aplicar todas las opciones de persistencia, al igual que en la descarga SSL. (Dirección de origen, dirección de destino, cookies, SSL, SIP, Universal, MSRDP)

Contenido relacionado

DevCentral: Paso directo SSL gh, descarga SSL gy puente SSL gen g K14343463: Configurar g el BIG-IP s ysistema para pasar a través de gh tráfico SSL La**implementación gProxy de reenvío SSL yen un solo gBIG-IP S ysistema** capítulo de la **IG-IP S ysistema: Administración SSL** guía

La**Acerca de la descarga SSL** sección de la**Administración de tráfico SSL gmento** capítulo de la**IG-IP S ysistema: Administración SSL** guía

Contenido recomendado por IA

Aviso de seguridad -**000156572: Trimestral ySeguridad yNotificación (octubre de 2025)** Política -**4309: Ciclo de vida del producto de hardware F5 ysoporte de cle ppolítica de servicio y** Aviso de seguridad -

000157334: Vulnerabilidad de BIND yCVE-2025-40778

Aviso de seguridad - **000157862: Vulnerabilidad de Apache Tomcat yCVE-2025-55754**

¿Le resultó útil esta información?

Sí o

¿Cómo podemos mejorar este contenido?

¿Podemos comunicarnos con usted directamente con respecto a estos comentarios?

Sí o

Protegido por reCAPTCHA: privacidad y Términos

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Proteja y ofrezca experiencias digitales extraordinarias

El portafolio de capacidades de automatización, seguridad, rendimiento e información de F5 permite a nuestros clientes crear, proteger y operar aplicaciones adaptables que reducen costos, mejoran las operaciones y protegen mejor a los usuarios.obtener más información ›

QUÉ OFRECEMOS

RECURSOS

SOPORTE

SOCIOS

EMPRESA

CONÉCTESE CON NOSOTROS

Wagner Peña

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Capítulo del manual : Interfaces

Se aplica a:

Mostrar versiones

Índice | << Capítulo anterior | Capítulo siguiente >>

Introducción a las interfaces del sistema BIG-IP

Una tarea clave de la configuración del sistema BIG-IP es la configuración de sus interfaces. Las interfaces de un sistema BIG-IP son los puertos físicos que se utilizan para conectar el sistema BIG-IP a otros dispositivos de la red. Estos dispositivos pueden ser routers de siguiente salto, dispositivos de capa 2, servidores de destino, etc. A través de sus interfaces, el sistema BIG-IP puede reenviar tráfico hacia o desde otros dispositivos de la red.

Nota: *El término* ***interfaz*** *se refiere a los puertos físicos del sistema BIG-IP.*

Cada sistema BIG-IP incluye múltiples interfaces. El número exacto de interfaces en el sistema BIG-IP depende del tipo de plataforma.

Un sistema BIG-IP tiene dos tipos de interfaces:

Una interfaz de gestión
La ***interfaz de administración*** es una interfaz especial dedicada a realizar un conjunto específico de funciones de administración del sistema.
Interfaces de conmutador TMM
Las interfaces de conmutación TMM son aquellas interfaces que el sistema BIG-IP utiliza para enviar o recibir tráfico de aplicaciones, es decir, tráfico destinado a la entrega de aplicaciones.
Cada una de las interfaces del sistema BIG-IP tiene propiedades únicas, como la dirección MAC, la velocidad del medio, el modo dúplex y la compatibilidad con el Protocolo de descubrimiento de capa de enlace (LLDP).

Además de configurar las propiedades de la interfaz, puede implementar una función conocida como ***duplicación de interfaz*** , que permite duplicar el tráfico de una o más interfaces a otra. También puede consultar las estadísticas del tráfico en cada interfaz.

Una vez configuradas las propiedades de cada interfaz, puede configurar otras funciones del sistema BIG-IP que controlan su funcionamiento. Por ejemplo, al crear una red de área local virtual (VLAN) y asignarle interfaces, el sistema BIG-IP puede insertar un ID de VLAN (etiqueta) en las tramas que pasan por dichas interfaces. De esta forma, una sola interfaz puede reenviar tráfico a varias VLAN.

452

Acerca del protocolo de descubrimiento de la capa de enlace

El sistema BIG-IP es compatible con el Protocolo de Descubrimiento de Capa de Enlace (LLDP). LLDP es un protocolo de capa 2 estándar de la industria (IEEE 802.1AB) que permite que un dispositivo de red, como el sistema BIG-IP, anuncie su identidad y capacidades a dispositivos vecinos de varios proveedores en una red. El protocolo también permite que un dispositivo de red reciba información de los dispositivos vecinos.

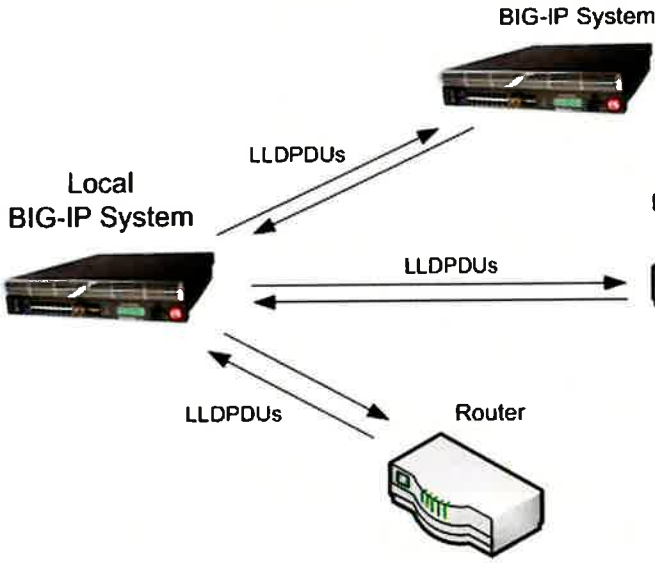
LLDP transmite información del dispositivo en forma de mensajes LLDP, conocidos como Unidades de Datos LLDP (LLDPDU). En general, este protocolo:

- Anuncia información de conectividad y administración acerca del dispositivo BIG-IP local a los dispositivos vecinos en la misma LAN IEEE 802.
- Recibe información de administración de red de dispositivos vecinos en la misma LAN IEEE 802.
- Funciona con todos los protocolos de acceso IEEE 802 y medios de red.

Con la utilidad de configuración de BIG-IP o tmsh , puede configurar las interfaces del sistema BIG-IP para transmitir o recibir LLDPDU. Más específicamente, puede:

- Especifique el contenido exacto de las LLDPDU que una interfaz del sistema BIG-IP transmite a un dispositivo vecino. Este contenido se especifica configurando los atributos LLDP en cada interfaz.
- Especifique globalmente las frecuencias de diversas propiedades de transmisión de mensajes y el número de vecinos de los que cada interfaz puede recibir mensajes. Estas propiedades se aplican a todas las interfaces del sistema BIG-IP.

Esta figura muestra un sistema BIG-IP local habilitado para LLDP, configurado para transmitir y recibir mensajes LLDP desde dispositivos vecinos en una LAN.



Un sistema BIG-IP local que transmite y recibe LLDPDUs

Propiedades de la interfaz

Cada interfaz del sistema BIG-IP tiene un conjunto de propiedades que se pueden configurar, como habilitar o deshabilitar la interfaz, configurar el tipo de medio y el modo dúplex solicitados, y configurar el control de flujo. Configurar las propiedades de cada interfaz es una de las primeras tareas tras ejecutar la utilidad de configuración en el sistema BIG-IP. Si bien se pueden modificar algunas de estas propiedades, como la velocidad del medio y el

modo dúplex, no se pueden modificar otras, como la dirección MAC (control de acceso al medio).

Nota: *Puede configurar propiedades relacionadas con STP en una interfaz configurando uno de los protocolos de árbol de expansión.*

Antes de configurar las propiedades de la interfaz, conviene comprender las convenciones de nomenclatura. Solo los usuarios con el rol de Administrador o Administrador de recursos pueden crear y administrar interfaces.

Convenciones de nomenclatura de interfaces
Por convención, los nombres de las interfaces del sistema BIG-IP utilizan el formato <s>.<p>, donde s es el número de ranura de la tarjeta de interfaz de red (NIC) y p es el número de puerto de la NIC. Ejemplos de nombres de interfaz son `1.1`, `1.2` y `2.1`. Las interfaces del sistema BIG-IP ya tienen nombres asignados; no se asignan explícitamente.

Una excepción a la convención de nombres de interfaz es la interfaz de administración, que tiene el nombre especial, MGMT.

Acerca de la información de la interfaz y las propiedades de los medios
Con la utilidad de configuración de BIG-IP, puede visualizar una pantalla que enumera todas las interfaces del sistema BIG-IP, así como su estado actual (**ARRIBA**o**ABAJO**). También puedes ver otra información sobre cada interfaz:

- Dirección MAC de la interfaz
- Disponibilidad de la interfaz
- Tipo de medio
- Velocidad de los medios
- Modo activo (como completo)

Esta información es útil para evaluar cómo una interfaz específica reenvía tráfico. Por ejemplo, puede usarla para determinar las VLAN específicas a las que una interfaz reenvía tráfico actualmente. También puede usarla para determinar la velocidad a la que opera una interfaz.

Estado de la interfaz
Puede habilitar o deshabilitar una interfaz en el sistema BIG-IP. De forma predeterminada, cada interfaz está habilitada y puede aceptar tráfico de entrada y salida. Si la interfaz está deshabilitada, no puede aceptar tráfico de entrada ni salida.

Medios solicitados fijos
La propiedad Medios solicitados fijos muestra que la interfaz detecta automáticamente el modo dúplex de la interfaz.

Acerca del control de flujo
Puede configurar cómo una interfaz gestiona las tramas de pausa para el control de flujo. ***Las tramas de pausa*** son tramas que una interfaz envía a una interfaz par para controlar la transmisión de tramas desde dicha interfaz. Pausar las transmisiones de tramas de un par evita que la cola FIFO (primero en entrar, primero en salir) de una interfaz se llene y provoque una pérdida de datos. Los valores posibles para esta propiedad son:

Pausa Ninguna
Desactiva el control de flujo.
Pausa TX/RX
Especifica que la interfaz respeta los marcos de pausa de su par y también los genera cuando es necesario. Este es el valor predeterminado.
Pausa TX
Especifica que la interfaz ignora los marcos de pausa de su par y genera marcos de pausa cuando es necesario

Pausa RX
Especifica que la interfaz respeta los marcos de pausa de su par, pero no genera marcos de pausa.

Acerca de la propiedad Tipo Ether
La propiedad "Tipo de Ether" aparece en la utilidad de configuración de BIG-IP solo cuando el sistema admite hardware ePVA. Un ***tipo de Ether*** es un campo de dos octetos en una trama Ethernet que indica el protocolo encapsulado en la carga útil. El sistema BIG-IP utiliza el valor de esta propiedad cuando una interfaz o troncal está asociada a una VLAN IEEE 802.1QinQ (doble etiqueta). De forma predeterminada, el sistema establece este valor en **0x8100** .

Acerca de la propiedad LLDP
La propiedad LLDP es una de las dos propiedades relacionadas con LLDP que se pueden configurar para una interfaz específica. Los valores posibles para esta configuración son:

Desactivado
Cuando se establece en este valor, la interfaz no transmite (envía) mensajes LLDP a dispositivos vecinos ni recibe mensajes LLDP de ellos.

Sólo transmitir
Cuando se establece en este valor, la interfaz transmite mensajes LLDP a los dispositivos vecinos, pero no recibe mensajes LLDP de estos dispositivos.

Recibir solo
Cuando se establece en este valor, la interfaz recibe mensajes LLDP de dispositivos vecinos, pero no transmite mensajes LLDP a dispositivos vecinos.

Transmitir y recibir
Cuando se establece en este valor, la interfaz transmite mensajes LLDP hacia y recibe mensajes LLDP de dispositivos vecinos.

Además de las configuraciones relacionadas con LLDP que puede configurar por interfaz, puede configurar algunas configuraciones globales de LLDP que se apliquen a todas las interfaces del sistema.

Además, puede ver las estadísticas correspondientes a cualquier dispositivo vecino que haya transmitido mensajes LLDP al sistema BIG-IP local.

Atributos LLDP
La configuración "Atributos LLDP" es una de las dos opciones relacionadas con LLDP que se pueden configurar para una interfaz específica. Esta configuración de interfaz se utiliza para especificar el contenido de un mensaje LLDP que se envía o recibe. Cada atributo LLDP que se especifica con esta configuración es opcional y se presenta en formato Tipo, Longitud y Valor (TLV).

Wagner Peña

IPX expert IPX SRL RNC 130-850151 Santo Domingo, RD

Acerca de la duplicación de interfaz

Por razones de confiabilidad, puede configurar una función conocida como duplicación de interfaces. Al configurar ***la duplicación de interfaces*** , el sistema BIG-IP copia el tráfico de una o más interfaces a otra que especifique. De forma predeterminada, la duplicación de interfaces está deshabilitada.

Configuraciones de vecinos

Cuando una interfaz del sistema BIG-IP recibe mensajes LLDP de dispositivos vecinos, el sistema BIG-IP muestra información del chasis, el puerto y el sistema sobre el contenido de dichos mensajes. En concreto, el sistema muestra los valores de los TLV estándar de cada vecino. Estos TLV son:

455

Identificación del chasis
Identifica el chasis que contiene la estación LAN IEEE 802 asociada con el agente LLDP transmisor.
ID de puerto
Identifica el componente de puerto del identificador del punto de acceso al servicio multimedia (MSAP) asociado con el agente LLDP de transmisión.
Descripción del puerto
Una cadena alfanumérica que describe la interfaz.
Nombre del sistema
Una cadena alfanumérica que indica el nombre asignado administrativamente al dispositivo vecino.
Descripción del sistema
Una cadena alfanumérica que constituye la descripción textual de la entidad de red. La descripción del sistema debe incluir el nombre completo y la identificación de la versión del tipo de hardware, el sistema operativo y el software de red del dispositivo vecino.
Capacidades del sistema
Las funciones principales del sistema y si estas funciones principales están habilitadas.
Dirección de administración
Una dirección asociada al agente LLDP local que se utiliza para acceder a las entidades de capa superior. Este TLV también puede incluir el número de interfaz del sistema asociado a la dirección de administración, si se conoce.

Configurar ajustes para una interfaz

Puede utilizar este procedimiento para configurar los ajustes de una interfaz individual en el sistema BIG-IP.

1. En la pestaña Principal, haga clic en **Red** > **Interfaces** > **Lista de interfaces** . La pantalla Lista de interfaces muestra la lista de interfaces del sistema.
2. En la columna Nombre, haga clic en un número de interfaz. Esto mostrará sus propiedades.
3. Para la configuración **de Estado** , verifique que la interfaz esté configurada en **Habilitada** .
4. De la lista **LLDP** , seleccione un valor.
5. Para la configuración **de Atributos LLDP** , verifique que la lista de atributos en el campo **Enviar** incluya todos los Valores de longitud de tiempo (TLV) que desea que la interfaz del sistema BIG-IP envíe a los dispositivos vecinos.
6. Haga clic en el botón **Actualizar** .

Después de realizar esta tarea, la interfaz se configura para enviar la información LLDP especificada a los dispositivos vecinos.

Wagner Pina

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Tareas de configuración relacionadas

Tras configurar las interfaces en el sistema BIG-IP, una de las principales tareas es asignarlas a las redes LAN virtuales (VLAN) que cree. Una ***VLAN*** es un subconjunto lógico de hosts en una red de área local (LAN) que residen en el mismo espacio de direcciones IP. Al asignar varias interfaces a una sola VLAN, el tráfico destinado a un host de esa VLAN puede circular a través de cualquiera de estas interfaces para llegar a su destino. Por el

456

contrario, al asignar una sola interfaz a varias VLAN, el sistema BIG-IP puede usar esa única interfaz para cualquier tráfico destinado a los hosts de esas VLAN.

Otra potente función que puede utilizar para las interfaces del sistema BIG-IP es el enlace troncal con agregación de enlaces. Un ***enlace troncal*** es un objeto que agrupa lógicamente las interfaces físicas para aumentar el ancho de banda. La agregación de enlaces, mediante el protocolo de control de agregación de enlaces (LACP), estándar de la industria, proporciona una monitorización regular del estado del enlace, así como conmutación por error si una interfaz deja de estar disponible.

Finalmente, puede configurar las interfaces del sistema BIG-IP para que funcionen con uno de los protocolos de árbol de expansión (STP, RSTP y MSTP). ***Los protocolos de árbol de expansión*** reducen el tráfico en su red interna al bloquear rutas duplicadas para evitar bucles de puenteo.

Índice | << Capítulo anterior | Capítulo siguiente >>

Wagner Peña

IPX SRL
RNC 130-850151
Santo Domingo, R.D.

458

Clouddocs (https://clouddocs-f5-com.translate.goog/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc) >> (https://clouddocs-f5-com.translate.goog/api/index.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc)Inicio de iApps

Página principal de iApps ¶ (https://clouddocs-f5-com.translate.goog/api/iapps/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc#iapps-home)

Advertencia

Las plantillas de servicios de aplicaciones de F5 (FAST) están reemplazando a las plantillas de iApp. Consulte https://support.f5.com/csp/article/K13422 para obtener más información.

La versión 10 de BIG-IP introdujo el concepto de plantillas de aplicaciones. El objetivo era proporcionar un asistente para múltiples aplicaciones bien implementadas, abstrayendo algunos de los detalles de configuración y reduciendo el error humano en las complejidades de seguir las guías de implementación de estas aplicaciones. Un gran avance, pero con algunas limitaciones, como la imposibilidad de personalizar la plantilla o su implementación, y la falta de una forma de limpiar de forma centralizada (e individual) una implementación basada en plantillas. Sin embargo, esto era solo el comienzo. Así nació F5 iApps® .

¿Qué son las iApps? ¶ (https://clouddocs-f5-com.translate.goog/api/iapps/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc#what-are-iapps)

iApps es el marco de sistema de BIG-IP® para implementar configuraciones basadas en servicios y plantillas en sistemas BIG-IP que ejecutan TMOS® 11.0.0 y versiones posteriores. Consta de tres componentes: Plantillas, Servicios de Aplicación y Analítica. Una Plantilla de iApps describe la aplicación y define los objetos (obligatorios y opcionales) mediante un lenguaje de presentación e implementación. Un Servicio de Aplicación de iApps es el proceso de implementación de una Plantilla de iApps, que agrupa todas las opciones de configuración para una aplicación específica. Por ejemplo, se dispone de un Servicio de Aplicación de iApps para SharePoint. La Analítica de iApps incluye métricas de rendimiento por aplicación y ubicación.

Ventajas de usar iApps ¶ (https://clouddocs-f5-com.translate.goog/api/iapps/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc#benefits-of-using-iapps)

- Personalizable por el usuario
- Fácil edición de configuraciones y limpieza
- Reingreso
- encapsulación de configuración
- gestión de la configuración desde la cuna hasta la tumba
- La rigurosidad protege contra cambios accidentales en la configuración.
- Tareas operativas y estado de salud de los objetos de la aplicación que se muestran en la vista de componentes específica de la aplicación (ver a la derecha).
- Capacidad de copiar/importar/exportar
- Soporte de la comunidad para las plantillas alojadas en DevCentral

Wagner Peña

expert IPX SRL RNC 130-850151 Santo Domingo, R.D.

459

Plantillas de iApps ¶ (https://clouddocs-f5-com.translate.goog/api/iapps/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc#iapps-templates)

La plantilla es donde se define toda la base para el despliegue de la aplicación. Una plantilla consta de tres secciones:

- **Implementación** : La sección de implementación (https://clouddocs-f5-com.translate.goog/api/iapps/implementation.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc) está escrita en el lenguaje de scripting tmsh, basado en TCL. Esta sección se encarga de compilar y aplicar la configuración. Todo lo que se puede hacer en tmsh se puede realizar con una plantilla de iApps. tmsh (https://clouddocs-f5-com.translate.goog/api/tmsh/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc) describe el entorno de scripting de tmsh, así como todos los comandos y la sintaxis. Se recomienda el uso del paquete iApp.iApp-Utility-Package (https://clouddocs-f5-com.translate.goog/api/iapps/iApp-Utility-Package.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc) .
- **Presentación** : La sección de presentación está escrita en APL (https://clouddocs-f5-com.translate.goog/api/iapps/APL.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc) (Application Presentation Language). Esto crea la interfaz de usuario para la plantilla iApp. La página APL (https://clouddocs-f5-com.translate.goog/api/iapps/APL.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc) define los comandos y la sintaxis disponibles.
- **Ayuda** - La sección de ayuda está basada en HTML y se utiliza para guiar a los usuarios en el uso de la plantilla iApp.

Las plantillas de iApps también se pueden crear, editar, copiar y eliminar dentro de tmsh en /sys application template. Para habilitar el resaltado de sintaxis, introduzca 'modify /cli preference tcl-syntax-highlighting enabled' en la línea de comandos de tmsh.

Plantillas de iApps de envío ¶ (https://clouddocs-f5-com.translate.goog/api/iapps/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc#shipping-iapps-templates)

En las versiones 12.0 a 15.0, BIG-IP incluía las siguientes plantillas de iApps. Las plantillas de F5 Application Services (FAST) están reemplazando a las plantillas de iApps. Consulte el artículo K13422 (https://translate.google.com/website?sl=en&tl=es&hl=es&client=srp&u=https://support.f5.com/csp/article/K13422) para obtener más información.

- CIFS
- Diámetro
- Balanceo de carga DNS
- FTP
- HTTP
- Reenvío de IP
- LDAP
- Microsoft IIS 7 y 7.5
- Microsoft SharePoint 2010
- nPath
- Oracle Application Server 10g (y SSO versión 10g Release 2 - v10.1.2.0.2)
- Oracle EBS 12
- Oracle PeopleSoft 9
- Oracle WebLogic Server 10.3 (BEA WebLogic 5.1 y 8.1)
- Radio
- Replicación
- SAP Enterprise Portal 6.0, mySAP ERP 2005
- Componente central de SAP ERP 6.0, mySAP ERP 2005

460

Plantillas compatibles con Microsoft Exchange y otras disponibles para su descarga en downloads.f5.com (https://translate.google.com/website?sl=en&tl=es&hl=es&client=srp&u=https://downloads.f5.com) (requiere inicio de sesión).

iControl para iApps ¶ (https://clouddocs-f5-com.translate.goog/api/iapps/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc#icontrol-for-iapps)

iApps son compatibles con iControl.

- Para crear, modificar o eliminar plantillas de iApps, consulte estos comandos, iApps Template iControl WIKI (https://clouddocs-f5-com.translate.goog/api/icontrol-soap/Management__ApplicationTemplate.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc) .
- Para implementar, volver a ingresar o eliminar iApps Application Services, consulte estos comandos en la wiki de iControl de iApps Application Service (https://clouddocs-f5-com.translate.goog/api/icontrol-soap/Management__ApplicationService.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc) .

Las iApps también se pueden configurar mediante iControl-REST. Aquí (https://translate.google.com/website?sl=en&tl=es&hl=es&client=srp&u=https://community.f5.com/t5/technical-articles/full-examples-of-icontrolrest-for-device-and-application-service/ta-p/276589) se documentan algunos ejemplos .

Consejos y técnicas para el desarrollo de iApps ¶ (https://clouddocs-f5-com.translate.goog/api/iapps/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc#iapps-development-tips-and-techniques)

- Consejos y técnicas para el desarrollo de plantillas iApps (https://clouddocs-f5-com.translate.goog/api/iapps/iApp-Template-Development-Tips-and-Techniques.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc)
- Primeros pasos con iApps (serie en DevCentral) (https://translate.google.com/website?sl=en&tl=es&hl=es&client=srp&u=https://community.f5.com/t5/tag/series-getting%2520started%2520with%2520iapps/tg-p/board-id/TechnicalArticles)

La documentación de referencia de la API de BIG-IP contiene contenido aportado por la comunidad. F5 no supervisa ni controla las contribuciones de código de la comunidad. No ofrecemos garantías sobre el código disponible, el cual puede contener errores, defectos, fallos, imprecisiones o vulnerabilidades de seguridad. El acceso y uso del código disponible en las guías de referencia de la API de BIG-IP es responsabilidad exclusiva del usuario.

Anterior (https://clouddocs-f5-com.translate.goog/api/index.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc)
/clouddocs-f5-com.translate.goog/api/iapps/AppSvcsiApp_overview.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc)

461

TTP: sts
Modo TTP: sts habilitar deshabilitar
Edad máxima de TTP: sts Incluir segundos
subdominios de TTP: sts habilitar habilitar

 # Introducido en la versión 13

Recarga de TTP: sts habilitar habilitar

Además del panel de acceso disponible a través de BIG-IQ Centralized Management for BIG-IP APM, el panel de políticas de acceso en el sistema BIG-IP ofrece una visión rápida de la salud del acceso. Puedes ver la plantilla predeterminada de sesiones activas, rendimiento de acceso a la red, nuevas sesiones y conexiones de acceso a la red, o crear vistas personalizadas
Usando el selector de ventanas del panel. Al arrastrar y soltar las estadísticas deseadas en el cristal de la ventana, obtienes una comprensión en tiempo real de la salud del acceso.

FLEXIBILIDAD Y, ALTO RENDIMIENTO Y ALABILIDAD SIN IGUAL.

BIG-IP APM ofrece acceso flexible a aplicaciones, red y nube, manteniendo a tus usuarios productivos y permitiendo que tu organización escale de forma rápida y rentable.

BIG-IP APM puede desplegarse de diversas formas para cubrir tus necesidades específicas de acceso. BIG-IP APM puede ser:

- Desplegado como módulo adicional para BIG-IP LTM para proteger aplicaciones públicas
- Entregado como un dispositivo BIG-IP independiente o como chasis independiente F5 VIPRION®
- Incluido con una BIG IP LTM Virtual Edition (VE) para ofrecer acceso flexible a aplicaciones en entornos virtualizados
- Funcionan en ediciones virtuales de alta gama y ediciones virtuales de alto rendimiento
- Ofrecido en una plataforma Turbo SSL

Wagner Pe

Además de estar licenciado para estas plataformas, BIG-IP APM también puede estar licenciado como el mejor paquete de la oferta Good-Better-Best de F5, como parte del Acuerdo de Licencia Empresarial (ELA) de F5 para BIG-IP VEs, y de modelos de licencias por suscripción.

BIG-IP APM está disponible en una plataforma de chasis y en todos los appliances BIG-IP. Es compatible con el entorno de Multiprocesamiento™ Virtual en Clúster (vCMP) F5. El hipervisor vCMP ofrece la capacidad de ejecutar múltiples instancias de BIG-IP APM, lo que resulta en multitenencia y efectividad
separación. Con vCMP, los administradores de red pueden virtualizar mientras alcanzan un mayor nivel de redundancia y control.

BIG-IP APM ofrece descarga SSL a velocidades de red y soporta hasta 3.000 inicios de sesión por segundo. Para organizaciones con una base de usuarios de aplicaciones web en constante crecimiento, esta solución escala de forma rápida y rentable.

El uso de BIG-IP APM se basa en dos tipos de sesiones de usuario: sesiones de acceso y sesiones de uso concurrente de conexión (CCU). Las sesiones de acceso se aplican a sesiones de autenticación, IAP, VDI y situaciones similares. CCU es aplicable para acceso a la red, como acceso VPN completo y aplicación

túneles o acceso a la web. La plataforma BIG-IP y la plataforma VIPRION —ambas compatibles con BIG-IP APM— gestionan exponencialmente más sesiones de acceso que sesiones CCU en casos de uso como autenticación, SAML, SSO y proxy forward. Esto significa que si tienes la intención de usar BIG-IP APM para autenticación, VDI y similares, el número de sesiones soportadas en VIPRION puede llegar hasta 2 millones, y la plataforma BIG-IP puede soportar hasta 1 millón.

Características de BIG-IP APM

Ya sea ejecutándose como módulo independiente o incluido en la plataforma BIG-IP, o en un blade de chasis VIPRION, BIG-IP APM se basa en el inteligente y modular sistema operativo F5 TMOS®, que ofrece visión, flexibilidad y control para ayudarte a habilitar mejor el acceso a aplicaciones, red y nube.

LAS GRANDES CARACTERÍSTICAS DE LOS APM DE IP INCLUYEN:

- Aplicación granular de políticas de acceso
- Creación y gestión de políticas conscientes de la identidad y del contexto
- Enrutamiento de políticas
- Soporte para el Proxy Consciente de la Identidad (IAP) que permite el acceso a aplicaciones de confianza cero
- Autorización basada en contexto con ACLs dinámicas L4/L7
- Soporte para federación de identidades SAML 2.0
- Soporte para el protocolo de autorización OAuth 2.0
- Federación simplificada de identidades para aplicaciones con atributos multivalorados
- Soporte SSO para autenticación clásica (Kerberos, basada en cabeceras, etc.), caché de credenciales, OAuth 2.0, SAML 2.0 y FIDO2 (U2F)

Integra con soluciones SSO de terceros

Caché de credenciales y proxy para SSO

Uniendo métodos modernos de autenticación y autorización (SAML, OAuth/OIDC) y los métodos clásicos de autenticación y autorización

- Soporte para la Clave de Prueba OIDC para el intercambio de códigos (PKCE)
- Soporte para autenticación basada en SAML usando BIG-IP Edge Client y acceso F5 para Android y iOS
- Soporte para la vinculación de artefactos SAML
- Soporte para el perfil SAML ECP
- Autenticación de servidores AAA y alta disponibilidad
- Soporte para autenticación step-up
- Soporte de cifrado web JSON para clientes públicos
- Autenticación multifactor (MFA) mediante contraseña de un solo uso (OTP)
- Integración fluida con soluciones MFA de terceros
- Modo DTLS 2.0 para entregar y asegurar aplicaciones
- Acceso remoto SSL VPN

LAS GRANDES CARACTERÍSTICAS DE LOS APM DE IP INCLUYEN (CON T):

- Acceso siempre conectado
- Establecer un túnel VPN siempre activo

(con inicio de sesión en el sistema operativo de Windows y cliente BIG-IP Edge para Windows)

- Soporte amplio para plataformas de cliente (véase F5 BIG-IP APM Matrices de Compatibilidad de Clientes para cada versión de BIG-IP)
- Soporte robusto para navegadores web (véase F5 BIG-IP APM Client Compatibility Matrices para cada versión)
- Comprobaciones continuas de integridad y seguridad en los puntos finales
- Soporte para seguridad en endpoints y VPN sin complementos para navegadores web
- Cifrado IPsec de sitio a sitio
- Túneles de aplicación
- "Webtops" dinámicos, basados en la identidad del usuario
- Integración con productos líderes de proveedores IAM (Microsoft, Okta, Ping Identity)
- Métodos de autenticación: formulario, certificado, Kerberos SSO, SecurID, básico, token RSA, tarjeta inteligente, factor N
- Protección de credenciales de usuario
- Protección y autorización de la API
- Acceso basado en riesgos aprovechando UEBA de terceros y motores de riesgo (HTTP Connector)
- Soporte para Identity-as-a-Service (IDaaS), incluyendo Azure Active Directory y Okta
- Editor Visual de Políticas (VPE) y Configuración Guiada por Acceso (AGC)
- Agente de geolocalización IP (en VPE)
- Soporte para certificados de máquina Windows
- Integración con el Administrador de Credenciales de Windows
- Soporte para páginas de inicio de sesión externas
- Soporte para control de acceso al servidor virtual BIG-IP LTM
- Escala hasta 2 millones de sesiones de acceso concurrentes
- BIG-IP Edge Client y F5 Access se integran con VMware Horizon ONE (AirWatch), Microsoft Intune e IBM MaaS360
- Integración del cliente de borde BIG-IP con Windows en ARM64
- Exportación e importación de políticas de acceso mediante BIG-IQ Centralized Management
- Tiempos de espera configurables
- Monitor de control de salud para la contabilidad RADIUS
- Soporte de variables URI de aterrizaje
- Soporte de caché/proxy DNS
- Soporta Google reCAPTCHA v2 para autenticación y autenticación contextual
- Listo para IPv6
- Hojas de estilo para una página de inicio de sesión personalizada
- Informes avanzados centralizados con Splunk
- vCMP
- Lenguaje de scripting F5 iRules®
- Proxy completo
- Capas BIG-IP APM y BIG-IP ASM

Wagner Pastor

expert IPX SRL RNC 130-850151 Santo Domingo, R.D.

Plataformas F5 BIG-IP

Por favor, consulte las hojas de datos de hardware del sistema BIG-IP, VIPRION y Virtual Edition para más detalles. Para información sobre el soporte específico de módulos para cada plataforma, consulte las últimas notas de versión en AskF5. Para la lista completa de hipervisores soportados, consulte la Matriz de Hipervisores Soportados por VE. Las plataformas F5 pueden gestionarse mediante un único panel de cristal con la Gestión Centralizada BIG-IQ.

Electrodomésticos BIG-IP iSeries

VE

Ediciones Virtuales BIG-IP

Chasis VIPRION

Servicios Globales F5

F5 Global Services ofrece apoyo, formación y consultoría de primer nivel para ayudarte a sacar el máximo partido a tu inversión en F5. Ya sea proporcionando respuestas rápidas a preguntas, formando equipos internos o gestionando implementaciones completas desde el diseño hasta el despliegue, F5 Global Services puede ayudar a garantizar que tus aplicaciones sean siempre seguras, rápidas y fiables. Para más información sobre F5 Global Services, contacta con consulting@f5.com o visita f5.com/support.

Para saber más sobre BIG-IP APM, visita f5.com/apm.

Wagner Pastor

paso	detalles
.	Inicie sesión en su consola Nutanix PRISM para cargar la imagen BIG-IP VE.
.	Importe la imagen BIG-IP
.	Crear una máquina virtual y adjuntar subredes
.	Inicie la herramienta de configuración de BIG-IP.
.	Licenciar BIG-IP (consulte el artículo 7752 (ttps://my.f5.com/manage/s/article/K7752) para conocer los pasos).
0.	Configura el par BIG-IP HA

Requisitos previos para BIG-IP Virtual Edition¶

Las plataformas de hardware del hipervisor utanix Acropolis están basadas en KVM y DEBEN cumplir los siguientes requisitos del sistema KVM.

-Precaución

Las plataformas de hardware del hipervisor Utanix Acropolis están sujetas a cambios sin el conocimiento de 5.

Requisitos de CPU del host¶

La CPU del hardware host debe cumplir los siguientes requisitos.

La CPU debe tener arquitectura de 64 bits.

La CPU debe tener habilitado el soporte de virtualización (AMD-V o Intel VT-x) en la BIOS (./ vm/kvm_qat.html#qatstep1

La CPU debe admitir una relación de uno a uno entre hilos y CPU virtuales definidas, o en arquitecturas de un solo hilo, admitir al menos un núcleo por cada CPU virtual definida.

Si su CPU es compatible con el estándar de cifrado avanzado AES-NI, el procesamiento del cifrado SSL en BIG-IP VE será más rápido. Póngase en contacto con el proveedor de su CPU para obtener más información sobre las CPU compatibles con AES-NI.

Configure la CPU adecuadamente según los MHz requeridos por núcleo. Por ejemplo, si el hipervisor tiene núcleos de 2,0 GHz y el VE está configurado para 4 núcleos, necesitará reservar 4 núcleos de 2,0 GHz para 8 GHz (o

468

8000MHz).

Requisitos de memoria del host¶

número de núcleos	Se requiere esmeril
1	GB
2	GB
4	GB
8	6 GB

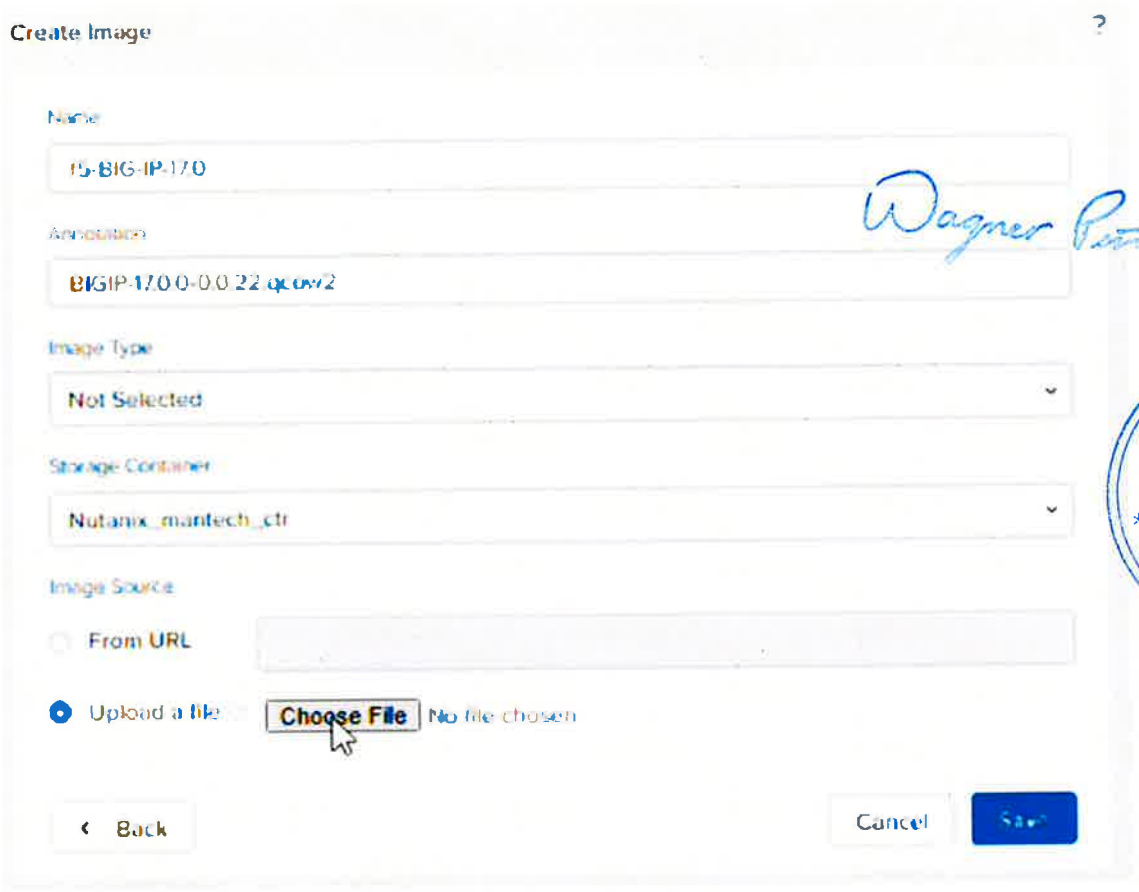
Subir la imagen BIG-IP VE¶

Los siguientes pasos muestran este proceso utilizando Nutanix AOS 5.20. Para obtener los pasos actualizados, consulte la documentación de Nutanix para AOS 6.5 (https://portal.nutanix.com/page/documents/details?targetId=Web-Console-Guide-Prism-v6_5:wc-image-configure-acropolis-wc-t.html).

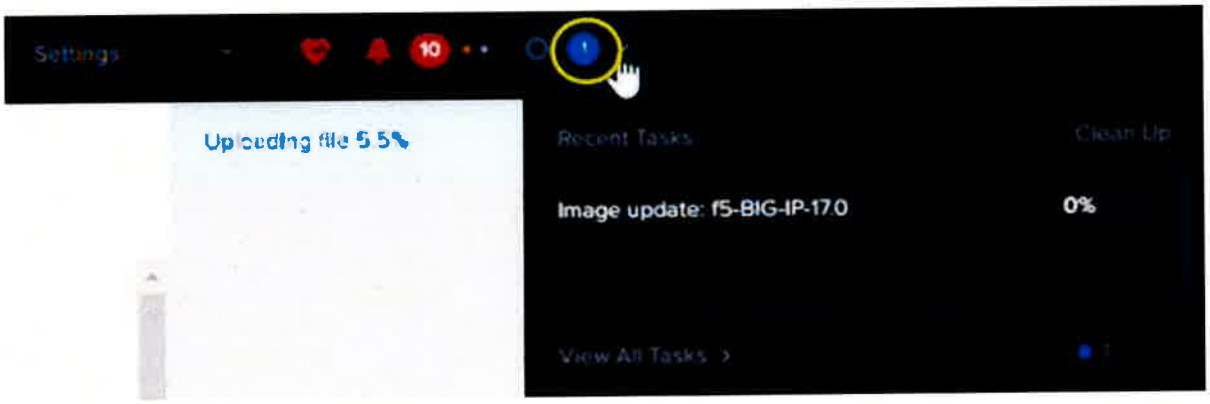
. og en la consola Nutanix AHV PRISM.

En el menú superior, expandaome -> Configuracióny luego seleccione elconfiguración de mago opción.

En elConfiguración de imagen Utanix AHV PRISMventana, haga clicSubir imagenNombre y anote su imagen, seleccionesubir un archivohacer clicSeleccionar archivoy seleccione el extraído IG-IP ALL.qcow2archivo y luego haga clicAhorrar



Para ver el progreso de la carga, en el menú superior, expanda el icono de alerta de archivo:

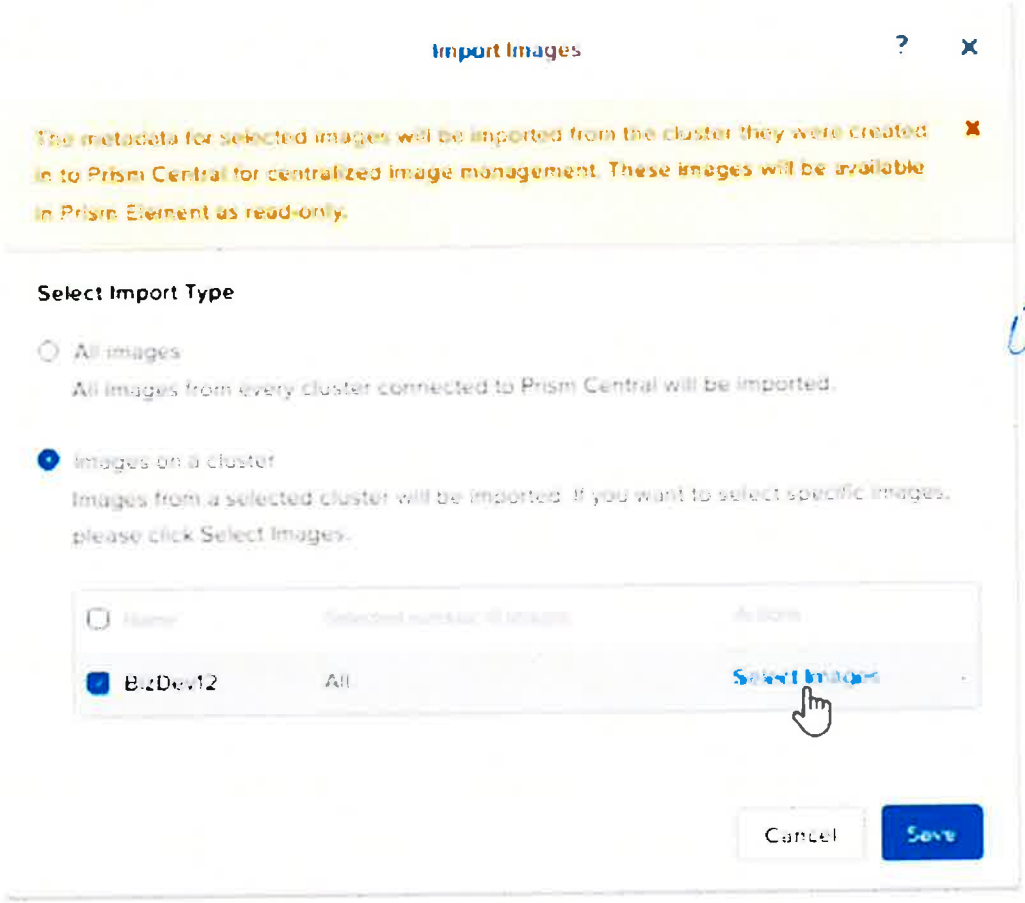


Importar la imagen BIG-IP VE¶

Los siguientes pasos muestran este proceso utilizando Nutanix AOS 5.20. Para obtener los pasos actualizados, consulte la documentación de Nutanix para AOS 6.5 (https://portal.nutanix.com/page/documents/details?targetId=Web-Console-Guide-Prism-v6_5:wc-image-configure-acropolis-wc-t.html).

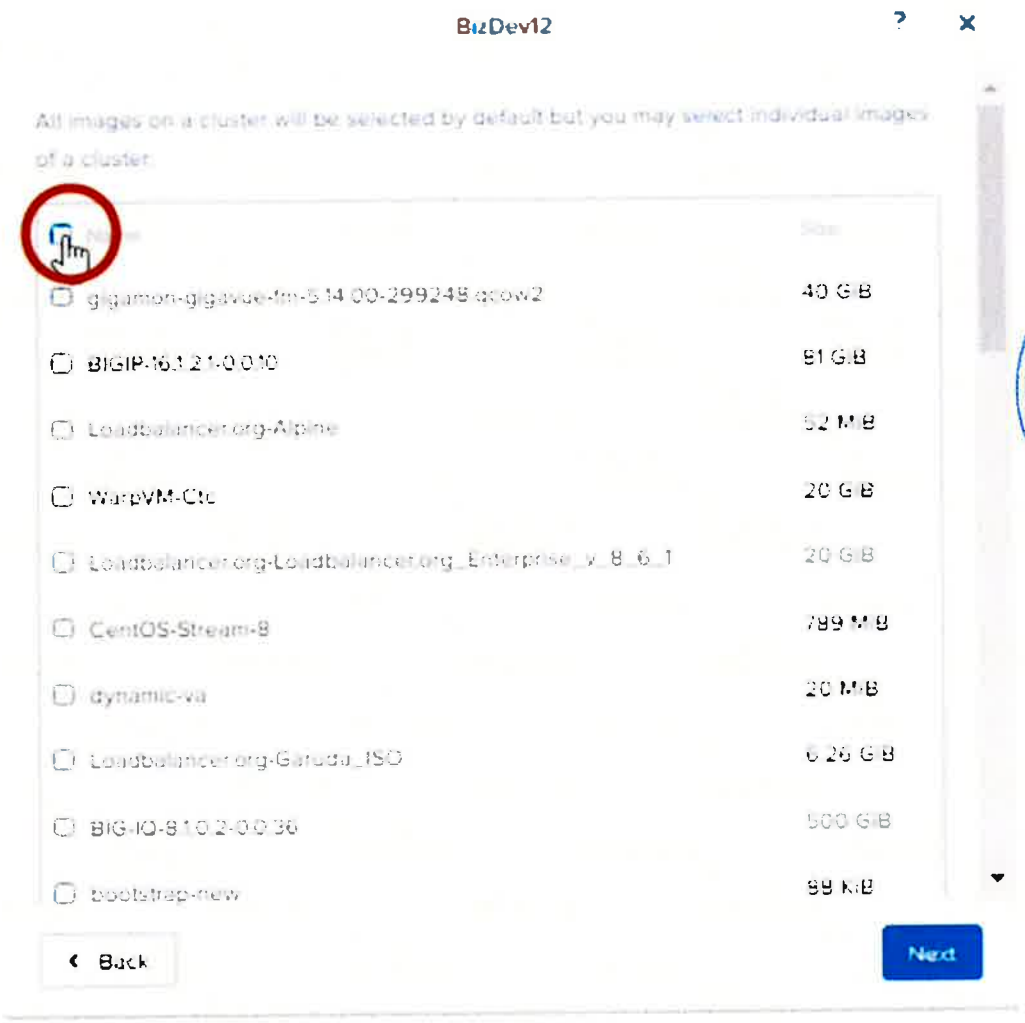
En la lista de todas las imágenes subidas, en el menú superior, haga clic enimágenes de importación

En el cuadro de diálogo emergente de importación de imágenes, seleccione lamagos en un grupoopción, seleccione la imagen de clústeropción que desea importar y, a continuación, haga clic enimágenes de selecciónenlace.



Wagner Peña

En la lista emergente de todas las imágenes de un clúster, en la parte superior de la lista, haga clic para borrarame casilla de verificación que deselecciona todos los archivos del clúster.



4. Desplácese por la lista y seleccione elIG-IPimagen en la lista, haga clicextensióny luego haga clicCra

Para ver el estado de la imagen importada, utilice lo siguiente:

En la parte superior de la ventana, haga clic enSolicitar detalles

En la esquina superior izquierda, haga clicmineraly luego seleccionarmagosDesde el menú de la izquierda, haga clic en la imagen de BIG-IP en la lista para ver el tamaño, el tipo, etc.

Crear una máquina virtual¶

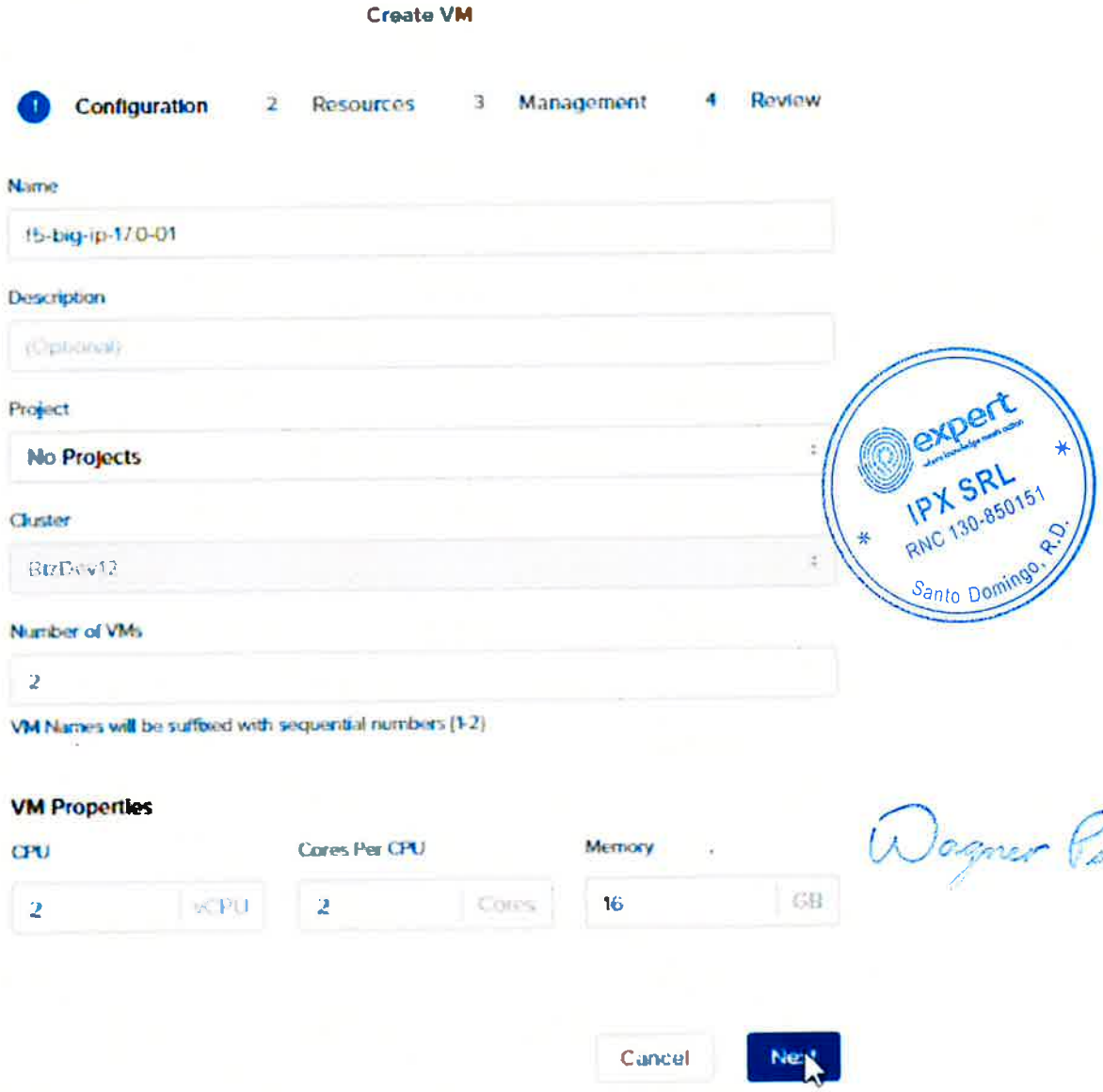
El siguiente proceso le guía en la creación de una máquina virtual de ejemplo con Nutanix AOS 5.2. Utilice esta máquina virtual para implementar un par BIG-IP VE HA. Puede configurar estos valores según los requisitos de su sistema. Para obtener los pasos actualizados, consulte la documentación de Nutanix AOS 6.5 (https://portal.nutanix.com/page/documents/details?targetId=vSphere-Admin6-AOS-v6_5:wc-vmcreate-esxi-t.html).

En el menú de la izquierda, haga clic.EMhacer clicCrear máquina virtualy luego complete el cuadro de diálogo emergente con un nombre número de máquinas virtualesestablecer en , y luego establecer lo siguientePropiedades de la máquina virtual

UPC -2 vCPU

Núcleos por CPU -2 núcleos

esmoria -16 GB



Haz clicextensión,en elrecursopestaña, clicAdjuntar disco,Complete lo siguiente y, a continuación, haga clic. Ahorrar

Tipo -Disco

Operación -Clonar a partir de la imagen

mago -Busque y seleccione la imagen BIG-IP.

Capacidad -81

a nosotros -SCSI

. en elredespanel, haga clicConectar a la subred(repita el proceso para adjuntar las siguientes subredes, por ejemplo), y luego haga clic.Ahorrar

R_PRT_DHCP

R_PRT_ESTÁTICO

R_INT_ESTÁTICO

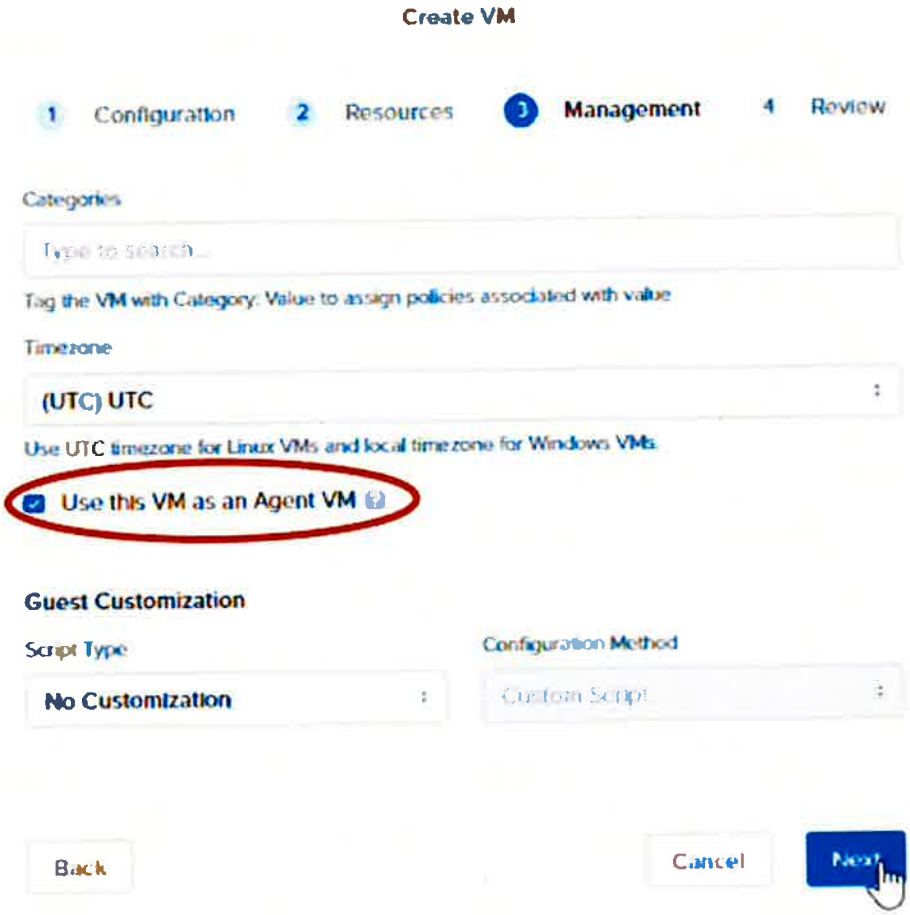
R_INT_DHCP

-beneficios según objetivos

Asigne las interfaces a las subredes adecuadas para su entorno.

475

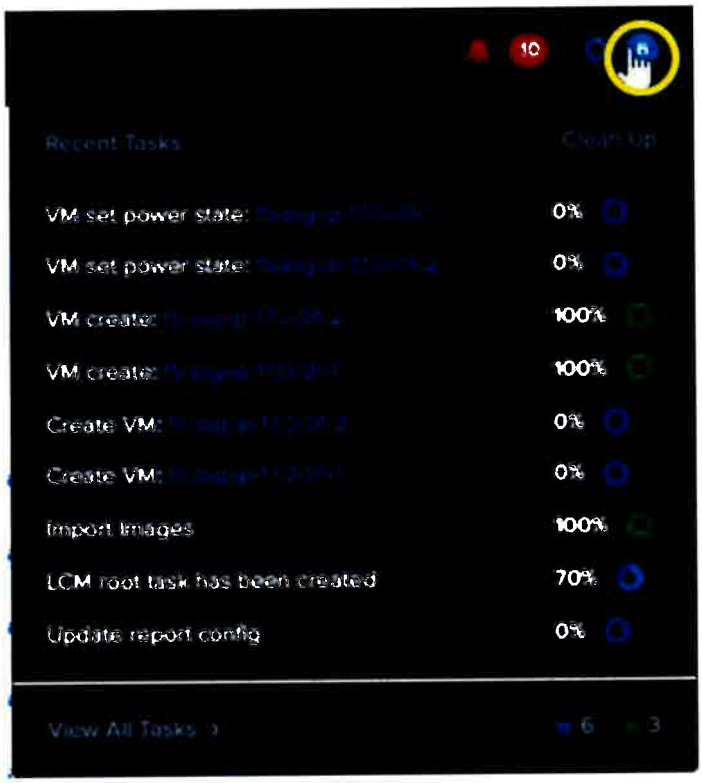
4. Haz clicextensión,en elgestiónpestaña, seleccione laUtilice esta máquina virtual como una máquina virtual agente.opción, y luego haga clicextensión



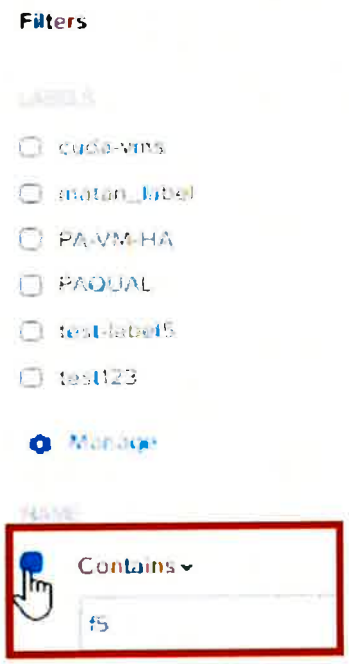
En elreseñapestaña, clicCrear máquina virtual

6. En la página de la lista de máquinas virtuales, haga lo siguiente:

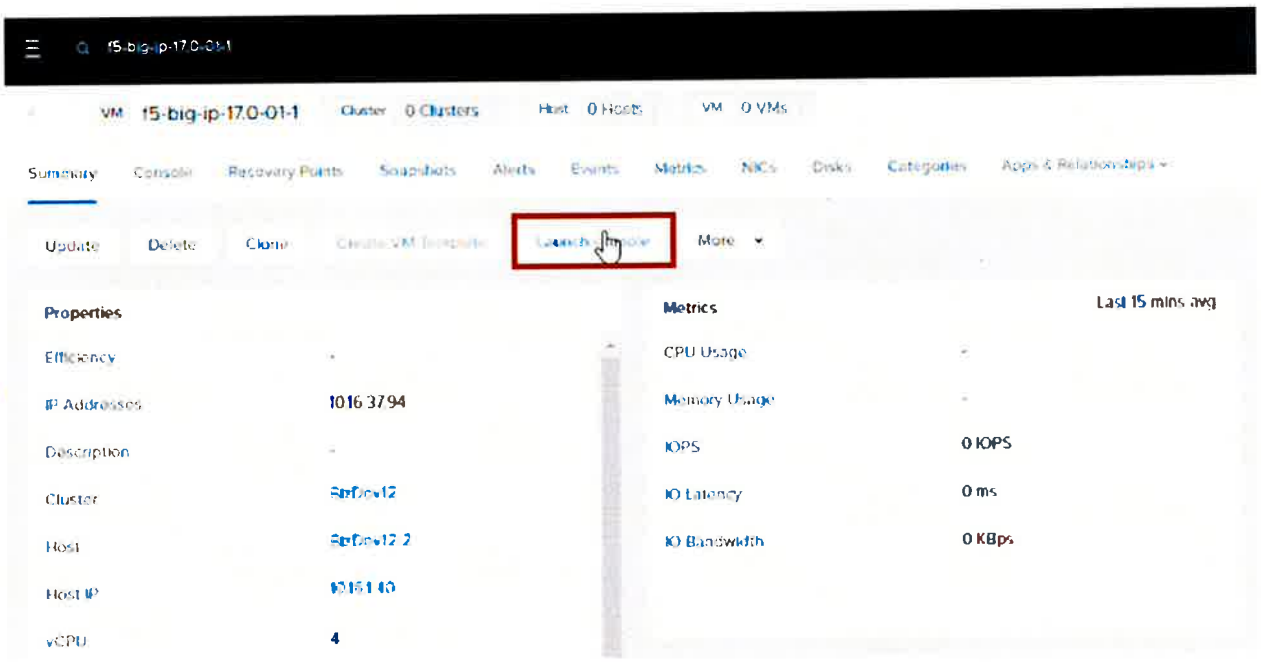
Para ver el progreso, haga clic en la esquina superior derecha azulicono.



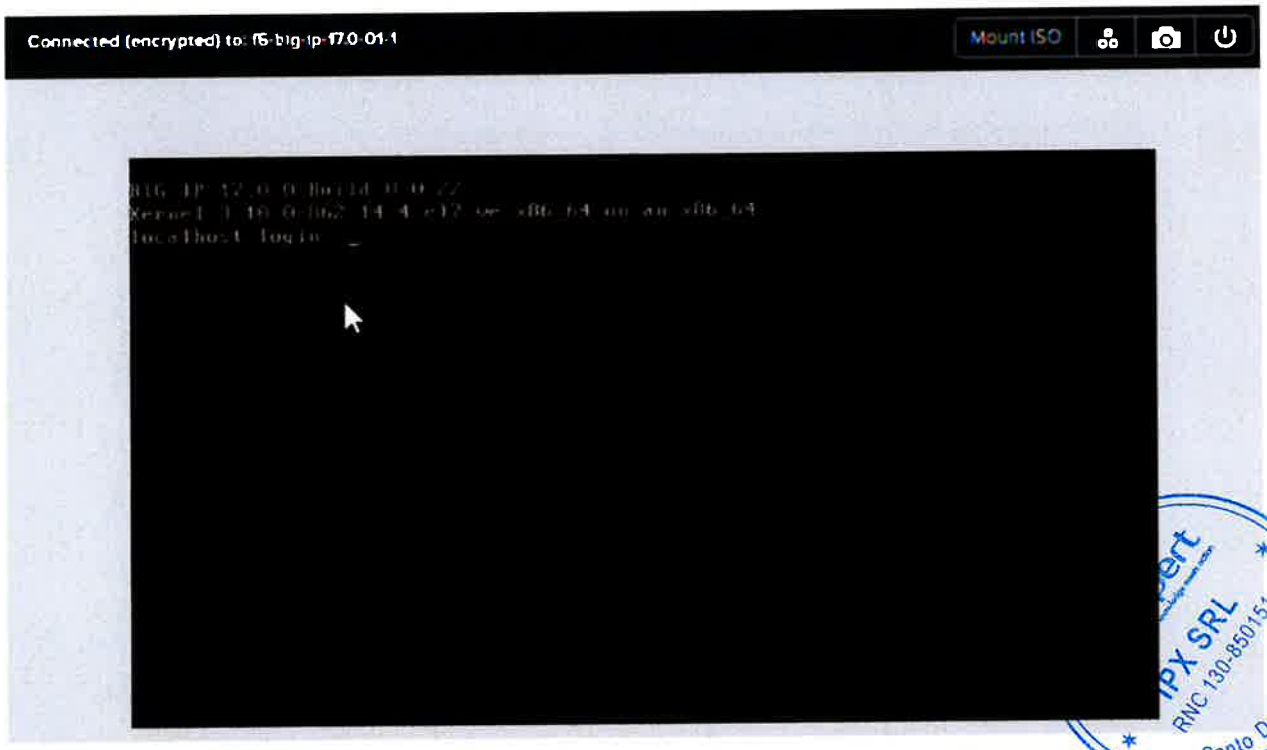
Para filtrar la lista de máquinas virtuales, haga clic en la esquina superior derecha.filtrosen elamepanel, seleccione elcontieneopción, y en el cuadro de texto ingrese5



Haz clic en el primer IG-IP VM-1en la lista filtrada para ver laresumenpágina, y luego en la menú superior, haz clic consola de lanzamientopara iniciar un cliente de Computación de Red Virtual (VNC).



Esto abre un cliente VNC y muestra la consola en una nueva pestaña o ventana. Utilice esta consola para acceder a la herramienta de configuración de BIG-IP y establecer la dirección IP de administración.



8. Utilice el cliente VNC para acceder a la herramienta de utilidad de configuración IG-IP y asigne una dirección IP de red de administración.

-importante

Debes repetirpasos 7-8seleccionando el segundoIG-IP VM-2y asignar el

Dirección IP de la red de administración.

Utilice la herramienta de utilidad de configuración de BIG-IP para configurar la dirección IP de administración.

Si su red utiliza DHCP, se asignará automáticamente una dirección IP a BIG-IP VE durante la implementación. Puede usar esta dirección para acceder a la utilidad de configuración de BIG-IP VE o a la utilidad de línea de comandos tmsh.

Si no se ha asignado ninguna dirección IP, puede asignarle una utilizando la herramienta de utilidad de configuración de BIG-IP.

Conéctese a la máquina virtual utilizando la consola del hipervisor.

En la pantalla de inicio de sesión, escribasalida

Cuando se le solicite la contraseña, escribapor defecto

-beneficios según objetivos

Si se le solicita, cambie su contraseña.

4. Tipofiguray prensanter

Se abre la pantalla de configuración del puerto de administración F5.

Haz clicDE ACUERDO

6. Seleccionaroy siga las instrucciones para asignar manualmente una dirección IP y una máscara de red al puerto de administración.

Puede utilizar una declaración genérica de hipervisor, como por ejemplo:tmsh cómo gestionar la IP de YSpara confirmar que la dirección IP de administración se configuró correctamente.

Ahora puede iniciar sesión en la utilidad de configuración de BIG-IP VE utilizando un navegador, y licenciar y aprovisionar BIG-IP VE.

Licencia tu BIG-IP¶

Para acceder a la utilidad de licencias de BIG-IP en una ventana del navegador, utiliceTTPS://y la dirección IP que asignó a la red de administración mediante la utilidad de configuración IG-IP.

Consulte el artículo 7752 (https://my.f5.com/manage/s/article/K7752) para obtener información completa sobre la licencia.

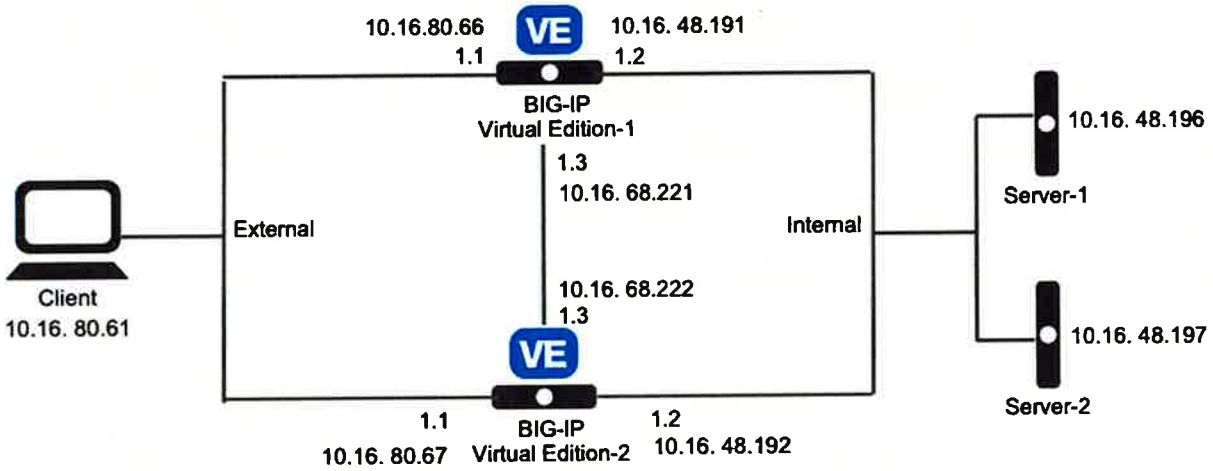
479

Pasos y demostración en vídeo. También puede consultar la Guía del usuario de utanix AVH: BIG-IP VE.

Consulte utanix_users.html para obtener información sobre la reutilización de licencias, licencias por aplicación, opciones de servidor virtual y otras opciones de licencia similares.

Configurar el par BIG-IP HA¶

Este ejemplo le guía a través de la configuración de dos BIG-IP VE para un par HA, utilizando el siguiente diagrama de ejemplo y configuración de red.



interfaz	LAN	Dirección P	máscara	ateway
gestión	R_PRT_DHCP	0.16.36.221 - 0.16.36.225	55.255.240.0	0.16.32.1
interno	R_PRT_ESTÁTICO	0.16.48.191 - 0.16.48.200	55.255.240.0	0.16.48.1
externo	R_INT_ESTÁTICO	0.16.80.61 - 10.16.80.70	55.255.240.0	0.16.80.1
A	R_INT_DHCP	0.16.68.221-10.16.68.230	55.255.240.0	0.16.64.1

-beneficios según objetivos

La convención de nombres utilizada es SOLO con fines demostrativos.

Servidor tipo	Dirección P
NS	0.16.0.200
TP	0.16.0.211

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

480

-beneficios según objetivos

Otras notas de configuración incluyen:

ignoró elcliente hcpen la interfaz mediante el usoNR_PRT_DHCPy

NR_INT_DHCPy utilizando una IP estática (proporcionada en la tabla anterior).

o almacenamiento, utilizado elcontenedor de errores-13584

La creación de un par HA implica las siguientes tareas:

Configure BIG-IP-1 e IG-IP-2. Complete

la conexión de alta disponibilidad.

Crear un grupo de direcciones y asignar miembros

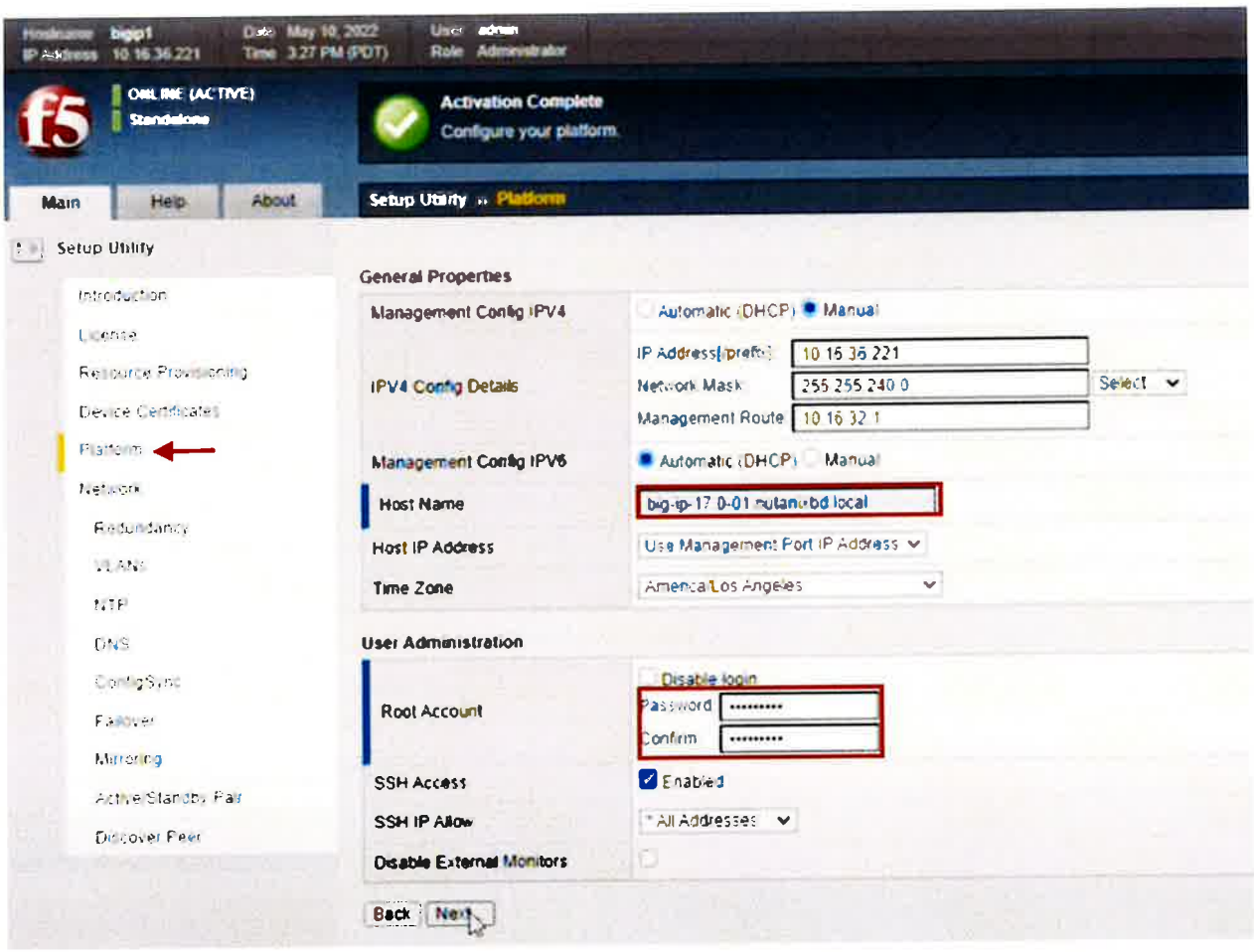
Sincroniza la configuración entre los grupos de dispositivos y prueba la conexión.

Configurar BIG-IP-1¶

o lo siguiente para configurar elPRIMER BIG-IP (1)en la configuración de pares HA:

. en el5. Utilidad de configuración de BIG-IPseleccionarain -> Plataforma,expandir elNombre del ost lista desplegable y seleccioneHost IG-IPCreado en Nutanix.

. en elCuenta de salidaingrese la raíznombre de usuarioyasswordy luego haga clicextensión



En elredhoja, en laConfiguración de red estándarpanel, haga clicextensión

4. En elVLANhoja, haga lo siguiente:

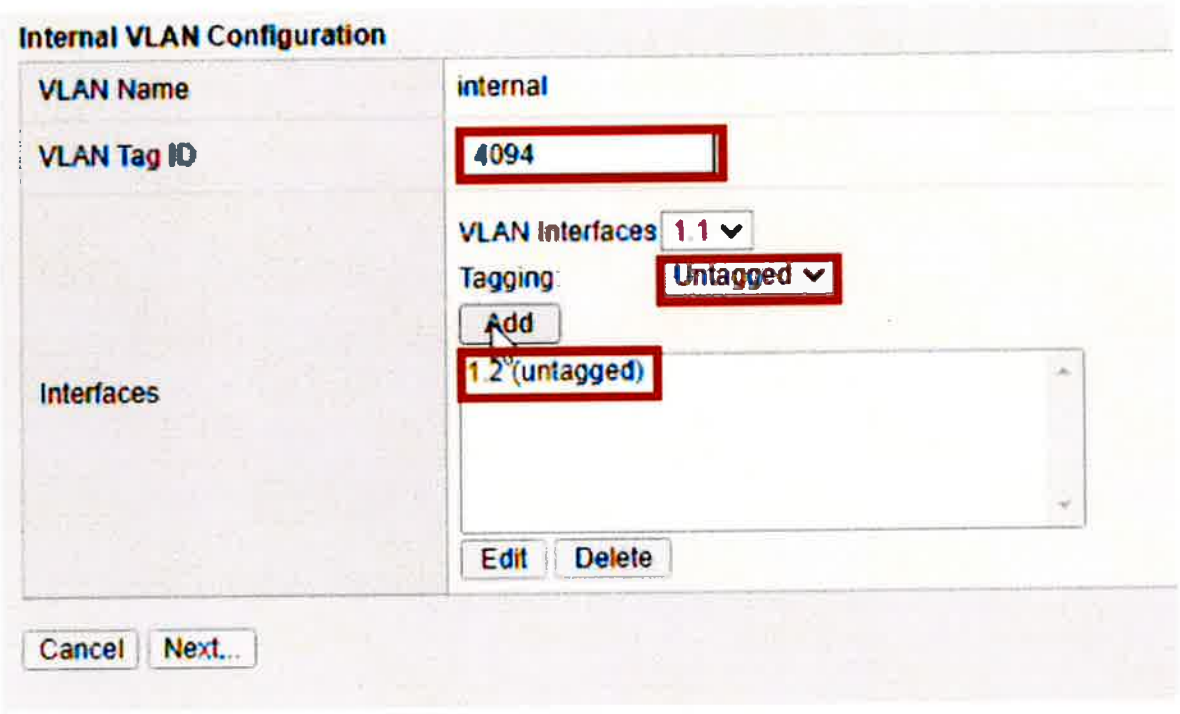
   a. en elConfiguración de VLAN internapanel, en elID de etiqueta LANEn el cuadro de texto, introduzca el número de etiqueta que identifica el tráfico de los hosts en la VLAN asociada (por ejemplo, 4094). Interfaz VLANcuadro de texto, seleccione .2,expandir elEtiquetadomenú desplegable, seleccione etiquetado

Haz clicAgregarpara agregar la VLAN a la lista de interfaces.

Wagner Pena

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

482



. en elConfiguración de red internapanel, haga lo siguiente:

a. en elPropiedad intelectual propiaEn esta sección, complete lo siguiente:

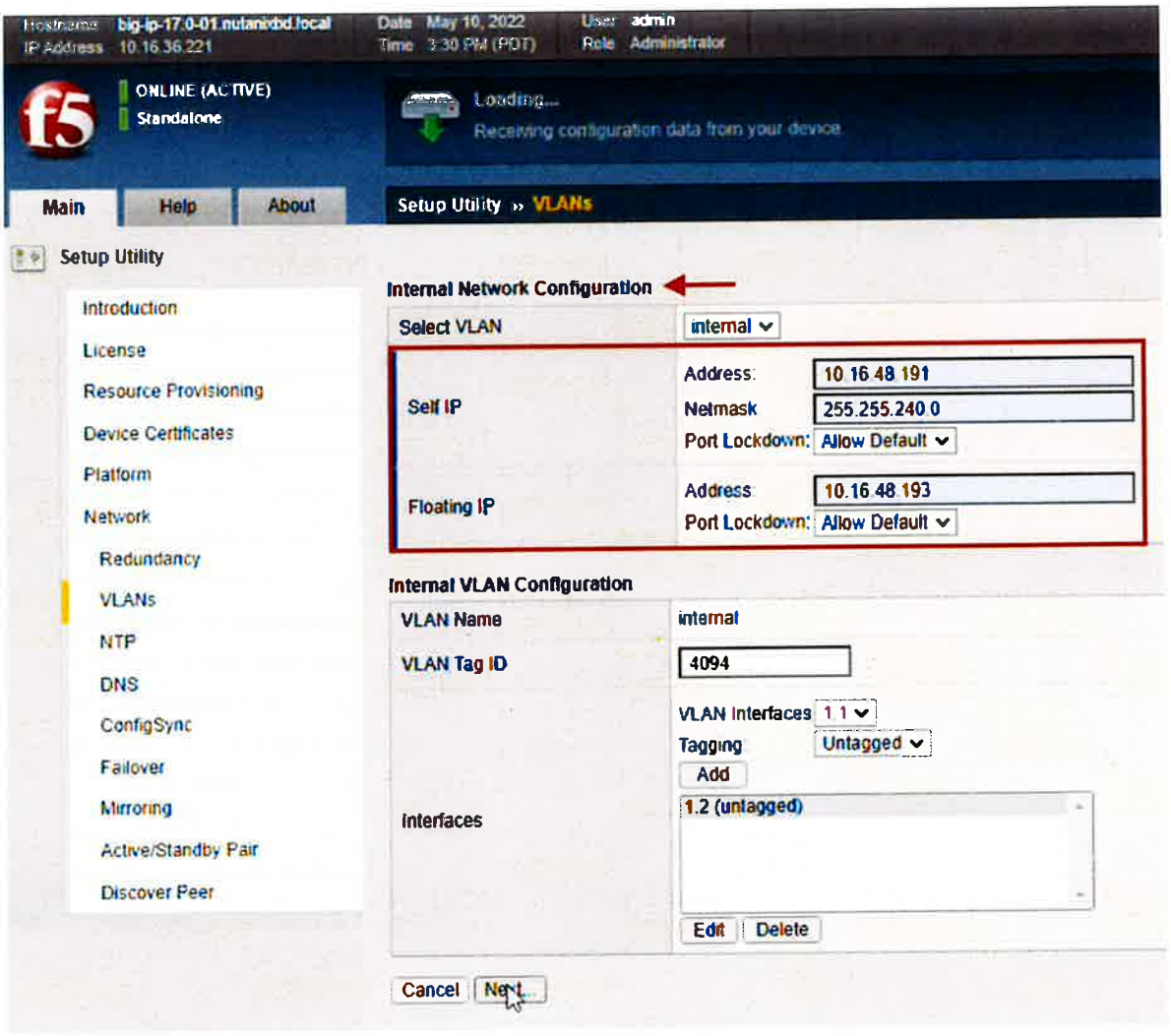
DIRECCIÓN -Introduzca la dirección IP del sistema BIG-IP que desea asociar con esta VLAN.

etmask -Introduzca la máscara de red asociada a la dirección seleccionada.

. en elIP de ubicaciónEn esta sección, complete lo siguiente:

DIRECCIÓN -Introduzca la dirección IP que desea compartir entre varios dispositivos BIG-IP en un grupo de dispositivos.

Confinamiento -dejar valor comoPermitir valor predeterminado



6. Haz clic extensión

. en el Configuración de red externapanel, haga lo siguiente:

a. en elPropiedad intelectual propiaComplete esta sección:

DIRECCIÓN -Introduzca la dirección IP del sistema BIG-IP que desea asociar con esta VLAN.

etmask -Introduzca la máscara de red asociada a la dirección seleccionada.

Confinamiento -dejar valor comoNo permitir ninguno

. en el Puerta de enlace de fallossección, ingrese unDirección P

c. en el IP de ubicaciónEn esta sección, complete lo siguiente:

DIRECCIÓN -Introduzca la dirección IP que desea compartir entre varios dispositivos BIG-IP en un grupo de dispositivos.

Confinamiento -dejar valor comoNo permitir ninguno

8. en elConfiguración de VLAN externapanel, haga lo siguiente:

a. Complete lo siguiente:

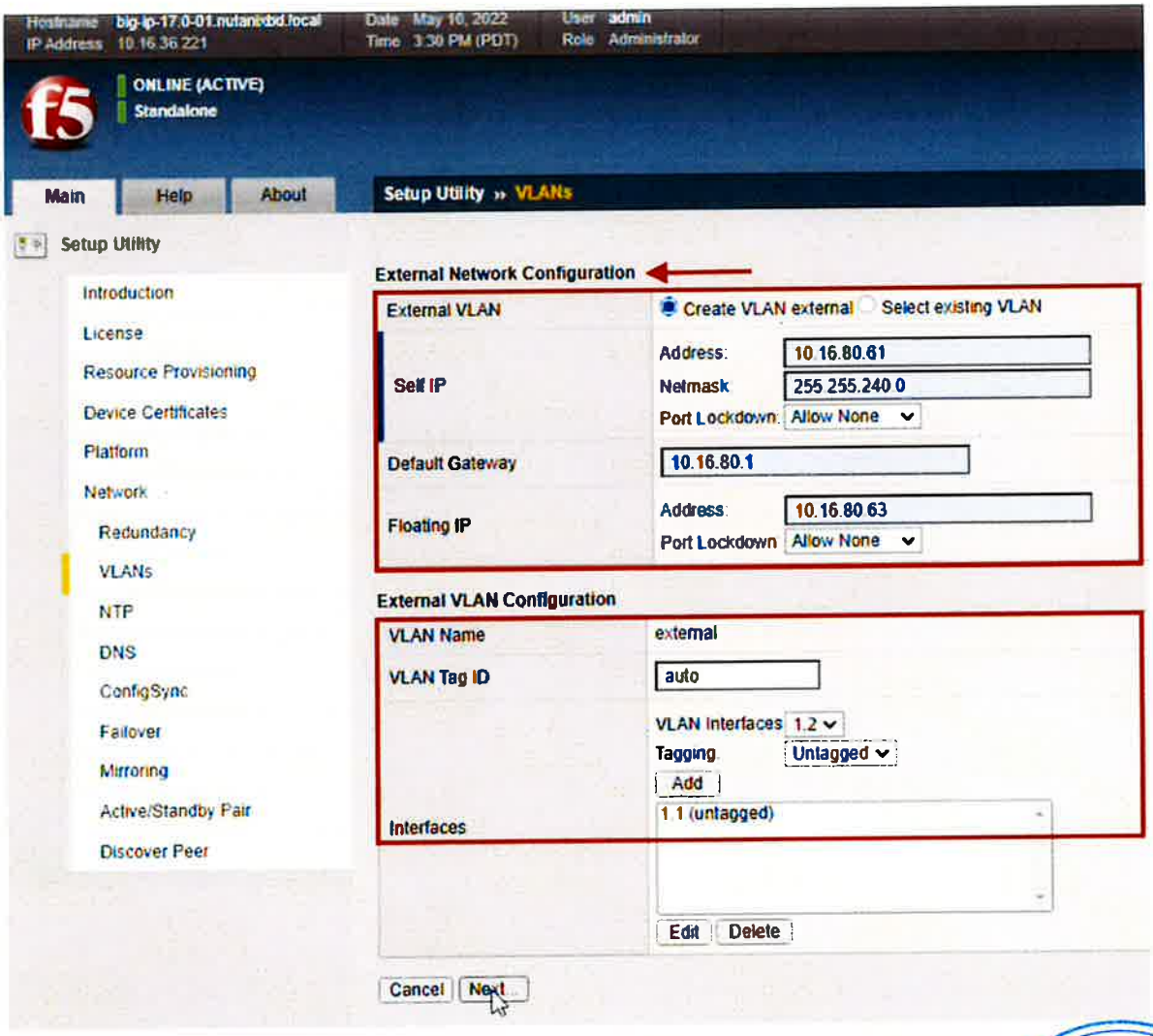
Nombre de VLAN -ingresarexterno

Nombre de la etiqueta VLAN -dejar elautovalor

predeterminado Interfaz VLAN -seleccionar1.1

Etiquetado -Amplíe la lista y seleccioneetiquetado

Haz clicAgregarpara agregar la VLAN externa a lainterfaceslista.



9. Haz clic extensión

0. en el Configuración de red de alta disponibilidadpanel, haga lo siguiente:

a. en elPropiedad intelectual propiapanel, complete lo siguiente:

DIRECCIÓN -Introduzca la dirección IP del sistema BIG-IP que desea asociar

con esta VLAN

etmask -Introduzca la máscara de red asociada a la dirección seleccionada.

. en elConfiguración de VLAN de alta disponibilidadpanel, complete lo siguiente:

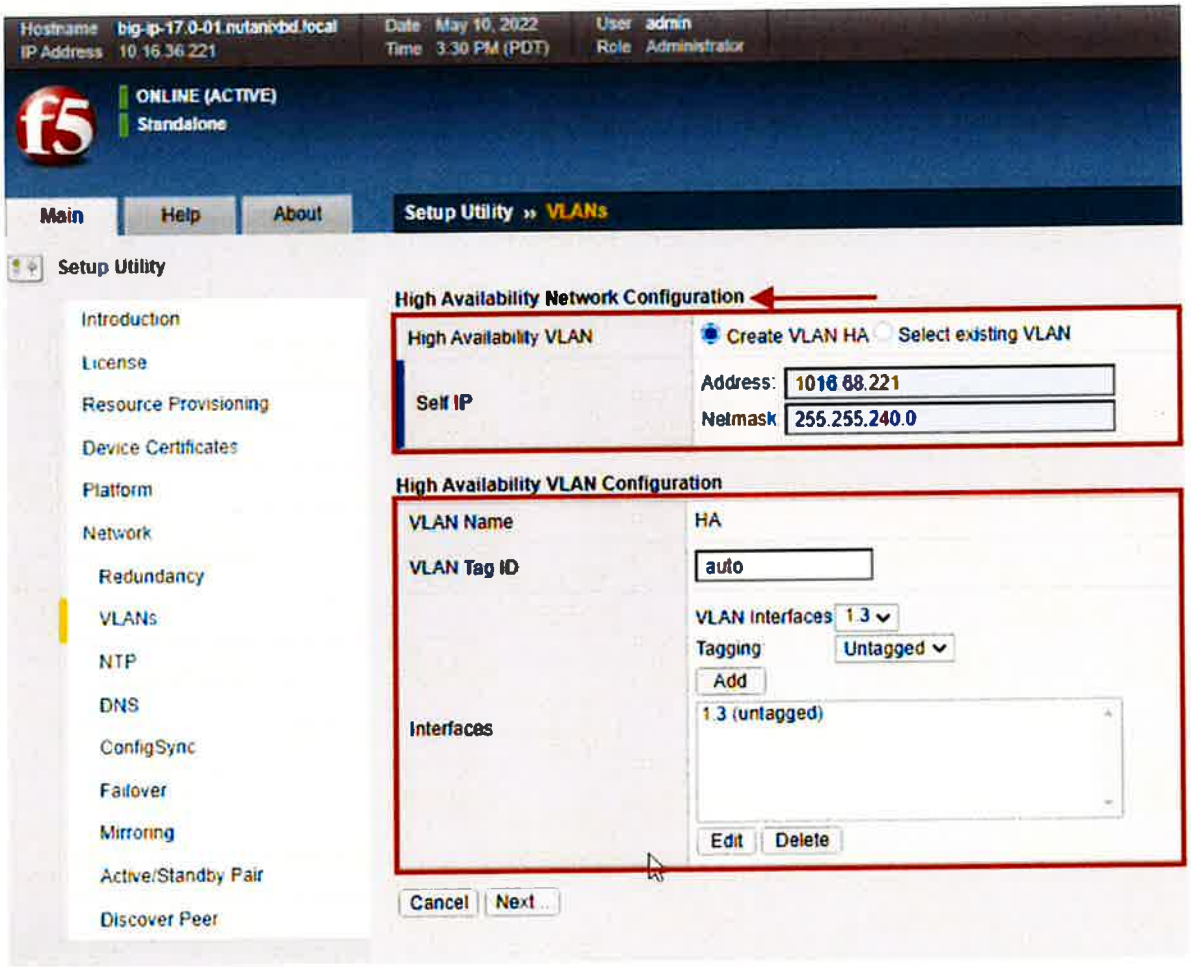
Nombre de VLAN -Deja elAvalor predeterminado ID de

etiqueta VLAN -dejar elautovalor predeterminado

Interfaces VLAN -seleccionar .3 Etiquetado -seleccionar

etiquetado

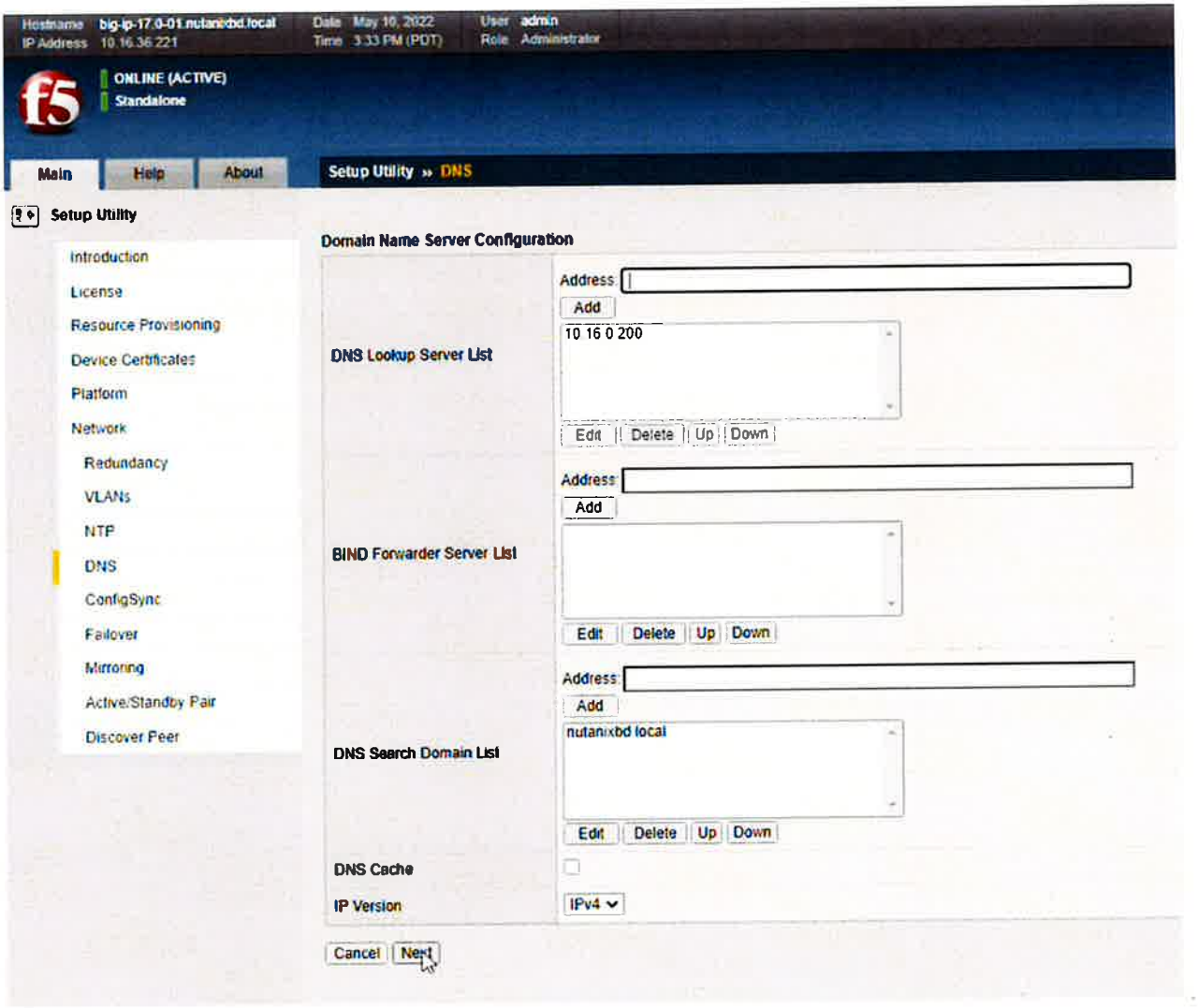
c. Haga clicAgregarpara agregar la VLAN a lainterfaceslista.



1. Haz clicextensión

2. En elred -> NTPhoja, en ladirecciónEn el cuadro de texto, introduzca la dirección del servidor NTP utilizado y haga clic.ddpara agregarlo a laLista de servidores de tiempoy luego haga clicextensión

3. En elred -> DNShoja, acepta todos los valores predeterminados y, a continuación, haz clicext (similar al siguiente ejemplo).



4. En elred -> Sincronización de configuraciónhoja, acepta el valor predeterminadoDirección local (Por ejemplo, 10.16.48.191 (interno)) valor, y luego haga clicextensión

5. En el red -> Conmutación por errorhoja, acepta todos los valores predeterminados y, a continuación, haz clic extensión

6. En el red -> Duplicaciónhoja, acepta todos los valores predeterminados y, a continuación, haz clic extensión

7. En el red -> par activo/en esperahoja, clicextensión,en eliscover Peercuchilla, extensión,Complete hacer clic lo siguiente y, a continuación, haga clic.Recuperar información del dispositivo

Tipo de dispositivo -seleccionareer

Dirección IP del dispositivo -Introduzca la dirección IP del dispositivo

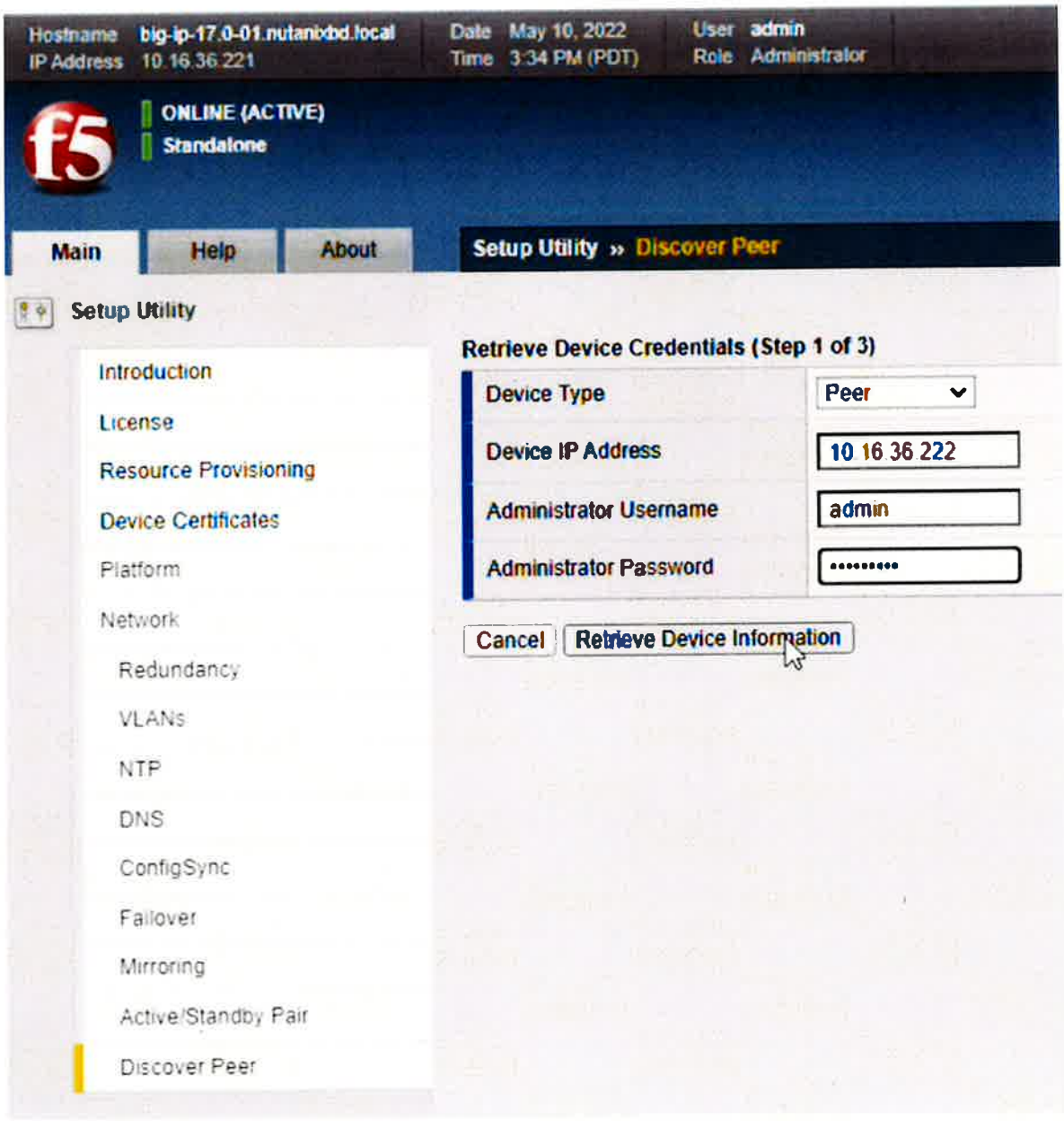
Nombre de usuario del administrador -Introduzca el valor correspondiente

Contraseña de administrador -Introduzca el valor correspondiente

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Wagner Peña

487



8. Antes de continuar, complete la configuración del segundo BIG-IP (2).

Configurar BIG-IP-2¶

o lo siguiente para configurar elSEGUNDO BIG-IP (2) (dispositivo redundante)en la configuración de pares HA:

. en la ventana del navegador, usandoTTPS://acceder al segundo BIG-IP.

En el ainapestaña, en laredhoja, en laConfiguración de red estándarcristal,

hacer clic extensión

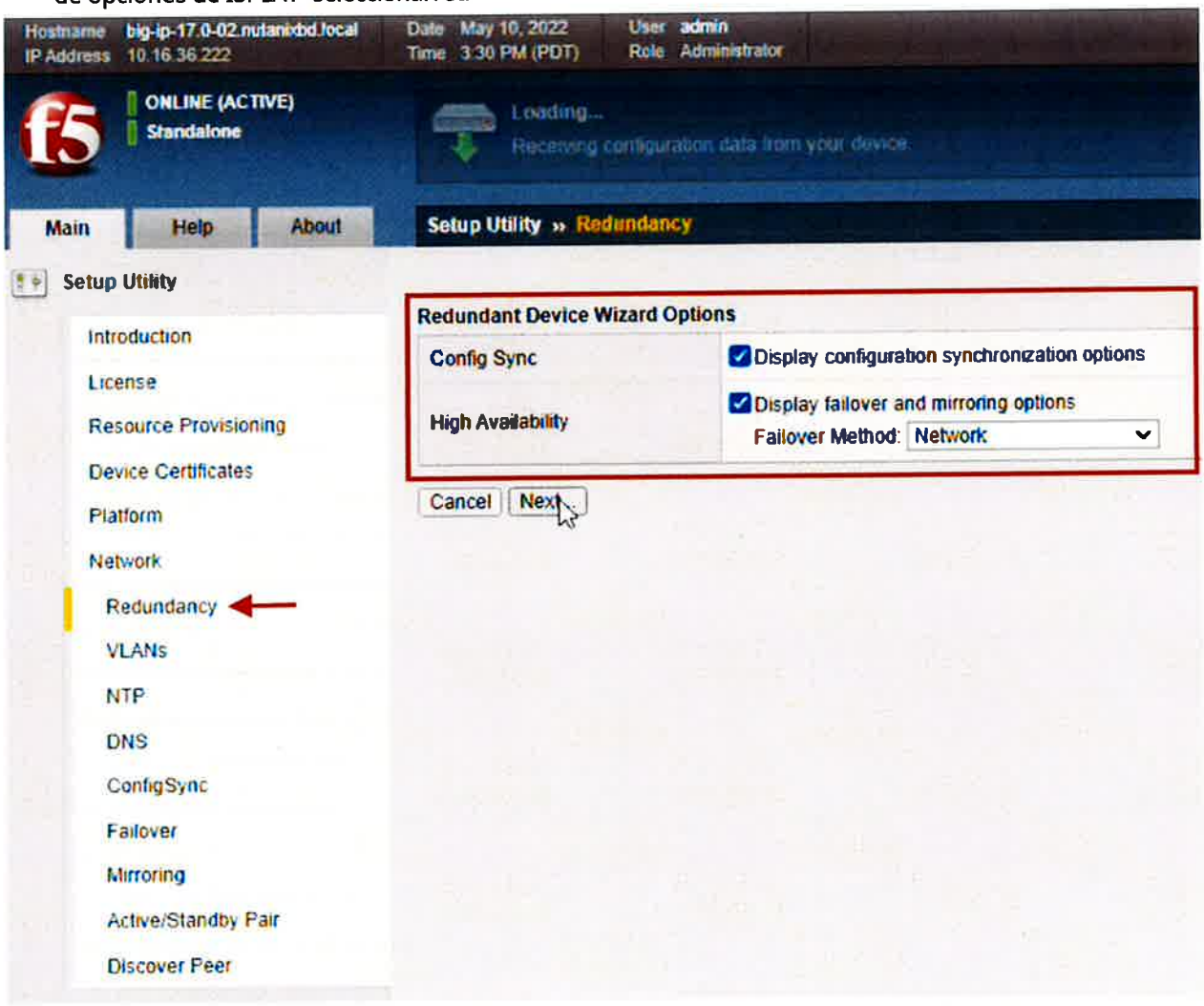
En elred -> redundanciahoja, en laOpciones del asistente de dispositivos redundantes

488

panel, complete lo siguiente:

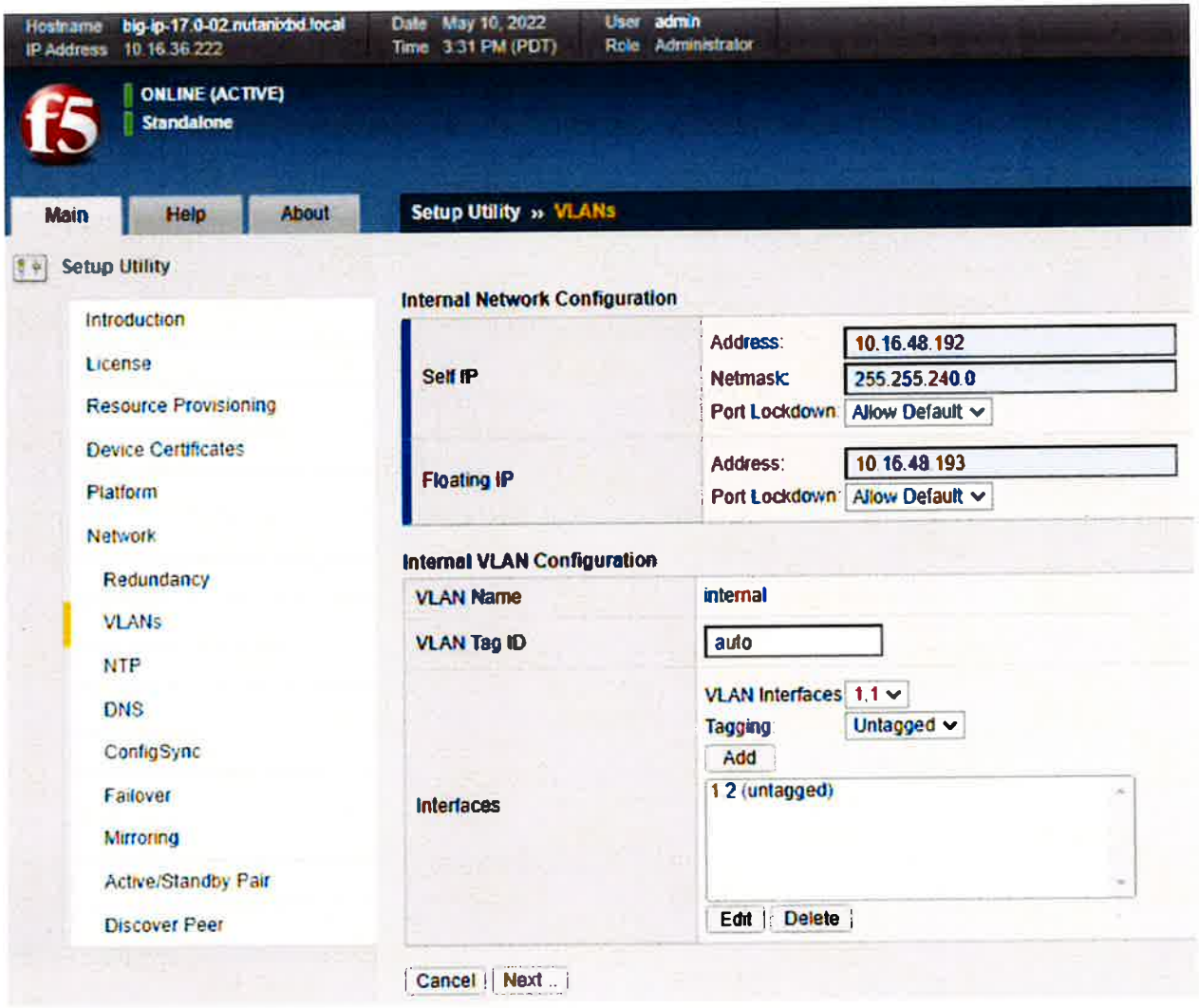
Sincronización de configuración -Haz clic para activarOpciones de sincronización de configuración de isplay

Alta disponibilidad -Haz clic para activarMétodo de conmutación por error y replicación de opciones de ISPLAY -seleccionarred



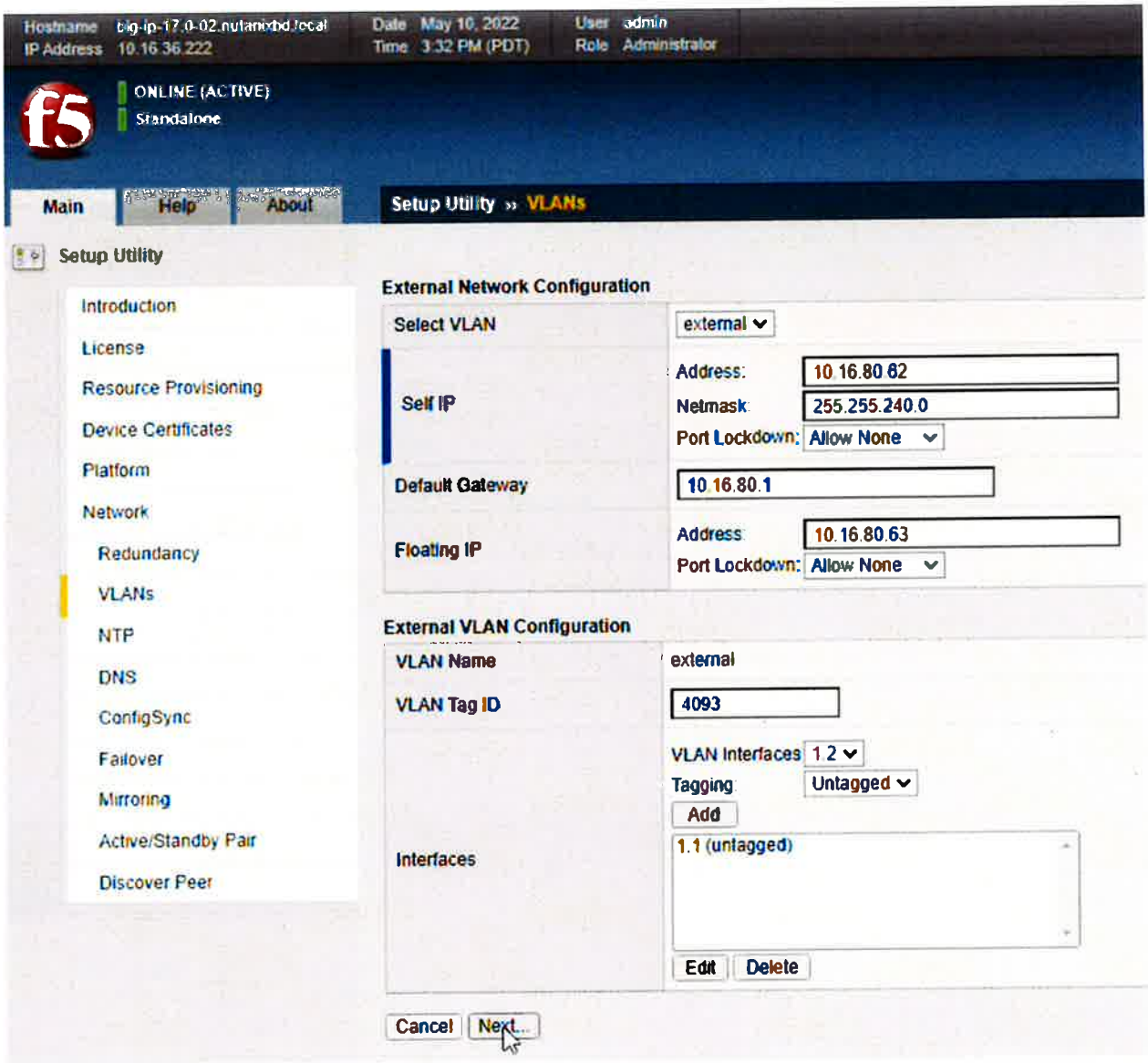
4. Haz clicextensión

En elred -> VLANPara configurar la hoja, repita los pasos anteriores.red interna configuración para el PRIMER BIG-IP (1), como el siguiente ejemplo:



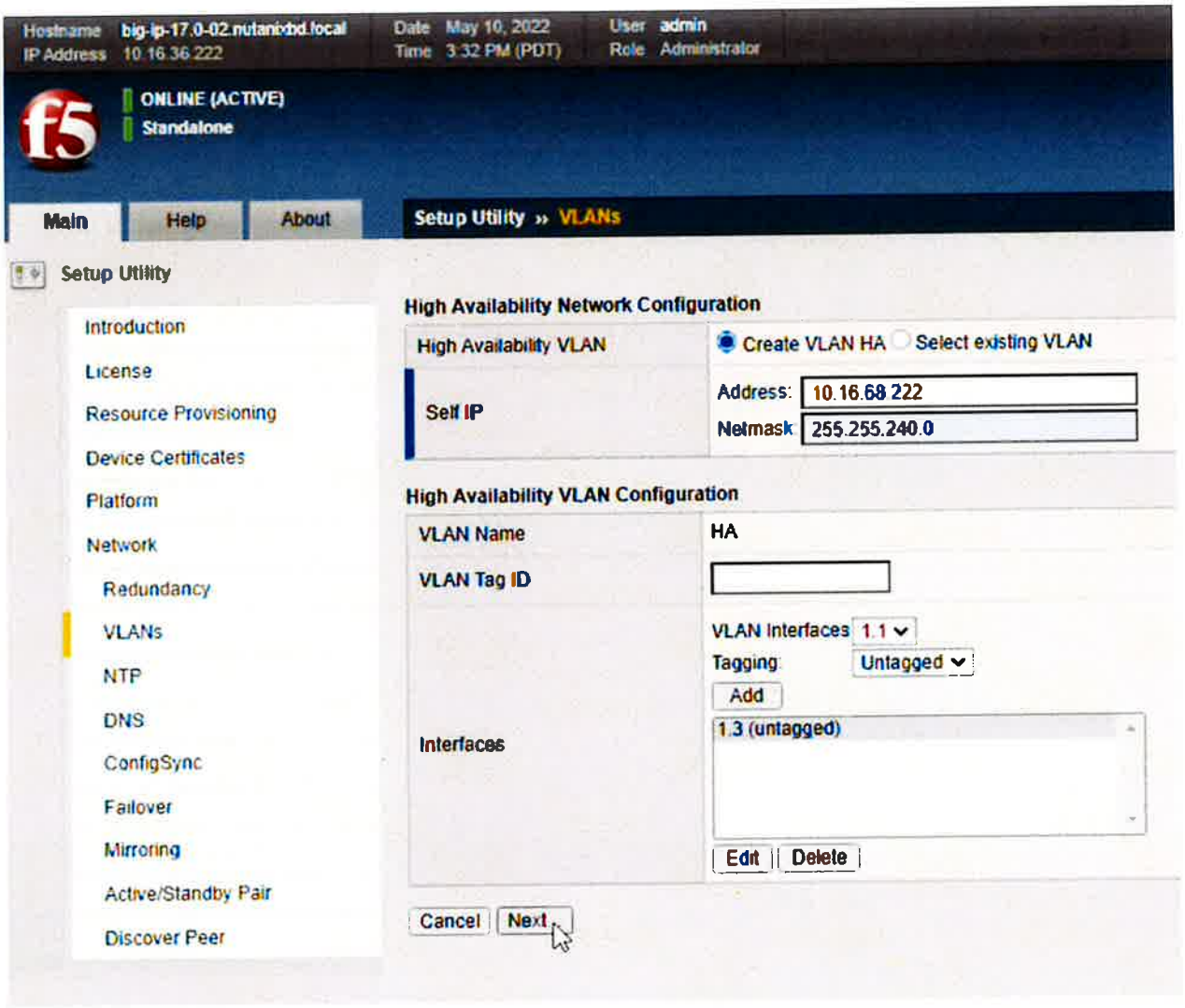
6. Haz clicextensión

En elred -> VLANPara configurar la hoja, repita los pasos anteriores.configuración de red externapara el PRIMER BIG-IP (1), como en el siguiente ejemplo:



8. Haz clicextensión

9. En la hoja Red -> VLAN, repita los pasos anteriores para configurar la configuración de red de alta disponibilidad para el FIRST BIG-IP (1), como en el siguiente ejemplo:



0. En elred -> NTPhoja, en ladirecciónEn el cuadro de texto, introduzca la dirección del NTP.

servidor utilizado, haga clicddpara agregarlo a laLista de servidores de tiempoy luego haga clicextensión

1. En elred -> Sincronización de configuraciónhoja, acepta el valor predeterminadoDirección local (Por ejemplo, 10.16.48.192 (interno)) valor, y luego haga clicextensión

2. En el red -> Conmutación por errorhoja, acepta todos los valores predeterminados y, a continuación, haz clic extensión

3. En el red -> Duplicaciónhoja, acepta todos los valores predeterminados y, a continuación, haz clic extensión

4. Haz clicterminado

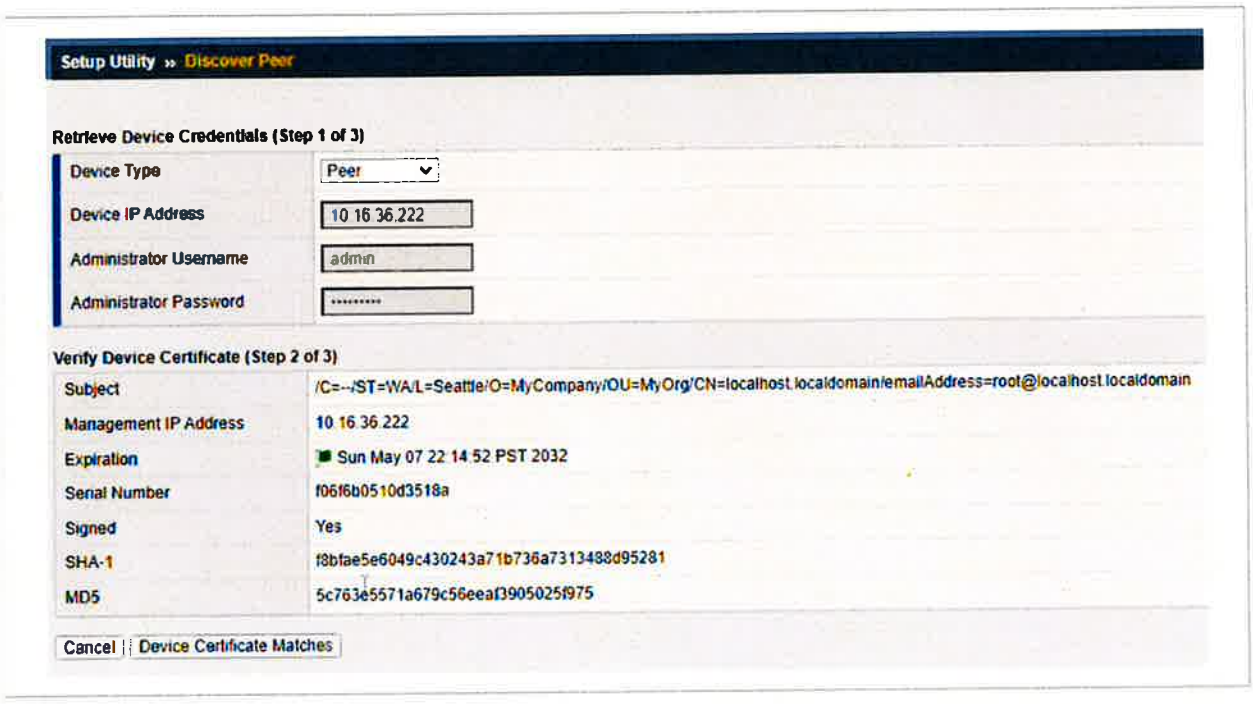
5. En la esquina superior izquierda, para ver la corrienteestado onfigSynchaga clic en elEsperando sincronización inicial tinta.

6. Complete la conectividad HA

Completar la conectividad HA¶

492

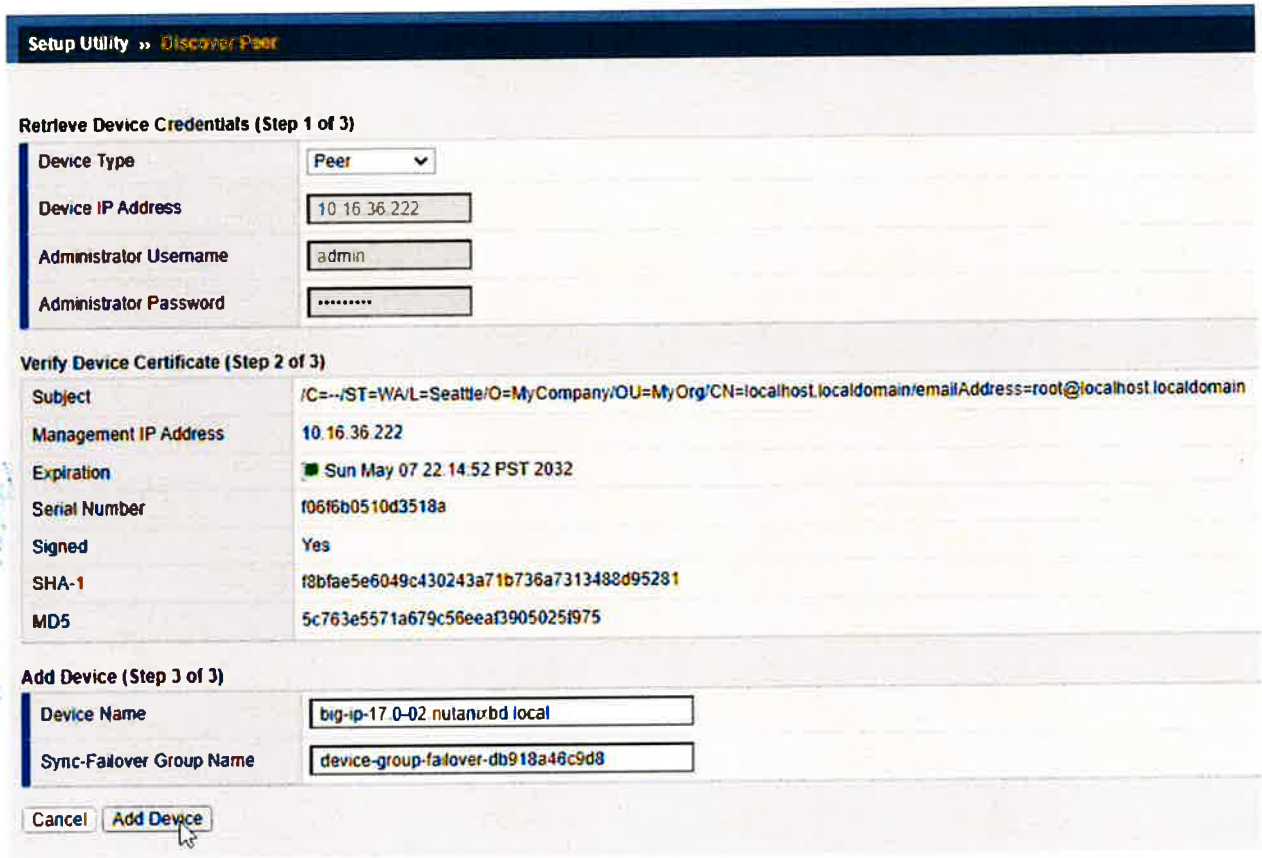
Para verificar el certificado del dispositivo, abra la pestaña del navegador correspondiente.PRIMER BIG-IP (1),hacer clic Coincidencias del certificado del dispositivo,y luego complete lo siguiente:



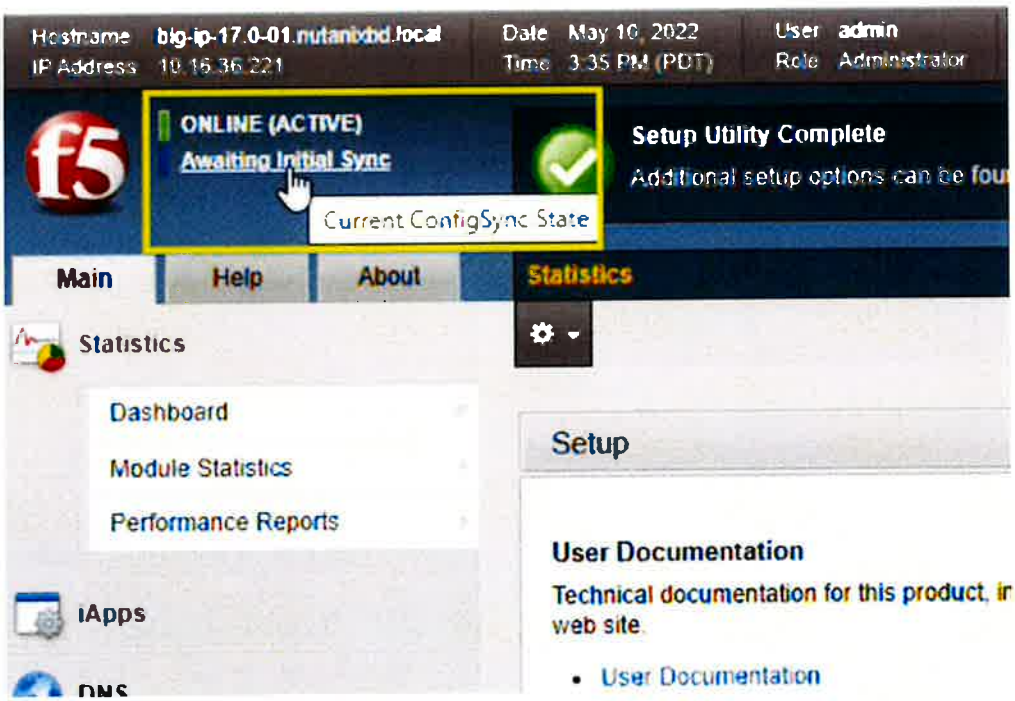
Nombre del dispositivo -dejar valores predeterminados

Nombre del grupo de conmutación por error de sincronización -dejar valores predeterminados

Haz clicAgregar dispositivo



. ElUtilidad de configuración InicioAparece la página. En ambas páginas del navegador, tanto para BIG-IP 1 como para BIG-IP 2, en la esquina superior izquierda, se muestra la información actual.Estado de sincronización de configuraciónhaga clic en elEsperando sincronización inicial tinta.



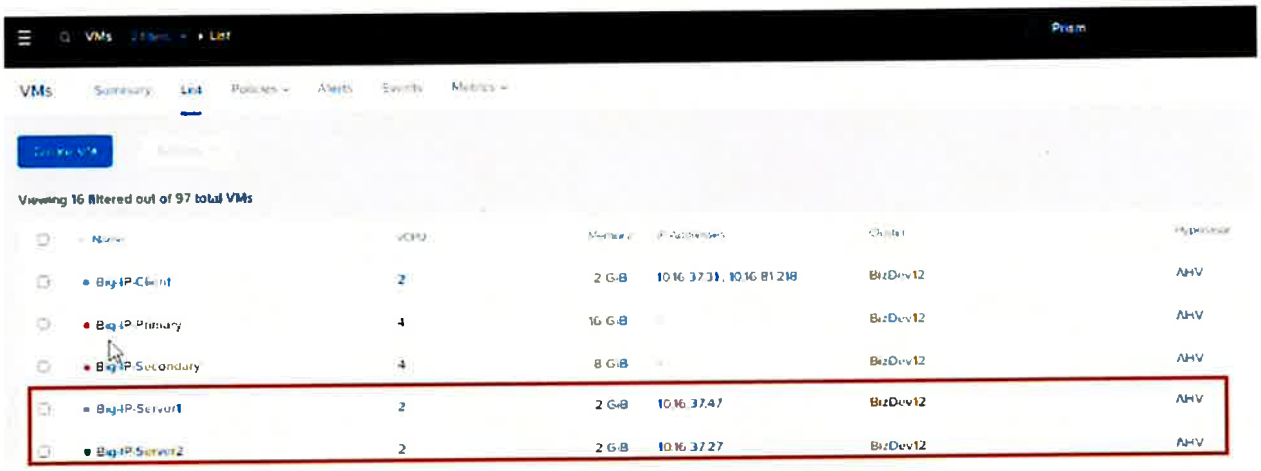
4. En el menú de la izquierda, seleccioneAdministración de dispositivos -> Descripción generalopción, haga clicync,y

Luego, en la esquina superior izquierda, espere unMensaje de sincronizaciónaparecer.

Crear un grupo de direcciones y agregar miembros¶

Los siguientes pasos muestran este proceso utilizando Nutanix AOS 5.20. Para obtener los pasos actualizados, consulte la documentación de Nutanix para AOS 6.5 (https://portal.nutanix.com/page/documents/details?targetId=Web-Console-Guide-Prism-v6_5:wc-system-nework-configuration-acropolis-wct.html).

. en elConsola Utanix AHVen elLista de máquinas virtuales filtrada por 5 elementosAnote las direcciones IP de las dos máquinas virtuales BIG-IP (por ejemplo, servidor-1 y servidor-2).



. en el5. Utilidad de configuración de BIG-IPEn el menú de la izquierda, haga clicTráfico local -> Grupos,En el extremo derecho de la ventana, haga clicCreary luego haga lo siguiente:

a. en elConfiguraciónpanel, en elameEn el cuadro de texto, ingrese/seleccione el nombre de su máquina virtual BIG-P.

. en elrecursospanel, complete lo siguiente:

Método de equilibrio de carreteras -seleccionar Conexiones del este (miembro)

Activación de grupo prioritario -seleccionar está habilitado

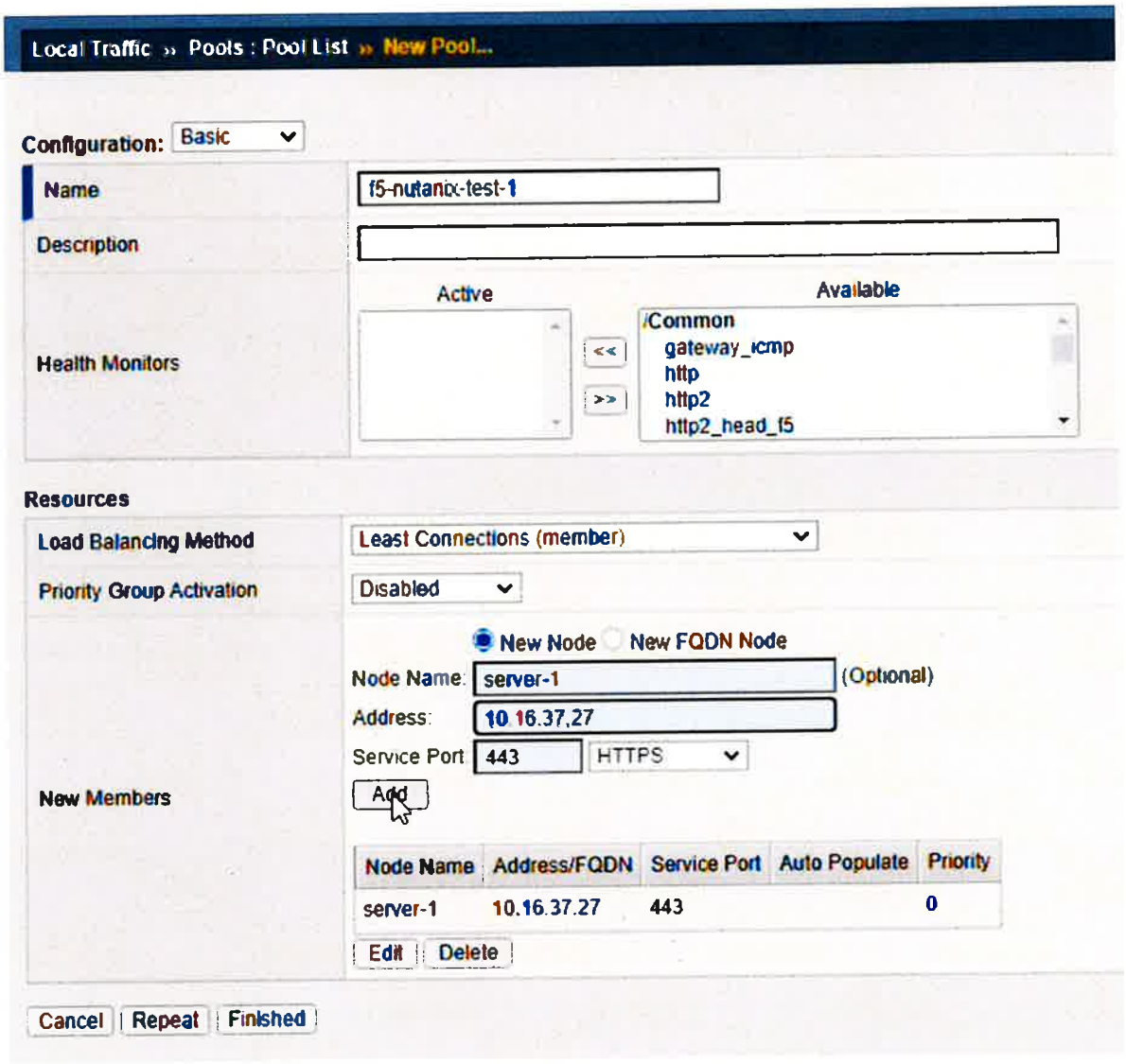
nuevo nodo -Seleccione para habilitar Nombre

de la oda -seleccionarservidor-1

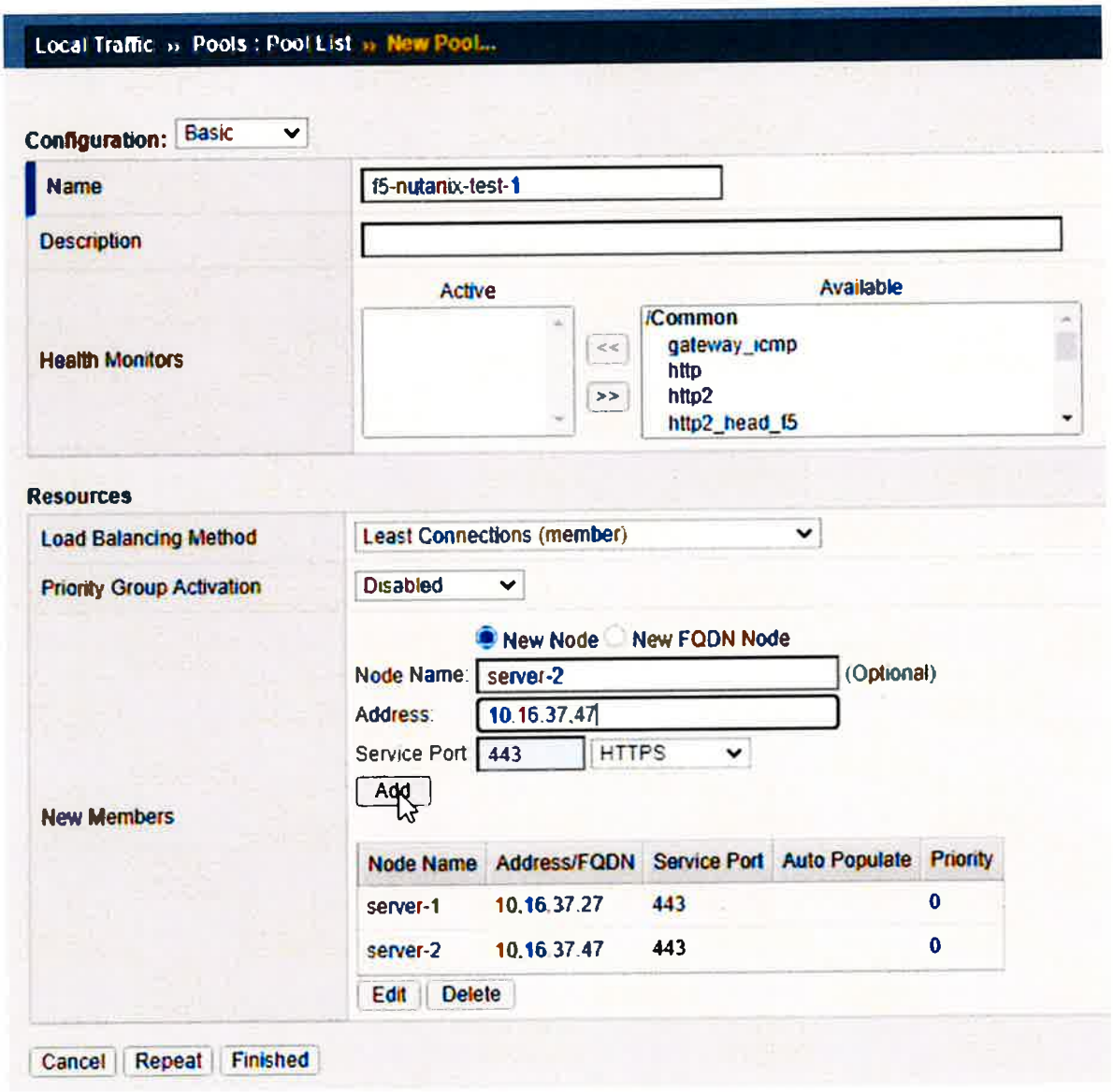
DIRECCIÓN -entrar en elDirección P del primer servidoren la lista filtrada de máquinas virtuales en utanix

Puerto del servidor -ingresar43y seleccionarTTPS

c. Haga clicAgregar



Repita estos pasos seleccionandoNombre de la oda -ingresarservidor-2y elDIRECCIÓN -entrar en el Dirección P del primer servidoren la lista filtrada de máquinas virtuales en Nutanix, y luego haga clic terminado



En elTráfico local -> Piscinas -> Lista de piscinasmenú, haga lo siguiente:

a. Haga clicCreary luego complete lo siguiente:

ame -seleccione elpiscinaacabas de crear monitor

de salud -seleccionarMétodo de equilibrio de

carga TTP -seleccionar Activación de grupo Robin sonaba

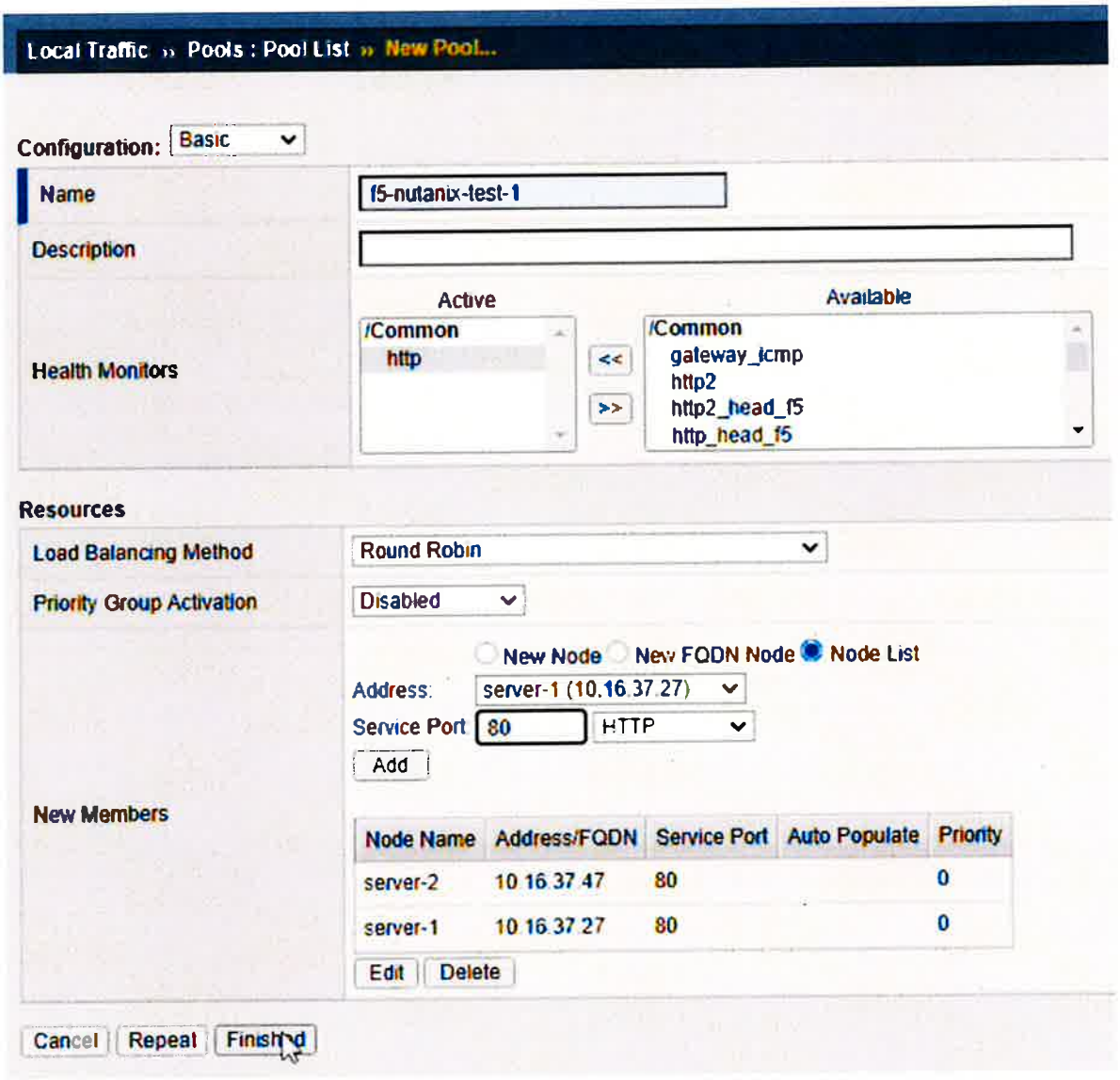
prioritario -seleccionar Nuevos miembros - está habilitado

seleccione el DIRECCIÓN -seleccionalista de la opción

TTPyPuerto de servicio 80

Haz clicAgregarexpandirDIRECCIÓNseleccionarServidor-1seleccionarTTP, puerto de servicio 80hacer clic

Agregarotra vez, y luegoterminado



4. en el5. Utilidad de configuración de BIG-IPEn el menú de la izquierda, haga clicTráfico local -> Servidores virtualesEn la parte derecha de la ventana, haga clic en la hoja.creary luego en elPropiedades generalesEl panel debe hacer lo siguiente:

a.ame -Ingrese un nombre que lo asocie con el grupo que acaba de crear (por ejemplo, seleccione el nombre del grupo y agregue "VS", que identifica el servidor virtual).

. Tipo -seleccionarestándar

do.Dirección de destino/Máscara -seleccionar osty luego ingrese unDirección P

. Puerto de servicio -seleccionarort 443,y TTPS

. Notificar estado a la dirección virtual -Seleccione para habilitar la opción

. en elConfiguración - Básicapanel, haga lo siguiente:

a.Perfil TTP (Cliente) -seleccionar ttp

. Perfil TTP (servidor) -seleccionar ttp

do.Perfil SSL (servidor) -seleccione elclientesopción de laDisponiblelista

. Traducción de direcciones de origen -seleccionarMapa de uto

6. en elrecursospanel, expanda elpiscina de falloslista desplegable y seleccioneoolAcabas de crear.

Haz clicterminado

Sincronizar la configuración entre grupos de dispositivos y probar la conexión.

Para sincronizar los cambios, haga clic en elServidor virtualEn la lista, en la esquina superior derecha, haga clic en Cambio pendienteenlace, y luego, en elGrupo de dispositivosclic en el menúyncEl mensaje de estado cambiará an Sincronización

Para probarlo, abre una nueva ventana del navegador en modo privado e introduce undirección IP externapara los dispositivos IG-IP y, a continuación, actualice el navegador.

Ver también

actualizar BIG-IP VE (./shared/update.html

Guía del usuario de Utanix AHV: BIG-IP VE (utanix_users.html)

-Anterior (./nutanixAHV_index.html)

extensión - (utanix_users.html)

¿TIENES ALGUNA PREGUNTA? Soporte y ventas > (https://www.f5.com/company/contact)

SÍGUENOS

499

ACERCA DE F5

Información corporativa (https://www.f5.com/company)

Sala de noticias (https://www.f5.com/company/news)

Relaciones con los inversores (https://www.f5.com/company/investor-relations)

Empleo (https://www.f5.com/company/careers)

Acerca de Clouddocs (/csp/about)

EDUCACIÓN

Formación (https://www.f5.com/services/training)

Certificación (https://www.f5.com/services/certification)

Gana dinero con F5 (https://account.f5.com/learnf5)

Formación online gratuita (https://www.f5.com/services/training/free-training-courses)

5 SITIOS

5.com (https://www.f5.com) evCentral

(https://community.f5.com) Portal de

soporte (https://my.f5.com/)

Partner Central (https://partnercentral.f5.com) 5

Labs (https://www.f5.com/labs)

TAREAS DE APOYO

Consulte las políticas de soporte (https://www.f5.com/services/support/support-offerings/supportpolicies)

Crear solicitud de servicio https://my.f5.com/manage/s/createcase

Comentarios sobre el alero [+]

500

Advanced WAF. Posteriormente, puede integrar el archivo OAS y las políticas de seguridad de API en su ciclo de desarrollo de CI/CD. El archivo OAS debe estar en formato JSON o YAML.

Un enfoque de diseño prioritario para la creación de API implica planificar y documentar la API mediante un archivo OAS (anteriormente llamado Swagger). Tras la fase seño inicial, el archivo OAS puede utilizarse para generar código del lado del servidor para la API durante el ciclo de compilación de CI/CD. Este enfoque de diseño prioritario para la creación de API también puede utilizarse para configurar las funciones que proporcionan protección de API en su sistema BIG-IP. Al ejecutar la Configuración guiada de BIG-IP y seleccionar el...**Seguridad de la API REST (especificación de API abierta)**Al seleccionar esta opción, se le solicitará que importe un archivo OAS existente y, a continuación, defina ajustes de seguridad adicionales para la API. Al importar el archivo OAS, se convierten los elementos de la API, como rutas, parámetros y respuestas, en entidades de política de seguridad de BIG-IP APM y Advanced WAF. Este proceso le permite integrar sus políticas de seguridad de API de BIG-IP APM y Advanced WAF en su ciclo de desarrollo de CI/CD, como se muestra en la siguiente figura:

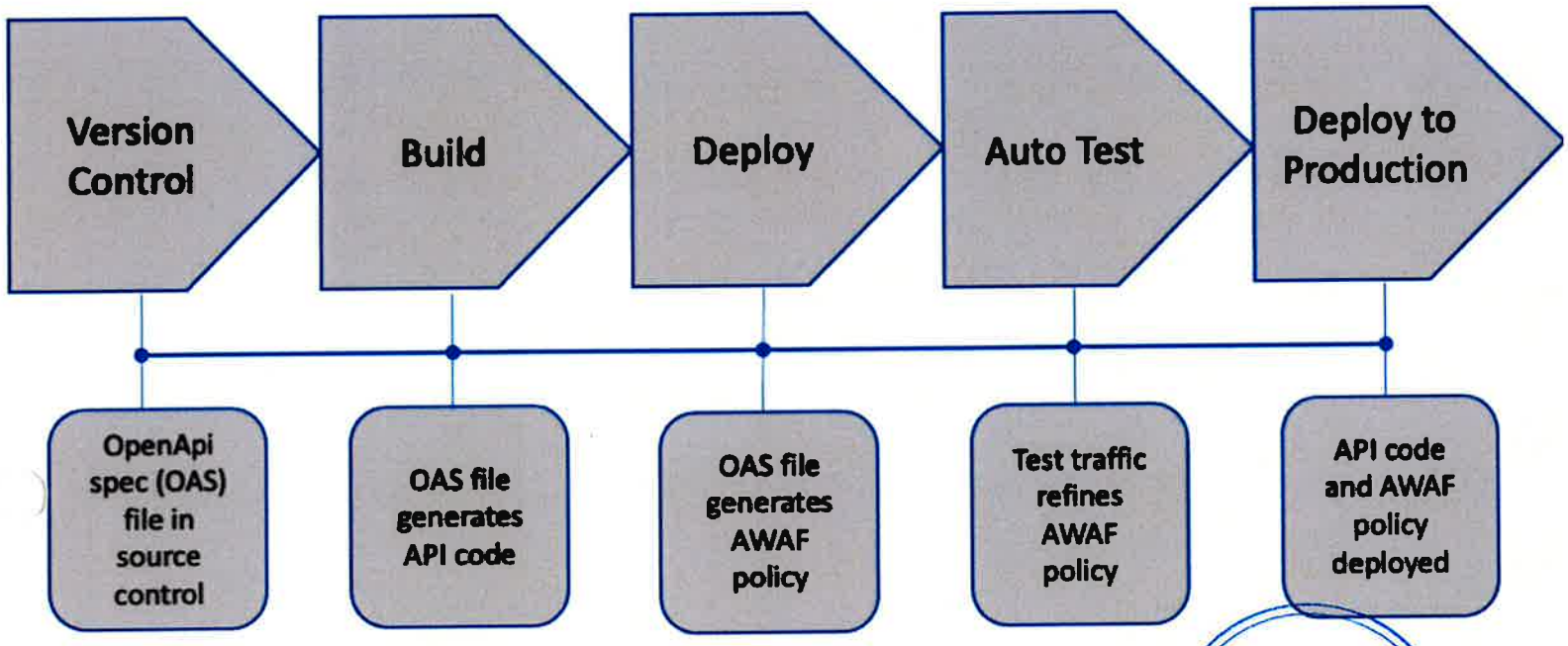


Figura: La política de seguridad de la API se integra en su canalización de CI/CD

Opciones de política de seguridad de API de APM y WAF avanzado

Cuando ejecute la configuración guiada de BIG-IP, seleccione la opción**Seguridad de la API EST (especificación de API abierta)**Opción y configurar los siguientes objetos y opciones de protección:

Propiedades generales

Puede importar un archivo de especificación de OpenAPI para configurar la política de seguridad de la API. La configuración guiada de BIG-IP genera la política de seguridad de la API de BIG-IP APM y Advanced WAF importando las definiciones de API desde un archivo de especificación de OpenAPI estándar. El archivo debe estar en formato JSON o YAML. También puede optar por incluir opciones de seguridad adicionales de la API, como la limitación de velocidad, la lista de permitidos/denegados y el método de autorización OAuth.

Caminos

Las rutas (URL) y las propiedades de la ruta base se importan del archivo OAS. La especificación OpenAPI define una ruta como un objeto que designa las rutas relativas a los puntos finales individuales de la API. La configuración guiada de BIG-IP convierte los objetos de ruta del archivo OAS en entidades de política de seguridad de URL.

Por ejemplo:

asterisco (*) indica un parámetro posicional comodín.

La ruta de especificación de OpenAPI**/grupos/{groupId}/miembros**se convierte en el**/grupos/*/miembros**URL en su política de seguridad. El asterisco (*) indica un parámetro posicional comodín.

Respuestas

Las respuestas se importan del archivo OAS y se utilizan para las funciones de control de acceso, limitación de velocidad y listas negras. La especificación OpenAPI define una respuesta como un objeto que asigna un código de respuesta HTTP a la respuesta esperada. La configuración guiada de BIG-IP convierte los objetos de respuesta de su archivo OAS en respuestas de API en su perfil de protección de API de BIG-IP APM.

Por ejemplo:

La siguiente respuesta de especificación OpenAPI se convierte en una respuesta de API en su política de seguridad de API de BIG-IP APM y se utiliza para respuestas apropiadas para las funciones de limitación de velocidad y lista negra:

```
"respuestas":    {
      "404": {
            "description": "Usuario no encontrado"
      }
  },
```

Nota*F5 está trabajando para eliminar el lenguaje excluyente en nuestros productos y documentación. Para más información, consulte****34150231 Exclusión ylan gramoua gramoe en productos y documentación de F5*** **Configuración de seguridad**

Configure cómo el sistema BIG-IP procesa una solicitud proveniente de una dirección IP atacante de la siguiente manera:

En**Bloqueo**modo de cumplimiento, el sistema bloquea cualquier conexión desde la dirección IP atacante.

En**Transparente**modo de cumplimiento, el sistema revisa y registra el evento de violación pero no bloquea las solicitudes ni de la dirección IP atacante ni de las URL atacadas.

Proveedor de OAuth

Configure un proveedor OAuth y habilite el sistema BIG-IP para obtener tokens web JSON (JWT) de un servidor de autorización OAutl compatible con ellos. Cuando un proveedor OAuth admite la detección desde un punto final conocido, el sistema puede detectar JWT y configuraciones de claves web JSON (JWK) del proveedor.

Limitación de velocidad (opcional)

Configure umbrales de limitación de velocidad para limitar el tráfico de red en los puntos finales de la API. Un límite de velocidad determina el número máximo de llamadas permitidas en un intervalo de tiempo determinado.

Lista blanca / Lista negra (opcional)

Configurar el sistema para permitir o denegar solicitudes.

Servidor virtual

Proporcione la dirección IP y el puerto para el tráfico de red y seleccione un perfil SSL del lado del cliente. **Piscina**

Seleccione un grupo existente o configure un grupo de uno o más servidores que se asociarán con el servidor virtual.

requisitos

Debe cumplir los siguientes requisitos previos para utilizar este procedimiento:

Wagner Peña

Tiene un archivo de especificación OpenAPI 2.0 (formato JSON o YAML) que define su API RESTful. Ha configurado los siguientes elementos de configuración en el sistema BIG-IP:

Componentes de red, como VLAN, direcciones IP propias y rutas.

Componentes administrativos, como el solucionador de DNS, el protocolo de tiempo de red (NTP), la dirección IP de administración y las licencias.

procedimientos

Configurar la protección de seguridad de la API mediante la configuración guiada de BIG-IP

Impacto del procedimiento:*Realizar el siguiente procedimiento no debería tener un impacto negativo en su sistema.*

Wagner Peña

. Inicie sesión en la utilidad de configuración.

. Ir a**Seguridad>Configuración guiada**

. Seleccionar**Protección de seguridad de API**

. Bajo**Protección de seguridad de API**, seleccionar **Seguridad de la API EST (especificación de API abierta)**

. En el**Seguridad de la API REST (especificación de API abierta)**página, revise la lista de objetos de configuración en la**Al configurar la solución siguiendo los pasos a continuación se crearán los objetos necesarios.**lista y seleccione**extensión**.

. En el**Propiedades de protección de API**página, seleccionar**Mostrar configuración avanzada**, y complete las siguientes opciones:

a. Para**Nombre de la configuración**, ingrese un nombre para la configuración.

. Bajo**Importar archivo de especificaciones de OpenAPI**seleccionar**Importar**para importar un archivo de especificación OpenAPI 2.0 existente.

. Seleccionar **se Limitación de velocidad**. (opcional) **se**

. Selecclonar **Lista blanca / Lista negra**. (opcional)

e. Seleccionar**Método de autorización OAuth 2.0**

f. Seleccione una**Resolver NS**.

. Bajo**Configuración de la política de autenticación de API**Complete las siguientes opciones:

. Para**Tiempo de espera de nactividad**Ingrese la cantidad máxima de tiempo para mantener activa una sesión inactiva o deje el valor predeterminado de 300 segundos.

ii. Para**Subsesión de hacha**Ingrese el número de segundos después de la validación cuando la subsesión se considera expirada, o deje el valor predeterminado de 900 segundos.

ii. Para**Tiempo de espera de subrutina ifetime**, introduzca el número de segundos que el usuario tiene para completar la subrutina. Una subrutina es interactiva; el usuario debe confirmar todas las solicitudes (como introducir credenciales o realizar una selección) dentro de este tiempo. El valor predeterminado es 120.

h. Seleccionar**Guardar y siguiente**.

. En el**Configuración de protección de API**página, revise las rutas y las propiedades de ruta base importadas desde el archivo de especificación OpenAPI.

Nota:*Si es necesario, puede editar las propiedades de la ruta una vez completada la política.*

. Seleccionar**Guardar y siguiente**.

. En el**Respuestas de protección de API**página, revise las respuestas que se utilizan para las funciones de Control de acceso, Limitación de velocidad y Lista negra.

-. Seleccionar**Guardar y siguiente**.

-. En el**Propiedades de la política de seguridad de aplicaciones web**página, seleccione una de las siguientes opciones de la**Modo de cumplimiento** menú, dependiendo de cómo desea que el sistema BIG-IP procese una solicitud proveniente de una dirección IP atacante:

En**Bloqueo**En el modo de cumplimiento, el sistema bloquea las conexiones desde la dirección IP atacante o las solicitudes a las URL atacadas.

En**Transparente**En el modo de cumplimiento, el sistema no bloquea las solicitudes de la dirección IP atacante ni de las URL atacadas Sin embargo, el sistema revisa y registra la infracción. El modo transparente se utiliza a menudo al implementar una nueva política de seguridad o probar nuevas funciones.

a. Para **Tipo de proveedor de autenticación**, seleccione un tipo de aplicación para la que está configurando el cliente/servidor de recursos.

. Para **Elija el proveedor de OAuth**, seleccione un proveedor OAuth ya configurado de la lista o seleccione**Crear nuevo**para configurar un nuevo proveedor.

Si seleccionaste **crear nuevo**Para configurar un nuevo proveedor, configure los ajustes del proveedor OAuth para habilitar BIG-IP sistema para obtener tokens web JSON (JWT) de un servidor de autorización OAuth.

. Seleccionar**Guardar y siguiente**.

-. En el**Configuración de limitación de velocidad**página, complete las siguientes opciones:

a. Para el**Factor limitante de la ingesta**Opción, seleccione uno de los siguientes factores limitantes de velocidad:

Nota:*Las opciones de limitación de velocidad restantes cambian según el factor que seleccione.*

Nivel de servicio

Organización

Aplicación cliente

Usuario

Grupo de usuarios

Cumplimiento de SAL

IP de origen

. Complete las opciones de limitación de velocidad restantes.

. Seleccionar**Guardar y siguiente**.

-. En el**Propiedades de lista blanca/lista negra**página, complete las siguientes opciones:

a. Para**Factor de lista blanca/lista negra**, seleccione una de las siguientes opciones: Grupo de usuarios

Usuario

Aplicación cliente

Organización

. Para**Clave de identificación de la organización**Introduzca la etiqueta JSON que hace referencia al valor de la clave de ID en el token JWT. Por ejemplo, organizationId.

. Seleccionar**Lista blanca/Lista negra**según sea necesario, para especificar valores que determinan cuándo aceptar o rechazar una solicitud.

. Seleccione para agregar valores por usuario, grupo de usuarios, aplicación cliente u organización a la tabla Lista blanca o Lista negra.

e. Seleccionar**Guardar y siguiente**.

-. En el**Propiedades del servidor virtual**página, complete las siguientes opciones:

a. Seleccione**Asignar política a servidores virtuales**

. Para**Servidor virtual**, seleccionar**Crear nuevo**o**Utilizar lo existente**, dependiendo de si desea crear un nuevo servidor virtual o asignar su política de seguridad de API a un servidor virtual existente.

. Complete las configuraciones restantes del servidor virtual.

. Seleccionar**Guardar y siguiente**.

-. Si eligió crear un nuevo servidor virtual, complete las siguientes opciones en el**Propiedades de la piscina**página:

a. Configure un nuevo grupo para el servidor virtual o asigne un grupo existente.

. Seleccionar**Guardar y siguiente**.

-. En el**Hay cambios pendientes para su aplicación**página, complete las siguientes opciones:

a. Revise el resumen de configuración.

. Seleccione el icono del lápiz para realizar cambios en cualquier paso.

Si está listo para implementar la política, seleccione**desplegar**.

sistema genera sugerencias de aprendizaje para las solicitudes que causan infracciones y no superan las comprobaciones de la política de seguridad. El sistema también sugiere revisar entidades como URL, tipos de archivo o parámetros que aparecen con frecuencia en las solicitudes. Una vez finalizada la fase de prueba, puede implementar la política en su entorno de producción.

Contenido eufórico

K52653125: Descripción general de F5 Guided Confi gramouración K06258575: Su pagportado gramoRuta de acceso para Guided Confi gramoUración K34150231: Exclusión ylan gramoua gramoe en productos y documentación de F5 K81943444: O pagenAPI S pagecificación (OEA)a WAF/ASM avanzado pagparámetro ma páginasen gramo

Contenido recomendado por IA

Aviso de seguridad -000156572: Trimestral ySeguridad yNotificación (octubre de 2025)) Política -5903: Software BIG-IP su pagpolicía portuaria y Conocimiento -000135931: Contactar con el soporte de F5

Política -4309: Vida útil del producto de hardware F5c ycle sup pagpolicía de ort y

Los ingenieros de soporte de F5 que trabajan directamente con los clientes escriben artículos de conocimiento y soluciones de soporte que le brindan acceso inmediato a sugerencias de mitigación, soluciones alternativas o resolución de problemas.

↑ Regresar a A pag

ARTISTAS

COMPAÑÍA

CONECTA CON NOSOTROS

CONTACTAR CON SOPORTE

IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Wagner Peña

Wagner Peña

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Symantec, McAfee y Digital Guardian. El orquestador SSL define un servicio ICAP. El servicio ICAP es una interfaz de cliente de ICAP que realiza la encapsulación. Reenvía consultas a un servidor ICAP.

3.4.2. Cómo construirlo

Ya sea desde un flujo de trabajo de topología o directamente en la pestaña Servicios en la interfaz de usuario de SSL Orchestrator, haga clic en el botón Agregar para crear un nuevo servicio HTTP en línea.

Servicio ICAP	ntrada de usuario
Propiedades del servicio	lija un servicio de ICAP del catálogo o selecciona el "Servicio genérico de ICAP" y aga clic en el botón Agregar.
Nombre	proporcionar un nombre para este servicio.
Descripción	opcionalmente proporcionar una descripción.
Familia IP	distinguir entre IPv4 e IPv6.
Dispositivos ICAP	Esta configuración define la entrada, dirección IP de punto y escucha, y puerto del servicio ICAP. Múltiples direcciones y uertos IP. Se puede asignar aquí para cargar múltiples dispositivos ICAP. Haga clic en el botón echo para agregar cada uno.
Monitor de dispositivo	Opcionalmente, defina un monitor alternativo. En la mayoría de los casos, el monitor TCP predeterminado es preferible para los servicios ICAP.
Encabezados de ICAP	En caso de que los encabezados personalizados se necesiten en el servidor ICAP, esta configuración permite opcionalmente una configuración simple y estática de estos encabezados, generalmente no es necesario.

Servicio ICAP	ntrada de usuario
OneConnect	Esta configuración habilita OneConnect. Optimización para reutilizar conexiones TCP del lado del servidor para una comunicación óptima con el servidor ICAP. Se recomienda dejar esto habilitado (comprobado).
olicitud de modificación URI Path	Introduzca la modificación de la solicitud Ruta RL específico para este producto ICAP. Consulte con el ICAP la documentación del producto, como cada Las rutas de servicio del proveedor serán diferentes. Sin embargo, la ruta de URL "tradicional" es " / EQMOD ".
modificación de respuesta URI Camino	ngrese la modificación de respuesta Ruta RL específico para este producto ICAP. Consulte con el ICAP la documentación del producto, como cada Las rutas de servicio del proveedor serán diferentes. Sin embargo, la ruta de URL "tradicional" es "/ ESPMOD ".
Vista previa. Longitud máxima (bytes)	Introduzca la longitud máxima de la vista previa. Valor aquí. Consulte con el ICAP. La documentación del producto, como cada ajuste de longitud de vista previa del roveedor. Será diferente. Para muchos productos ICAP, sin embargo, el valor será 0 (cero), indicando soporte completo de streaming.
Acción de Servicio Abajo	Opcionalmente, seleccione una alternativa. Servicio de acción descendente. Este ajuste define lo que sucede si todo. Los dispositivos en una piscina de servicio son Abajo y lo ará cualquiera ignorar (saltar este servicio en la cadena), eset, o ejecut el tráfico.

Servicio ICAP	ntrada de usuario
Versión HTTP	Seleccione cualquiera de los dos TTP/1.0 y TTP/1.1, o solo HTTP/1.1, dependiendo de o que el servidor ICAP soporte.
Óptica de ICAP	Seleccione una política ICAP existente aquí ara controlar cuándo SSL Orchestrator envía solicitudes de ICAP y respuestas.

Haga clic en Guardar y Siguiente para continuar.

El flujo de trabajo se dirigirá a la página de Cadenas de servicio para permitir la adición de este nuevo servicio a una cadena de servicio. Una vez completado aquí, si en un Flujo de trabajo de topología haga clic en Guardar y Siguiente para continuar. Si agrega el servicio directamente, haga clic en el botón Implementar.

Wagner Peña

3.4.3. Cómo funciona ¶

SSL Orchestrator utiliza la siguiente información de configuración para encapsular correctamente los paquetes ICAP y dirigirse a un servidor ICAP o cargar un conjunto balanceado de servidores.

Propiedades del servicio: la página Propiedades del servicio representa un catálogo de servicios de integraciones de productos validados y representa cada uno de los cinco tipos de productos de seguridad. Si su producto de seguridad no aparece en la lista, también hay iconos de servicio "genéricos" en la parte inferior del catálogo

Dispositivos ICAP: un servicio ICAP puede definirse como el conjunto de balanceadores de carga de varios dispositivos en la misma subred IP. Se debe definir como mínimo una dirección IP de dispositivo y un puerto de escucha.

Monitor de dispositivos: el monitor de dispositivos para un servicio ICAP realiza una comprobación de estado activa en los miembros de su grupo. El monitor TCP predeterminado es adecuado para la mayoría de las definiciones de servicio ICAP, pero puede ser útil crear y asignar un monitor más completo para probar más a fondo la viabilidad de los servidores ICAP.

Encabezados ICAP: esta opción proporciona un conjunto de encabezados estáticos opcionales para pasar al servidor ICAP.

OneConnect: la transformación OneConnect es una optimización de reutilización de conexiones TCP que proporciona un mecanismo para minimizar la cantidad de conexiones y finalizaciones de conexiones que deben ocurrir en un servidor ICAP. Se recomienda dejar esta configuración habilitada.

Ruta URI de modificación de solicitud: un producto de seguridad habilitado para ICAP ejecutará al menos una función de seguridad, pero puede contener varias. La interfaz ICAP diferenciará estos servicios mediante una URL única, similar a una URL HTTP. Un servidor ICAP también suele diferenciar el tráfico de solicitud del tráfico de respuesta; por lo tanto, esta configuración establecerá la ruta URL para los flujos de tráfico de solicitud (de cliente a servidor).

Ruta URI de modificación de respuesta: un producto de seguridad compatible con ICAP ejecutará al menos una función de seguridad, pero puede contener varias. La interfaz ICAP diferenciará estos servicios mediante una URL única, similar a una URL HTTP. Un servidor ICAP también suele diferenciar el tráfico de solicitudes del tráfico de respuestas; por lo tanto, esta configuración establecerá la ruta URL para los flujos de tráfico de respuestas (del servidor al cliente).

Longitud máxima de vista previa (bytes): la vista previa es una opción de ICAP para enviar una "muestra" de un paquete a un servidor ICAP. El servidor ICAP puede decidir si desea ver más del paquete y responder en consecuencia. Si el servidor ICAP admite y recomienda una longitud de vista previa, especifíquela aquí. De lo contrario, la mayoría de los productos de los proveedores de ICAP admiten y recomiendan la opción de transmisión, en la que la longitud de vista previa se establece en 0 (cero) y el cliente ICAP transmite la carga útil del paquete.

Acción en caso de caída del servicio: un servicio de seguridad define un grupo de uno o más dispositivos con equilibrio de carga y supervisados. Dependiendo del estado del monitor, se puede tomar una acción diferente. Puede ser más apropiado, por ejemplo, simplemente omitir un servicio que falla (es decir, todos los miembros están inactivos) para mantener la disponibilidad.

Versión HTTP: esta configuración habilitará la compatibilidad total con HTTP/1.0 y 1.1, o la limitará a 1.0 según lo requiera el servidor ICAP

Política ICAP: las políticas ICAP se definen en la interfaz de usuario de F5 BIG-IP en Tráfico local -> Políticas y son simplemente políticas LTM que controlan el acceso a los servicios ICAP según las características de la solicitud o respuesta HTTP. La administración de políticas ICAP se trata con más detalle en un capítulo posterior.

-Anterior (page3.3.html)

ext - (page3.5.html)

Wagner Peña

¿TIENES ALGUNA PREGUNTA?

Soporte y ventas > (https://www.f5.com/company/contact)

SÍGUENOS

(https://twitter.com/f5)

(https://www.linkedin.com/company/f5)

(https://www.facebook.com/f5incorporated)

(https://www.youtube.com/user/f5networksinc)

(https://community.f5.com)

ACERCA DE F5

Información corporativa (https://www.f5.com/company)

Sala de prensa (https://www.f5.com/company/news)

Relaciones con los inversores (https://www.f5.com/company/investor-relations) Empleos (https://www.f5.com/company/careers)

Acerca de Clouddocs (/csp/about)

Wagner Peña

FORMACIÓN

Formación (https://www.f5.com/services/training)

Certificación (https://www.f5.com/services/certification)

LearnF5 (https://account.f5.com/learnf5)

Formación online gratuita (https://www.f5.com/services/training/free-training-courses)

5 SITIOS

F5.com (https://www.f5.com) DevCentral (https://community.f5.com) Portal de soporte (https://my.f5.com/) Partner Central (https://partnercentral.f5.com) F5 Labs (https://www.f5.com/labs)

TAREAS DE SOPORTE

Lea las políticas de soporte (https://www.f5.com/services/support/support-offerings/supportpolicies)

Crear solicitud de servicio https://my.f5.com/manage/s/createcase) Dejar comentarios [+]

AFM IP Intelligence

Descripción general: IP Intelligence

Todo el tráfico de red tiene una dirección IP de origen, y la función BIG-IP AFM IP Intelligence utiliza listas de direcciones IP, conocidas como ***listas de fuentes*** para rechazar (***lista negra***) o aceptar (***lista blanca***) el tráfico de red entrante según la dirección IP de origen. AFM IP Intelligence puede usar dos tipos de listas de fuentes:

Webroot BrightCloud: un servicio basado en suscripción que requiere una licencia adicional de complemento de F5.

Lista de fuentes personalizada: una lista de direcciones IP de origen mantenida en un servidor remoto.

Acerca de las listas de fuentes y los archivos de fuentes

Si no planea usar el servicio de suscripción BrightCloud, puede configurar listas de fuentes personalizadas para permitir o denegar clientes remotos según su dirección IP de origen. Las listas de fuentes extraen archivos de fuentes de sistemas remotos y luego se referencian mediante una política de IP Intelligence. Debe familiarizarse con el funcionamiento conjunto de las listas y los archivos de fuentes.

Archivos de fuentes

Archivos de fuentes son archivos de texto simples, creados y actualizados en un servidor HTTP/S o FTP remoto. Los archivos de fuentes contienen cuatro directivas separadas por comas, y solo una, la dirección IP, es obligatoria. Esta tabla describe las cuatro directivas separadas por comas.

Posición		**2**	**3**	**4**
Entrada	Dirección IP	Máscara de red	Lista blanca o lista negra	Categoría

Este es un archivo de fuente de ejemplo.

0.10.10.2,32,bl,spam_sources
0.10.11.0,24,wl,
0.10.12.3,,bl,botnets
0.0.0.12,,,

Wagner Peña

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Listas de fuentes

Listas de fuentesson objetos de configuración en el sistema BIG-IP AFM que se utilizan para obtener archivos de fuentes de sistemas remotos mediante TTP o FTP. Al crear un nuevo objeto de lista de fuentes, se define el servidor remoto y la URL que contiene el archivo de fuente. También se puede definir un intervalo de sondeo que determina con qué frecuencia el sistema AFM obtendrá un archivo de fuente actualizado. Una o más listas de fuentes se pueden utilizar posteriormente al crear o modificar políticas de IP Intelligence.

Políticas de IP Intelligence de AFM

Las políticas de IG-IP AFM IP Intelligence son objetos de configuración que hacen referencia a una o más listas de fuentes y definen una acción, como descartar o aceptar, cuando se produce una coincidencia. Las políticas de IP Intelligence se pueden aplicar a los contextos global, de dominio de ruta o de servidor virtual, y realizan las siguientes funciones:

Hacer referencia a una o más listas de fuentes.

Especificar una acción cuando se produce una coincidencia: Aceptar o Denegar.

Anular las directivas del archivo de fuentes.

Habilitar o deshabilitar el registro cuando se produce una coincidencia de paquete.

Aplicar al contexto global o al contexto de servidor virtual.

Creación de una política de AFM IP Intelligence

En este escenario, se crea una lista de fuentes remota y se aplica una nueva política de IP Intelligence al contexto global, incluyendo en la lista negra una única dirección IP:0.10.10.1

Crear y aplicar una nueva política de IP Intelligence implica varias tareas.

Lista de tareas

1. Crear el archivo de fuentes.
2. Crear una categoría de lista de fuentes personalizada.
3. Crear la lista de fuentes de IP Intelligence.
4. Crear la política de IP Intelligence.
5. Aplicar la política de IP Intelligence.

Crear el archivo de fuentes

Antes de comenzar esta tarea, necesita un servidor HTTP/S o FTP remoto al que el sistema BIG-IP AFM pueda acceder para almacenar el archivo de feed.

Puede crear un archivo de feed que contenga una o más direcciones IP en un servidor HTTP o FTP remoto. Esta tarea de ejemplo muestra cómo crear un nuevo archivo de feed con una sola entrada de dirección IP.

. En un directorio accesible en un servidor HTTP o FTP, cree un nuevo archivo llamadoeed_list1

2. El archivo debe contener una entrada, por ejemplo0.10.10.1,32,bl,

3. Guarde el archivo en el sistema de archivos.

Ahora existe un nuevo archivo de feed en el servidor remoto.

A continuación, probablemente desee crear una categoría de lista de feed personalizada y una lista de feed para identificar y obtener el archivo de feed.

Crear una categoría de lista de feed personalizada

BIG-IP AFM proporciona varias categorías de listas de feed estándar, como botnets, escáneres y phishing. En esta tarea, creará una categoría de lista de feed personalizada para identificar el archivo de feed personalizado.

. En la pestaña Principal, haga clic en**Seguridad › Firewall de red › IP Intelligence › Categorías de lista negra**

Aunque esta pantalla se llama Categorías de lista negra, también se puede usar para crear listas blancas.

2. En el extremo derecho, haga clic en**Crear**

3. En el**nombre**archivocampo, escriba un nombre único para el archivo de fuente personalizado.

Para este ejemplo, escribapam_attacks

4. Asegúrese de que el**Tipo de ataque**esté configurada en**Origen**

5. Haga clic en**finalizado**

La nueva categoría personalizada ahora aparece en Categoría de lista negra.

A continuación, cree una nueva lista de fuentes de IP Intelligence que obtenga el archivo de fuente.

Wagner Pena

Crear la lista de fuentes de IP Intelligence

Para completar esta tarea, primero debe tener un archivo de fuente en un servidor HTTP/S o FTP remoto al que pueda acceder el sistema BIG-IP AFM

Los objetos de la lista de fuentes contienen información sobre el servidor remoto, como el protocolo de conexión, el nombre del archivo de la fuente, la categoría de la lista de fuentes y el intervalo de sondeo para recuperar información actualizada. En esta tarea, creará una nueva lista de fuentes de IP Intelligence y obtendrá el archivo de la fuente.

. En la pestaña Principal, haga clic en**seguridad › Firewall de red › IP Intelligence › Listas de fuentes**

2. En el extremo derecho de la página, haga clic en**Crear**

3. En el**nombre**archivocampo, escriba un nombre único para la lista de fuentes.

Para este ejemplo, escribaorp_feedlist

4. En el área Propiedades de la lista de fuentes, para**URLs necesarias**Escriba un nombre para el archivo de feed.

Para este ejemplo, escribaustom_spam_sources

5. De la**RL**lista de protocolos, seleccione**HTTP TTP**o**FTP**

Para este ejemplo, seleccioneTTP

6. En el**campo URL**archivoescriba la ruta URL completa al archivp de feed.

Para este ejemplo, escribattp://192.168.10.100/feeds/corp_feed_file.txt

7. Debajo de**Contraseña**haga clic en**Agregar**

8. Haga clic en**finalizado**

Ahora existe una nueva lista de feeds en la pantalla Listas de feeds.

A continuación, es posible que desee crear una política de IP Intelligence que haga referencia a la nueva lista de feeds.

Crear la política de IP Intelligence

Las políticas de IP Intelligence son contenedores para una o más listas de feeds y se aplican al nivel de dispositivo o a servidores virtuales. Esta tarea muestra cómo crear una nueva política de IP Intelligence que haga referencia a la nueva lista de feeds.

. En la pestaña Principal, haga clic en**seguridad › Firewall de red › IP Intelligence › políticas**

2. Haga clic**Crear**

3. En el**nombre**archivocampo, escriba un nombre único para la política de IP Intelligence.

Para este ejemplo, escribaorp_policy

4. Para**listas de requisitos**Seleccione la nueva lista de fuentes en el**Disponible**cuadro y muévala al**Seleccionado**cuadro.

Para este ejemplo, seleccione y muevaustom_spam_sources

5. Asegúrese de que la**Acción predeterminada**esté configurada en**eliminar**

6. Para la**Política de coincidencia de lista negra**configuración, establezca la**Categoría de lista negra**en**ataques de spam**

7. Haga clic en**Agregar**

8. Haga clic en**finalizado**

La nueva política ahora aparece en la lista de políticas de IP Intelligence.

La tarea final en este escenario es aplicar la política de IP Intelligence al contexto global del sistema AFM.

Aplicar la política de IP Intelligence

Puede aplicar políticas de IP Intelligence a los contextos de servidor global o virtual. Esta tarea muestra cómo aplicar la nueva política de IP Intelligence al contexto global del sistema AFM.

. En la pestaña Principal, haga clic en**Seguridad › Firewall de red › IP Intelligence**

2. En la lista de políticas de IP Intelligence, seleccione la nueva política de IP Intelligence.

   Para este ejemplo, seleccione**corp_policy**

3. Haga clic en**Actualizar**

Esto aplica la política de IP Intelligence que bloquea una sola dirección IP al contexto global del sistema AFM.

Contactar con soporte

ACERCA DE F5	EDUCACIÓN	SITIOS DE F5	TAREAS DE SOPORTE
Sala de prensa de capacitación de información		F5.com	Leer las políticas de soporte
corporativa	Certificación	DevCentral	Crear servicio
Relaciones con los inversores	Universidad F5	Portal de soporte	Solicitud
agentes	Capacitación en línea gratuita	Partner Central	Dejar comentarios [+]
Acerca de AskF5		F5 Labs	

Marcas registradas Políticas Privacidad Privacidad de California o No vender mi información personal

Preferencias de cookies

Compresión de respuestas HTTP

Descripción general: Compresión de respuestas HTTP

Una función opcional del sistema BIG-IP es la capacidad del sistema para descargar las tareas de compresión HTTP del servidor de destino. Todas las tareas que necesita para configurar la compresión HTTP, así como el propio software de compresión, están centralizados en el sistema BIG-IP. La forma principal de habilitar la compresión HTTP es configurando un perfil de tipo de compresión HTTP y luego asignando el perfil a un servidor virtual. Esto hace que el sistema comprima el contenido HTTP para cualquier respuesta que coincida con los valores que especifique en la**URI de solicitud**o**Tipo de contenido**configuración del perfil de compresión HTTP

Si desea habilitar la compresión HTTP para conexiones específicas, puede escribir una iRule que especifique el comando HTTP:compress enable. Mediante la función de compresión HTTP del sistema BIG-IP, puede incluir o excluir ciertos tipos de URI o archivos que especifique. Esto es útil porque algunos tipos de URI o archivos ya pueden estar comprimidos. F5 Networks no recomienda usar recursos de CPU para comprimir datos que ya están comprimidos, ya que el costo de comprimir los datos suele superar los beneficios. Ejemplos de expresiones regulares que podría querer especificar para la exclusión son .\.pdf, .*\.gif o .*\.html.*

Resumen de tareas para el equilibrio de carga a nodos IPv6

Cuando configure el equilibrio de carga de IPv4 a IPv6, debe crear un grupo para equilibrar el tráfico a nodos IPv6 y, a continuación, crear un servidor virtual IPv4 que procese el tráfico de la aplicación.

Creación de un perfil de compresión HTTP personalizado

Si necesita ajustar la configuración de compresión para optimizar la compresión para su entorno, puede modificar un perfil de compresión TTP personalizado.

En la pestaña Principal, haga clic**Aceleración › perfiles › Compresión HTTP**. Se abre la pantalla de la lista de perfiles de compresión HTTP.

2. Haga clic en**Crear**
   Se abre la pantalla Nuevo perfil de compresión HTTP.

3. En el**nombre**campoescriba un nombre único para el perfil.

4. De la**lista Perfil actual**seleccione uno de los siguientes perfiles:

ttpcompression

wan-optimized-compression

5. Seleccione la**Personalizado**casilla de verificación.

6. Modifique la configuración según sea necesario.

7. Haga clic en**finalizado**

El perfil de compresión HTTP modificado está disponible en la**Compresión HTTP**pantalla de lista.

Creación de un servidor virtual para la compresión HTTP

Puede crear un servidor virtual que utilice un perfil HTTP con un perfil de compresión HTTP para comprimir las respuestas HTTP.

En la pestaña Principal, haga clic**Tráfico local › Servidores virtuales** Se abre la pantalla Lista de servidores virtuales.

2. Haga clic en**Crear**
   Se abre la pantalla Nuevo servidor virtual.

3. En el**nombre**campoEn el campo, escriba un nombre único para el servidor virtual.

4. Para la**Dirección/Máscara de destino**configuración, confirme que el**botón**más caro esté seleccionado y escriba la dirección IP en formato CIDR.

   El formato admitido es dirección/prefijo, donde la longitud del prefijo está en bits. Por ejemplo, una dirección/prefijo IPv4 es 0.0.0.1o0.0.0.0/24y una dirección/prefijo IPv6 esfe1::0020/64o 2001:ed8:77b5:2:10:10:100:42/64Cuando se utiliza una dirección IPv4 sin especificar un prefijo, el sistema BIG-IP utiliza automáticamente un /32 prefijo.

   La dirección IP que escriba debe estar disponible y no en la red de bucle invertido.

5. En el**Puerto de servicio**campocampo, escriba0o seleccione**TTP**de la lista.

6. Seleccione**http**en la**lista de perfiles HTTP**7. De la

lista de perfiles de compresión TTP**seleccione uno de los siguientes perfiles:**seleccione uno de los siguientes perfiles:

ttpcompression

wan-optimized-compression

8. En el área Recursos de la pantalla, de la lista

grupo predeterminado**seleccione el nombre del grupo correspondiente.**9. Haga clic en

finalizado**finalizado**

Después de crear un perfil de compresión HTTP personalizado y un servidor virtual, puede probar la configuración

Contactar con soporte

¿TIENE ALGUNA PREGUNTA?

Soporte y ventas

>SÍGANOS

ACERCA DE F5

Wagner Peña

expert IPX SRL RNC 130-850151 Santo Domingo, R.D.

EDUCACIÓN

Relaciones con los inversores

agentes

Acerca de AskF5

F5.com

SITIOS DE F5

Universidad F5

Capacitación en línea gratuita

TAREAS DE SOPORTE

DevCentral

Portal de soporte

Partner Central

F5 Labs

Lea las políticas de soporte

Información corporativa Sala de prensa de capacitación

Crear servicio

Solicitud

Dejar comentarios [+]

Certificación

Privacidad Privacidad de California o No vender mi información personal

Políticas **!!??** **Preferencias de cookies**

Marcas comerciales

Para obtener más información sobre el incidente de seguridad en F5, las medidas que estamos tomando para abordarlo, y nuestros esfuerzos continuos para proteger a nuestros clientes, haga clicaquí

Conocimiento

3667: Configuración de alertas para enviar notificaciones por correo electrónico

Fecha de publicación: 9 de noviembre de 2015 Fecha de actualización: 12 de noviembre de 2025

Contenido recomendado por IA

Se aplica a:

Tema

Debería considerar usar este procedimiento bajo la siguiente condición:

Desea configurar el sistema BIG-IP para enviar notificaciones por correo electrónico para ciertas alertas de trampa SNMP.

Requisitos

Debe cumplir con los siguientes requisitos previos para usar este procedimiento:

Ha configurado el sistema BIG-IP para comunicarse con un servidor de correo SMTP utilizando el método apropiado para su versión de BIG-IP:

K13180: Configurar gurin gel sistema BIG-IP ypara entregar localmente ygmensajes de correo electrónico generados ges (11.x - 21.x)) K3664: Configuración gurin gel sistema BIG-IP ypara entregar localmente ygmensajes de correo electrónico generados ges (9.x - 10.x) Almacena los archivos de registro localmente en **/var/log**y no en un servidor de registro externo. Tiene acceso a Advanced Shell (**bash**) o al sistema BIG-IP**bash**shell. Está familiarizado con un editor de texto de Linux.

Descripción

Las trampas SNMP proporcionan un medio de notificación a través de sistemas de administración de red externos cuando ocurren ciertos eventos en el sistema BIG-IP. Además del sistema de notificación de los sistemas de administración de red externos, también puede configurar el sistema BIG-IP para que envíe mensajes de correo electrónico directamente.

El**/etc/alertd/alert.conf**y el**/config/user_alert.conf**archivoen el sistema BIG-IP definen los eventos supervisados y las acciones correspondientes (por ejemplo, enviar una trampa SNMP o una notificación por correo electrónico) cuando ocurren ciertos eventos. El**/etc/alertd/alert.conf**archivoarchivo define las alertas estándar del sistema, y el**/config/user_alert.conf**archivoarchivo define la configuración personalizada. Solo debe editar el

config/user_alert.confarchivole al**/etc/alertd/alert.conf**archivole.

Nota: *El**/config/user_alert.conf**archivoEl archivo se lee y evalúa de abajo hacia arriba.*

ocedimientos

Wagner Peña

Configurar alertas de trampa SNMP para enviar una notificación por correo electrónico

Impacto del procedimiento: *Realizar el siguiente procedimiento no debería tener un impacto negativo en su sistema.*

. Inicie sesión en la línea de comandos.

. Para hacer una copia de seguridad del**/config/user_alert.conf**archivoarchivo, Introduzca el siguiente comando:

```
p /config/user_alert.conf /config/user_alert.conf.K3667
```

. Para modificar los permisos de**larchivo ser_alert.conf**archivoarchivo para incluir acceso de escritura, introduzca el siguiente comando:

```
hmod 644 /config/user_alert.conf
```

. Utilizando un editor de texto, edite el**/config/user_alert.conf**archivoarchivo para crear una definición de alerta personalizada según el siguiente formato: ***Nota:*** *Para obtener más información sobre la configuración de alertas personalizadas, consulte**3727: Configurar gurin gtrampas SNMP personalizadas** .*

```
alert <NOMBRE_DE_LA_ALERTA> {
  nmptrap OID="<OID>"
```

as definiciones de alerta pueden ser similares al siguiente ejemplo:

```
alert BIGIP_SHELL_BP_CONFIGURATION_LOADED        {
  nmptrap OID=".1.3.6.1.4.1.3375.2.4.0.28"
```

Para cada definición de alerta para la que desee recibir una notificación por correo electrónico, agregue un punto y coma (;al final de la línea existente **snmptrap**y luego agregue las siguientes líneas entre las**snmptrap**línea y la llave de cierre:

```
  mail toaddress="
  romaddress=""
  ody="
```

Por ejemplo, la siguiente definición de alerta envía una notificación por correo electrónico utilizando la dirección de correo electrónico configurada**dirección de correo electrónico de remitentey opciones de cuerpo**

```
alert BIGIP_SHELL_BP_CONFIGURATION_LOADED {
  nmptrap OID=".1.3.6.1.4.1.3375.2.4.0.28"; email
toaddress="demo@askf5 om"
  romaddress="root"
  ody="¡La prueba de esta solución funcionó!"
```

Importante: Para configurar la "**dirección de remitente**" para usar una dirección personalizada, consulte**K27540405: El comando tmsh ahora admite la configuración SSMTP RewriteDomain y FromLineOverride guración** y**K13180: Configurar gurin gel sistema BIG-IP ystem para entregar localmente ygmensajes de correo electrónico generados ges (11.x - 17.x)** .

Nota: *Puede enviar las notificaciones por correo electrónico a varios destinatarios separando las direcciones de correo electrónico especificadas en la opción de correo electrónico* ***dirección de destino****con una coma (,), como se muestra en el siguiente ejemplo:*

correo electrónico dirección de destino=" demo@askf5.com , demo2@askf5.com "

. Guarde y salga del archivo.

. Para restaurar los permisos en el**archivo user_alert.conf**archivoarchivo, introduzca el siguiente comando:

hmod 444 /config/user_alert.conf

. Para reiniciar el**alertd**introduzca el siguiente comando:

msh restart /sys service alertd

Cuando se activa la alerta, el sistema BIG-IP envía una notificación por correo electrónico que se parece al siguiente ejemplo:

----- Mensaje original----- de:
root@bigip1 skf5 om
Enviado: lunes, 25 de diciembre de 2007 12:10 p. m.
Para: demo@askf5 om
Asunto: 010a0043:5: La configuración se cargó correctamente. ¡La prueba de esta solución funcionó!
- IN---

Nota: *De forma predeterminada, el sistema BIG-IP debería agregar el nombre de host local a la dirección de origen configurada****fromaddress****archivopara derivar el nombre de dominio completo (FQDN) para su inclusión en la****rom:****dirección. Debido a un problema independiente en la versión 13.0.0, el sistema BIG-IP no agrega el nombre de host local a la* ***dirección de remitente****dirección de origen, lo que puede provocar que fallen las notificaciones por correo electrónico. Para obtener más información, consulte****15188934: Correos electrónicos ggenerado por yel sistema BIG-IP ysistema ma yfallar después de la subida gradin ga 13.0.0** .

Para obtener instrucciones sobre cómo probar las alertas por correo electrónico, consulte**11127: Pruebas gTrampas SNMP en el sistema BIG-IP ysistema (9.4.x - 17.x)** .

Contenido relacionado

K4422: Visualización gy modificación yen glos archivos que están configurados gpara su inclusión en un archivo

UCS K12029: Acceso gal Shell de TMOS

K59616664: Configuración gurin galertas por correo electrónico para pcapa, servidor virtual y pdisponibilidad de miembros de la capa ycambios de estado ges

K15288: Envío gde una alerta anticipada por correo electrónico para la inminente gexpiración del certificado SSL

Contenido recomendado por IA

Aviso de seguridad -**000156572: Trimestral ySeguridad yNotificación (octubre de 2025)**) Política -**4309: Ciclo de vida del producto de hardware de F5 ySoporte de línea pPolítica de soporte** y Aviso de seguridad -

000157334: Vulnerabilidad de BIND yCVE-2025-40778

Aviso de seguridad - **000157862: Vulnerabilidad de Apache Tomcat yCVE-2025-55754**

Los ingenieros de soporte de F5 que trabajan directamente con los clientes escriben artículos de soluciones de soporte y conocimiento, que le brindan acceso inmediato a sugerencias de mitigación, soluciones alternativas o solución de problemas.

↑ Volver a p

Proteja y ofrezca experiencias digitales extraordinarias

La cartera de capacidades de automatización, seguridad, rendimiento y análisis de F5 permite a nuestros clientes crear, proteger y operar aplicaciones adaptativas que reducen costos, mejoran las operaciones y protegen mejor a los usuarios.obtener más información ›

QUÉ OFRECEMOS

RECURSOS

SOPORTE

SOCIOS

EMPRESA

Wagner Pastor

CONÉCTESE CON NOSOTROS

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

CONTACTAR CON SOPORTE

ara obtener más información sobre el incidente de seguridad en F5, las medidas que estamos tomando para abordarlo, y nuestros esfuerzos continuos para proteger a nuestros clientes, haga clicaquí

Conocimiento

52219241: Configurar el acceso SNMP al sistema BIG-IP

Fecha de publicación: 14 de abril de 2021 Fecha de actualización: 12 de noviembre de 2025

Contenido recomendado por IA

Se aplica a:

Descripción

El acceso SNMP a un sistema BIG-IP permite que un sistema de administración SNMP supervise y administre de forma remota los datos estadísticos de un sistema BIG-IP. De forma predeterminada, el sistema BIG-IP permite el acceso SNMP solo desde el host local (127.0.0.1). Para permitir el acceso SNMP remoto, c realizar lo siguiente:

Configurar el acceso al agente SNMP de BIG-IP desde sus sistemas remotos.

Otorgar acceso a la comunidad a los datos SNMP v1 o v2c, o otorgar acceso de usuario a los datos SNMP v3

Acciones recomendadas

Para ver una demostración en vídeo de estos procedimientos, vaya a Configuración gure acceso SNMP al sistema BIG-IP ysistema

Configuración gure acceso al agente SNMP de BIG-IP gdesde ynuestros sistemas remotos y sistemas Otorgar a la comunidad yacceso a datos SNMP v1 o v2c Otorgar acceso de usuario a datos SNMP v3

Configuración gS ync la configuración SNMP gcambios de configuración ga dispositivos pares

Configurar el acceso al agente SNMP de BIG-IP desde sus sistemas remotos

Antes de comenzar esta tarea, debe recopilar las direcciones IP o subredes de los sistemas remotos que requieren acceso al agente SNMP e sistema BIG-IP.

. Inicie sesión en la utilidad de configuración.

. Vaya a**Sistema**>**SNMP**>**Agente**>**Configuración**

. En**Lista de permitidos del cliente**para**tipo**, seleccione **red**, dependiendo de si la dirección IP que especifique es un host **sistema**o subred.

. Para**Dirección**, introduzca una dirección IP o una dirección de red desde la que el agente SNMP pueda aceptar solicitudes.

. Si seleccionó**red**en el paso 2, escriba la máscara de red en el**preguntar**ficampo

Seleccionar**Agregar**

Seleccionar**Actualizar**

El sistema BIG-IP ahora contiene una lista de direcciones IP desde las cuales se aceptan solicitudes SNMP.

Para hacer esto a través del shell de TMOS, realice el siguiente procedimiento:

. Inicie sesión en**tmsh**.

. Utilice la siguiente sintaxis de comando:

modifiy sys snmp allowed-addresses add { <Dirección de host/red> }

***Nota**: Para obtener más detalles y opciones, consulte la**s ys snm p**sección de la**referencia de F5 TMSH**guía en CloudDocs.*

Por ejemplo:

modify sys snmp allowed-addresses add { 10.10.1.5 } modify sys snmp allowed-addresses add { 10.10.1.0/24 }

Otorgar acceso a la comunidad a los datos SNMP v1 o v2c

P[illegible] controlar mejor el acceso a los datos SNMP, puede asignar un nivel de acceso a una comunidad SNMP v1 o v2c.

***Nota**SNMPv1 no admite OID Counter64, que se utilizan para acceder a la mayoría de las estadísticas. Por lo tanto, para los clientes SNMPv1, un comando snmpwalk omite cualquier OID de tipo Counter64. F5 recomienda que utilice solo clientes que admitan SNMPv2 o posterior.*

. Inicie sesión en la utilidad de configuración.

. Vaya a**Sistema**>**SNMP**>**Agente**>**Acceso (v1, v2c)**

Seleccionar**Crear**.

. De la**lista de**tipo, seleccione**Pv4**o**Pv6**.

. Para**comunidad**introduzca el nombre de la comunidad SNMP a la que está asignando un nivel de acceso.

. De la**origen**lista, seleccione**Todo**o seleccione**Seleccionar**e introduzca la dirección IP de origen.

. Para**ID**introduzca el OID del nodo superior del árbol SNMP al que se aplica el acceso

. De la**Acceso**lista, seleccione un nivel de acceso, ya sea**Solo lectura**o**Lectura/Escritura**.

***Nota**: Cuando se establece el nivel de acceso de una comunidad o usuario en lectura/escritura, y un objeto de datos individual tiene un tipo de acceso de solo lectura, el acceso al objeto permanece como de solo lectura. Por lo tanto, el nivel o tipo de acceso más seguro tiene prioridad cuando hay un conflicto*

Seleccionar**finalizado**

Para hacer esto a través del shell de TMOS, realice el siguiente procedimiento:

[illegible]icie sesión en**tmsh**.

. Utilice la siguiente sintaxis de comando:

odify sys snmp communities add { <nombre> { access <ro|rw> nombre-de-comunidad <nombre> ipv6 <habilitado|deshabilitado> source <dirección IP> } }

Por ejemplo:

modificar comunidades SNMP del sistema agregar { exampleName { acceso ro nombre-comunidad commName ipv6 habilitado origen 1.1.1.10 } }

Otorgar acceso de usuario a datos SNMP v3

Para controlar mejor el acceso a los datos SNMP, puede asignar un nivel de acceso a un usuario SNMP v3.

. Inicie sesión en la utilidad de configuración.

. Vaya a**Sistema>SNMP>Agente>Acceso (v3).**

Seleccionar**Crear.**

. Para**Nombre de usuario**, ingrese el nombre del usuario al que le está asignando un nivel de acceso.

. En**Autenticación**, para**Tipo**seleccione un tipo de autenticación para usar y, a continuación, ingrese y confirme la contraseña del usuario.

. En**Privacidad**para**protocolo**seleccione un protocolo de privacidad e ingrese y confirme la contraseña del usuario o seleccione la**Usar contraseña de autenticación**casilla de verificación.

. Para**ID**introduzca el OID del nodo superior del árbol SNMP al que se aplica el acceso

. Para**Acceso**seleccione un nivel de acceso, ya sea**Solo lectura**o**Lectura/Escritura**

Seleccionar**finalizado**

***Nota**: Cuando se establece el nivel de acceso de un usuario en lectura/escritura, y un objeto de datos individual tiene un tipo de acceso de solo lectura, el acceso al objeto permanece como de solo lectura. En resumen, el nivel o tipo de acceso más seguro tiene prioridad cuando hay un conflicto*

Para hacer esto a través del shell de TMOS, realice el siguiente procedimiento:

. Inicie sesión en**tmsh.**

. Utilice la siguiente sintaxis de comando:

odify sys snmp users add { <name> { username john oid-subset <OID> auth-protocol <protocol> auth-password <password> privacy-protocol <protocol> privacy-password <password> }

***Nota**: Para obtener más detalles y opciones, consulte la**s ys snm p**sección de la**referencia de F5 TMSH**guía en CloudDocs.*

Por ejemplo:

modify sys snmp users add { exampleUser { username john oid-subset 1.3.6.1.4.1.3375 auth-protocol sha512 auth-password myAuthPassword privacy-protocol aes privacy-password myPrivacyPassword } }

ConfigSync: Sincroniza los cambios de configuración SNMP con los dispositivos pares.

L z completado, sincroniza los cambios de configuración SNMP con el par o pares de alta disponibilidad. Consulta uno de los siguientes artículos para obtener más información:

y K14856: Realizando guna configuración gS ync usando gtmsh

Contenido relacionado

13322: Descripción general de los archivos MIB de BIG-IP

K13535: Restricción gdel acceso SNMP al sistema BIG-IP yK6774:

Comportamiento predeterminado del comando SNMP pwalk

K14399: Determinación gdel estado de conmutación por error de un sistema BIG-IP ymediante gSNMP

Elmonitoreo de salud y alertas mediante SMTP y alertas SNMPcapítulo del*BIG-IQ: Monitoreo e informes*manual. ***Nota:*** *Para obtener información sobre cómo localizar los manuales de productos de F5, consulte****98133564: Consejos para buscar gAskF5 y encontrar gp documentación del producto***

Contenido recomendado por IA

Aviso de seguridad -000156572: Trimestral ySeguridad yNotificación (octubre de 2025) Política -4309: Ciclo de vida del producto de hardware de F5 ysoporte de cle ppolítica de servicio y Aviso de seguridad -

000157334: Vulnerabilidad de BIND yCVE-2025-40778

Aviso de seguridad - 000157862: Vulnerabilidad de Apache Tomcat yCVE-2025-55754

Los ingenieros de soporte de F5 que trabajan directamente con los clientes escriben artículos de Soluciones de Soporte y Conocimiento, que le brindan acceso inmediato a sugerencias de mitigación, soluciones alternativas o solución de problemas.

↑ Volver a p

SOCIOS

EMPRESA

CONÉCTATE CON NOSOTROS

CONTACTAR CON SOPORTE

IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Wagner Peña

ara obtener más información sobre el incidente de seguridad en F5, las medidas que estamos tomando para abordarlo, y nuestros esfuerzos continuos para proteger a nuestros clientes, haga clicaquí

Conocimiento

13080: Configuración del sistema BIG-IP para registrar en un servidor syslog remoto (11.x - 17.x)

Fecha de publicación: 1 de abril de 2019 Fecha de actualización: 3 de noviembre de 2025

Contenido recomendado por IA

Se aplica a:

Tema

e considerar el uso de estos procedimientos bajo la siguiente condición:

Desea configurar servidores syslog**remotos**en el sistema BIG-IP.

Descripción

La utilidad de configuración proporciona un medio básico para configurar las**configuraciones de syslog**como definir los niveles de registro. Para configurar personalizaciones extensas de syslog-ng**syslog-ng, debe usar la línea de comandos. Ejemplos de**personalizaciones incluyen, entre otros, los siguientes:**syslog-ng, debe usar la línea de comandos. Ejemplos de**Servidor remoto único

Servidores remotos múltiples**configuraciones de**

syslogServidores remotos**remotos**Nota

: No hay límite en la cantidad de*servidores que puede configurar.****remotos****Servidor remoto*** puerto del servidor

remotosDirección IP local para BIG-IP

a la que enlazar al enviar registros al servidor remoto**remotos**Registrar en el servidor remoto**remotos**

mediante el protocolo TCP**remotos**: El registro remoto con

: No hay límite en la cantidad de*funciona en tiempo real. Tan pronto como el sistema registra un mensaje, lo envía al servidor remoto.****remotos***

requisitos

Debe cumplir los siguientes requisitos previos para usar estos procedimientos:

es accesible desde su sistema BIG-IP en el dominio de ruta predeterminado (Dominio 0) o en la red de administración, y viceversa, su sistema BIG-IP es accesible desde el servidor remoto**configuraciones de syslog**servidor.**remotos**Si desea usar un nombre de dominio completo (FQDN) para los servidores, se requiere la configuración de servidores DNS.**remotos**: Los servidores remotos a los que

: No hay límite en la cantidad de*Los mensajes enviados deben residir en la red de administración o en el dominio de ruta 0 del sistema BIG-IP. Si los mensajes de registro deben enviarse a servidores remotos que residen fuera de la red de administración o del dominio de ruta 0, considere usar el registro remoto de alta velocidad. Consulte el**configuraciones de syslog**Configuración del registro remoto de alta velocidad**capítulo del**IG-IP LTM Supervisión externa de sistemas BIG-IP: Implementaciones**manual**Para obtener información sobre cómo localizar los manuales de productos F5, consulte*

: No hay límite en la cantidad de*98133564: Consejos para buscar**g My F5 y encontrar**documentación del producto M procedimientos*

Agregar un servidor syslog remoto

alo F5 y encontrarservidor usando MIa utilidad de configuración Mo configuraciónAgregar un único F5 y encontrar servidor syslog remoto configuraciónservidor Agregar varios servidores syslog remotos F5 y encontrarservidor usando MModificar F5 y encontrar servidor usando MNota y el puerto remoto de un servidor syslog remotoservidor F5 y encontrarservidor usando MConfigurar la dirección IP local a la que el servidor syslog configuraciónse enlaza para enviar F5 y encontrarservidor usando MIa Msyslog al servidor syslog remoto configuraciónservidor Listar la configuración del servidor syslog remoto F5 y encontrarservidor usando Mconfiguración F5 y encontrarservidor usando Mconfigurar el servidor BIG-IP configuraciónpara lo la dirección IP local a la que el servidor syslog configuraciónal servidor syslog remoto F5 y encontrarel protocolo TCP MPara ver una demostración en vídeo de este procedimiento, vaya a F5 y encontrarservidor usando MIa utilidad de configuración MAgregar un servidor syslog remoto

MAgregar un servidor syslog remoto usando la utilidad de configuración F5 y encontrarservidor usando MConfigurar Impacto del procedimiento

: Realizar el siguiente procedimiento no debería tener un impacto negativo en su sistema.

: Agregar un servidor syslog remoto*El uso de la utilidad de configuración está disponible en BIG-IP 11.1.0 y versiones posteriores.*

: No hay límite en la cantidad de*Inicie sesión en la utilidad de configuración.**remotos**Vaya a*

Sistema

>**Para**(Opcional) Para **ogs>configuración>Registro remoto**

IP local **IP remota**Introduzca el destino**remotos**dirección IP del servidor o FQDN. (Se requiere configuración del servidor DNS) **Puerto remoto**

IP local Introduzca el puerto UDP del servidor remoto**remotos**(el valor predeterminado es 514).

Introduzca la dirección IP local del sistema BIG-IP**Local IP**, enter the local IP address of the BIG-IP system.

: No hay límite en la cantidad de*Para sistemas BIG-IP en una configuración de alta disponibilidad (HA), se recomienda la dirección IP propia no flotante si se utiliza una dirección IP basada en el microkernel de administración de tráfico (TMM).*

. Seleccionar**Agregar**

. Seleccionar**actualizar**

. Para sistemas BIG-IP en una configuración de alta disponibilidad (HA), realice una ConfigSync para sincronizar los cambios con los demás dispositivos del grupo de dispositivos.

Agregar un único servidor syslog remoto

. Inicie sesión en la consola TMOS (**tmsh**introduciendo el siguiente comando:

msh

ara agregar un único servidor remoto**remotos**utilice la siguiente sintaxis de comando:

modifique /sys syslog remote-servers add { <nombre> { host <dirección IP o FQDN> remote-port <puerto> }}

Por ejemplo, para agregar un servidor remoto**remotos**servidor**172.28.31.40**con el puerto**514**y el nombre**ysyslog**, ingrese el siguiente comando:

modify /sys syslog remote-servers add { mysyslog { host 172.28.31.40 remote-port 514 }}

: No hay límite en la cantidad de: *Si no ingresa un número de puerto, el sistema configura el número de puerto predeterminado,**514**Impacto del procedimiento*

. Para guardar la configuración, ingrese el siguiente comando:

ave /sys config

. Para sistemas BIG-IP en una configuración de alta disponibilidad (HA), realice una ConfigSync para sincronizar los cambios con los demás dispositivos del grupo de dispositivos.

Agregar varios servidores syslog remotos

: No hay límite en la cantidad de: *El tráfico que contiene la misma carga útil se envía a todos los servidores configurados en las**remotos**instrucciones de configuración. El sistema BIG-IP no balancea la carga de datos entre los servidores**remotos**configurados.*

: Agregar un servidor syslog remoto*El uso de la utilidad de configuración está disponible en BIG-IP 11.1.0 y versiones posteriores.*

. Inicie sesión en**tmsh**introduciendo el siguiente comando:

msh

Para agregar varios servidores remotos**remotos**utilice la siguiente sintaxis de comando:

odify /sys syslog remote-servers add { <nombre> { host <dirección IP> puerto-remoto <puerto> } <nombre> { host <dirección IP> puerto-remoto <puerto> }}

Por ejemplo, para agregar un servidor remoto**remotos**servidor**172.28.31.40**con el puerto**514**y nombre **ysyslogA**, así como el servidor remoto**remotos**Configurar **172.28.31.37**con el puerto**514**y el nombre**mysyslogB**ingrese el siguiente comando:

modify /sys syslog remote-servers add { mysyslogA { host 172.28.31.40 remote-port 514 } mysyslogB { host 172.28.31.37 remote-port 514 }}

: No hay límite en la cantidad de: *Si no ingresa un número de puerto, el sistema configura el número de puerto predeterminado,**514**Impacto del procedimiento*

. Para guardar la configuración, ingrese el siguiente comando:

ave /sys config

Para sistemas BIG-IP en una configuración de alta disponibilidad (HA), realice una ConfigSync para sincronizar los cambios con los demás dispositivos del grupo de dispositivos.

Modificar el puerto remoto de un servidor syslog remoto

. Inicie sesión en**tmsh**introduciendo el siguiente comando:

msh

ra configurar un servidor remoto**remotos**para usar un puerto remoto distinto del puerto predeterminado**514**, utilice la siguiente sintaxis de comando:

odify /sys syslog remote-servers modify { <nombre> { remote-port <puerto> }}

Por ejemplo, para modificar el servidor remoto**remotos**servidor**ysyslogB**para usar el puerto**51400**ingrese el siguiente comando:

modify /sys syslog remote-servers modify { mysyslogB { remote-port 51400 }}

. Para guardar la configuración, ingrese el siguiente comando:

ave /sys config

. Para sistemas BIG-IP en una configuración de alta disponibilidad (HA), realice una ConfigSync para sincronizar los cambios con los demás dispositivos del grupo de dispositivos.

Configure la dirección IP local a la que se enlaza syslog para enviar registros al servidor syslog remoto

: Agregar un servidor syslog remoto*El uso de la utilidad de configuración está disponible en BIG-IP 11.1.0 y versiones posteriores.*

. Inicie sesión en**tmsh**introduciendo el siguiente comando:

msh

a configurar la dirección IP a la que BIG-IP**configuraciones de syslog**se enlaza al enviar registros al servidor remoto**configuraciones de syslog**utilice la siguiente sintaxis de comando:

modifique /sys syslog remote-servers modify { <nombre> { ip-local <dirección IP> }}

Por ejemplo, para configurar BIG-IP**remotos**para que se enlace a**172.28.68.42**al enviar registros al servidor remoto**remotos**
Configurar **mysyslogB**ingrese el siguiente comando:

modifique /sys syslog remote-servers modify { mysyslogB { ip-local 172.28.68.42 }}

: No hay límite en la cantidad de: *Para sistemas BIG-IP en una configuración de alta disponibilidad, se recomienda la dirección IP propia no flotante si se utiliza una dirección IP basada en TMM.*

*Para obtener más información, consulte**000135645: Configuración configuraciónurin Mla dirección IP local que s F5 y encontrarservidor usando Mse enlaza en un entorno de alta disponibilidad*

. Para guardar la configuración, ingrese el siguiente comando:

ave /sys config

. Para sistemas BIG-IP en una configuración de alta disponibilidad (HA), realice una ConfigSync para sincronizar los cambios con los demás dispositivos del grupo de dispositivos.

Liste la configuración del servidor syslog remoto

: Agregar un servidor syslog remoto*El uso de la utilidad de configuración está disponible en BIG-IP 11.1.0 y versiones posteriores.*

. Inicie sesión en**tmsh**introduciendo el siguiente comando:

msh

Para listar la configuración de los servidores syslog remotos, ejecute /sys syslog remote-servers

El siguiente es un ejemplo de la salida del comando en un sistema BIG-IP configurado con dos servidores syslog

remotos:**remotos**ys

syslog { remote-servers

mysyslogA 172.28.31.40

host 172.28.31.40

{ }

mysyslogB

IP local 172.28.31.40

{ 172.28.68.42

172.28.31.37 Configure el sistema BIG-IP para registrar en el servidor syslog remoto mediante el protocolo TCP

mysyslogB

mysyslogB

. Para sistemas BIG-IP en una configuración de alta disponibilidad (HA), realice una ConfigSync para sincronizar los cambios con los demás dispositivos del grupo de dispositivos.

. Para registrar en el servidor remoto

: Agregar un servidor syslog remoto*El uso de la utilidad de configuración está disponible en BIG-IP 11.1.0 y versiones posteriores.*

. Inicie sesión en**tmsh**introduciendo el siguiente comando:

msh

mediante el protocolo TCP, utilice la siguiente sintaxis de comando:**remotos**odify /sys syslog include "destination remote_server {tcp(\"<IP del servidor syslog remoto>\" ort (514));};filter f_alllogs {level (debug..emerg);};log

source(s_syslog_pipe);filter(f_alllogs);destination(remote_server);};"

Nota

: No hay límite en la cantidad de*remoto.****Para obtener más información, consulte u****ID 998649*** ***MPor ejemplo, para iniciar sesión en el servidor remoto***

servidor**remotos**servidor**172.28.68.42**ingrese el siguiente comando:

514));};filter f_alllogs {level (debug..emerg);};log {source(s_syslog_pipe);filter(f_alllogs);destination(remote_server);};"

Si se necesitan varios servidores syslog remotos de destino, la sintaxis de "destino" anterior se puede replicar para cada servidor "destino" adicional. Por ejemplo:

modify /sys syslog include "destination remote_server_1 {tcp(\"172.28.68.42\" port

514));};filter f_alllogs {level (debug..emerg);};log {source(s_syslog_pipe);filter(f_alllogs);destination(remote_server_1);};destination

emote_server_2 {tcp(\"172.28.68.43\" port (514));};filter f_alllogs {level debug..emerg);};log

{source(s_syslog_pipe);filter(f_alllogs);destination(remote_server_2);};"

Contenido relacionado

. Para guardar la configuración, ingrese el siguiente comando:

ave /sys config

. Para sistemas BIG-IP en una configuración de alta disponibilidad (HA), realice una ConfigSync para sincronizar los cambios con los demás dispositivos del grupo de dispositivos.

K13284: Descripción general de la administración

g configuraciónK13083: Configuración configuración

urin configuraciónurin Mconfiguración F5 y encontrarservidor usando Ms desde la línea de comandos configuración(11.x - 17.x) .

el nivel de información que s configuraciónurin M-n F5 y encontrarservidor usando configuraciónenvía a lo Marchivos (12.x - 17.x MK5532: Configuración) el nivel de .

información lo configuraciónurin Mgg ed para la gestión del tráficoeventos relacionados con el ement K86480148: Solución de problemas configuraciónproblemas al enviar

Mlo Msyslog al servidor syslog remoto configuraciónservidor F5 y encontrarservidor usando MConfigurar 5 Referencia de TMSHpágina en CloudDocs. Para obtener más

información sobre servidores remotos

yslogconfiguraciones de syslog Guías de administración de la edición de código abierto**configuración F5 y encontrarservidor usando configuraciónenvía a lo M: Este enlace lo lleva a un recurso externo a MyF5, y es posible que el documento se elimine sin nuestro conocimiento.**

: No hay límite en la cantidad de*Contenido recomendado por IA*

Contenido recomendado por IA

000156572: Trimestraly **el puerto remoto de un servidor syslog remotoSecurit el puerto remoto de un servidor syslog remotoNotificación (octubre de 2025)** Política **-4309: Ciclo de vida del producto de hardware de F5 F5 y encontrarsoporte de cle ppolítica de servicio F5 y encontrar** Aviso de seguridad -

000157334: Vulnerabilidad de BIND el puerto remoto de un servidor syslog remotoCVE-2025-40778

Aviso de seguridad - **000157862: Vulnerabilidad de Apache Tomcat el puerto remoto de un servidor syslog remotoCVE-2025-55754**

Los ingenieros de soporte de F5 que trabajan directamente con los clientes escriben artículos de Soluciones de Soporte y Conocimiento, que le brindan acceso inmediato a sugerencias de mitigación, soluciones alternativas o solución de problemas.

↑ **Volver a p** -

Wagner Pa

QUE OFRECEMOS

RECURSOS

OPORTE

SOCIOS

EMPRESA

CONÉCTATE CON NOSOTROS

CONTACTAR CON SOPORTE

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Wagner Pastor

Capítulo del manual : Gestión del tráfico con limitación de velocidad

Aplica a:

Mostrar versiones

Índice | << Capítulo anterior | Capítulo siguiente >>

Gestión del tráfico mediante la limitación de velocidad

Introducción a la configuración de tarifas

El sistema BIG-IP® incluye una función llamada limitación de velocidad. ***Esta función*** permite aplicar una política de rendimiento al tráfico entrante. Las políticas de rendimiento son útiles para priorizar y restringir el ancho de banda en determinados patrones de tráfico.

La gestión de la velocidad de transferencia de datos puede ser útil para un sitio de comercio electrónico con clientes preferenciales. Por ejemplo, el sitio podría ofrecer un mayor ancho de banda a los clientes preferenciales y un menor ancho de banda al resto del tráfico.

La función de modelado de velocidad funciona poniendo en cola los paquetes seleccionados dentro de una clase de velocidad y, a continuación, desencolándolos a la velocidad y en el orden indicados por dicha clase. Una ***clase de velocidad*** es una política de modelado de velocidad que define las limitaciones de rendimiento y un método de programación de paquetes que se aplicará a todo el tráfico gestionado por esa clase.

La configuración de la limitación de velocidad se realiza creando una o más clases de velocidad y asignándolas a un filtro de paquetes o a un servidor virtual. También puede usar la función iRules® para indicar al sistema BIG-IP que aplique una clase de velocidad a una conexión específica.

Puede aplicar una clase de velocidad específicamente al tráfico de un servidor a un cliente o viceversa. Si configura la clase de velocidad para el tráfico que se dirige a un cliente, el sistema BIG-IP no aplicará la política de rendimiento al tráfico destinado al servidor. Del mismo modo, si configura la clase de velocidad para el tráfico que se dirige a un servidor, el sistema BIG-IP no aplicará la política de rendimiento al tráfico destinado al cliente.

Acerca de las clases de tarifas

Una clase de velocidad define las limitaciones de rendimiento y el método de programación de paquetes que el sistema BIG-IP® aplicará a todo el tráfico que gestione dicha clase. Las clases de velocidad se asignan a servidores

virtuales y reglas de filtrado de paquetes, así como mediante iRules® .

Si el mismo tráfico está sujeto a clases de velocidad asignadas desde más de una ubicación, el sistema BIG-IP aplica únicamente la última clase de velocidad asignada. El sistema BIG-IP aplica las clases de velocidad en el siguiente orden:

- La primera clase de velocidad que asigna el sistema BIG-IP proviene de la última regla de filtro de paquetes que coincidió con el tráfico y especificó una clase de velocidad.
- La siguiente clase de velocidad que asigna el sistema BIG-IP proviene del servidor virtual; si el servidor virtual especifica una clase de velocidad, esta anula cualquier clase de velocidad que seleccione el filtro de paquetes.
- La última clase de tarifa asignada proviene de la iRule; si la iRule especifica una clase de tarifa, esta clase de tarifa anula cualquier clase de tarifa seleccionada previamente.

Nota: *Las clases de tarifas no pueden residir en particiones. Por lo tanto, la capacidad de un usuario para crear y administrar clases de tarifas se define por su rol, en lugar de por la asignación de acceso a particiones.*

Puede crear una clase de velocidad mediante la utilidad de configuración de BIG-IP. Una vez creada, debe asignarla a un servidor virtual o a una regla de filtro de paquetes, o bien especificarla desde una iRule.

Nombre de la clase de tasa

El primer ajuste que se configura para una clase de tarifa es su nombre. Los nombres de las clases de tarifa distinguen entre mayúsculas y minúsculas y solo pueden contener letras, números y guiones bajos (_). No se permiten palabras clave reservadas.

Cada clase de tarifa que defina debe tener un nombre único. Esta configuración es obligatoria.

Para especificar un nombre de clase de tarifa, localice el **Name** campo en la pantalla Nueva clase de tarifa y escriba un nombre único para la clase de tarifa.

Tasa base

La configuración **de Velocidad Base** especifica la velocidad de transferencia base permitida para el tráfico que gestiona la clase de velocidad. La suma de las velocidades base de todas las clases de velocidad secundarias asociadas a una clase de velocidad principal, más la velocidad base de la clase de velocidad principal, no puede superar el límite máximo de la clase de velocidad principal. Por este motivo, F5 Networks® recomienda que siempre configure la velocidad base de una clase de velocidad principal en 0 (el valor predeterminado).

Puede especificar la velocidad base en bits por segundo (bps), kilobits por segundo (Kbps), megabits por segundo (Mbps) o gigabits por segundo (Gbps). La unidad predeterminada es bits por segundo. Este ajuste es obligatorio.

Nota: *Estos números son potencias de 10, no potencias de 2.*

Tasa máxima

La configuración **de Velocidad máxima** especifica el límite absoluto de tráfico permitido durante las ráfagas o el préstamo de datos. Puede especificar la velocidad máxima en bits por segundo (bps), kilobits por segundo (Kbps),

megabits por segundo (Mbps) o gigabits por segundo (Gbps). La unidad predeterminada es bits por segundo.

Si la clase tarifaria es una clase tarifaria principal, el valor del límite máximo define la tarifa máxima permitida para la suma de las tarifas base de todas las clases tarifarias secundarias asociadas a la clase tarifaria principal, más la tarifa base de la clase tarifaria principal.

Nota: *Una clase de tasa hija puede tomar prestado del límite máximo de su clase de tasa madre.*

Tamaño de ráfaga

La configuración de Tamaño de ráfaga se utiliza cuando se desea permitir que la velocidad del flujo de tráfico controlado por una clase de velocidad supere la velocidad base. Superar la velocidad base se conoce como ***ráfaga*** . Al configurar una clase de velocidad para permitir ráfagas (especificando un valor distinto de 0), el sistema BIG-IP® guarda el ancho de banda no utilizado y lo emplea posteriormente para permitir que la velocidad del flujo de tráfico supere temporalmente la velocidad base. Especificar un tamaño de ráfaga resulta útil para suavizar patrones de tráfico que tienden a fluctuar o superar la velocidad base, como el tráfico HTTP.

El valor de la configuración **Tamaño de ráfaga** define el número máximo de bytes que se permiten en las ráfagas. Por lo tanto, si se configura el tamaño de ráfaga en 5000 bytes y la tasa de flujo de tráfico supera la tasa base en 1000 bytes por segundo, el sistema BIG-IP permite que el tráfico se transmita en ráfagas durante un máximo de cinco segundos.

Al especificar un tamaño de ráfaga, el sistema BIG-IP crea una reserva de ráfaga de ese tamaño. Esta reserva almacena ancho de banda que el sistema BIG-IP utiliza para ráfagas posteriores. La reserva de ráfaga se agota cuando el flujo de tráfico supera la tasa base y se repone cuando el flujo de tráfico cae por debajo de la tasa base. El valor del tamaño de ráfaga que se configura en una clase de velocidad representa, por lo tanto:

- El número máximo de bytes que transmite la clase de velocidad cuando la tasa de flujo de tráfico supera la tasa base.
- El número máximo de bytes que el sistema BIG-IP puede reponer en el depósito de ráfaga.
- La cantidad de ancho de banda inicialmente disponible para ráfagas más allá de la velocidad base

El tamaño de ráfaga se mide en bytes. Por ejemplo, un valor de 10000 o 10K equivale a 10 000 bytes. El valor predeterminado es 0.

Agotamiento del depósito de reserva.

Cuando la tasa de flujo de tráfico supera la tasa base, el sistema BIG-IP® agota automáticamente el depósito de ráfaga, a una tasa determinada por el número de bytes por segundo en que el flujo de tráfico supera la tasa base.

Continuando con nuestro ejemplo anterior en el que el flujo de tráfico supera la tasa base en 1.000 bytes por segundo, si la tasa de flujo de tráfico solo supera la tasa base durante dos segundos, entonces se consumen 2.000 bytes del tamaño de ráfaga y el máximo de bytes disponibles para ráfagas disminuye a 3.000.

Nota: *En algunos casos, una clase de velocidad puede tomar prestado ancho de banda del depósito de ráfagas de su clase principal.*

Recarga de un depósito averiado

Cuando el flujo de tráfico cae por debajo de la tasa base, el sistema BIG-IP® almacena el ancho de banda no utilizado (es decir, la diferencia entre la tasa base y el flujo de tráfico real) en la reserva de ráfagas. Posteriormente, el sistema BIG-IP utiliza este ancho de banda cuando el flujo de tráfico supera la tasa base. De esta forma, el sistema BIG-IP repone la reserva de ráfagas cada vez que se agota debido a que el flujo de tráfico supera la tasa base.

El tamaño del depósito de ráfaga no puede superar el tamaño de ráfaga especificado. Por este motivo, el sistema BIG-IP repone el depósito con ancho de banda no utilizado solo hasta que alcanza la cantidad especificada en la configuración **de Tamaño de ráfaga** . Así, si el tamaño de ráfaga se establece en 5000, el sistema BIG-IP solo puede almacenar 5000 bytes de ancho de banda no utilizado para su uso posterior cuando la tasa de flujo de tráfico supere la tasa base.

Nota: *Especificar un tamaño de ráfaga no permite que la clase de velocidad exceda su límite máximo.*

Acerca de especificar un tamaño de ráfaga distinto de cero

Este ejemplo ilustra el comportamiento del sistema BIG-IP ® cuando se configura el ajuste **Tamaño de ráfaga** en un valor distinto de 0.

Este ejemplo muestra el rendimiento en bytes por segundo en lugar de bits por segundo (el valor predeterminado). Esto se hace únicamente para simplificar el ejemplo. Para obtener bytes por segundo a partir de bits por segundo, simplemente divida la cantidad de bits por segundo entre 8.

Supongamos que configura los ajustes de la clase de velocidad con estos valores:

- Velocidad base: 1000 bytes por segundo
- Velocidad máxima: 4000 bytes por segundo
- Tamaño de ráfaga: 5.000 bytes

Consideremos el siguiente escenario:

Si el tráfico fluye actualmente a 800 bytes por segundo

No es necesario realizar ráfagas porque la tasa de flujo de tráfico es inferior a la tasa base definida en la clase de tasa. Dado que el tráfico fluye a 200 bytes por segundo menos que la tasa base, el sistema BIG-IP podría añadir potencialmente 200 bytes de ancho de banda no utilizado al depósito de ráfagas. Sin embargo, como aún no se ha producido ninguna ráfaga, el depósito ya está lleno con los 5000 bytes especificados, lo que impide que el sistema BIG-IP almacene los 200 bytes de ancho de banda no utilizado. En este caso, el sistema BIG-IP simplemente descarta el ancho de banda no utilizado.

Si el tráfico aumenta a 1.000 bytes por segundo (igual a la velocidad base)

Todavía no se produce ningún pico de tráfico y no hay ancho de banda sin usar.

Si el tráfico aumenta a 2500 bytes por segundo

Por cada segundo que el tráfico continúa fluyendo a 2500 bytes por segundo, el sistema BIG-IP libera 1500 bytes de la reserva de ráfagas (la diferencia entre la velocidad de flujo de tráfico y la velocidad base). Esto permite poco más de tres segundos de ráfagas a esta velocidad antes de que se agote la reserva de 5000 bytes. Una vez agotada la reserva, el sistema BIG-IP reduce la velocidad de flujo de tráfico a la velocidad base de 1000 bytes por segundo, sin permitir ráfagas.

Si el tráfico vuelve a bajar a 800 bytes por segundo

No es necesario realizar ráfagas, pero ahora el sistema BIG-IP puede añadir los 200 bytes por segundo de ancho de banda no utilizado al depósito de ráfagas, ya que este se encuentra vacío. Si el tráfico continúa fluyendo a 800 bytes por segundo, el depósito de ráfagas se recarga completamente de 0 a 5000 bytes en 25 segundos (a una

velocidad de 200 bytes por segundo). Si el tráfico se detiene por completo, generando 1000 bytes por segundo de ancho de banda no utilizado, el sistema BIG-IP añade 1000 bytes por segundo al depósito de ráfagas, recargándolo así de 0 a 5000 bytes en tan solo 5 segundos.

Acerca de la configuración de la dirección

Mediante la configuración **de Dirección** , puede aplicar una clase de velocidad al tráfico de cliente o servidor. De este modo, puede aplicar una clase de velocidad al tráfico dirigido a un cliente, a un servidor o a ambos. Los valores posibles son **Cualquiera** , **Cliente** y **Servidor** . El valor predeterminado es **Cualquiera** .

Especificar la dirección es útil cuando el tráfico está sesgado hacia una dirección. Por ejemplo, si ofrece un servicio FTP a clientes externos, le interesará más limitar el ancho de banda para los clientes que suben archivos a su sitio que para los que los descargan. En este caso, debería seleccionar «Servidor» como dirección para su clase de velocidad FTP, ya que este valor solo aplica la restricción de ancho de banda al tráfico que va del cliente al servidor.

Acerca de la clase principal

Al crear una clase de tarifa, puede usar la configuración **de Clase Principal** para especificar que la clase de tarifa tiene una clase principal. Esto permite que la clase de tarifa secundaria tome prestado el ancho de banda no utilizado del límite máximo de la clase principal. Una clase secundaria puede tomar prestado el ancho de banda no utilizado del límite máximo de su clase principal, pero una clase principal no puede tomar prestado de una clase secundaria. Tampoco es posible el préstamo entre dos clases secundarias de la misma clase principal ni entre dos clases de tarifa no relacionadas.

Una clase padre puede tener a su vez otra clase padre, siempre que no se cree una dependencia circular. Una ***dependencia circular*** es una relación en la que una clase de tasa es hija de sí misma, directa o indirectamente.

Si una clase de velocidad tiene una clase padre, la clase hija puede tomar ancho de banda no utilizado del límite máximo de la clase padre. El proceso ocurre de la siguiente manera:

- Si la tasa de flujo de tráfico a la que se aplica la clase secundaria supera su tasa base, la clase secundaria comienza a agotar su reserva de ráfaga como se describió anteriormente.
- Si el depósito está vacío (o no se ha definido un tamaño de ráfaga para la clase de velocidad), el sistema BIG-IP® toma el ancho de banda de velocidad base no utilizado del límite superior de la clase principal y se lo da a la clase secundaria.
- Si se agota el ancho de banda no utilizado de la clase padre, la clase hija comienza a utilizar la reserva de la clase padre.
- Si el depósito de la clase padre está vacío (o no se ha definido un tamaño de ráfaga para la clase padre), entonces la clase hija intenta tomar prestado ancho de banda de la clase padre, si la clase padre tiene una clase padre.
- Este proceso continúa hasta que no quede ancho de banda disponible para tomar prestado o no haya un proveedor principal del que tomar prestado.

El préstamo solo permite al niño extender la duración de su ráfaga; la clase del niño no puede exceder el límite máximo bajo ninguna circunstancia.

Nota: *Aunque la descripción anterior utiliza el término "préstamo", el ancho de banda que una clase hija toma prestado no se devuelve posteriormente a la clase padre, ni el ancho de banda no utilizado de una clase hija s*

devuelve a su clase padre.

Sobre la formulación de políticas

Esta configuración especifica una política de modelado que incluye valores personalizados para la política de descarte y el método de cola. El valor predeterminado es Ninguno.

Puede crear políticas de modelado adicionales utilizando el shell de administración de tráfico (tmsh).

Acerca del método de cola

La configuración **del método de cola** determina el método y el orden en que el sistema BIG-IP® extrae los paquetes de la cola ·

Una clase de tasa admite dos métodos de cola:

Cola justa estocástica

El método de colas estocásticas justas (***SFQ***) organiza el tráfico en múltiples listas, seleccionando la lista específica según un hash de la información de conexión que cambia periódicamente. Esto garantiza que el tráfico de la misma conexión siempre se encole en la misma lista. Posteriormente, SFQ extrae el tráfico de las listas de forma rotativa. El resultado es una extracción justa, ya que ninguna conexión de alta velocidad puede monopolizar la cola a expensas de las conexiones más lentas.

Prioridad FIFO

El método de colas ***Priority FIFO*** (***PFIFO***) encola todo el tráfico en cinco listas según el campo Tipo de Servicio (ToS). Cuatro de las listas corresponden a los cuatro valores posibles de ToS (retardo mínimo, rendimiento máximo, fiabilidad máxima y coste mínimo). La quinta lista representa el tráfico sin valor ToS. El método PFIFO procesa estas cinco listas intentando preservar al máximo el significado del campo ToS. Por ejemplo, un paquete con el campo ToS establecido en "Coste mínimo" podría ceder su lugar a un paquete con el campo ToS establecido en "Retardo mínimo".

Acerca de la política de lanzamiento

El sistema BIG-IP® descarta paquetes cuando se supera el límite de velocidad especificado. Una política de descarte especifica cómo desea que el sistema descarte los paquetes. El valor predeterminado es **fred** .

Nota: *No puede usar* ***fred*** *o* ***red*** *si selecciona* ***sfq*** *en la configuración* ***del método de cola*** .

Los valores posibles son:

Fred

Especifica que el sistema utiliza la detección temprana aleatoria basada en flujo para determinar si se deben descartar paquetes, según la agresividad de cada flujo. Si se requiere equidad de flujo en toda la clase de velocidad, seleccione **fred** .

rojo

Especifica que el sistema descarta paquetes aleatoriamente.

cola

Especifica que el sistema descarta el final del flujo de tráfico.

Puede crear políticas de descarte adicionales utilizando el shell de administración de tráfico (tmsh).

Contacta con el servicio
de asistencia

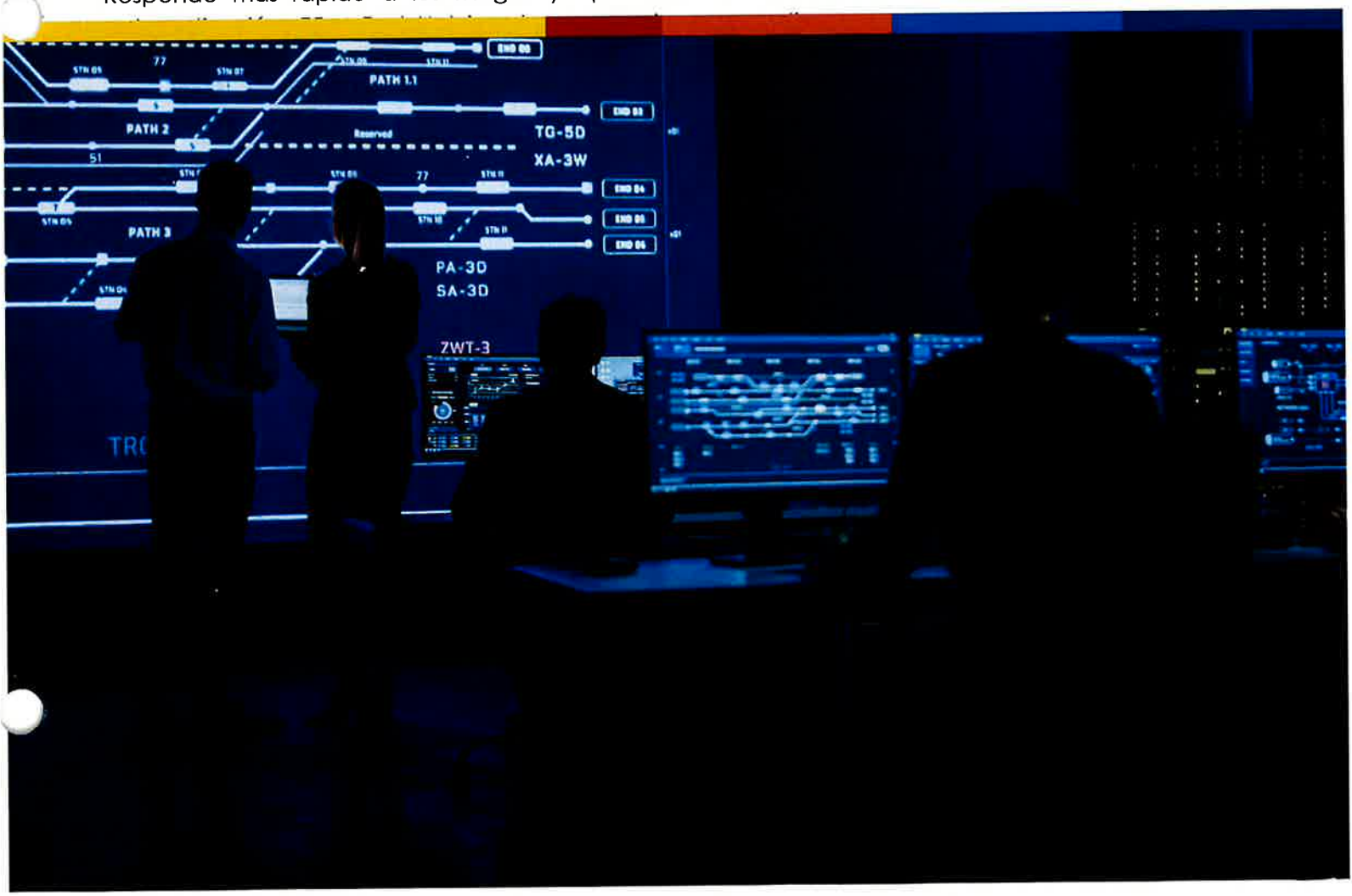
¿TIENES ALGUNA PREGUNTA? Soporte y ventas > **SÍGANOS**

RESUMEN DE LA SOLUCIÓN

Wagner Peña

Automatización y seguridad impulsadas por eventos con F5 y Red Hat

Responde más rápido a los riesgos y optimiza las tareas con



BENEFICIOS CLAVE

Acelerar el tiempo medio hasta la resolución
Implementa cambios instantáneos con automatización para bloquear amenazas de seguridad o evitar cortes las 24 horas.

Mejorar el cumplimiento
Rastrear los cambios de configuración y las versiones de software a través de un Fuente única de verdad para registros y auditorías precisas.

Reducir el riesgo
Prevenir incidentes y mitigar riesgos con manuales y respuestas automáticas que permitan una seguridad proactiva.

Aliviar la presión sobre los recursos . Automatizar tareas básicas para liberar recursos limitados de TI para trabajos de alto valor.

Asegurar políticas coherentes Despliega políticas de forma consistente en todas las nubes, redes o dispositivos para evitar configuraciones erróneas.

El aumento de la complejidad pone de manifiesto la ineficiencia de los procesos manuales

A medida que los entornos de TI se vuelven más avanzados, gestionar las operaciones de red y seguridad requiere recursos significativos. Sin embargo, con una escasez estimada de 3,4 millones de trabajadores de ciberseguridad a nivel mundial1 y el 73% de los CIO preocupados por la pérdida de talento en TI,2 simplemente no hay más recursos disponibles.

Muchos procesos actuales para operaciones de red y seguridad son altamente manuales. Los operadores de red inician sesión en componentes individuales, cambian configuraciones, cierran sesión y repiten en otros dispositivos. Este enfoque manual ralentiza los cambios en la configuración y aumenta el riesgo de pasar por alto componentes durante el proceso de cambio.

Para los equipos de seguridad, la creciente variedad de soluciones de seguridad resulta en un número creciente de alertas que investigar, transformando el proceso de triaje en una tarea que consume mucho tiempo. Además, el creciente volumen de amenazas de seguridad puede abrumar fácilmente a un equipo con falta de personal.

Emplea Ansible Orientado a Eventos para Agilizar las Tareas Rutinarias

La automatización puede acelerar el tiempo medio hasta la resolución de cortes de energía o incidentes de seguridad siguiendo manuales predefinidos que se activan por eventos específicos descubiertos mediante telemetría. Las tareas pueden incluir la aplicación rápida y constante de nuevas configuraciones, la gestión de usuarios o la investigación de actividades sospechosas.

Sin embargo, los equipos de red y seguridad pueden no tener suficiente experiencia con tecnologías de automatización para construir, implementar y mantener los scripts necesarios para operarlas. Los paquetes preconstruidos y validados que incluyen reglas, manuales de juego, roles y complementos para conectar soluciones facilitan el inicio de la automatización. Los equipos también necesitan poder escribir nuevas reglas o configurar integraciones fácilmente según sea necesario.

Las colecciones de contenido de F5 para Red® Hat Event-Driven Ansible están certificadas por Red Hat para garantizar una automatización fiable de soluciones de redes, entrega de aplicaciones y seguridad de F5. Juntos, te ayudan a gestionar tu red, aplicaciones y operaciones de seguridad de forma eficiente.

Automatiza soluciones F5 con Red Hat Ansible orientado a eventos para operaciones proactivas de red y seguridad

Las integraciones totalmente compatibles con la API REST en las Colecciones Ansible de F5 permiten gestionar objetos F5 de forma imperativa. Con la automatización basada en eventos, puedes usar Ansible para generar acciones instantáneas desde F5® BIG-IP® para operaciones de red, aplicación de políticas, políticas de firewall, protección DDoS y más para protección proactiva.

CARACTERÍSTICAS PRINCIPALES

Colecciones de contenido certificado Garantizar una automatización y soporte fiables con un paquete conveniente de módulos, plugins, manuales y documentación creados por F5 y certificados por Red Hat.

Crea un libro de reglas Ansible , conecta las fuentes de eventos con acciones correspondientes para proporcionar instrucciones o incrusta Libros de Juego Ansible usando estructuras similares a YAML familiares.

Lograr una amplia cobertura de seguridad . Actúa de inmediato activando flujos de trabajo avanzados de WAF F5, incluyendo protección DoS conductual, defensa contra bots y seguridad de la API, para mitigar amenazas.

Habilitar la automatización sin agentes Evitar problemas de interoperabilidad transfiriendo instrucciones a través de mecanismos de transporte existentes, como APIs y webhooks.

Cómo funciona

Crea flujos de trabajo de automatización preaprobados que contengan una serie de acciones a realizar en respuesta a un evento. Luego monitoriza tu red o aplicaciones con soluciones como Elasticsearch y Kibana. Cuando se descubre un evento calificativo, se activan las reglas de automatización de Ansible para que BIG-IP ejecute el flujo de trabajo aprobado al instante.

Por ejemplo, si se detecta a un usuario malicioso intentando acceder a una aplicación segura, el monitor de eventos activará las reglas Ansible, que a su vez indicará automáticamente a F5® BIG-IP® Advanced WAF® bloquear al usuario malicioso en tiempo real, permitiendo el acceso a usuarios legítimos.

Casos de uso

La automatización con Red Hat Event-Driven Ansible y BIG-IP está diseñada tanto para operaciones de red como de seguridad. Los usos de NetOps incluyen:

- Configuraciones de red consistentes para estandarizar y hacer cumplir las mejores prácticas
- Gestión del estado operativo para determinar las necesidades de mantenimiento preventivo y reducir los riesgos de cortes
- Cumplimiento y trazabilidad de los cambios de configuración para auditorías precisas

Los casos de uso de automatización de SecOps incluyen:

- Enriquecimiento de investigación mediante la recopilación de información adicional de los registros para reducir los tiempos de triaje
- Búsqueda de amenazas para identificar amenazas más rápido mediante correlación de datos
- Respuesta a incidentes que toma medidas inmediatas para actualizar las políticas de seguridad o bloquear el acceso

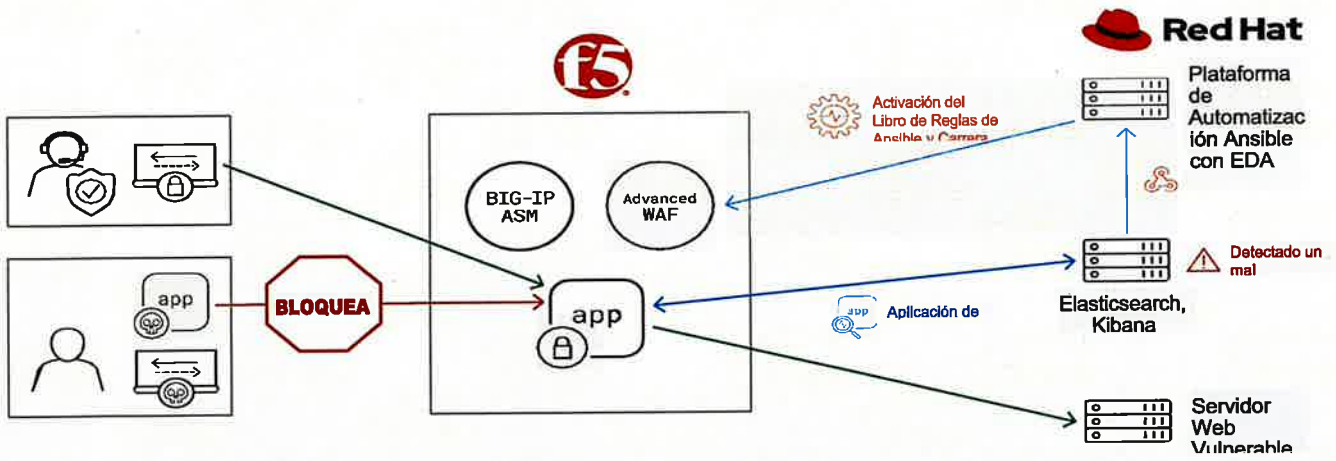


Figura 1: Cuando Elasticsearch y Kibana detectan actividad sospechosa, se activa un Ansible Rulebook para actuar de inmediato usando BIG-IP Advanced WAF para bloquear al usuario malicioso.

Ventajas de F5 BIG-IP y Red Hat Ansible Impulsado por Eventos

Juntos, F5 y Red Hat pueden proteger mejor tu entorno mediante acciones rápidas y automatizadas que mejoran la eficiencia operativa y el cumplimiento, reduciendo el riesgo de seguridad. A su vez, esto reduce la carga de trabajo de los equipos de TI ocupados, permitiéndoles centrarse en tareas de alto valor. A medida que los entornos híbridos se vuelven más complejos, la necesidad de automatización fiable solo aumentará para escalar, optimizar y proteger tu negocio de forma eficiente.

Descubre más sobre la colaboración entre F5 y Red Hat en f5.com/redhat

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Wagner Peña

(ISC)², Estudio de la Fuerza Laboral en Ciberseguridad 2022, junio de 2022.
Gartner, ¿significan los recientes despidos que ha terminado la crisis de talento tecnológico?, marzo de 2023.

Integración del balanceador de carga de la serie F5 BIG-IP y Red Hat OpenShift Container Platform

Actualizado27 de marzo de 2024 a las 7:06 a. m.- Inglés

Los balanceadores de carga de la serie F5 Big-IP Local Traffic Manager (LTM) incluyen dispositivos virtuales/dispositivos programables listos para la nube con rendimiento y velocidades de conexión de Capa 4 y Capa 7. Al ser un estándar de la industria (una solución ampliamente implementada), es natural que los departamentos de TI quieran aprovechar los dispositivos existentes para proporcionar un alto rendimiento a las implementaciones de Kubernetes (OpenShift).

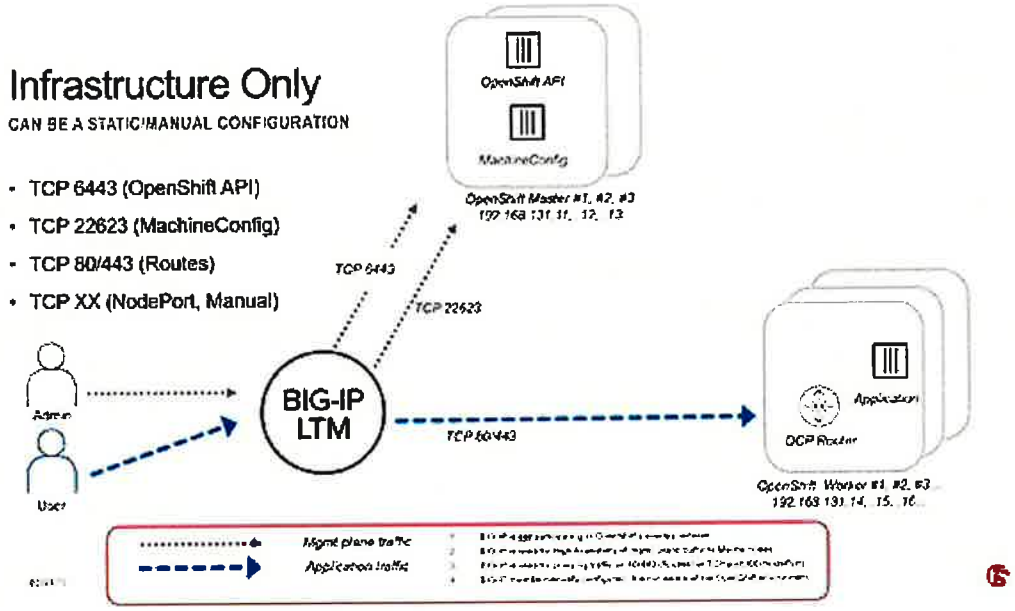
Dado que Red Hat y F5 son socios de mercado que han desarrollado conjuntamente una integración entre nuestros dos productos, es importante que describamos exactamente cómo y de qué manera los clientes pueden y deben aprovechar los dos productos juntos.

A través de esta colaboración, brindamos soporte conjunto para las soluciones que ofrecemos y diseñamos. Para más información, consulte nuestra declaración de soporte de terceros .

- Tanto Red Hat como F5 son socios de soporte de TSANet.

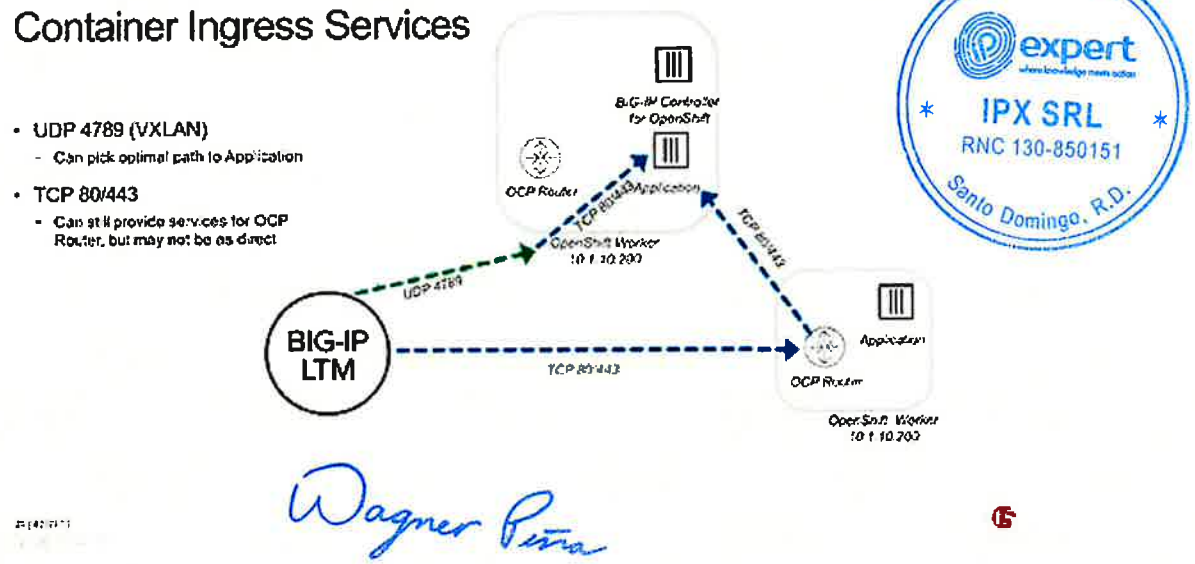
Con la flexibilidad de OpenShift, puede implementar OCP como front-end o reemplazar o ampliar nuestra solución de entrada con una opción de terceros. Esto permite a proveedores como F5 crear una experiencia de integración fluida con OpenShift. F5 se integra con OpenShift de dos maneras clave:

1. F5 BIG-IP Local Traffic Manager (LTM) puede "frontalizar" los servicios principales



- Esto se puede 'configurar'/'instalar' utilizando una plantilla FAST
- Para utilizar esto en el momento de la instalación, debe asegurarse de que su configuración cumpla con los Requisitos del producto OpenShift [1]
- Recomendaciones al utilizar F5 BIG-IP como balanceador de carga externo

2. Servicios de ingreso de contenedores de F5 (CIS): F5 BIG-IP Local Traffic Manager (LTM) como reemplazo del enrutador OpenShift



Wagner Pena

- Consulte la documentación del Servicio de ingreso de contenedores F5 (CIS) para obtener instrucciones de instalación y configuración para comenzar con esta configuración.

1. Requisitos , concéntrese en **la Tabla 3. Balanceador de carga de API** y **la Tabla 5. Registros DNS requeridos** ↩

Producto(s) **Plataforma de contenedores Red Hat OpenShift** **Categoría** **Configurar**

Tipo de artículo **General**

Comentarios

Inicia sesión para ver los comentarios.

Wagner Pena

expert
IPX SRL
RNC 130-850151
Santo Domingo, R.D.

Wagner Piña

IPX SRL
RNC 130-850151
Santo Domingo, R.D.