Resumen de la guía de diseño de la tecnología del IPS y el firewall

Descripción general

Este documento proporciona un resumen de la *Guía de diseño de la tecnología del IPS y el firewall* y los casos de uso clave que cubre.

Los Cisco Validated Designs (CVD) brindan un marco al diseño de sistemas en función de los casos de uso comunes o las prioridades actuales del sistema de ingeniería. Incorporan un amplio grupo de tecnologías, funciones y aplicaciones para abordar las necesidades de los clientes. Los ingenieros de Cisco han probado exhaustivamente y documentado cada CVD a fin de garantizar una implementación más rápida, confiable y predecible.

La guía de diseño de la tecnología ofrece detalles de implementación, información sobre software y productos validados, y mejores prácticas para la implementación del firewall y el IPS. Detalla los siguientes casos de uso:

- Aplicación de políticas de seguridad para el tráfico de red entre la Red interna, las redes de la zona perimetral (DMZ) e Internet.
- Acceso resistente a Internet.
- Detección y bloqueo de ataques entrantes a los servicios de Internet en las DMZ.
- Detección de tráfico malicioso en las Redes internas.

La seguridad del firewall es una parte integral de cada implementación de extremo de Internet, dado que protege la información mientras que satisface la necesidad de redes seguras y confiables, y aplica las políticas a fin de mantener la productividad de los empleados. Donde se aplican las regulaciones de la industria, los firewalls desempeñan una función crucial en la capacidad de las organizaciones para abordar los requisitos de cumplimiento regulatorio. Los requisitos regulatorios varían por país e industria; este documento no cubre requisitos de cumplimiento regulatorio específicos.

Los servicios de Internet se han convertido en una parte clave de las operaciones diarias de muchas organizaciones hoy en día. Brindar un acceso seguro a Internet y evitar el ingreso de contenidos maliciosos a la organización es fundamental para mantener la productividad de los empleados. Además del acceso de los clientes a Internet, las organizaciones tienen la necesidad casi universal de contar con una presencia web disponible para que los partners y clientes accedan a la información sobre la organización. Colocar información corporativa en Internet acarrea el riesgo de exponer los datos a un ataque en los servicios públicos. Para que una organización use Internet eficazmente, se debe encontrar la solución de todos estos problemas.

Alcance

La *Guía de diseño de la tecnología del IPS y el firewall* se centra en los servicios de seguridad del sistema de prevención de intrusiones (IPS) y el firewall de extremo de Internet que protegen la gateway a Internet de su organización. Las opciones de enrutamiento y conectividad del proveedor de servicio de Internet ofrecen resistencia al diseño. Esta guía cubre la creación y el uso de segmentos de DMZ con servicios expuestos a Internet, como una presencia web. La guía del IPS cubre las implementaciones de extremo de Internet en línea y las implementaciones del sistema de detección de intrusiones (IDS) en la capa de distribución interna, también denominadas implementaciones *promiscuas*.

Esta guía cubre las siguientes áreas de tecnología y productos:

- Firewalls de próxima generación Cisco ASA de la serie 5500-X de para la prevención de intrusiones y la seguridad del firewall de extremo de Internet.
- Sensores del IPS de la serie 4300 de Cisco para la prevención de intrusiones en la Red interna.[1]
- Conmutación LAN de red exterior y DMZ.
- Integración de lo expuesto anteriormente a la infraestructura de la conmutación LAN.

Casos de uso de la tecnología

El extremo de Internet es el punto en que la red de la organización se conecta a Internet. Es el perímetro de la red, donde se traza una línea entre los recursos de Internet pública y privada contenidos en la red de la organización. Las infiltraciones de gusanos, virus y redes robot suponen amenazas sustanciales para el rendimiento de la red, la disponibilidad y la seguridad de los datos. Para agravar estos problemas, la conexión a Internet de una organización puede contribuir a la pérdida de productividad de los empleados y a la fuga de datos confidenciales.

Los atacantes basados en Internet son una amenaza para las infraestructuras y los recursos de datos de la red de la organización. La mayoría de las redes conectadas a Internet está sujeta al bombardeo constante de gusanos, virus y ataques específicos. Las organizaciones deben proteger vigilantemente la red, los datos de los usuarios y la información de los clientes. Además, la mayoría de las direcciones de red debe traducirse a direcciones enrutadas a Internet y el firewall es la ubicación lógica para esta función.

La seguridad de la red, aplicada en el firewall, debe garantizar la protección de los recursos de datos de la organización contra la intromisión y la manipulación, y debe evitar que los gusanos, los virus y las redes robot que consumen recursos comprometan los hosts. Asimismo, la política de firewall debe establecer un equilibrio adecuado para brindar seguridad sin interferir en el acceso a las aplicaciones basadas en Internet ni obstaculizar la conectividad de los datos de los partners empresariales a través de conexiones VPN en la extranet.

[1] Tenga en cuenta que Cisco ha agregado opciones de IPS adicionales a su cartera desde la compleción de esta guía, incluidos un IPS de firewall de próxima generación integrado y un IPS de Sourcefire de próxima generación.

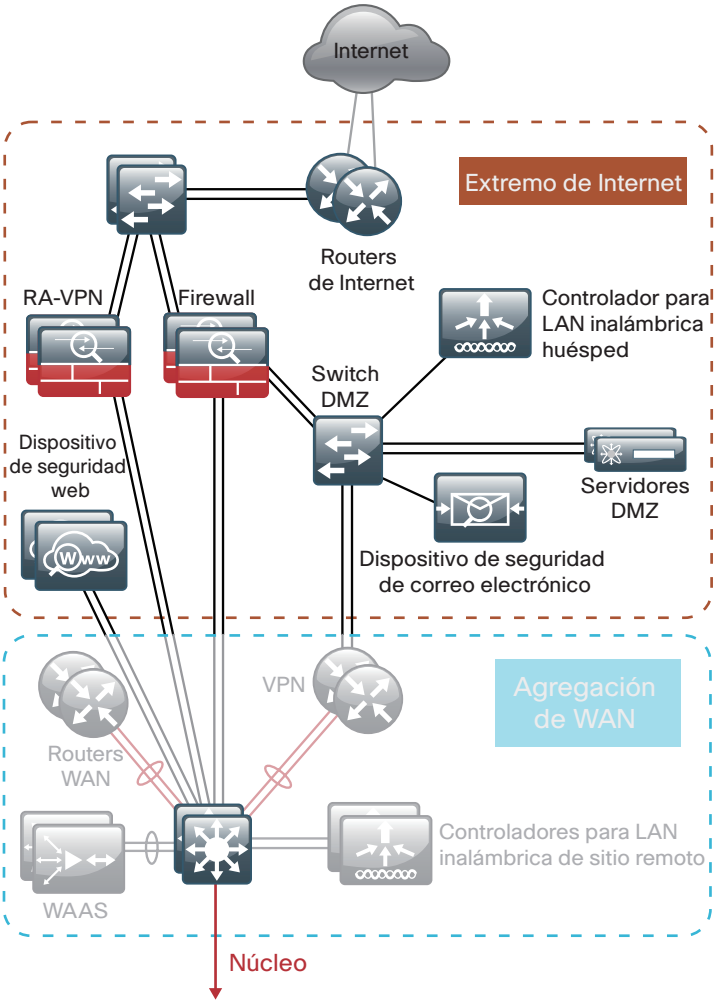
Escenarios de casos de uso

Caso de uso: aplicación de políticas de seguridad para el tráfico de red entre la Red interna, las redes de DMZ e Internet

Las redes de sitios remotos y sedes centrales son zonas internas e Internet se considera una zona externa. Las redes de la zona perimetral (DMZ) configuradas para otros servicios en el extremo de Internet se sitúan en un punto intermedio entre la clasificación interna y externa.

Esta guía de diseño permite las siguientes capacidades de seguridad:

- **Ocultar direcciones de Red interna mediante el uso de la traducción de direcciones de red (NAT)**: la mayoría de las organizaciones usa direcciones privadas (RFC 1918) no enrutadas a Internet, por lo que el firewall debe traducir las direcciones privadas a direcciones externas enrutadas a Internet.
- **Permitir el acceso a la Red interna a Internet**: todo el tráfico de la zona interna, excepto las categorías específicas explícitamente denegadas, se dirige a Internet. El firewall inspecciona cada sesión y permite implícitamente la remisión del tráfico de retorno asociado a la zona interna.
- **Permitir el acceso a la Red interna a las redes de DMZ**: todo el tráfico de la zona interna, excepto las categorías específicas explícitamente denegadas, se dirige a las redes de DMZ. El firewall inspecciona cada sesión y permite implícitamente la remisión del tráfico de retorno asociado a la zona interna.
- **Permitir el acceso de Internet a las redes de DMZ**: solo se dirigen tipos de tráfico específicos de Internet explícitamente permitidos a las redes de DMZ. El firewall inspecciona cada sesión y permite implícitamente la remisión del tráfico de retorno asociado a Internet.
- **Bloquear todo el tráfico restante**: todos los demás tipos de tráfico se bloquean implícitamente.



Caso de uso: acceso resistente a Internet

Una red de extremo de Internet bien diseñada debe tolerar los tipos de fallas observados más comunes. Este tipo de resistencia puede lograrse con un diseño de sitio único que incluya solo dos firewall con enrutamiento predeterminado estático a Internet.

Esta guía de diseño permite las siguientes capacidades de red:

- En el caso de que falle el hardware, conmutación por error con estado entre unidades activas y auxiliares de los dos firewall resistentes.
- Reenrutamiento automático del tráfico de Internet del ISP primario al ISP secundario mediante sondas activas de monitoreo que simulan el tráfico de los usuarios en Internet.

Caso de uso: detección y bloqueo de ataques entrantes a los servicios de Internet en la DMZ

Monitorear y bloquear los ataques basados en la red con un IPS mejora la confiabilidad y el rendimiento de la presencia web de una organización y mantiene la disponibilidad de los recursos para los partners y clientes.

Esta guía de diseño permite las siguientes capacidades de seguridad:

- **Migración y detección basadas en la red**: el IPS implementa la inspección profunda de paquetes de tráfico de red para conciliar firmas de ataques conocidas y bloquear el tráfico malicioso.
- **Filtros de reputación**: el IPS determina si la fuente de un ataque está asociada a grupos peligrosos conocidos.
- **Protección contra amenazas del día cero**: el IPS aprende el comportamiento normal de la red y alerta cuando detecta actividades anómalas.

Caso de uso: detección de tráfico malicioso en las Redes internas

Monitorear y detectar gusanos, virus y otros tipos de software malicioso con un IPS usado para detectar las intrusiones es fundamental para mantener una red de alto rendimiento.

Esta guía de diseño permite las siguientes capacidades de seguridad:

- **Detección y alertas basadas en la red**: el IPS implementa la inspección profunda de paquetes de tráfico de red para conciliar firmas de ataques conocidas y además generar alertas de tráfico malicioso.
- **Filtros de reputación**: el IPS determina si la fuente de un ataque está asociada a grupos peligrosos conocidos.
- **Protección contra amenazas del día cero**: el IPS aprende el comportamiento normal de la red y alerta cuando detecta actividades anómalas.

Descripción general del diseño

La *Guía de diseño del IPS y el firewall* es un componente del diseño mayor del extremo de Internet, que utiliza un modelo de diseño modular para dividir el perímetro de Internet en bloques funcionales por servicio. Al modularizar el diseño, una organización puede implementar los servicios según lo requiera.

El diseño del extremo de Internet incluye los siguientes bloques funcionales:

- **Firewall**: controla el acceso a diferentes segmentos del extremo de Internet y hacia este, y proporciona un conjunto de otros servicios, como la traducción de direcciones de red (NAT) y la creación de DMZ.
- **Prevención de intrusiones**: inspecciona el tráfico que atraviesa el extremo de Internet y busca comportamientos maliciosos.
- **VPN de acceso remoto**: brinda un acceso uniforme y seguro a los recursos, independientemente de dónde se encuentra el usuario cuando se conecta.
- **Seguridad de correo electrónico**: proporciona un servicio de filtrado de correo no deseado y software malicioso para administrar el riesgo asociado con el correo electrónico.
- **Seguridad web**: brinda monitoreo y control de uso aceptable mientras administra el creciente riesgo asociado a los clientes que navegan por Internet.

Las principales diferencias entre las opciones de diseño del módulo son la escalabilidad, el rendimiento y la resistencia. A fin de satisfacer estos requisitos, cada módulo del diseño de extremo de Internet es independiente de otros, de manera que pueda combinar y conciliar los diferentes componentes del diseño para cumplir mejor con los requisitos empresariales.

Haga clic aquí para obtener la *Guía de diseño de la tecnología del IPS y el firewall completa de 106 páginas* en inglés.

Lectura relacionada

La *Guía de diseño de VPN de acceso remoto* y la *Guía de diseño de acceso móvil remoto* se centran en abastecer la red a fin de proporcionar servicios de acceso remoto (RA). Las implementaciones incluyen el acceso a VPN como parte de los firewalls de extremo de Internet, así como la capacidad de implementar servicios de VPN de RA en dispositivos dedicados independientes.

La *Guía de diseño de WSA de Cisco con seguridad web* cubre la implementación de Cisco Web Security Appliance para clientes con acceso a Internet. Esta cubre la protección contra software malicioso y virus, así como los controles de uso aceptable para los sitios apropiados para visitar.

La *Guía de diseño de ASA de Cisco con seguridad web en la nube* cubre la implementación de la seguridad web en la nube de Cisco para clientes con acceso a Internet. Esta cubre la protección contra software malicioso y virus, así como los controles de uso aceptable para los sitios apropiados para visitar.

La *Guía de diseño de ESA de Cisco con seguridad de correo electrónico* cubre la implementación del dispositivo de seguridad de correo electrónico de Cisco a fin de ofrecer protección para los sistemas de correo electrónico de la organización. La inspección de los correos electrónicos entrantes en busca de correos electrónicos no deseados y contenidos maliciosos es el centro de la implementación. También cubre la adición de una zona perimetral (DMZ) de correo electrónico en el firewall de Internet para incrementar la seguridad general.

C07-730895-00 02/14