Guía rápida

Ventajas

- **Protección de nivel superior frente a amenazas** con la misma tecnología de seguridad líder en el sector que se encuentra en los firewalls de última generación más grandes de Cisco®
- **Tamaño apropiado y precio asequible** para los presupuestos de las pequeñas y medianas empresas, incluido un bajo coste total de propiedad
- **Administración simplificada en el propio dispositivo** o administración centralizada opcional para las instalaciones de múltiples dispositivos

Cisco ASA con FirePOWER Services

Seguridad avanzada para pequeñas y medianas empresas y empresas descentralizadas

Las organizaciones, independientemente de su tamaño, se enfrentan a amenazas cada vez más costosas que ponen en peligro los datos de los clientes, los secretos empresariales y la propiedad intelectual. La encuesta **2013 Information Security Breaches Survey**, encargada por el gobierno del Reino Unido, desveló que el 87% de las pequeñas empresas estuvieron en situación de riesgo a lo largo de 2012. Por su parte, las grandes organizaciones desean aumentar su seguridad y presionan a sus socios como, por ejemplo, los bufetes de abogados que trabajan para ellas, para que mejoren sus propias tecnologías de protección para reducir el riesgo de convertirse en un vector de amenazas.

Las pequeñas y medianas empresas y las empresas descentralizadas tienen una gran necesidad de protección frente a amenazas avanzadas. Hasta ahora, sin embargo, han obtenido resultados poco satisfactorios con los productos de gestión unificada de amenazas (UTM) y los firewalls de última generación (NGFW) de la competencia. En contraposición a estos enfoques anticuados, los NGFW de Cisco cuentan con protección frente a malware avanzado (AMP) e IPS de última generación (NGIPS). Los modelos más recientes que se han incorporado a la familia de NGFW Cisco® ASA con FirePOWER™ Services están diseñados específicamente para las aplicaciones en las pequeñas y medianas empresas (PYMES) y las sucursales, y ofrecen defensa integrada frente a amenazas, bajos costes de adquisición y de operación, y gestión simplificada de la seguridad.

La solución está disponible en formato de escritorio (5506-X) y de 1RU (5508-X, 5516-X). Las variantes del modelo de escritorio están disponibles con un punto de acceso inalámbrico integrado (5506W-X) para simplificar la gestión de redes para las PYMES.

Existe también un dispositivo reforzado (5506H-X) diseñado específicamente para los sistemas de control industriales y las aplicaciones más importantes de las infraestructuras. Cuenta con un amplio rango de temperatura de funcionamiento y está disponible para su implementación en escritorio, en raíl DIN[1], en rack o en la pared.

Valor superior. Excelente protección frente a amenazas. Opciones de administración flexibles.

Las soluciones de firewall de última generación de Cisco ofrecen un valor superior y funciones de protección frente a amenazas, como firewall, control de aplicaciones, NGIPS, filtrado de URL, protección frente a malware avanzado (AMP) de Cisco y VPN. Gracias a su excepcional visibilidad y capacidad de control y a la priorización automática de las amenazas, las alertas de falsos positivos que, de otro modo, saturarían al personal, se pueden gestionar de manera eficiente.

[1] Raíl DIN: El término deriva de las especificaciones originales publicadas por el Deutsches Institut für Normung (DIN) de Alemania, que se han adoptado desde entonces como normas europeas (EN) e internacionales (ISO).

Puntos de prueba

- En el estudio Worldwide Quarterly Security Appliance Track Study 2014 de IDC, se cita al Cisco ASA como el firewall más implementado del mundo.
- El cliente VPN AnyConnect de Cisco es el cliente VPN líder a nivel mundial, con más de 100 millones de implementaciones, y es totalmente compatible con Cisco ASA con FirePOWER Services.
- Cisco ASA con FirePOWER Services utiliza fuentes de información sobre amenazas diarias de Cisco Security Intelligence para proporcionar funciones que permiten detectar amenazas justo a tiempo.

Características

Cisco ASA 5506-X, 5506W-X, 5506H-X, 5508-X y 5516-X con FirePOWER Services

Capacidad de usuarios/nodos	Ilimitada de manera predeterminada
Formato de escritorio (5506-X, 5506W-X)	7,92" x 8,92" x 1,73"
Formato de montaje en rack (5508-X, 5516-X)	17,2" x 11,288" x 1,72"
Formato reforzado (5506H-X)	9,05" x 9,05" x 2,72"
Puertos integrados de E/S	8 x 1 GE

VPN

Puntos de VPN	Entre 50 y 300
Compatibilidad con movilidad	AnyConnect 4.x; clientes nativos de Android y Apple iOS

Velocidad

Max. stateful firewall	750 Mbps –1,8 Gbps
AVC máximo	250 – 850 Mbps
AVC y NGIPS máximo	125 – 600 Mbps
Alta disponibilidad	Sí: modo activo/en espera* activo/activo (solo 5508-X y 5516-X)

Funciones de NGFW

AVC	Incluido con SmartNet
Aplicaciones admitidas	Más de 3000
Filtrado de URL	Suscripción
Categorías; Total	+ de 80; + de 280 millones
NGIPS	Suscripción
Firmas	+ de 6000
AMP – Defensa frente a amenazas	Suscripción

Gestión

Gestión integrada	Incluida por defecto
Gestión centralizada	Licencia opcional

*Se necesita una licencia Security Plus

Para conocer las especificaciones técnicas adicionales, consulte la hoja de datos de ASA con FirePOWER Services.

Estas soluciones de seguridad de Cisco también aceleran el tiempo de respuesta ante incidentes; incluso hay clientes que han informado de que a menudo se ha reducido de semanas a horas el tiempo necesario para la remediación.

Aunque estos modelos de NGFW de Cisco están diseñados específicamente para PYMES y organizaciones de tamaño medio, proporcionan las mismas tecnologías de nivel superior de protección frente a amenazas que otros firewalls de última generación ASA de Cisco serie 5500-X, que incluyen los modelos 5525-X y 5585-X, que han obtenido la calificación más alta en cuanto a eficacia en materia de seguridad en el informe **Next-Generation Firewall Security Value Map 2014** de NSS Labs. Estos NGFW de Cisco incluyen administración integrada en el propio dispositivo en aquellas situaciones en las que solo se instala un equipo, y cuentan con administración centralizada mediante Cisco FireSIGHT Management System, si así se requiere.

Funciones estándar de Cisco ASA con FirePOWER Services

- **Visibilidad y control granular de las aplicaciones (AVC) de Cisco:** Cisco AVC es compatible con más de 3000 controles del nivel de aplicación y basados en los riesgos. Por ejemplo, puede hacer que aplicaciones más conocidas de redes sociales sean de solo lectura para permitir el cumplimiento de normativas, como la Financial Industry Regulatory Authority (FINRA) y la Health Insurance Portability and Accountability Act (HIPAA), así como para aplicar las políticas de uso aceptable.
- **Firewall de red y compatibilidad con VPN tradicional de sitio a sitio y de acceso remoto líderes en el sector:** Cisco ofrece el firewall y la VPN más fiables e implementados del mundo. El cliente opcional de VPN AnyConnect® de Cisco se puede integrar fácilmente con Cisco ASA con FirePOWER Services. Cisco AnyConnect 4.0 ofrece VPN granular siempre activo en el nivel de aplicación. Además, Cisco ASA es compatible con el cliente Cisco AnyConnect Mobile y los clientes VPN nativos de Android y iOS.

Opciones de suscripción de Cisco FirePOWER Services

- **NGIPS** ofrece una información contextual líder en el sector, visibilidad completa y control para usuarios, dispositivos, aplicaciones y contenido, así como prevención de amenazas líder en el sector.
- **AMP** proporciona capacidad de detección, análisis, detención y, si es necesario, remediación de malware y de amenazas emergentes que han pasado desapercibidas para las otras capas de seguridad. Todas estas funciones que son líderes en el sector.
- **El filtrado de URL basado en la reputación** bloquea las direcciones web de alto riesgo. El spam, los virus basados en URL, los ataques de suplantación de identidad y el spyware pueden redirigir a los usuarios a URL maliciosas. Cisco analiza de manera precisa las URL y asigna una puntuación de reputación a cada una de ellas, lo que permite a los usuarios evitar las direcciones web de alto riesgo.

Siguientes pasos

Comience poniéndose en contacto con un partner de Cisco de su región: Encuentre un partner de Cisco.

C45-733830-01 03/15