IBM Security Network Intrusion Prevention System

Protecting the network Ahead of the threat®

Aspectos principales

- Detiene amenazas antes del impacto sin sacrificar el desempeño de la red de alta velocidad
- Proporciona una plataforma de seguridad convergente que ayude a reducir costos de implementación y gestione soluciones puntuales
- Protege de amenazas maliciosas las redes, servidores, desktops y aplicativos de generación de ingresos

Bloqueo de amenazas en la red con seguridad convergente

IBM Security Network Intrusion Prevention System (IPS) está diseñado para detener amenazas de internet antes que impacten su negocio. La protección preventiva - protección que trabaja antes de la amenaza – está disponible en IBM a través de su combinación patentada de velocidad de la línea de desempeño, inteligencia de seguridad y un motor de protección modular que permite la convergencia de la seguridad. A través de la consolidación de las demandas de redes de seguridad para seguridad de datos y protección de aplicativos web, IBM Security Network IPS sirve como una plataforma de seguridad que reduce los costos y la complejidad de la implementación y gestión de soluciones puntuales.

Al evaluar tecnologías de prevención de intrusión los negocios generalmente tienen dificultad para equilibrar y optimizar las siguientes 6 áreas:

- *Desempeño*
- *Seguridad*
- *Fiabilidad*
- *Implementación*
- *Gestión*
- *Confianza*

IBM Security Network IPS cumple con estos seis aspectos con desempeño, protección preventiva, alta disponibilidad, implementación sencilla y gestión, así como excelente apoyo al cliente. Las organizaciones que desean transferir la carga de la protección de su red a un socio de confianza pueden confiar en IBM para que maneje sus productos. Los clientes IBM también se benefician de una serie de servicios de consultoría complementares para evaluación, diseño, implementación, gestión y educación.

Entregando desempeño superior y protección

La seguridad debe mejorar el desempeño de la red, no comprometerla. Las soluciones específicas de IBM para seguridad de redes ofrecen alta tasa de transferencia, baja latencia y rápido tiempo de funcionamiento para mantener eficientes las operaciones de red. Esto incluye las siguientes características de desempeño:

- *Un amplio espectro de soluciones de alto rendimiento que pueden llegar a 8 Gbps de protección con un dispositivo y a 40 Gbps con sistema de tarjetas blade*
- *Inspección inteligente profunda de paquetes usado la tecnología FlowSmart*
- *Latencia limitada*
- *Flujo de tráfico en el caso de errores del sistema o pérdida de energía*

Consolidando redes de seguridad con protección preventiva

Con su arquitectura modular de producto, IBM Security Network IPS transporta seguridad convergente añadiendo módulos de protección completamente nuevos al paso que la amenaza evoluciona. Desde gusanos informáticos hasta botnets pasando a la seguridad de aplicativos, IBM Security Network IPS proporciona la protección necesaria para la continuidad de su negocio, seguridad de datos y cumplimiento.

El equipo de investigación y desarrollo IBM X-Force® diseñó el módulo de análisis de protocolo y proporciona las actualizaciones de contenido para un mantenimiento preventivo de la protección contra amenazas. X-Force también diseñó los módulos de protección que incluyen:

- *Tecnología IBM Virtual Patch®- Blindaje contra vulnerabilidades desde la explotación, independiente de un programa parche.*
- *Aplicación de protección del cliente- Protege al usuario final de ataques dirigidos a aplicativos usados diariamente como archivos de Microsoft Office, Adobe, multimedia y navegadores web.*
- *Protección de Red avanzada – Prevención avanzada de intrusión incluyendo protección DNS.*

Tecnología Modular de Análisis de Protocolo IBM

La tecnología modular de análisis de protocolo IBM (IBM Protocol Analysis Modular Technology - PAM) proporciona seguridad convergente para entregar protección de red que va más allá del tradicional IPS incluyendo ahora aplicativos de protección para el cliente, seguridad de datos, protección para aplicativos web y control de aplicativos.

- *Seguridad de datos - Vigilancia e identificación de información personal identificable no cifrada (PII) y otros datos confidenciales.*
- *Seguridad de aplicativos web – Protección para aplicativos web 2.0 y bases de datos (misma protección utilizada en el Firewall para aplicativos web).*
- *Control de aplicativos – Recuperación de ancho de banda y bloqueo de Skype, redes punto a punto y tunneling.*

Estos módulos potencializan IBM Security Network IPS para proteger a las redes de categorías de ataques y amenazas, incluyendo:

- *Gusanos informáticos*
- *Programas espías*
- *Punto a punto (P2P)*
- *Ataque de denegación de servicio (DoS) y ataque de denegación de servicio distribuido (DDoS)*
- *Botnets*
- *Ataques dirigidos contra aplicativos web*
- *Datos sensibles o de propiedad dejando la red*
- *Agujero de seguridad XSS (Cross-site scripting)*
- *Inyección SQL*
- *Desbordamiento de buffer*
- *Escalado de directorios web*

El equipo de investigación y desarrollo IBM X-Force® rastrea niveles de amenaza en el internet alrededor del mundo desde su sede de operaciones para Amenazas Globales a fin de intensificar la protección inherente en IBM Security Network IPS.

Entregando Fiabilidad

Los dispositivos localizados en el flujo de tráfico de la red deben ser extremamente confiables. Nuestro IBM Security Network IPS ofrece alta disponibilidad (activo/activo o activo/pasivo), fuentes de alimentación redundantes con cambio en caliente y discos duros redundantes con cambio en caliente, para ayudar a mantener el flujo del tráfico de la red. Adicionalmente, nuestra opción de alta disponibilidad geográfica puede usar el puerto de gestión para compartir decisiones de bloqueo en cuarentena a fin de asegurar conmutación por error en un dispositivo de sistema de prevención de intrusión remoto en espera.

Proporcionando facilidad de Implementación

IBM Security Network IPS ofrece la arquitectura de 2 capas que no requiere reconfiguración de la red. Adicionalmente, los administradores de red y seguridad sentirán familiaridad y comodidad con el comportamiento de los dispositivos escogiendo uno de los tres siguientes modos de operación:

- *Protección activa (modo de prevención de intrusión)*
- *Detección pasiva (modo de prevención de intrusión)*
- *Simulación en línea (prevención de simulación en línea)*

Del mismo modo, con nuestra nueva y mejorada gestión local de interfaz, la gestión de configuración de políticas básicas ahora toma 30% menos de tiempo en la liberación de recursos para tareas de misiones críticas.

Además, al iniciar con Firmware 4.1 IBM Security Network IPS proporciona gestión administrativa de IPv6 del aplicativo, exhibe eventos IPv6 y ofrece la posibilidad de exhibir la dirección IP fuente y destino del IPv6.

Centralizando la gestión de seguridad

IBM Security Network IPS es gestionado centralmente por el sistema de gestión de seguridad IBM SiteProtector™ .SiteProtector provee configuración simple y potente y control de agentes IBM, junto con fuerte generación de informes, correlación de eventos y alerta global.

Ganando su confianza con experiencia en seguridad y apoyo

IBM es el líder en detección y prevención de intrusión con un registro establecido de soporte al cliente. IBM fue una de las primeras industrias a recibir el Certificado del Centro de Practicas de Apoyo Global (Global Support Center Practices - SCP) y es miembro de la junta asesora de la Asociación de Servicio y Apoyo Profesional (Service & Support Professionals Association - SSPA).

¿Por qué IBM?

IBM comprende las amenazas a su red y el balance crítico entre desempeño y protección. Por lo tanto, IBM ha permitido que su tecnología de seguridad de vulnerabilidad de ámbito global detenga amenazas de internet antes de que ataquen su negocio. Con el IBM Security Network IPS usted se beneficia de una solución altamente efectiva y rentable que le proporciona:

- *Protección preventiva respaldada por el equipo de investigación y desarrollo IBM X-Force*
- *Tecnología líder de seguridad, incluyendo el modulo de análisis de protocolo (PAM) para inspección profunda de paquetes*
- *Alto rendimiento que le ayuda a mantener la disponibilidad de su red.*
- *De fácil instalación, configuración y mantenimiento.*

Protección preventiva para su red

Con una línea completa de modelos de alto rendimiento, el IBM Security Network IPS IBM está diseñado para entregar protección inflexible para cada camada de la red, protegiendo sus negocios de amenazas tanto internas como externas.

Especificaciones Técnicas						
Modelo	**GX4004-V2-200**	**GX4004-V2**	**GX5008-V2**	**GX5108-V2**	**GX5208-V2**	**GX6116**
Características de Funcionamiento[1]						
Tasa Transferencia Insp.	Hasta 200 Mbps	Hasta 800 Mbps	Hasta 1.5 Gbps	Hasta 2.5 Gbps	Hasta 4 Gbps	Hasta 8 Gbps
Latencia promedio	<200 Microsegundos	<200 Microsegundos	<200 Microsegundos	<200 Microsegundos	<200 Microsegundos	<150 Microsegundos
Conexiones por segundo	35,000	35,000	37,000	40,000	50,000	296,000
Sesiones simultaneas (máximo nominal)	1,300,000	1,300,000	1,500,000	1,700,000	2,200,000	5,000,000
Gestión de IPv6	**Si**	**Si**	**Si**	**Si**	**Si**	**Si**
Protección de IPv6 y Generación de Informes	**Si**	**Si**	**Si**	**Si**	**Si**	**Si**
Características Físicas						
Factor de forma	1 unidad rack	1 unidad rack	2 unidades rack	2 unidades rack	2 unidades rack	2 unidades rack
Dimensiones						
Altura (in/mm)	1.75/44	1.75/44	3.5/88	3.5/88	3.5/88	3.5/88
Anchura (in/mm)	16.9/429	16.9/429	16.9/429	16.9/429	16.9/429	16.9/429
Profundidad (in/mm)	15.5/394	15.5/394	21.5/546	21.5/546	21.5/546	21.5/546
Peso (lb/kg)	24.5/11.1	24.5/11.1	40.0/18	40.0/18	40.0/18	37.5/17
Interfaz de Gestión	10/100/1,000 (Soporta IPv6)	10/100/1,000 (Soporta IPv6)	10/100/1,000 (Soporta IPv6)	10/100/1,000 (Soporta IPv6)	10/100/1,000 (Soporta IPv6)	10/100/1,000 (Soporta IPv6)
Interfaces de Monitoreo	4x10/100/1,000 solo copper	4x10/100/1,000 solo copper	8x10/100/1,000 copper o 8x SFP/ mini puertos GBIC (1,000 TX/SX/LX)	8x10/100/1,000 copper o 8x SFP/ mini puertos GBIC (1,000 TX/SX/LX)	8x10/100/1,000 copper o 8x SFP/ mini puertos GBIC (1,000 TX/SX/LX)	16x SFP/ minipuertos GBIC (1,000 TX/SX/LX)
Segmentos protegidos en línea	2 segmentos de red	2 segmentos de red	4 segmentos de red	4 segmentos de red	4 segmentos de red	8 segmentos de red
Fuentes de alimentación redundantes	No	No	Si	Si	Si	Si
Almacenamiento redundante	No	No	Si	Si	Si	Si

Especificaciones Técnicas						
Modelo	**GX4004-V2-200**	**GX4004-V2**	**GX5008-V2**	**GX5108-V2**	**GX5208-V2**	**GX6116**
Alta disponibilidad	Activo-activo: no; Activo-pasivo: no; Bypass de nivel de Hardware: bypass integrado	Activo-activo: no; Activo-pasivo: no; Bypass de nivel de Hardware: bypass integrado	Activo-activo: si; Activo-pasivo: si; HA Geo-disperso: si; Bypass de nivel de Hardware: by-pass externo (opc.)	Activo-activo: si; Activo-pasivo: si; HA Geo-disperso: yes; Bypass de nivel de Hardware: by-pass externo (opc.)	Activo-activo: si; Activo-pasivo: si; HA Geo-disperso: yes; Bypass de nivel de Hardware: by-pass externo (opc.)	Activo-activo: si; Activo-pasivo: si; HA Geo-disperso: si; Bypass de nivel de Hardware: bypass externo (opcional)
Parámetros Eléctricos y Ambientales						
Voltaje:	100/240 V ac	100/240 V ac	100/240 V ac	100/240 V ac	100/240 V ac	100/240 V ac
Rango de Entrada:	100 - 240 V a 50/60 Hz, rango completo	100 - 240 V a 50/60 Hz, rango completo	100 - 240 V a 50/60 Hz, rango completo	100 - 240 V a 50/60 Hz, rango completo	100 - 240 V a 50/60 Hz, rango completo	100 - 240 V a 50/60 Hz, rango completo
KVA:	0.141 KW	0.141 KW	0.389 KW	0.389 KW	0.389 KW	0.377 KW
Calor:	0.481 kBTU/hr	0.481 kBTU/hr	1.328 kBTU/hr	1.328 kBTU/hr	1.328 kBTU/hr	1.287 kBTU/hr
Temperatura de operación:	0° a 40° C (32° a 104° F)	0° a 40° C (32° a 104° F)	0° a 40° C (32° a 104° F)	0° a 40° C (32° a 104° F)	0° a 40° C (32° a 104° F)	10° a 40° C (32° a 104° F)
Humedad relativa:	5% a 85% a 40° C (104° F)	5% a 85% a 40° C (104° F)	5% a 85% a 40° C (104° F)	5% a 85% a 40° C (104° F)	5% a 85% a 40° C (104° F)	20% a 90% a 40° C (104° F)
Certificación/ Declaración de seguridad	UL 60950-1, CAN/CSA C22.2, No. 60950-1, EN 60950-1, (CE Mark), IEC 60950-1					
Certificación/ Declaración de compatibilidad electromagnética (CEM)	FCC Parte 15, Verificación clase A Canadá ICES-003, Clase A EN 55022, Clase A (Marca CE) EN55024 (Marca CE) EN 61000-3-2 (CE Mark) EN 61000- 3-3 (Marca CE) VCCI Clase A	FCC Parte 15, Verificación clase A Canadá ICES-003, Clase A EN 55022, Clase A (Marca CE) EN55024 (Marca CE) EN 61000-3-2 (Marca CE) EN 61000- 3-3 (Marca CE) VCCI Clase A	FCC Parte 15, Verificación clase A Canadá ICES-003, Clase A EN 55022, Clase A (Marca CE) EN55024 (Marca CE) EN 61000-3-2 (Marca CE) EN 61000- 3-3 (Marca CE) VCCI Clase A	FCC Parte 15, Verificación clase A Canadá ICES-003, Clase A EN 55022, Clase A (Marca CE) EN55024 (Marca CE) EN 61000-3-2 (Marca CE) EN 61000- 3-3 (Marca CE) VCCI Clase A	FCC Parte 15, Verificación clase A Canadá ICES-003, Clase A EN 55022, Clase A (Marca CE) EN55024 (Marca CE) EN 61000-3-2 (Marca CE) EN 61000- 3-3 (Marca CE) VCCI Clase A	FCC Parte 15, Verificación clase A Canadá ICES-003, Clase A EN 55022, Clase A (Marca CE) EN55024 (Marca CE) EN 61000-3-2 (Marca CE) EN 61000- 3-3 (Marca CE) VCCI Clase A
Declaración ambiental	ROHS	ROHS	ROHS	ROHS	ROHS	ROHS

[1] Las mediciones de tasa de transferencia fueron alcanzadas basadas en los estándares RFC2544 (http://www.ietf.org/rfc/rfc2544.txt) y han sido validados por otras organizaciones de pruebas.

Para más información

Para saber más sobre IBM Security Network IPS entre en contacto con un representante de Ventas IBM o un asociado de negocios IBM o visite nuestra página web: **ibm.com**/tivoli/solutions/threat-mitigation

Sobre el software Tivoli de IBM

El software Tivoli® de IBM ayuda a la organización de manera eficiente y efectiva a gestionar sus recursos de TI, tareas y procesos para cumplir con los requisitos de los negocios en evolución y entregar un servicio de gestión de TI flexible y sensible ayudando a reducir costos. La cartera Tivoli abarca software para seguridad, cumplimiento, almacenamiento, rendimiento, disponibilidad, configuración, operaciones y gestión de ciclo de vida de TI, con el respaldo de los servicios de clase mundial de IBM, apoyo e investigación.

IBM Corporation Software Group,
Route 100,
Somers, NY 10589,
EE.UU.

Producido en los Estados Unidos de América
Septiembre 2010

WGD03002-USEN-02