

Protección de contenidos en el perímetro de la red



Nuevo Panda **GateDefender** Performa Serie 9000

Su primera línea de defensa

La Importancia de Proteger el Perímetro

Las amenazas procedentes de Internet incrementan su impacto y frecuencia entre las empresas de hoy en día. El correo no deseado ocasiona graves problemas para todas las compañías, ya sea en forma de amenazas de seguridad, consumiendo excesivo ancho de banda o reduciendo la productividad de los usuarios, al permitir la llegada de grandes volúmenes de spam.

Según el MAAWG (Messaging Anti-Abuse Working Group), actualmente entre el 82% y el 87% de todo el tráfico de correo entrante es categorizado como Spam o correo inútil. La cantidad entrante de spam es enorme y aumenta año tras año.

- 1978 – Un correo Spam es enviado a 600 direcciones de correo
- 1994 – El primer spam de gran escala es enviado a 6000 [newsgroups](#), llegando a millones de personas.
- 2005 – (Junio) 30 mil millones de correos Spam enviados al día
- 2006 – (Junio) 55 mil millones de correo Spam enviados al día
- 2006 – (Diciembre) mil millones de correo Spam enviados al día
- 2007 – (Febrero) 90 billones de correo Spam enviados al día

Las amenazas mas peligrosas procedentes de Internet están dirigidas a las empresas. Estas amenazas por lo general, son motivadas política o económicamente.

Un artículo reciente de BBC News ilustra dramáticamente esta tendencia. Un ordenador desprotegido Windows XP fue conectado a Internet, sin un software corta fuegos o antivirus, con el fin de determinar cuanto tiempo pasaba antes de que fuera golpeado por algún agente devastador de la red. En solo 8 segundos, el ordenador desprotegido fue golpeado por Sasser - uno de los gusanos más rápidos en expandirse por Internet.

Las preocupaciones recientes sobre seguridad tienen origen en las redes internas. La pérdida de información sensible almacenada en las redes corporativas puede afectar dramáticamente a las organizaciones.

La información personal o económica que se envía desde la red corporativa, puede causar daños legales y económicos inestimables. Estos daños deben evitarse a través de una Política de seguridad racional y personalizada, reforzada por una herramienta robusta y adecuada con una posición estratégica en la red.

Asimismo, cualquier solución de seguridad debe garantizar la recepción de información importante. Un falso positivo que detecta spam o contenidos potencialmente peligrosos, puede causar retrasos y pérdida de información, convirtiendo la solución en parte del problema.

Adicionalmente, el volumen de tráfico recibido o enviado por las empresas, crece continuamente día tras día, lo que convierte a la pasarela en un punto crítico para la red; cualquier dispositivo agregado en este punto debe garantizar el flujo de tráfico sin interferencia.

Soluciones Gestión de Contenidos Seguros (SCM)

Los dispositivos de protección perimetral previenen efectivamente, que las amenazas originadas en Internet alcancen la red corporativa.

Sin embargo, los diferentes tipos de amenazas basadas en Internet necesitan ser manejadas con diferentes categorías de dispositivos dedicados. Algunas soluciones ofrecen protección contra amenazas basadas en contenidos y otras incluyen protección frente a amenazas a nivel de red.

Los dispositivos que protegen la red frente a amenazas basadas en contenidos se conocen como dispositivos para Gestión de Contenidos Seguros. Sin embargo, muy pocos vendedores son capaces de ofrecer una solución dedicada con protección completa para redes corporativas. Algunos, ofrecen únicamente soluciones especializadas para detectar un tipo de amenazas de contenido, como spam.

Otros vendedores ofrecen dispositivos especializados para protocolos específicos. Estos dispositivos se concentran únicamente en un tipo de tráfico como e mail (SMTP, POP3 o IMAP) o el tráfico de navegación (http).

De acuerdo con los analistas de mercado, la tendencia en seguridad perimetral, se orienta a la combinación de protecciones tanto de correo como de navegación, en un solo dispositivo; debido a la complejidad y variedad de amenazas de contenido.

“En el 2010 las soluciones viables ofrecerán no solo análisis de entrada de todos los protocolos para impedir el acceso de los contenidos maliciosos, sino también análisis de salida de todos los protocolos”.

- Gartner

Panda GateDefender Performa es un dispositivo hardware SCM de alto rendimiento y software dedicado para evitar que amenazas basadas en contenidos, como malware, contenidos potencialmente peligrosos spam, aplicaciones IM/P2P y contenidos web inadecuados entren en la red corporativa. Combina protecciones reactivas con un motor heurístico preventivo para garantizar la seguridad, incluso frente a amenazas desconocidas.

Panda GateDefender Performa – Su primera línea de defensa

Panda GateDefender Performa ofrece protección perimetral para compañías de cualquier tamaño, con alta escalabilidad y protección frente a todos los tipos de amenazas basadas en contenidos.

Panda GateDefender Performa es el dispositivo SCM más potente de su clase. Más que un appliance especializado, es una solución completa gracias a su estructura modular. Las empresas pueden seleccionar los módulos que quieran activar, entre antimalware, antispam y filtrado web. El sistema modular de Panda GateDefender Performa hace posible que la solución se ajuste a las necesidades de seguridad de la empresa. Los módulos de protección se ilustran en la siguiente tabla:

Módulo de Panda GateDefender Performa	Protección incluida
Módulo Anti-malware	Protección Anti-malware
	Filtrado de Contenido
Módulo Anti-spam	Protección Anti-spam
Módulo Filtro Web	Bloqueo de Aplicaciones P2P y Mensajería Instantánea
	Filtrado Web

Tabla 1. Módulos y protecciones de contenidos en Panda GateDefender Performa.

Protecciones incluidas

- 1. Protección Anti-Malware:** Panda GateDefender Performa detecta y bloquea todo tipo de códigos maliciosos que provienen de Internet, antes de que alcancen la red corporativa. Los ficheros que contienen malware desconocido o no desinfectable, pueden ser almacenados en una cuarentena especial, y ser eliminados posteriormente. El malware sospechoso puede ser enviado automáticamente a PandaLabs para ser clasificado y desinfectado respectivamente sin intervención del administrador.
- 2. Content Filter:** GateDefender Performa permite a los administradores establecer políticas de seguridad corporativas para filtrar contenidos potencialmente peligrosos y prevenir que la información confidencial o personal salga de la empresa.
- 3. Protección Anti-Spam:** Verifica todo el tráfico de correo entrante y saliente. Todos los mensajes son clasificados como spam, probable spam o no spam.
- 4. Bloqueo de aplicaciones P2P e IM:** Las aplicaciones P2P consumen el ancho de banda de las empresas y constituyen un hueco en la seguridad, ya que los ficheros divididos no pueden ser analizados. La Mensajería Instantánea también afecta a la productividad de la empresa, pues por lo general es utilizada por los empleados con fines personales. Panda GateDefender Performa bloquea el uso de este tipo de aplicaciones dentro de la red corporativa.
- 5. Filtrado Web:** Los administradores pueden definir categorías de contenidos Web inapropiados. También, pueden establecer listas blancas y negras, de páginas permitidas o restringidas; lo cual optimiza el uso de recursos y mejora la productividad del usuario. También bloquea el acceso a contenidos ofensivos, violentos u otros.

Si una empresa utiliza sólo algunos protocolos de comunicación, GateDefender Performa tiene la opción de desactivar cualquiera de los seis protocolos que puede analizar: HTTP, FTP, SMTP, POP3, IMAP4 y NNTP. Al analizar menos protocolos, el rendimiento de la máquina se optimiza. Si la empresa necesita protección para analizar otros protocolos en el futuro, tiene la posibilidad de activar protocolos para ampliar el alcance de protección.

Panda GateDefender Performa ofrece la protección más actualizada de la red, ya que descarga archivos de firmas de malware y URLs clasificadas cada hora, mientras que las firmas de spam, se descargan cada minuto, automática y transparentemente; esto garantiza la respuesta más veloz frente a estas amenazas. Adicionalmente, el dispositivo contiene las tecnologías líderes del mercado en cada módulo, para asegurar los mejores resultados incluyendo Antimalware de Panda Security, Anti-spam de Cloudmark y Filtrado Web de Cobion.

Panda GateDefender Performa permite definir perfiles de usuarios y refuerza la política de seguridad de la empresa adaptándose a las necesidades de cada usuario o grupo de usuarios, asegurando la protección más robusta y flexible para responder a todo tipo de requerimientos.

Características clave

- **Tecnología Proactiva Integrada:** Los motores Heurísticos, la Inteligencia Colectiva y la cuarentena combinados en el perímetro, optimizan la detección de amenazas garantizando la recepción de información importante.
- **Protección Completa:** Ofrece protección contra amenazas basadas en contenidos. Incluye protecciones Best of breed (mejor del ramo) contra Malware y contenidos potencialmente peligrosos (Panda); spam (Cloudmark); y contenidos web no deseados (Cobion). Además, el uso de aplicaciones potencialmente peligrosas como P2P e IM es también restringido. Por otro lado analiza los protocolos más utilizados tanto en sentido de entrada como de salida.

- **Políticas de Seguridad Adaptables:** Se pueden definir diferentes perfiles de usuarios y grupos con el fin de establecer Políticas de Seguridad diferentes para cada miembro de la red, reforzando así el sistema de gestión de riesgos. Cualquier contenido entrante o saliente se analiza de acuerdo al tipo de contenido y el perfil particular de cada remitente o destinatario.
- **Conectar y Olvidar:** La configuración se puede hacer fuera de línea y una vez conectado, comienza a funcionar al instante, lo que reduce los costes de operación.
- **Alta disponibilidad y Balanceo de Carga:** Analiza gran cantidad de tráfico y el rendimiento puede crecer, gracias al balanceo de carga nativo y automático, que asegura alta disponibilidad del servicio en caso de cualquier fallo inesperado.
- **Protección Desatendida:** La actualización continua de firmas y los reportes gráficos en tiempo real permiten su funcionamiento desatendido tras la instalación.
- **Administración Centralizada:** Se pueden configurar todas las unidades desplegadas a lo largo de toda la red desde una única consola.
- **Monitorización Centralizada:** Permite ver informes gráficos definidos por el administrador, de las diferentes protecciones activas en una única consola.
- **Garantía de Flujo de Tráfico:** La opción de bypass evita que el flujo de tráfico se detenga, a pesar de posibles fallos del sistema, lo que confiere una garantía de continuidad del negocio.

Panda GateDefender Performa dispone de cuatro modelos de hardware, para adaptar la protección perimetral a las necesidades de cualquier empresa. Ofrecen flexibilidad completa y la posibilidad de migrar de un modelo de hardware a otro.

Tabla de Rendimientos	GateDefender Performa 9050	GateDefender Performa 9100	GateDefender Performa 9200	GateDefender Performa 9500
				
HTTP (Mbps)	275	320	420	510
SMTP (mensajes/seg.)	115	135	200	220
Conexiones Concurrentes	600	1800	3600	7200

Tabla 2. Comparación de los cuatro modelos de GateDefender Performa.

Beneficios para la Organización.

Panda GateDefender Performa ofrece una amplia gama de beneficios a compañías de cualquier tamaño:

- **Evita la complejidad** por su comportamiento en modo bridge transparente que permite una fácil instalación sin necesidad de cambiar la arquitectura de la red.
- **Incrementa la productividad de los usuarios** gracias a la liberación del spam en sus correos; el uso restringido de aplicaciones Peer to peer y de Mensajería Instantánea; y el control de los contenidos web a los que pueden acceder.
- **Reduce los costes de operación:** gracias a las actualizaciones continuas que permiten su funcionamiento desatendido tras la instalación
- **Contribuye a que la compañía cumpla los estándares reguladores** evitando la pérdida de datos sensibles, basándose en el contenido del mensaje o personalizado según el perfil del usuario.
- **Refuerza el sistema de Gestión de Riesgos** porque es altamente preventivo para detectar y desinfectar amenazas desconocidas, en el perímetro sin intervención del administrador.
- **Posibilita la Continuidad de Negocio** optimizando el uso del ancho de banda al bloquear el tráfico inútil (alrededor del 70%).

Comparado con...	GateDefender Performa tiene...
Otros appliances SCM dedicados	El mayor rendimiento del mercado
Appliances dedicados especializados por protección	Mejor rendimiento
	Escalabilidad con la posibilidad de incluir otras protecciones
Appliances especializados por protocolo	Rendimiento mejor
	Mayor capacidad de protección
Appliances UTM	Mejor Rendimiento
	La mejor seguridad utilizando dispositivos separados.

Tabla 3. Comparación de GateDefender Performa con otras categorías de seguridad perimetral.

Conclusión

Panda GateDefender Performa es el dispositivo SCM de mayor rendimiento, que protege el perímetro de la red corporativa. Ofrece una potente y funcional protección perimetral frente a todos los tipos de amenazas originadas en Internet. Gracias a las características de Antimalware, Antispam y filtrado web, cumple con todos los requerimientos de seguridad de los administradores de red detectando y eliminando todas las amenazas basadas en contenido, eliminando correo inútil, y protegiendo a los usuarios de contenido web improductivo. Además, el contenido de tráfico saliente, también es analizado evitando la fuga de datos críticos o envíos involuntarios de spam o software malicioso que puede afectar a clientes, socios, proveedores, etc.

Adicionalmente, las configuraciones personalizadas para cada usuario o grupo garantizan una flexible, pero estricta aplicación de las Políticas de Seguridad Corporativa.