Panda GateDefender**Integra**

Protección empresarial unificada

La creciente variedad y complejidad de las amenazas procedentes de Internet deberían bloquearse antes de llegar a su red, evitando así daños en su empresa.

Cerca del 99% de las amenazas que afectan a las redes corporativas provienen de Internet. Esto convierte a la pasarela de conexión en un punto crítico para la seguridad de la red. Una protección en este punto reducirá en gran medida problemas potenciales antes de que accedan a la red interna.

Las amenazas relacionadas con Internet pueden clasificarse en dos grupos distintos:

- Amenazas a nivel de red (conexiones no autorizadas, intrusiones …).
- Amenazas basadas en contenidos (virus, gusanos, spyware, spam, etc.).

Esta diversidad de posibles amenazas crea una necesidad evidente para los administradores de red de disponer de soluciones que sean capaces de integrar toda la protección bajo un único interfaz, fácil de usar, que pueda centralizar la seguridad en un punto crítico de la red, como la conexión a Internet.

Andrew Jaquith, analista de Yankee group: **"Es una cuestión de supervivencia para los fabricantes de Antivirus, que, cada vez más, buscan formas de reinventarse a sí mismos mientras sus productos fracasan en la lucha contra los nuevos tipos de infecciones. Los servicios de Inteligencia Colectiva basados en la nube son el próximo gran hito para el Anti-malware. Yo vaticino que todos los fabricantes de Antivirus necesitarán adoptar una aproximación similar si esperan sobrevivir."**

La solución: Panda GateDefender Integra

Panda GateDefender Integra es un dispositivo de seguridad perimetral unificado muy fácil de comenzar a usar, que proporciona protección frente a cualquier tipo de amenaza, tanto a nivel de red como basada en contenidos, a través de una única y sencilla interfaz para todas las protecciones. Los distintos tipos de protección incluidos son:

- **Firewall**: Comunicaciones internas y externas dentro de la política de seguridad.
- **Intrusion Prevention System (IPS)**: Impide ataques de intrusión.
- **VPN**: Protege la información confidencial que se transmite a través de Internet.
- **Anti-malware**: Protege frente a todos los tipos de software malicioso.
- **Content Filter**: Permite definir la Política de seguridad de la empresa.
- **Web Filter**: Restringe el acceso a contenidos web no relacionados con el trabajo.

Un modelo de hardware que cubre las necesidades de seguridad de las pequeñas empresas:

Modelo Hardware	Número de usuarios recomendado	Firewall Throughput	Sesiones Concurrentes	10/100/1000 Eth ports
 SB	Hasta 50	400 Mbps	180.000	4

Principales beneficios

- **Enchufar y Proteger.** No requiere configuración alguna para comenzar a proteger desde el primer minuto.
- **Reduce la complejidad.** Incluye todas las funciones necesarias bajo un único y sencillo interfaz.
- **Minimiza los costes operativos** a través de una protección que apenas requiere supervisión, al contemplar actualizaciones automáticas e informes gráficos de actividad en tiempo real.
- **Aumenta la productividad de los usuarios** gracias a la liberación de tráfico spam y el acceso restringido a contenidos web no productivos.
- **Impide la pérdida de información confidencial** controlando el contenido de los datos entrantes y salientes, llegando incluso a cifrar la información transmitida por Internet.

Características clave

- **Único UTM "Enchufar y Proteger".** Activa por defecto las protecciones antimalware, antispam y filtrado web, protegiendo desde el inicio sin intervención del usuario.
- **Protección completa contra todas las amenazas.** Incluye las mejores protecciones: frente a malware y contenidos potencialmente peligrosos (Panda), spam (Cloudmark), y contenidos web no deseados (Cobion), junto con un Firewall de inspección profunda de paquetes, un IPS rico en reglas y una VPN para centralizar toda la seguridad de la red en un único punto.
- **Continuas actualizaciones automáticas:** Las reglas y huellas digitales se actualizan cada 90 minutos en el caso del malware, IPS o Web Filter y cada minuto en el caso del spam, cerrando la ventana de riesgo.
- **Optimización de la carga de red:** El acceso restringido a las páginas web no productivas optimiza el uso del ancho de banda y el ratio de detección de spam del 98% libera los servidores de correo y la red interna del tráfico basura.
- **Protección de Contenidos Proactiva:** analiza el tráfico entrante y saliente en busca de contenidos peligrosos según la política de seguridad establecida. Todas las comunicaciones pueden ser cifradas a través de VPN.

PANDA SECURITY | 20 Aniversario 1990-2010

Protección de acceso

Tanto el hardware como el software de Panda GateDefender Integra han sido diseñados para proporcionar la máxima protección y el mayor rendimiento posible a nivel de gateway (acceso). Analiza los protocolos más utilizados en tiempo real:

- HTTP, FTP, SMTP, IMAP4, POP3 y NNTP para contenidos
- TCP, UDP e ICMP para intrusiones en la red
- IPSec, SSL, L2TP y PPTP para VPN.

Control optimizado

El firewall controla la comunicación entre la red e Internet o entre todas las áreas de la red, los usuarios, los grupos, etc.

Hay dos tipos de filtrado:

1. **Estático a nivel de red**, basado en reglas establecidas por el administrador para el tráfico tanto entrante como saliente.
2. **Dinámico a nivel de aplicación** con
   a. **'Stateful Inspection'** seguimiento del estado y contenido de las comunicaciones básicas en todos los protocolos y estados, timeouts, conexiones establecidas, etc. de comunicaciones avanzadas en FTP, PPTP, L2TP, IPSEC.
   b. **'Deep Packet Inspection'**, analiza el contenido de los paquetes inspeccionando los mensajes en HTTP, FTP, SMTP, IMAP, POP3, etc., mientras que están activos otros módulos.

Transmisiones seguras

El VPN proporciona túneles de comunicación seguros con oficinas o usuarios remotos a través de Internet, La información transferida que se cifra en origen y descifra en destino.

Opera bajo configuraciones host to host, host to net y net to net y soporta protocolos IPSec, SSL, L2TP y PPTP en modo cliente y servidor.

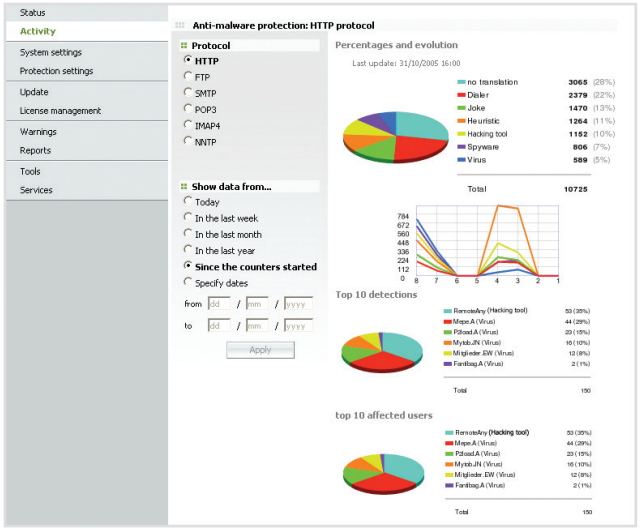
Seguridad reforzada

El IPS previene la propagación rápida de los ataques externos analizando los protocolos IP, ICMP, TCP y UDP a través de un archivo basado en reglas.

Los administradores pueden especificar el umbral para cada regla, reduciendo de esta manera los falsos positivos al configurarlo para que bloquee automáticamente las intrusiones detectadas.

Sistema de seguimiento en tiempo real

La consola ofrece informes gráficos en tiempo real de cada actividad de protección. También es posible configurar informes de síntesis periódicos. Asimismo genera informes detallados para cada protección.



Protección preventiva completa

Panda GateDefender Integra detecta y bloquea cualquier tipo de amenaza relacionada con Internet que trata de acceder a la red. Protege frente a:

Virus	Gusanos	Riesgos de seguridad
Troyanos	Phising	Dialers
Jokes	Spyware	Herramientas de Hacking

También detecta malware desconocido gracias a su motor heurístico genético combinado con la Inteligencia Colectiva.

Política de seguridad

La protección de Content Filter permite a los administradores definir la política de seguridad de su empresa. Pueden predeterminar qué archivos y/o correos electrónicos pueden ser recibidos o enviados desde la red. De esta manera, se evita la filtración de información confidencial y otros riesgos potenciales.

Bloqueo de correo basura

La protección antispam de Panda GateDefender Integra evita la saturación de la red, impidiendo que penetre el spam, desde el punto de acceso a la red. Asimismo, clasifica los mensajes como spam o probable spam y lleva a cabo diferentes acciones en consecuencia.

Navegación web optimizada

Gracias al Filtrado web, Panda Gatedefender Integra aumenta la productividad de los usuarios impidiendo el acceso a las páginas web inadecuadas o no relacionadas con el trabajo.

El administrador elige entre 60 categorías cuáles se pueden visitar desde la red interna y cuales no únicamente para usuarios VIP.

Seguimiento centralizado

El sistema envía avisos de eventos personalizados a través de SMTP, SNMP y/o Syslog. El administrador puede elegir qué eventos deberían enviarse a través de cada método.

Actualizaciones automáticas

Tanto el fichero de firmas para Anti-malware y Content Filter, como la base de datos para Filtrado web y el archivo de reglas para IPS se actualizan de forma automática cada 90 minutos.

Las huellas digitales del spam se actualizan cada minuto para así poder garantizar el mayor ratio de detección posible.

Certificaciones de Panda Security

Revisión 1.06 2009

Compruébelo en **www.pandasecurity.com**
Consiga su versión de evaluación de GateDefender Integra.

PANDA SECURITY | 20 Aniversario 1990-2010