



Los dos conectores de red son la única vía de comunicación para el Panda Appliance.

#### SISTEMA DE PROTECCIÓN PERIMETRAL PARA LA EMPRESA

# Panda Antivirus Appliance

La compañía da un paso hacia adelante con la presentación del Appliance, un dispositivo de hardware de alto rendimiento para la protección de la empresa

#### INFORMACIÓN

**PRECIO** 4.704,76 € (50 licencias)  
**CONTACTO** Panda  
**TELÉFONO** 902 243 651  
**WWW** www.pandasoftware.es

#### CARACTERÍSTICAS

Administración: consola Web remota.  
 Integración en red: configurable como bridge (precisa una dirección IP).  
 Actualizaciones: automáticas de firmas y motor.  
 Protocolos: HTTP (incluyendo Java y ActiveX), FTP, SMTP, POP3, IMAP4.  
 Tarjetas de red: 2 10/100.  
 Capacidad de transferencia máxima: 12 Mbps.  
 Informes y alertas: Sí (a través de Web, correo, etcétera).  
 Acción antivirus: los virus se destruyen automáticamente.  
 Dimensiones: estándar para un rack 1U 19" (17 x 17 x 175 pulgadas).  
 Certificaciones: FCC y CE.

**D**esarrollar un producto con las características del Appliance no es sencillo, aunque se trata de un tipo de solución bastante atractiva que complementa perfectamente a otras alternativas ya instaladas basadas en herramientas de software.

**B**ásicamente, el Appliance es una máquina para filtrar paquetes de red a la que llegan tramas procedentes del exterior con dirección a las máquinas del interior, y viceversa, desde la red local se envían tramas hacia fuera a través de Internet. Justo en el medio se instalaría el Appliance, de modo que actuase de filtro para posibles virus o tráfico no deseado por algún motivo, que no necesariamente tenga que ver con un contenido vírico, pero que sí ocasione efectos tan perniciosos como la denegación de servicio en servidores (Ataques DOS o *Denial of Service*). El capítulo de la protección de tráfico saliente es igualmente importante a la hora de frenar la propagación de este tipo de agresiones contra la integridad de redes y equipos, ofreciendo en

conjunto una respuesta que realmente tiene sentido y encaja en cualquier estructura de red donde las soluciones software se muestren insuficientes.

El filtrado del tráfico entrante permite liberar de un porcentaje elevado de trabajo a los servidores internos de una red corporativa, al requerir menos operaciones de mantenimiento y trabajo con los sistemas de ficheros. Existe también una parte dedicada al filtrado de contenidos, aunque es uno de los capítulos donde más posibilidades de evolución tiene el Appliance. De momento se limita a establecer reglas básicas definidas por el usuario que afectan a apartados como el de los ficheros ZIP anidados, de modo que puede establecerse un tiempo máximo de exploración para un fichero determinado y evitar la caída en

bucles infinitos o que se ralentice en demasía el sistema.

En el supuesto de que el tráfico de red fuese tan elevado que incluso el Appliance se viese afectado por ello, se pueden conectar dos de ellos en una topología con carga balanceada entre ambos sin que apenas haya que hacer algo más aparte de activar una casilla en uno de los menús de configuración. De este modo se repartirá el análisis del tráfico entre los dos, reduciendo el impacto en las prestaciones. Una advertencia llegados a este punto: el análisis cuantitativo del rendimiento no pudo ser evaluado a causa de limitaciones en la estructura de red empleada en las pruebas, por lo que será recomendable contactar con Panda para dilucidar cualquier duda sobre este particular.

#### Instalación y puesta a punto

El montaje del Appliance no revestirá complicación alguna para cualquier administrador de red con un mínimo de experiencia y conocimiento de la estructura de la misma. Tan sólo habrá que buscar un punto lo más externo que se pueda, pero con un mínimo de protección frente a posibles intrusiones. Justo detrás de un *firewall* es la ubicación recomendada y la que más lógica parece tener en una primera aproximación, filtrando el tráfico para el resto de los servidores y, por ende, reduciendo su carga de trabajo a la hora de limpiar ficheros con virus o evitar que se manifiesten ataques de tipo DOS o similares.

Una vez instalado, entrando en la consola de administración se podrán definir los comportamientos ante las alertas y las detecciones de virus, el tipo de registro que se empleará, el nivel de detalle del mismo, la transmisión por correo de las alertas, el envío de los registros a otra máquina (que podrá recogerlos de forma automática a través del uso de una pequeña aplicación MS-DOS), etcétera. Si es preciso explorar más puertos aparte de los estándar para los protocolos soportados, también se podrán configurar cómodamente desde la consola Web.

Por otra parte, es conveniente advertir que el idioma con el que se trabaja es el inglés; un detalle que para el perfil técnico de muchos administradores de sistemas puede incluso pasar desapercibido, aunque no deja de ser un tanto curioso al ser un producto lanzado en España. De todos modos, en un equipo como

éste, revisado periódicamente, no sería de extrañar que pronto se solventase tan atípica circunstancia. Asimismo, para poder acceder a los servicios de actualización del motor de exploración y de las firmas, es preciso dotar al Appliance de una dirección IP; si bien esto no tendrá uso práctico alguno más allá que el implícito al propio mecanismo de actualización.

### Administración y mantenimiento

Este capítulo es uno de los más agradecidos del Appliance, pues prácticamente no requiere mantenimiento alguno. Las actualizaciones, tanto de las firmas víricas como del propio motor, se realizan de forma automática y con frecuencia suficiente como para confiar en su capacidad de respuesta ante las amenazas más acuciantes. Sí será recomendable al principio asegurarse de que las alertas y los ficheros de registro de actividad cumplen su cometido correctamente el tiempo necesario para "fiarse" del Appliance, pero siempre como un complemento para las soluciones ya existentes o como un medio para liberarlas de cargas excesivas de trabajo. A modo de ejemplo, decir que los sistemas de Appliance estuvieron listos para hacer frente al gusano *SQLSlammer* con total eficiencia sin necesitarse intervención alguna más allá de la monitorización de los registros de alertas.

### Tecnología

El Appliance es un sistema microprocesador completo con NT, pero bajo la forma de una configuración cerrada y lista para instalar en un rack sin que sea necesario acceder a su hardware. Es más, en caso de que apareciese algún fallo en el equipo, la estrategia de Panda es la de sustituirlo de inmediato por otro. Las únicas vías de comunicación con el exterior son sendas conexiones de red (una de entrada y otra de salida) con un tráfico máximo de 12 Mbps. De este modo se limita el acceso físico al dispositivo, que está también muy protegido a nivel de entradas a través de la red. De todos modos, una de las primeras tareas del administrador del sistema será la de establecer una contraseña para evitar que se pueda acceder al servidor Web del Appliance.

Un punto "original" si cabe, es el sistema elegido para hacer trabajar al Appliance. Frente a la tendencia generalizada a emplear Linux como

The image shows two overlapping screenshots from a web browser. The top screenshot displays the 'Antivirus settings' page, which includes sections for 'About the appliance', 'General settings', 'Product settings', 'Access to the Internet configuration', 'Mail scanning', 'Web scanning', and 'Maximum size of Message to be scanned'. The bottom screenshot shows the 'ANTIVIRUS STATISTICS' page, which contains a table summarizing network activity and detected threats.

**Antivirus Vendor: Panda Software**  
**Scan Engine Version: 3.1.6.211**  
**Pattern File Version: 3.65615 (Timestamp)**

**Machine name: PandaAppliance**  
**Machine IP address: 10.3.5.15**  
**Client: 10.3.5.222**  
**Protocol: HTTP**

**Virus: "EICAR-AV-TEST-FILE" found!**  
**Downloaded file "http://www.rexswain.com"**  
**SUBJECT=Panda Antivirus Appliance Admin**

protocol	files scanned	viruses detected
HTTP	0	0
FTP	0	0
POP3	0	0
SMTP	0	0
NNTP	0	0
IMAP4	0	0
OVERALL	0	0

sistema operativo para este tipo de dispositivos al más puro estilo "caja negra", aquí se emplea una versión de NT especialmente configurada para Appliance. En cualquier caso, según se ha hecho saber desde Panda, el precio de NT no supone un incremento respecto al que pudiese tener el producto si incluyese Linux. La política de precios se basa en el número de licencias contratadas (la cantidad de equipos a proteger). En este sentido, está claro que la audiencia de este modelo se engloba dentro del sector profesional para la protección de redes corporativas a partir de unos 30 equipos. Por debajo de esta cifra no resulta rentable ni supone un ahorro sustancial a la hora de liberar de carga a los posibles servidores que hubiese instalados. De todos modos, se trata de un producto que potencialmente puede tener una buena acogida, lo cual hará que siga evolucionando.

En cuanto a los protocolos de red que son vigilados de forma directa, se tienen los más comunes de Internet: HTTP, FTP, POP3, SMTP, NNTP e IMAP4. En las pruebas se pudo constatar cómo la detección de los virus se realizaba al acuerdo con lo esperado, generando las alertas correspondientes y mostrando las estadísticas puntualmente. En el caso de que se empleen más puertos para redirigir el tráfico de estos protocolos a puntos diversos dentro de la red, pueden ser dados de alta como "explorables" sin más que rellenar las casillas correspondientes en la consola Web. No estaría de más, llegados a este punto, disponer de un opción para

La consola Web y los archivos de registro están exentos de cualquier añadido que no tenga que ver con una función dentro del Appliance, algo que agradecerán los administradores de red deseosos de ir "al grano".

conservar la configuración y poder restaurarla en cualquier momento sin necesidad de teclear todos los parámetros de nuevo, o para guardar los ficheros infectados para recuperarlos en caso de emergencia.

En resumidas cuentas, un producto adecuado para la empresa en cuanto a concepción y ejecución, aunque en el apartado de las prestaciones no se ha podido contar con un banco de pruebas adecuado para obtener resultados válidos y concluyentes. De todos modos, la adquisición de este sistema debe sopesarse con rigor, siendo recomendable entrevistarse en profundidad con los responsables de producto en Panda para tomar o no una decisión firme de compra de acuerdo con las necesidades de su empresa o compañía.

**Manuel Arenas**

### Valoración PCPlus

#### PANDA ANTIVIRUS APPLIANCE

##### A FAVOR

- ✓ Protección para los protocolos más comunes de red.
- ✓ Administración sencilla.

##### EN CONTRA

- ✗ Interfaz en inglés.
- ✗ Podría haber más flexibilidad para establecer reglas de filtrado de contenidos.

**Calidad/precio** ●●●●●●●●●●

**Características** ●●●●●●●●●●

**Prestaciones** ●●●●●●●●●●

**Total** ●●●●●●●●●●