

¿Es suficiente un cortafuegos corporativo para mantener las comunicaciones de mi empresa con el exterior libre de virus e intrusos?

ISA (Internet Security and Acceleration) es el servidor de navegación y cortafuegos corporativo de Microsoft Corp. Además de **gestionar el acceso a Internet** de los empleados, con ISA es posible cerrar protocolos y puertos de comunicaciones innecesarios y susceptibles de recibir ataques. Pero ISA precisa de un complemento que analice el tráfico que pasa por los protocolos permitidos con el fin de filtrar contenidos peligrosos o no productivos como el spam.

Es necesaria una solución integrada con ISA capaz de detener el malware

Panda Security for ISA Servers es la protección antimalware que analiza y desinfecta, con un filtro web (ISAPI) y un filtro de aplicación, todos los formatos de ficheros, enviados y recibidos a través de los protocolos HTTP, SMTP y FTP (sobre HTTP), en su paso por el servidor ISA de Microsoft.

Esta solución antimalware protege frente a virus, gusanos, troyanos, software espía, adware, correo basura, hoaxes, phishing, dialers, herramientas de hacking, riesgos de seguridad, etc. **Panda for ISA es el complemento perfecto** a la protección que ofrecen los módulos de seguridad y proxy caché de los servidores MS ISA, incorporando como valor añadido un innovador módulo para el filtrado de contenidos.

Estrategia de protección preventiva por capas

Panda for ISA Servers protege las capas perimetrales de navegación web y firewall corporativo.



Beneficios Principales

- Permite la **administración**, despliegue, monitorización y definición de políticas de seguridad de manera **centralizada y sencilla**.
- Facilita la toma de **decisiones en tiempo real**.
- **Protege** sus servidores **ISA a todos los niveles**.
- **Aumenta la productividad** de los usuarios finales y administradores de la red.

Características Clave

- **Correo SMTP blindado** ante los ataques de phishing y hackers. Con capacidad de desinfección de virus en mensajes anidados y ficheros comprimidos a todos los niveles.
- **Versátil filtrado de contenidos** con usuarios VIP para el tráfico web y el correo electrónico SMTP.
- **Óptimo rendimiento** gracias al uso combinado de las tecnologías PartFile y VirtualFile, y el soporte a procesadores de 64 bits.
- **Potente motor heurístico de páginas web**, para la detección de códigos víricos no sólo en el cuerpo HTML del sitio web, sino también en aquellos ficheros contenidos en la propia página.
- **Administración centralizada remota** de la red, con múltiples vistas de los servidores, informes gráficos y cuarentena centralizada para la gestión de elementos sospechosos.
- **Actualizaciones automáticas cada hora** del Archivo de Identificadores de Malware.
- **Flexible configuración** con el sistema personalizado de notificación de alertas.

Correo blindado frente a ataques

Panda for ISA previene la propagación de infecciones desde el correo electrónico. Detecta ataques de phishing y analiza mensajes anidados de varios niveles, archivos adjuntos y comprimidos en formatos como ZIP y ARJ. Incluso, **detecta virus de red en paquetes** y otros virus en objetos OLE, incrustados en el cuerpo de los mensajes.

Además, si el mensaje infectado ha sido generado automáticamente por un gusano, el **mensaje es suprimido en su totalidad**, ya que ni el archivo adjunto ni el cuerpo del mensaje son de valor para el destinatario.

Filtrado de contenidos para correo SMTP y tráfico HTTP

Con su filtrado de contenidos para correos SMTP, se pueden filtrar **mensajes cifrados**, crear reglas de filtrado que combinan varios criterios (asunto y cuerpo del mensaje, nombre, extensión y contenidos de los archivos adjuntos) para así, eliminar referencias externas, archivos comprimidos sospechosos o remitentes indeseados.

El filtrado HTTP de **Panda for ISA** permite que determinadas direcciones IP y usuarios VIP puedan descargar archivos sin restricciones mientras navegan. También, permite la importación de listas negras de máquinas que tienen vedado el acceso a páginas web.

Así mismo, incluye filtrado en función del uso de contraseñas o macros, el tamaño, la extensión, nombre o tipo MIME de los ficheros descargados. Además, este módulo garantiza que applets de Java, controles ActiveX y scripts queden bloqueados antes de su descarga por parte del usuario.

Óptimo rendimiento

La tecnología *VirtualFile* de Panda **analiza en memoria todos los ficheros** -incluso los comprimidos-, obteniendo una velocidad muy superior a la obtenida cuando es necesario desviarlos al disco duro.

Por otro lado, la tecnología *PartFile* permite al administrador de red equilibrar directamente los parámetros de rendimiento y seguridad del servidor ISA, reteniendo para su análisis y desinfección sólo los ficheros sospechosos.

Potente motor heurístico

Su potente y avanzado motor de análisis de HTML, capaz de encontrar tanto los virus como los objetos maliciosos ocultos en las páginas web, detiene y destruye las amenazas sin dejarlas pasar a la red interna.

Panda for ISA, también incorpora el *Genetic Heuristic Engine* (GHE), un potente motor heurístico de alta eficacia en la detección de nuevas amenazas, lo que permite enviar los elementos sospechosos a cuarentena temporalmente hasta que Panda los desinfecta automáticamente.

Administración centralizada y remota

Panda for ISA se gestiona de forma remota y centralizada, mediante un interfaz único: **Panda AdminSecure**. Gracias a él, se instalan y controlan todas las soluciones Panda, contando para ello con vistas, informes gráficos, avisos, etc. en tiempo real.

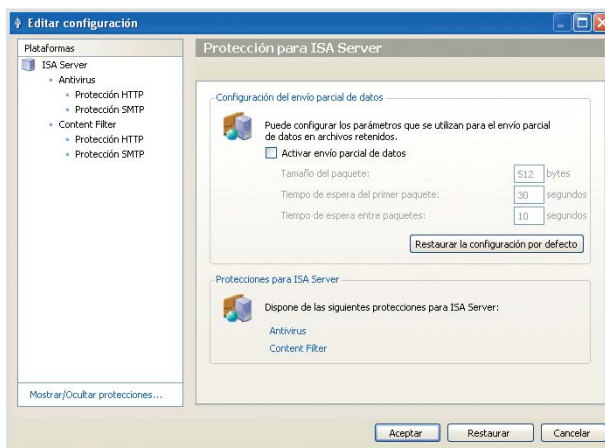
Así, en lugar de gestionar individualmente cada servidor o las protecciones (antivirus, antispam, antispysware...) instaladas en los servidores, basta con una consola. Desde **AdminSecure** se administra de forma consistente todas las protecciones incluso, cuando se despliegan en plataformas heterogéneas.

Actualizaciones automáticas cada hora

Panda for ISA se puede configurar para que, cada hora y sin intervención por parte del usuario, compruebe si existen nuevos ficheros de firmas y en ese caso, se actualice automáticamente. Las actualizaciones incrementales del Archivo de Identificadores de Malware contribuyen a la reducción del consumo total de ancho de banda y a suavizar los picos que se producen en las comunicaciones.

Flexible configuración

Los administradores reciben alertas directamente por correo SMTP, a través de la red con un mensaje en pantalla. Estas alertas admiten parámetros para evitar la saturación con mensajes innecesarios.



Requerimientos técnicos

Panda AdminSecure

Consola

Pentium II 266 MHz o superior.
RAM: 140MB.
Disco duro: 140MB.
Internet Explorer 5.5.
Windows installer 2.0.

Sistemas operativos: Windows 2000 / XP / XP 64 bits, Terminal Server, Windows 2000 Server SBS, Windows Server 2003 Enterprise Edition/SBS/R2, Windows Server 64-bit, Windows Vista 32 bits/64 bits, Windows Server 2008 (32 y 64 bits).

Panda Security for ISA Servers

ISA Server 2004 Standard o Enterprise
Pentium III 550MHz o superior.
RAM 1GB.

Partición Local NTFS con 200MB de disco duro más 60MB para el caché web content.

ISA Server 2006 Standard o Enterprise

Pentium III 733MHz.

RAM 1GB.

Partición Local NTFS con 200MB de disco duro más 60MB para el caché web content.

Sistemas operativos: Windows Server 2003/R2, Windows Server 2003 SP1.

"Para todos los que recibimos mucho correo electrónico siempre es una garantía tener Panda Antivirus instalado en nuestros sistemas para evitar la proliferación de virus en nuestra red."

Iñigo Arias. Director de Marketing Área Hipermercados. Grupo Eroski. ESPAÑA.

Certificaciones Panda Security



Recuerde que **Panda for ISA** se puede adquirir de forma independiente o integrado en **Panda Security for Enterprise**.