

SOLUCIONES

Seguridad



Villarroel, 36 - Entlo
08011 - BARCELONA
Telf: 93 218 85 00
Fax: 93 218 82 57
www.capris.es
info@capris.es





Soluciones de Seguridad de Contenido



Protecciones contra amenazas de red

Firewall

Máximización del control

Las comunicaciones entre todas las zonas de red, usuarios, grupos, etc. serán controladas por el sistema firewall y conocidas por el administrador para conseguir el mayor rendimiento posible de la red.

Realiza dos tipos diferentes de filtrado:

1. Estático a nivel de red.
2. Dinámico a nivel de aplicación.
 1. El estático a nivel de red se basa en reglas definidas por el administrador para tráfico entrante y saliente.
 2. El dinámico a nivel de aplicación con "Stateful Inspection" realiza un seguimiento del estado y contexto de las comunicaciones, básico en todos los protocolos y avanzado en FTP, PPTP, L2TP, IPSEC, estado de la comunicación, timeouts, conexiones realizadas... y "Deep Packet Inspection" que realiza el análisis de contenido del paquete para inspeccionar los mensajes HTTP, FTP, SMTP, IMAP, POP3, etc., cuando hay otros módulos habilitados.

Servicio VPN

Transmisiones seguras

El servicio VPN proporciona túneles seguros de comunicación con usuarios remotos o con otras sedes, adaptándose al modo de trabajo actual de la empresa. Permite conectar a la red corporativa desde ordenadores remotos de modo que la información que viaja por Internet sea cifrada en origen y descifrada al llegar al destino, evitando así que información relevante caiga en manos inadecuadas. El servicio VPN funciona en configuraciones Host to Host, Host to Net y Net to Net, soportando los protocolos IPSec, SSL, L2TP y PPTP, en modo servidor. Además, sobre SSL e IPSec funciona también en modo cliente.

Sistema de prevención contra intrusiones (IPS)

Refuerzo de la seguridad

Evita los ataques externos de rápida expansión, que son capaces de eludir los antivirus tradicionales. Detecta los intentos de intrusión por medio de un fichero de identificadores de intrusiones ofrecido por Panda Software y que se actualiza automáticamente cada 90 minutos. Los protocolos analizados son IP, ICMP, TCP y UDP. Se puede configurar el bloqueo automático de intrusiones detectadas, además de especificar valores límite y umbral para cada regla, que reducirán los falsos positivos.

Protecciones contra amenazas de contenidos

Anti-malware

Protección completa

Detiene todo tipo de malware, incluso el aún no catalogado y siempre está actualizado.

Ofrece protección tanto proactiva como reactiva contra toda amenaza que pueda llegar a través de los 6 protocolos más utilizados de Internet (HTTP, FTP, SMTP, POP3, IMAP4 y NNTP). Entre estas amenazas encontramos: virus, programas espía, troyanos, gusanos, dialers, jokes, intentos de phishing y otros riesgos tales como las hacking tools o Security Risks. Además, bloquea virus desconocidos gracias a su análisis heurístico.

Content Filter

Adaptabilidad

La protección es totalmente personalizable por el administrador de la red, según las políticas de seguridad de la compañía.

Filtra los contenidos potencialmente peligrosos que puedan estar dentro de ficheros comprimidos, archivos ejecutables, controles ActiveX, etc. Se configura separadamente para protocolos de correo/noticias o para protocolos de navegación/descarga.

Anti-spam

Correo limpio

Evita el tráfico de correo basura optimizando los recursos de red y liberando a los usuarios de la red de mensajes improductivos que ralentizan su trabajo. Verifica todo el correo entrante en la red y los mensajes analizados se clasifican como spam, probable spam o no spam, utilizando técnicas de evaluación multifunción (bayesianas, heurística, reglas...), lo que permite bloquear el correo no deseado antes de que llegue a los buzones de sus destinatarios o modificar el asunto para ahorrar tiempo a los usuarios de la red.

Filtrado web

Incremento de la productividad

Controla el acceso a contenidos web no necesarios o inadecuados para el desarrollo del trabajo diario, mejorando la productividad de los empleados. Permite definir categorías de contenidos web no deseables y listas de páginas web permitidas o prohibidas. Así, el administrador controla el uso de los recursos de la red corporativa y corta de raíz el acceso a contenidos de carácter ofensivo, violento, comercial, etc.

