



Firewall Advanced 2.0

Hoja de especificaciones



El Firewall Advanced 2.0 es la culminación del extenso desarrollo de una solución definitiva para el uso seguro de recursos de red, llevado a cabo por ProLinux.

La protección perimetral es el avance tecnológico más importante en esta herramienta, proveyendo seguridad y control para que sus redes funcionen sin interrupciones y con el menor tiempo de espera posible.

Conectable a cualquier medio de acceso a Internet

Línea directa.
Wireless.
ADSL dinámico o estático.

Filtrado de paquetes

Control de acceso multidireccional.
Limitación de acceso desde la red interna a Internet.
Protección contra accesos desde el exterior.

Anti-Virus perimetral

Cada archivo que intente ser descargado de la web, será escaneado en busca de virus. Si el resultado es positivo, el sistema no permitirá que el archivo sea descargado en el equipo del usuario.
Se escanea tráfico Web, FTP y correo electrónico.
El sistema anti-virus se actualiza automáticamente cada 8 horas.
Notificación de denegación de descarga del virus por e-mail al administrador de sistemas designado.
Reportes automatizados con estadísticas de la protección anti-virus.

IDS (Intrusion detection system)

Sistema de detección de intrusos activo 100% automático.
Permite configuraciones especiales basadas en las posibles vulnerabilidades del software, permitiendo proteger servidores en la DMZ o equipos de clientes en la LAN.
Escaneo de tráfico en tiempo real en busca de patrones de ataque, portscans, exploits o respuestas de sistemas crackeados.
Análisis on-the-fly de tráfico anómalo, detección de LZs (Landing Zones) de shellcodes diseñados para explotar buffer-overflows para todas las arquitecturas y alertas automáticas en caso de intento.
Estadísticas detalladas a través de interfaz web.
Base de reglas actualizable en forma periódica para cubrir nuevos formatos de ataque, mantenida mediante gestión remota (*).

Control de acceso a los usuarios

Gestión de usuarios para el acceso a la web.
Integración con servidores Microsoft Windows NT/2000/2003, Samba o Novell para autenticación de usuarios.

Filtrado de contenido

Restricciones de acceso a ciertos sitios web desde la red interna.
Establecimiento de horarios de acceso a ciertos servicios o sitios.
Proxy web transparente con control de tráfico.
Filtrado de mensajes de correo SPAM, reduciendo en un 80% el tráfico entrante del mismo.
Control de acceso a servicios como:

- Sistemas de mensajería electrónica.
 - MSN Messenger.
 - AOL Instant Messenger.
 - Yahoo Messenger.
 - Etc.
- Webmail externo.
- Correo electrónico personal.
- Sitios web de información y noticias.
- Restricción de tamaño de archivos transferidos.

ProLinux S.R.L. Maldonado 1707 – Montevideo, Uruguay – Telefono +(5982)4864740

Web: <http://www.prolinux.net.uy> – E-Mail: info@prolinux.net.uy

Todos los derechos reservados

Todas las marcas nombradas en este documento son propiedad de sus respectivos dueños

Firewall Advanced 2.0

Hoja de especificaciones

- Limitación y control de servicios y software de P2P como Kazaa, E-Mule, Napster, BitTorrent, Azureus, Ares, etc.
- Cualquier servicio definido por el cliente

Reconfiguración dinámica de reglas de acceso mediante gestión remota (*)

Protección de servidores ubicados en la(s) DMZ.	El IDS previene ataques desde el exterior y protege todos los servidores situados dentro del perímetro protegido
--	--

Gestión de ancho de banda y priorización de tráfico	El clasificador de tráfico permite definir prioridades y asignar ancho de banda específico para tipos de tráfico diferenciales. Se proveen hasta 6 canales con prioridades distintas y funciones de clasificación dinámica de paquetes para proveer QoS.
--	---

De 2 a 6 zonas de seguridad definidas (segmentos físicos).	<ul style="list-style-type: none">● LAN1, LAN2, etc.● DMZ1, DMZ2, etc.● Internet1, Internet2, etc. Múltiples enlaces posibles, balance de ancho de banda, soporte para enlaces de distintos proveedores. Si uno de los N enlaces a Internet cae, todo el tráfico se reconfigura automáticamente para pasar por los restantes enlaces, y al volver, se restaura el estado anterior. Avisos automáticos por e-mail de cambio de estado de los enlaces.
---	--

DHCP para las LAN (auto configuración de direcciones IP para cada host)	Asignación de IP desde el firewall según MAC del host. Filtrado de paquetes por dirección MAC.
--	---

Monitoreo y auditoria de tráfico	La interfaz de análisis avanzado de tráfico provee información en tiempo real sobre el acceso de cada equipo de la red al exterior y viceversa, sin excepciones. Información sobre quien está navegando en donde. Información sobre cual es el equipo que consume más ancho de banda. Información sobre qué tipo de tráfico y servicios son los más usados en su red.
---	--

Gateway de VPN (Red Privada Virtual)	Interconectividad entre sucursales remotas Conexión de equipos que viajan, como notebooks, PDA y Handhelds con soporte de VPN (road warriors) desde cualquier lugar del mundo. Aprovechamiento de recursos distribuidos.
---	--

Gestión y reconfiguración remota bajo demanda	Cambios de configuración, nuevos accesos, modificación de políticas y esquemas de funcionamiento desde nuestro NOC. (**)
--	--

Monitoreo remoto	Herramientas de monitoreo interno y externo del firewall conectable a servicio de monitoreo central de ProLinux (**)
-------------------------	--

Configuraciones especiales a medida	Reconfiguración del firewall para contemplar casos no standard.
--	---

(*) El servicio de gestión remota se contrata aparte

(**) El servicio de monitoreo se contrata aparte

Requerimientos mínimos de hardware:

Procesador: Intel Pentium III o compatible de 450 Mhz

Memoria: 256 Mb de RAM

ProLinux S.R.L. Maldonado 1707 – Montevideo, Uruguay – Telefono +(5982)4864740

Web: <http://www.prolinux.net.uy> – E-Mail: info@prolinux.net.uy

Todos los derechos reservados

Todas las marcas nombradas en este documento son propiedad de sus respectivos dueños

Firewall Advanced 2.0

Hoja de especificaciones

Almacenamiento: Disco 20 Gb
Red: 1 tarjeta de red 10/100/1000 por zona

Hardware recomendado:

Procesador: Intel Pentium IV de 1 Ghz
Memoria: 512 Mb de RAM ECC.
Almacenamiento: RAID L1 o L5 de 40Gb
Red: 1 tarjeta de red 10/100/1000 por zona

Compatibilidad:

El **Firewall ProLinux Advanced 2.0** es compatible con cualquier esquema de red de computadoras y puede ser instalado independientemente de cualquier configuración de hardware o software de los equipos servidores y clientes.

La instalación y configuración del software serán realizadas por personal de **ProLinux** solamente.

El hardware para la instalación de este software puede ser provisto por el cliente, pero siempre dentro de las especificaciones de requerimientos definidos en este documento.

ProLinux no se hace responsable por el funcionamiento del hardware provisto por el cliente, aunque puede prestar asistencia al cliente para solucionar cualquier inconveniente a pedido del mismo.

ProLinux S.R.L. Maldonado 1707 – Montevideo, Uruguay – Telefono +(5982)4864740

Web: <http://www.prolinux.net.uy> – E-Mail: info@prolinux.net.uy

Todos los derechos reservados

Todas las marcas nombradas en este documento son propiedad de sus respectivos dueños