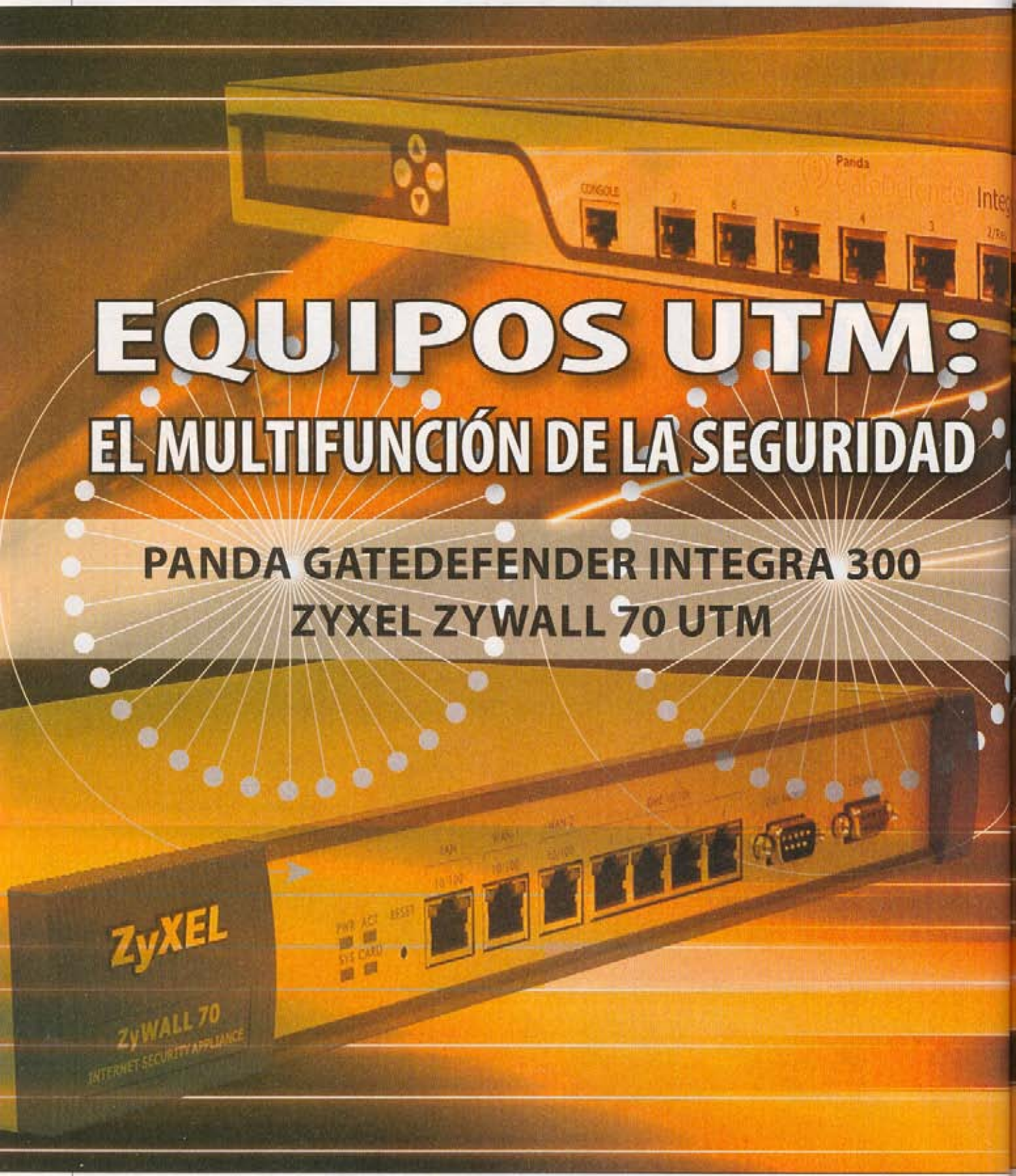
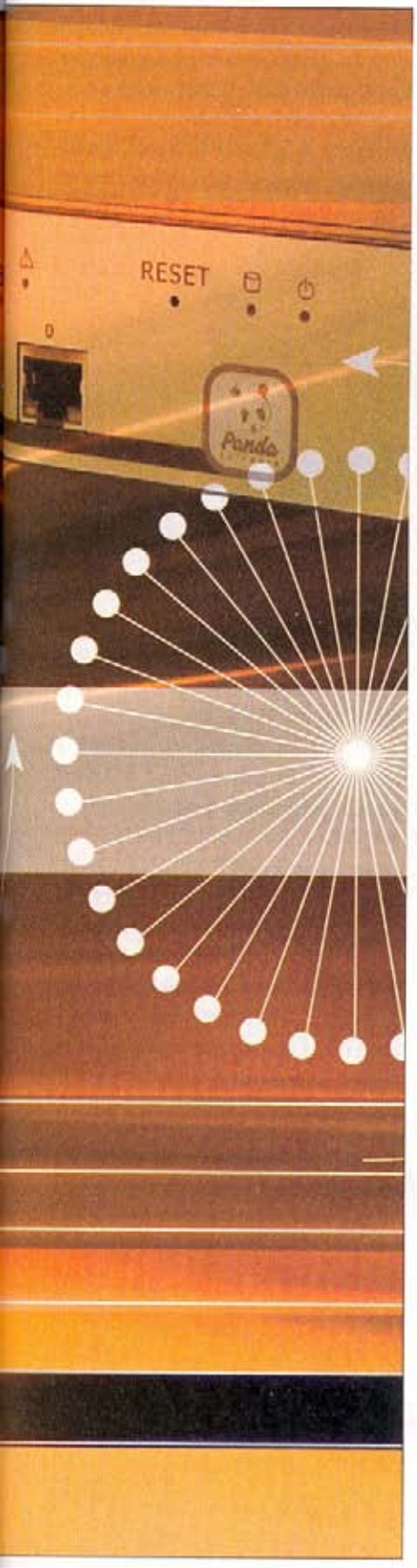


EQUIPOS UTM:
EL MULTIFUNCIÓN DE LA SEGURIDAD

PANDA GATEDEFENDER INTEGRA 300
ZYXEL ZYWALL 70 UTM



Los equipos UTM (Unified Threat Management, o gestión unificada de amenazas) son dispositivos que integran múltiples funciones de protección en un único chasis. A continuación, analizamos dos modelos UTM enfocados a soportar diferente carga de tráfico, Panda GateDefender Integra 300 (hasta 250 usuarios), y Zyxel Zywall 70 UTM (hasta 100 usuarios).

Daniel Comino Lucendo [dcomino@idg.es]

Tomarse en serio la seguridad de la empresa es un reto que cada vez están entendiendo más organizaciones. No obstante, el parque de redes sin proteger (o deficientemente protegidas) en nuestro país es todavía bastante elevado, por lo que es necesario tomar las medidas pertinentes.

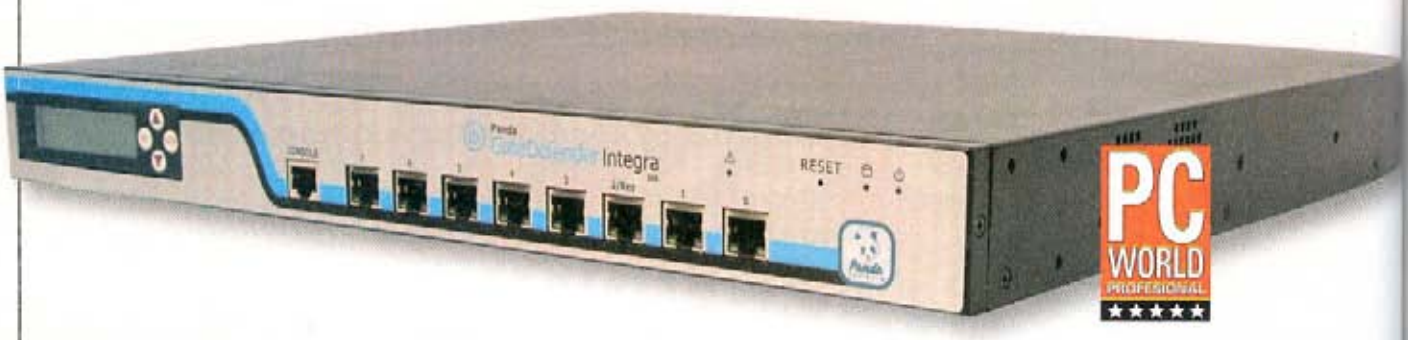
Los dispositivos UTM son elementos que aglutinan en un único producto protección antivirus, un cortafuegos (firewall) y un sistema de prevención de intrusos. No obstante, en la mayor parte de los casos, los fabricantes son capaces de incluir otras ventajas, como gestión de túneles VPN entre otros.

Por otra parte, al contrario de lo que mucha gente piensa, los dispositivos UTM no son la única medida a tomar si queremos mantener nuestra red protegida, ya que existen otras muchas amenazas que no quedan cubiertas por estos productos, pero lo cierto es que sirven para dar la cara en negocios pequeños y medianos, evitando gran parte de los ataques "automáticos" que se reciben en una organización.

A continuación presentamos dos modelos concebidos bajo la misma premisa (protección UTM). Se trata de los últimos modelos de Panda Software (GateDefender Integra 300), y Zyxel (Zywall 70 UTM). Ambos permiten la opción de actuar en modo transparente dentro de la red (bridge, integrándose en la red existente) o en modo router (sería quien da la cara a Internet y canalizase la información entre la parte interna e Internet).

PANDA SOFTWARE GATEDEFENDER INTEGRA 300

En la pasada edición de PC World (septiembre, número 234) ya analizamos la gama Performa de Gatedefender. En este caso se trata de retomar el hilo que deja el Performa para comentar las ventajas adicionales que aportan los modelos UTM, en nuestro caso hemos analizado el Gatedefender Integra 300 (el más alto de gama).



A nivel externo, el Integra 300 cuenta con ocho puertos gigabit Ethernet; uno de ellos es para la zona pública (desde donde se actualizará el sistema), y el resto son para la zona interna (uno de ellos será el encargado de aceptar las conexiones de administración, y el resto se pueden distribuir dentro de los diferentes servicios de la topología interna).

En primer término, cabe comentar que la gama Integra, al igual que ocurre con el Zywall 70 UTM de Zyxel, cuenta con dos modalidades de funcionamiento. En la primera de ellas, modo bridge (puente), actúa de mero intermediario dentro de la red, analizando paquetes y devolviéndolos a su estado inicial a través de sus módulos antivirus, antispam, filtrado de contenidos y Web. Si activamos el modo router (lo más recomendable en los dispositivos Integra), sin embargo, además de los beneficios que tiene el modo bridge, quedará activado el cortafuegos, el gestor de VPN y la protección contra intrusiones.

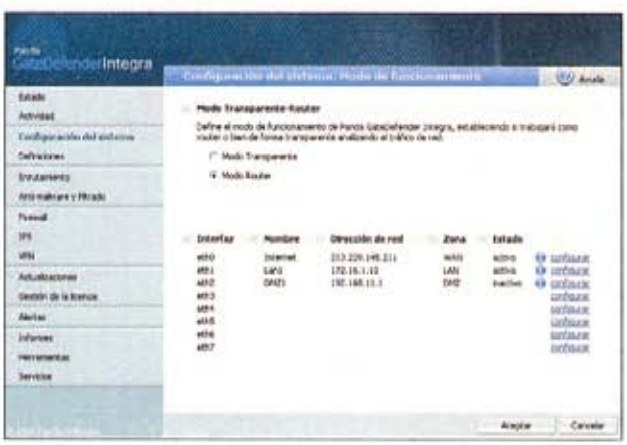
FABRICANTE	Panda Software
MODELO	GateDefender Integra 300
WEB	www.pandasoftware.es
TELÉFONO	902 365 505
PRECIO (*)	7.006,4 € (iva incluido)
NOTA	8,9

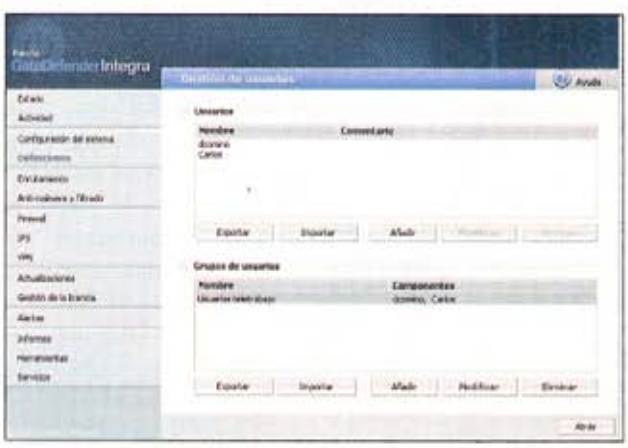
(*) incluye producto + licencias de AV, antispam, IDS y filtrado de contenidos y 8 horas de instalación y puesta en marcha (1.113,60 euros)

Por otra parte, si nos centramos en sus diferentes vertientes nos encontramos con que, además del módulo antivirus (lógicamente mantenido por Panda Software), el apartado de antispam se confía a Mailshell (como ya vimos en la gama Performa). Igualmente, el apartado de VPN se basa en una iniciativa de software libre, OpenVPN, mientras que el módulo de detección de intrusos viene de la mano de Snort (código abierto de nuevo).

En cuanto al nivel de análisis, el motor de antivirus es capaz de buscar en seis protocolos, entre los que se encuentran los más utilizados en el sector profesional (HTTP, FTP, SMTP, POP3, IMAP4 Y NNTP), asegurando así una alta protección.

Del mismo modo que sucede con el Performa, la gama Integra se administra fácilmente a través de un navegador Web. Para acceder a la página de gestión simplemente habremos de validarnos en el sistema con un usuario previamente configurado, y accede-





remos a la consola de control. Como viene siendo habitual en los nuevos productos de Panda Software, la gestión cuenta con una interfaz realmente intuitiva, sencilla de manejar, y totalmente traducida al castellano, algo poco habitual en dispositivos de este tipo. Esto permite que tanto la puesta en marcha como en mantenimiento del producto sea bastante sencillo.

Otra de las ventajas del Integra 300 es la posibilidad de configurarlo en modo de alta disponibilidad, lo que nos permite anidar tantos Integra como sea necesario, con el fin de que, en caso de caída, otro sea quien tome las riendas del análisis, manteniendo la red en todo momento protegida.

Como puntos débiles del Integra 300 podemos señalar que cuenta con una deficiente gestión de logs (tan sólo podemos verlos en modo texto). Por otra parte, aunque sí es posible gestionar múltiples usuarios con el fin de utilizarlos en el apartado de VPN, echamos en falta la posibilidad de poder segmentar a los distintos usuarios que acceden remotamente al sistema.

Por último, en el nivel de producto del Panda GateDefender Integra 300, nos parecería interesante la posibilidad de integrar en el producto la posibilidad de generar consultas LDAP, con el fin de poder llevar al plano del GateDefender la estructura real de usuarios que tenemos en la empresa. Una de las principales ventajas de esta medida sería el hecho de descartar directamente todos los correos que vayan dirigidos a usuarios no existentes en nuestro Active Directory. No obstante, por el momento, no es posible realizar este tipo de consultas.

FABRICANTE	Zyxel
MODELO	Zywall 70 UTM
WEB	www.zyxel.es
TELÉFONO	902 195 420
PRECIO (*)	1.909,68 € (iva incluido)
NOTA	8,3

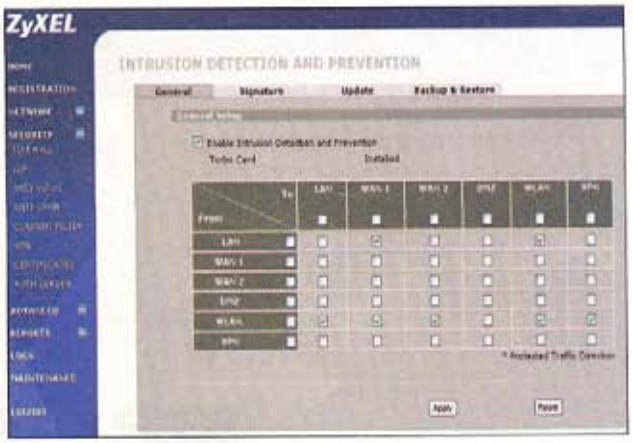
(*) incluye producto + licencias de AV, antispam, IDS y filtrado de contenidos

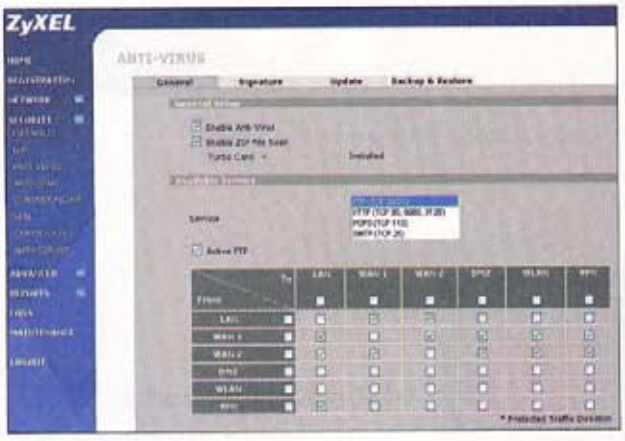
ZYXEL ZYWALL 70 UTM

El modelo ZyWall 70 UTM es, por el momento, el dispositivo UTM más ambicioso que comercializa Zyxel, aunque en este caso, el nivel de rendimiento que alcanza Integra 300 no es comparable con el de Zywall 70.

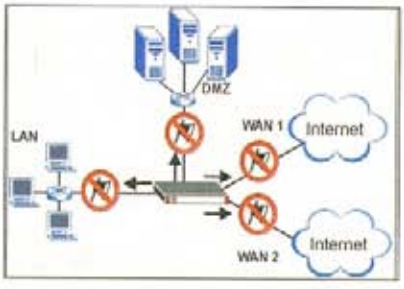
Se trata de un chasis de 1U que cuenta con tres zonas diferenciadas para facilitar la gestión de la red, cada una con puertos 10/100 Mbps (zona LAN, que tiene un puerto Ethernet, zona WAN, con dos puertos Ethernet, y zona DMZ, que dispone de hasta cuatro puertos Ethernet).

Esto significa que con el ZyWall 70





es posible gestionar dos redes distintas de acceso a Internet (por ejemplo dos ADSL de diferentes proveedores de Internet). Esto tiene varias ventajas, como la posibilidad de ofrecer calidad de servicio a ciertas tareas, asegurando un cierto ancho de banda, o utilizar



una de ellas como respaldo. Por último, el Zywall cuenta con un sistema de balanceo de carga, que permite direccionar tráfico a una y otra interfaz en base al nivel de carga que tenga cada una, lo que optimiza el sistema.

A la hora de configurar el producto necesitaremos como mínimo una IP pública (para que se actualice el producto) y una dirección del rango interno de nuestra red para poder acceder a la configuración del sistema, (funciona vía navegador Web, como en GateDefender).

Con el fin de aumentar el nivel de potencia del producto, el ZyWall 70 UTM tiene la opción de insertar una tarjeta PCMCIA (Turbo Card) con SecuASIC, que acelera el rendimiento, tanto del módulo de antivirus como de detección de intrusos (hasta 20 veces, según afirman en Zyxel).

Una vez que tenemos integrado el producto, podremos activar cada uno de los módulos del sistema, como antispam o antivirus (antes de activar el antivirus es necesario descargar el último fichero de firmas), y comenzar la configuración personalizada (tanto de las reglas del cortafuegos, como de los equipos que pueden acceder a la VPN, entre otros).

La administración Web cuenta con un menú perfectamente categorizado (en inglés) que nos permite modificar

TABLA DE CARACTERÍSTICAS

CARACTERISTICAS	GATEDEFENDER INTEGRA 300	ZYWALL 70 UTM
Capacidad del producto (usuarios)	250	50-100
Cortafuegos integrado	Sí	Sí
Antivirus	Sí (Panda)	Sí (Kaspersky)
Antispam	Sí (Mailshell)	Sí (Mailshell)
Filtrado contenidos	Sí	SI
Filtrado Web	Sí	No
Gestión de intrusos (IDS/IPS)	Sí (Snort)	Sí
VPN	Sí	Sí
Número de puertos WAN (*)	1	2
Alta disponibilidad	Sí, con otro GateDefender	Sí, con dos líneas
Capacidad del cortafuegos (Mbps)	850	100

(*) Líneas a Internet que soporta

bastantes parámetros del Zywall 70. No obstante, dentro de los grandes grupos en los que está dividido, probablemente los más importantes sean el apartado Network (donde tenemos la configuración de cada interfaz de red), y sobre todo Security, ya que engloba todos los módulos de configuración del dispositivo, entre los que se encuentran el cortafuegos, el detector de intrusiones, antivirus, antispam, filtrado Web o gestor de VPN entre otros.

Hemos de reconocer que la gestión del sistema no es la más intuitiva que hemos visto. De hecho, durante nuestras pruebas, tuvimos algunos problemas a la hora de configurar nuevos accesos VPN, ya que el interfaz no es del todo sencillo de entender.

El apartado para VPN tiene capacidad para mantener hasta 100 sesiones simultáneas. No obstante, al igual que nos ocurre con el Integra 300, lo cierto es que nos parece algo deficiente, ya que no cuenta con direccionamiento IP interno, o políticas de restricción avanzadas. No obstante, es posible montar túneles mediante IKE, PKI, y encriptar las comunicaciones mediante DES, 3DES o AES. También puede utilizar MD5 o SHA-1 como algoritmos de autenticación.

El módulo antivirus está basado en las firmas de Kaspersky, y es capaz de analizar los protocolos FTP, POP3 HTTP y SMTP. Puede detectar toda clase de virus, troyanos, gusanos desbordamiento de Buffer o puertas traseras (también cuenta con un detector para escaneos de puertos). Asimismo es capaz de analizar el tráfico y bloquear sesiones P2P, de mensajería instantánea o ataques encapsulados en Web. PCW