

## BIOS TECHNOLOGY SOLUTIONS S.L.

### Bios Security Box – Unified Threat Management



## Bios Security Box – Unified Threat Management

### Firewall

Gateways			
Name	RTT	Loss	Status
RADIOKABLEGW	37.130.146.129	25.8ms	0% <span>Online</span>
OrangeGW	192.168.2.1	177.9ms	0.0% <span>Online</span>

Interface Statistics			
	RADIOKABLE	LAN	ORANGE
Packets In	38094260	148050623	140194238
Packets Out	48111988	171741544	124282233
Bytes In	10.74 GB	62.94 GB	129.88 GB
Bytes Out	37.22 GB	140.04 GB	35.76 GB
Errors In	0	0	0
Errors Out	0	0	0
Collisions	0	0	0

Dyn DNS Status			
Int.	Service	Hostname	Cached IP
ORANGE	No-IP (free)	biosts.no-ip.org	90.170.156.23

SMART Status		
Drive	Ident	SMART Status
ad0	W1D1J8PH	PASSED

Thermal Sensors	
Core 0: 41.0 °C	
Core 1: 44.0 °C	

interpretación por el destino final del paquete. La directiva “scrub” también ensambla los paquetes fragmentados , protegiendo algunos sistemas operativos de algunas formas de ataque, y descarta los paquetes TCP que tengan combinaciones de indicadores válidos.

- Desactivación de filtros: Se puede desactivar el filtro de firewall por completo si se desea convertir Bios Security Box en un router puro.
- Tabla de estado global.

- Filtrado por origen y destino de IP, protocolo IP, puerto de origen y destino para el tráfico TCP y UDP.
- Limitar las conexiones simultáneas por reglas.
- Bios Security Box utiliza p0f , una utilidad de OS fingerprinting / red pasiva avanzada para permitir filtrar por el sistema operativo que inicia la conexión.
- Opción para registrar o no registrar el tráfico que coincide con cada regla.
- Política muy flexible de enrutamiento, gracias a la selección de la puerta de enlace en función de cada regla (para el balanceo de carga , conmutación por error, múltiple WAN, etc. )
- Alias: permiten agrupar por denominación de IPs , redes y puertos. Esto ayuda a mantener el conjunto de reglas de firewall limpio y fácil de entender, especialmente en entornos con múltiples direcciones IP públicas y numerosos servidores.

- Capa 2 Transparente: Permite agrupar interfaces y filtrar el tráfico entre ellos, incluso teniendo en cuenta un firewall IP.

➤ Paquete de normalización: Descripción de la documentación de grupo. Define la normalización de los paquetes para que no haya ambigüedades en la

System Information	
Name	biostsutm.localdomain
Version	2.1.5-RELEASE (amd64) built on Mon Aug 25 07:41:15 EDT 2014 Headless 8.3-RELEASE-316
	You are on the latest version.
Platform	pfSense
CPU Type	Intel(R) Pentium(R) CPU G630 @ 2.70GHz 2 CPU(s): 1 package(s) x 2 core(s)
Uptime	57 Days 02 Hours 03 Minutes 01 Seconds
Current date/time	Thu Nov 21 11:29:27 CET 2014
DNS server(s)	127.0.1.1 8.8.8.8 8.8.4.4
Last config change	Thu Nov 20 09:21:52 CET 2014
State table size	1% (574/191300) Show states
MBUF Usage	10% (256/2560)
Temperature	40.0°C
Load average	0.31, 0.31, 0.29
CPU usage	25%
Memory usage	27% of 1914 MB
SWAP usage	0% of 4096 NB
Disk usage	0% of 47G

- Tabla de estado del firewall: Mantiene información sobre las conexiones de red abiertas.
- Stateful firewall: Todas las reglas van con un estado asociado.
- La mayoría de las soluciones UTM comerciales de seguridad carecen de la capacidad para controlar finamente la tabla de estado . Bios Security Box tiene numerosas características que permiten un control granular de la tabla de estado.
- Tamaño de la tabla de estado ajustable: Bios Security Box permite poner en producción varios cientos de miles estados. El tamaño de la tabla de estado predeterminado varía en función de la memoria RAM instalada en el sistema, pero se puede aumentar sobre la marcha a medida que se requiera. Cada estado tiene aproximadamente 1 KB de memoria RAM.

Interfaces		
	<u>RADIOKABLE</u>	↑ 100baseTX <full-duplex> 37.130.146.176
	<u>LAN</u>	↑ 1000baseT <full-duplex> 192.168.0.253
	<u>ORANGE</u>	↑ 100baseTX <full-duplex> 192.168.2.2

Services Status		
Service	Description	Status
apinger	Gateway Monitoring Daemon	
bandwidthd	BandwidthD bandwidth monitoring daemon	
captiveportal	Captive Portal: Control_Ancho_de_Banda	
dhcpd	DHCP Service	
dnsmasq	DNS Forwarder	
nrpe2	Nagios NRPE Daemon	
ntpd	NTP clock sync	
openvpn	OpenVPN server: VPNBIOSTS	
squid	Proxy server Service	
squidGuard	Proxy server filter Service	

### Reglas Flexibles:

- Limitar las conexiones simultáneas de clientes.
- Estados Límite por host.
- Límite de nuevas conexiones por segundo.
- Definir tiempo de espera de estado.
- Definir el tipo de estado.
- Tipos de Estado - Bios Security Box ofrece múltiples opciones para manejar el estado.
- Mantener el estado - Funciona con todos los protocolos. Por defecto para todas las reglas.

Firewall: Rules														
Floating	RADIOKABLE	LAN	ORANGE	OpenVPN	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
					1	*	*	*	ANYAddress	12	*	*	*	Anti Leech Rule
					2	IPv4	conexión	*	*	*	FAILOVER_RK_ORANGE	none		GBASE-SALIDA_PRAL_RK_SECUNDARIA_ORANGE
					3	IPv4	192.168.0.53	*	*	*	RADIOKABLE0	none		Default allow LAN to any rule
					4	IPv4	192.168.0.201	*	*	*	FAILOVER_RK_ORANGE	none		GBASE-SALIDA_PRAL_RK_SECUNDARIA_ORANGE
					5	IPv4	192.168.0.175	*	*	*	FAILOVER_RK_ORANGE	none		GBASE-SALIDA_PRAL_RK_SECUNDARIA_ORANGE
					6	IPv4	192.168.0.202	*	*	*	FAILOVER_RK_ORANGE	none		FTP-SALIDA_PRAL_RK_SECUNDARIA_ORANGE
					7	IPv4	192.168.0.47	*	*	*	RADIOKABLE0	none		FTP-SALIDA_PRAL_RK_SECUNDARIA_ORANGE
					8	IPv4	LAN test	*	*	*	WANFAILOVER	none		Default allow LAN to any rule
					9	IPv6	LAN test	*	*	*	*	none		Default allow LAN IPv6 to any rule

- Estatados “Sloppy” - Funciona con todos los protocolos. Menos seguimiento estricto del estado, útil en casos de enrutamiento asimétrico.
- Estado Modular: Bios Security Box generará fuertes números de secuencia inicial ( ISNs ) en nombre del host.
- Estado Synproxy : Conexiones Proxies TCP entrantes para ayudar a proteger los servidores de paquetes falsificados o inundaciones TCP SYN. Esta opción incluye la funcionalidad de mantener el estado y el estado modular combinado .
- Estado Nulo: No guardar las entradas del estado para este tráfico. Esto es raramente deseable , pero está disponible , ya que puede ser útil en algunas circunstancias limitadas .
- Opciones de optimización de la tabla del Estado - Bios Security Box ofrece cuatro opciones para la optimización de la tabla de estado .
- Definición de algoritmos en reglas de estados.
- Alta latencia - Util para enlaces de alta latencia , como las conexiones por satélite . Expira conexiones inactivas después de lo normal .
- Agresivo - Expira conexiones inactivas más rápidamente. Un uso más eficiente de los recursos de hardware.
- Conservador - Trata de evitar que se caiga conexiones legítimas a expensas de un mayor uso de la memoria y de la CPU.

### Network Address Translation ( NAT)

- Delante del puerto a traducir; incluyendo los rangos y el uso de varias direcciones IP públicas
- NAT 01:01 para las direcciones IP individuales o subredes enteras.
- NAT saliente
- Permite establecer una configuración predeterminada de NAT: Todo el tráfico saliente a la WAN IP . En múltiples escenarios WAN , el tráfico de salida NAT a la dirección IP de la interfaz WAN.

Firewall: NAT: Port Forward

Port Forward								
if	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
WANLINK	TCP	*	*	WANLINK address	21 ( 1 )	192.168.0.202	21 ( 1 )	Acceso a IP por RadioGlobe
ORANGE	TCP	*	*	ORANGE address	21 ( 1 )	192.168.0.204	21 ( 1 )	Acceso a IP por Orange
RADONWIFI	TCP	*	*	RADONWIFI address	22 ( 1 )	192.168.0.47	22 ( 1 )	Acceso SSH A MUM por RadioGlobe
RADONWIFI	TCP	*	*	RADONWIFI address	9763	192.168.0.47	9763	Acceso a MUM por RadioGlobe
RADONWIFI	TCP	*	*	RADONWIFI address	9443	192.168.0.47	9443	Acceso A MUM por RadioGlobe
RADONWIFI	TCP	*	*	RADONWIFI address	443 ( HTTPS )	192.168.0.47	443 ( HTTPS )	Acceso A MDM Itius por RadioGlobe
RADONWIFI	TCP	*	*	RADONWIFI address	8000 ( 102 )	192.168.0.47	8000 ( 102 )	Acceso A RADONWIFI 3000 por RadioGlobe
RADONWIFI	TCP	*	*	RADONWIFI address	3001	192.168.0.47	3001	Acceso A MUM TCP 3001 por RadioGlobe
RADONWIFI	TCP	*	*	RADONWIFI address	80 ( HTTP )	192.168.0.46	80 ( HTTP )	Acceso A Radio por RadioGlobe
ORANGE	TCP	*	*	ORANGE address	80 ( HTTP )	192.168.0.46	80 ( HTTP )	Acceso A Radio por Orange
ORANGE	TCP	*	*	ORANGE address	80 ( HTTP )	192.168.0.211	80 ( HTTP )	Acceso A RADONWIFI por RadioGlobe
RADONWIFI	TCP	*	*	RADONWIFI address	8069	192.168.0.201	8069	Acceso a OpenCRP por RadioGlobe
ORANGE	TCP	*	*	ORANGE address	8069	192.168.0.201	8069	Acceso a OpenCRP por Orange

- Advanced Outbound NAT: Permite este comportamiento predeterminado que se utilice y permite la creación de NAT muy flexible (o no crear reglas NAT)
- NAT Reflexión: NAT reflexión es capaz de permitir que los servicios puedan acceder a través de IP pública desde las redes internas.

## DNS dinámico

- Un cliente de DNS dinámico se incluye para permitir a registrar su dirección IP pública con una serie de proveedores de servicios de DNS dinámico.
- Custom: Permite la definición de método de actualización para los proveedores que no estén específicamente aquí. También incluye la mayoría de los clientes DNS Dinámicos comerciales: DNS- O- Matic, DynDNS, DHS, DNSexit, DYNS, easyDNS, FreeDNS, HE.net, Loopia, Namecheap, No-IP, ODS.org, OpenDNS, Ruta 53, SelfHost, ZoneEdit.
- Un cliente para RFC 2136 : Actualizaciones de DNS dinámicas , para su uso con servidores DNS , como BIND que apoyan este medio de actualización.

## Balanceo de carga o WAN Failover

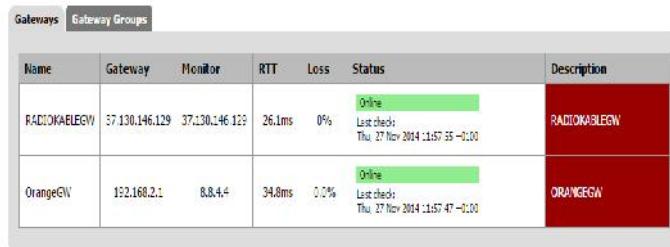
- Balanceo de carga en tráfico saliente / Salida de todo el tráfico por la interfaz WAN que esté operativa
- El balanceo de carga del tráfico de salida se utiliza con múltiples conexiones WAN para proporcionar capacidades de balanceo de carga y comutación por error. El tráfico se dirige a la puerta de enlace deseada o al pool de carga sobre una base de reglas por cortafuegos.
- Balanceo de carga en tráfico de entrada.

Status: Gateway Groups



Group Name	Gateways		Description		
WANFAILOVER	Tier 1	OrangeGW, Online	Tier 2	RADIOKABLEGW, Online	WANFAILOVER
FAILOVER_RK_ORANGE	Tier 1	RADIOKABLEGW, Online	Tier 2	OrangeGW, Online	FAILOVER RP ALINK SECUNDARIA ORANGE

### Status: Gateways



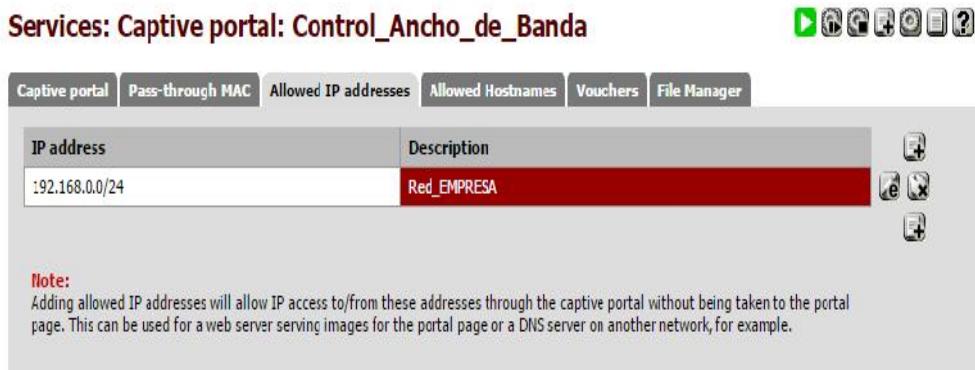
Name	Gateway	Monitor	RTT	Loss	Status	Description
RADIOKABLEGW	57.130.146.129	37.130.146.129	26.1ms	0%	Online Last check: Thu, 27 Nov 2014 1:15:35 -01:00	RADIOKABLEGW
OrangeGW	192.168.2.1	8.8.4.4	34.8ms	0.0%	Online Last check: Thu, 27 Nov 2014 1:15:47 -01:00	ORANGEGW

- El equilibrio de carga de entrada se utiliza para distribuir la carga entre varios servidores. Esto es comúnmente utilizado con los servidores web , servidores de correo , y otros. Los servidores que no responden a las solicitudes de ping o conexiones de los puertos TCP se eliminan del pool.

## Portal cautivo

- Un Portal cautivo obliga al usuario a su autenticación a través de una página web de acceso (personalizable por su organización) a la red de su corporación (una página web visible para cualquier dispositivo; ya sea un PC, un Tablet, un teléfono móvil..). Esto es comúnmente utilizado en las redes de puntos calientes (HotSpot) , pero también se usa ampliamente en las redes corporativas para una capa adicional de seguridad en el acceso inalámbrico o Internet.
- Las características principales del Portal Cautivo son:

**Services: Captive portal: Control\_Ancho\_de\_Banda**



**Note:**  
 Adding allowed IP addresses will allow IP access to/from these addresses through the captive portal without being taken to the portal page. This can be used for a web server serving images for the portal page or a DNS server on another network, for example.

- Número máximo de conexiones simultáneas: Limitar el número de conexiones con el propio portal por IP del cliente. Esta característica evita
- que una denegación de servicio desde PC clientes que envían tráfico de la red en varias ocasiones sin autenticar o accediendo a la página de bienvenida.
- Intervalo de espera inactivo: Desconectar a los clientes que están en reposo durante más de un número preestablecido de minutos.
- Timeout duro: Fuerza una desconexión de todos los clientes después de que el número definido de minutos se cumpla.
- Logon ventana emergente: Opción para que aparezca una ventana con un botón de cierre de sesión .
- Redirección de URL: Despues de la autenticación o accediendo el portal cautivo , los usuarios puede ser la fuerza redirigidos a la URL definida.
- Filtrado MAC : Bios Security Box filtra usando direcciones MAC. Si se dispone de una red detrás de un router en una interfaz de portal cautivo habilitada , todas las máquinas detrás del router serán autorizados después de que se autorizó un usuario. Filtrado MAC se puede desactivar para estos escenarios
- Opciones de autenticación: Hay tres opciones de autenticación disponibles.
- Sin autenticación - Esto significa que el usuario simplemente hace clic a través de la página del portal sin necesidad de introducir las credenciales.

- Gestión de usuarios locales - Una base de datos de usuarios locales puede ser configurada y utilizada para la autenticación.
- Autenticación RADIUS - Este es el método de autenticación preferido para entornos corporativos y proveedores de Internet . Se puede utilizar para autenticar contra un Microsoft Active Directory y numerosos servidores RADIUS.

#### Capacidades del Servidor RADIUS:

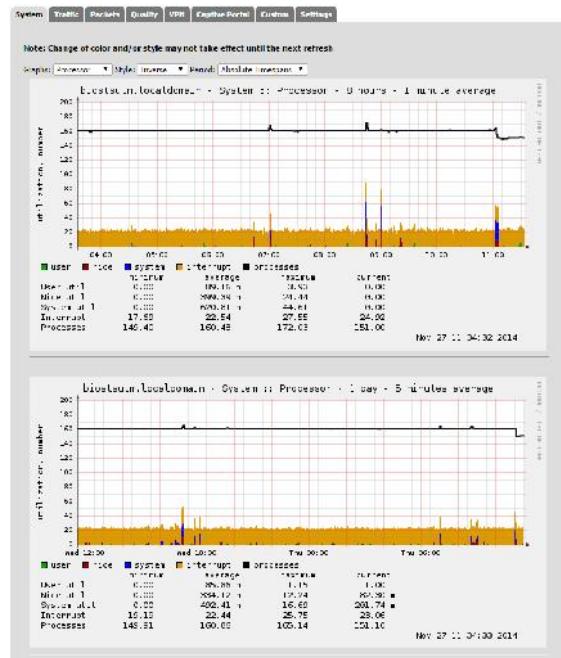
- Forzado re-autenticación
- Capaz de enviar actualizaciones a los usuarios conectados según las normas definidas.
- Autenticación RADIUS MAC: Permite al portal cautivo autenticar a un servidor RADIUS utilizando la dirección MAC del cliente como el nombre de usuario y contraseña.
- Permite la configuración de los servidores RADIUS redundantes.
- HTTP o HTTPS - La página del portal puede ser configurado para utilizar HTTP o HTTPS.
- Pass- a través de direcciones MAC e IP - direcciones MAC e IP pueden ser definidas como transparentes para evitar el portal.

Host IP	Bandwidth In	Bandwidth Out
192.168.0.106	9.18M Bits/sec	187.50k Bits/sec
192.168.0.69	59.14k Bits/sec	0.00 Bits/sec
192.168.0.45	10.31k Bits/sec	0.00 Bits/sec
192.168.0.201	4.10k Bits/sec	15.90k Bits/sec
192.168.0.48	3.83k Bits/sec	0.00 Bits/sec
192.168.0.103	0.00 Bits/sec	2.89k Bits/sec

- Administrador de archivos - Esto le permite subir imágenes para su uso en las páginas del portal.

#### Alta Disponibilidad

- CARP : Permite la commutación por error de hardware. Dos o más servidores de seguridad (UTM) se pueden configurar como un grupo de commutación por error . Si una interfaz falla en la UTM primaria, esta se desconecta por completo, pasando a ser la UTM secundaria.



➤ Bios Security Box también incluye capacidades de sincronización de configuración , para que realice los cambios de configuración en la primaria y que sincroniza automáticamente con el servidor de seguridad secundario.

➤ Pfsync asegura tabla de estado del servidor de seguridad y se replica en todos los servidores de seguridad configurados como secundarios (Alta

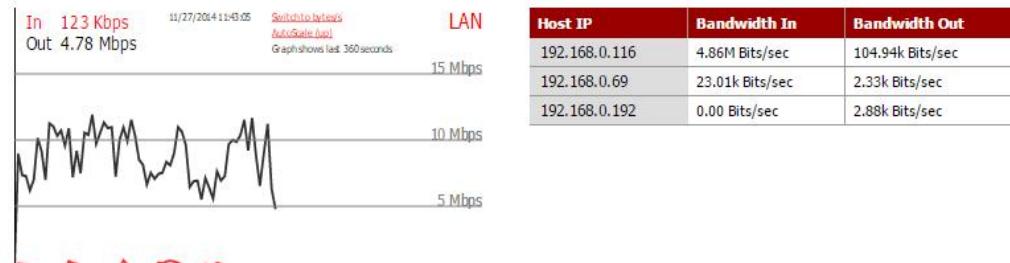
➤ Disponibilidad) . Esto significa que sus conexiones existentes se mantendrán en el caso de fallo, lo cual es importante para evitar interrupciones de la red en caso de un fallo físico de la UTM.

## Información en tiempo real

➤ La información histórica es importante, pero a veces es más importante ver la información en tiempo real.

### Status: Traffic Graph

Interface: LAN, Sort by: Bw In, Filter: Local, Display: IP Address



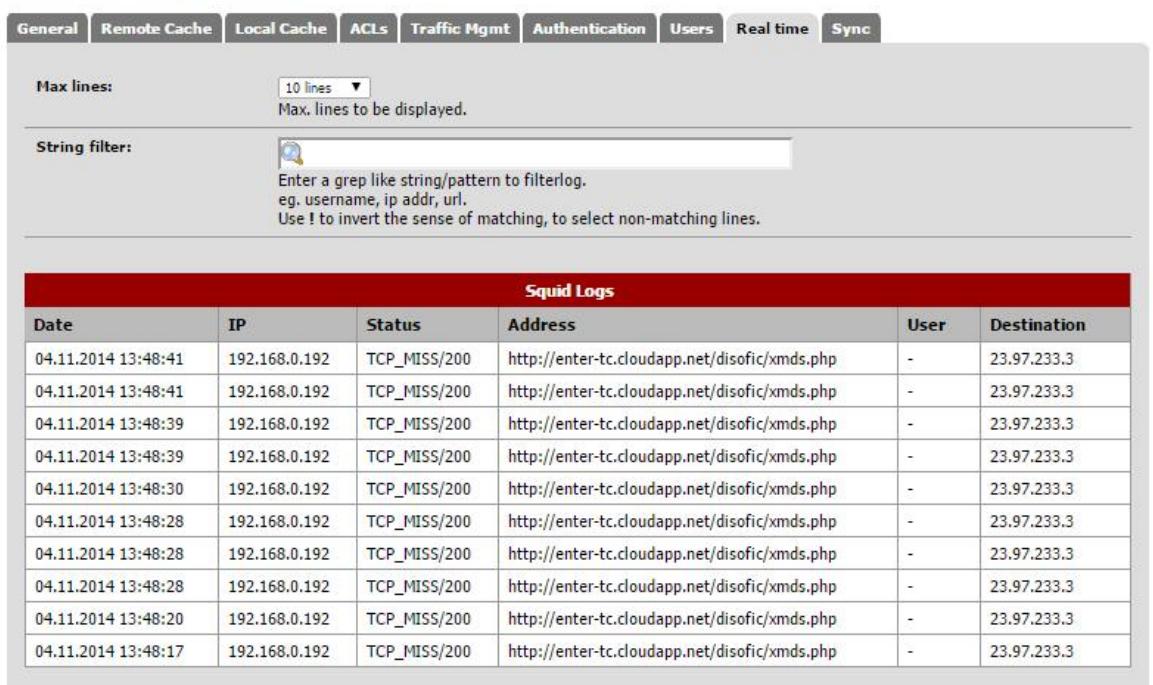
Note: the Adobe SVG Viewer, Firefox 1.5 or later or other browser supporting SVG is required to view the graph.

➤ Gráficos SVG están disponibles en Bios Security Box; muestran el rendimiento en tiempo real para cada interfaz .  
 ➤ Pantalla de colas: Proporciona una visualización en tiempo real del uso de colas utilizando AJAX con indicadores actualizados.  
 ➤ La portada incluye medidores de AJAX para la visualización de la CPU en tiempo real , memoria, swap y el uso del disco y el tamaño de la tabla de estado .

## Proxy Transparente

- Proxy con caché de HTTP, FTP y demás protocolos configurables.
- Squid proporciona un servicio de proxy que soporta peticiones HTTP, HTTPS y FTP a equipos que necesitan acceder a Internet y a su vez provee la funcionalidad de caché especializado en el cual almacena de forma local las páginas consultadas recientemente por los usuarios. De esta forma, incrementa la rapidez de acceso a los servidores de información Web y FTP que se encuentran fuera de la red corporativa.
- Squid también es compatible con SSL (Secure Socket Layer) con lo que también acelera las transacciones cifradas, y es capaz de ser configurado con amplios controles de acceso sobre las peticiones de usuarios.
- Squid puede formar parte de una jerarquía de cachés. Diversos servidores trabajan conjuntamente atendiendo las peticiones.
- Squid sigue los protocolos, HTCP, CARP y caché digests que tienen como objetivo permitir a un proxy «preguntarle» a otros cachés si tienen almacenado un recurso determinado.

### Status: Proxy Monitor

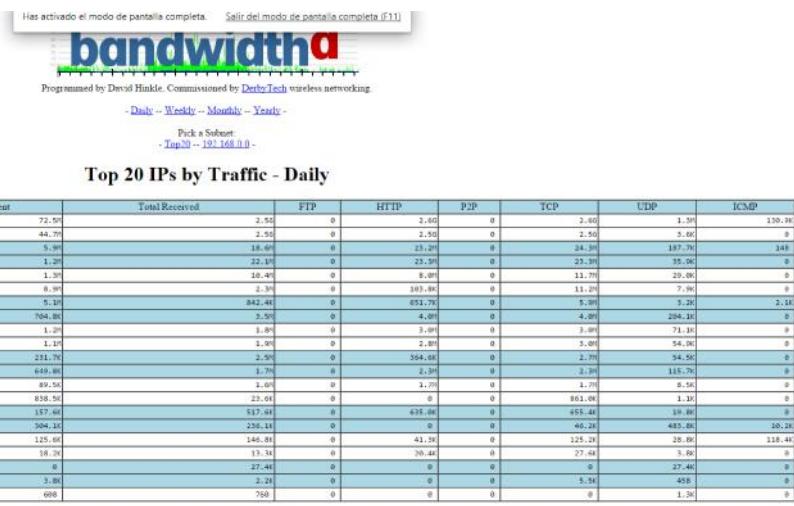


The screenshot shows the 'Proxy Monitor' interface with the 'Squid Logs' tab selected. The interface includes a 'General' tab and other tabs like 'Remote Cache', 'Local Cache', 'ACLs', 'Traffic Mgmt', 'Authentication', 'Users', 'Real time', and 'Sync'. The 'Squid Logs' table has the following columns: Date, IP, Status, Address, User, and Destination. The data in the table is as follows:

Squid Logs					
Date	IP	Status	Address	User	Destination
04.11.2014 13:48:41	192.168.0.192	TCP_MISS/200	http://enter-tc.cloudapp.net/disofic/xmds.php	-	23.97.233.3
04.11.2014 13:48:41	192.168.0.192	TCP_MISS/200	http://enter-tc.cloudapp.net/disofic/xmds.php	-	23.97.233.3
04.11.2014 13:48:39	192.168.0.192	TCP_MISS/200	http://enter-tc.cloudapp.net/disofic/xmds.php	-	23.97.233.3
04.11.2014 13:48:39	192.168.0.192	TCP_MISS/200	http://enter-tc.cloudapp.net/disofic/xmds.php	-	23.97.233.3
04.11.2014 13:48:30	192.168.0.192	TCP_MISS/200	http://enter-tc.cloudapp.net/disofic/xmds.php	-	23.97.233.3
04.11.2014 13:48:28	192.168.0.192	TCP_MISS/200	http://enter-tc.cloudapp.net/disofic/xmds.php	-	23.97.233.3
04.11.2014 13:48:28	192.168.0.192	TCP_MISS/200	http://enter-tc.cloudapp.net/disofic/xmds.php	-	23.97.233.3
04.11.2014 13:48:28	192.168.0.192	TCP_MISS/200	http://enter-tc.cloudapp.net/disofic/xmds.php	-	23.97.233.3
04.11.2014 13:48:20	192.168.0.192	TCP_MISS/200	http://enter-tc.cloudapp.net/disofic/xmds.php	-	23.97.233.3
04.11.2014 13:48:17	192.168.0.192	TCP_MISS/200	http://enter-tc.cloudapp.net/disofic/xmds.php	-	23.97.233.3

- Caché transparente: Squid se puede configurar para ser usado como proxy transparente empleando un cortafuegos que intercepte y redirija las conexiones sin configuración por parte del cliente, e incluso sin que el propio usuario conozca de su existencia.

- Permite la configuración de un proxy transparente para la navegación HTTP (Squid) .
- Ahorro de ancho de banda en su corporación gracias a la caché dinámica en tiempo real.
- Permite definir las tablas y objetos de cache, rendimiento y velocidad de respuesta.
- Permite la obtención de INFORMES de navegación por IP / usuario



## Filtro de Contenidos

- La herramienta DansGuardian es código abierto, está desarrollada en C++ y permite una configuración flexible adaptándose a las necesidades de su corporación.
- El Ministerio de Educación, Cultura y Deporte – Gobierno de España- hace uso de esta herramienta, entre muchas otras organizaciones a nivel mundial.
- DansGuardian utiliza un sistema de “peso de las frases” para mejorar el objetivo de bloqueo y permite filtrar por un gran número de criterios.
- Los métodos más característicos son:
- Realizar filtros utilizando el sistema de etiquetas PICS (Platform for Internet Content Selection). Filtrar comprobando que las extensiones de los archivos
- y los tipos MIME no estén en una lista de extensiones y tipos MIME prohibidos.
- Filtrar de acuerdo con las URLs, incluyendo expresiones regulares.

- Trabajar con listas blancas y listas negras. Compara el contenido de las páginas con el de una lista de palabras prohibidas. Esta lista contiene palabras asociadas con la pornografía y otros contenidos no deseados.
- Todos estos métodos se apoyan en la utilización de unos archivos de filtros que almacenan frases, palabras, URLs, etc, cuyo acceso queda prohibido.

#### Red Privada Virtual (VPN )

- Bios Security Box ofrece tres opciones para la conectividad VPN , IPSec , OpenVPN y PPTP.

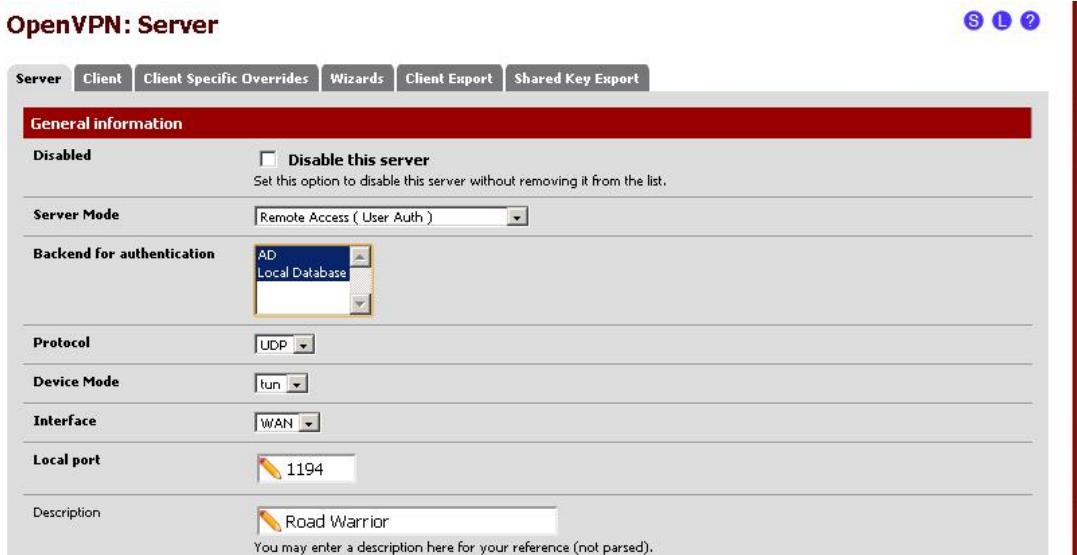
#### IPsec:

- IPsec permite la conectividad con cualquier dispositivo que soporte estándar IPsec. Esto es comúnmente utilizado para la conectividad entre sedes. Conectividad entre servidores VPN de otras instalaciones o bien hacia otros dispositivos Bios Security Box o bien otro tipo de routers/ UTMs, tales como: m0n0wall Zentyal, etc. También se puede interconectar con la mayoría de todas las soluciones de cortafuegos comerciales (Cisco , Juniper , etc.) También se puede utilizar para la conectividad de un cliente móvil .

#### OpenVPN:

- OpenVPN es una potente solución flexible , SSL VPN compatible con una amplia gama de sistemas operativos cliente . (Linux, Windows, Mac, Iphone, Android..)

#### OpenVPN: Server



The screenshot shows the 'OpenVPN: Server' configuration page. At the top, there are tabs for Server, Client, Client Specific Overrides, Wizards, Client Export, and Shared Key Export. The Server tab is selected. The main area is titled 'General information'. It includes the following settings:

- Disabled:** A checkbox labeled 'Disable this server' with the note: 'Set this option to disable this server without removing it from the list.'
- Server Mode:** A dropdown menu set to 'Remote Access ( User Auth )'.
- Backend for authentication:** A dropdown menu showing 'AD' and 'Local Database'.
- Protocol:** A dropdown menu set to 'UDP'.
- Device Mode:** A dropdown menu set to 'tun'.
- Interface:** A dropdown menu set to 'WAN'.
- Local port:** A text input field containing '1194'.
- Description:** A text input field containing 'Road Warrior' with the note: 'You may enter a description here for your reference (not parsed)'.

## Servidor PPTP

- PPTP fue una opción popular VPN debido a que casi todos los sistemas operativos ha construido en un cliente PPTP , incluyendo cada versión de Windows desde Windows 95 OSR2.

## PPPoE servidor

- Bios Security Box ofrece un servidor PPPoE. Para obtener más información sobre el protocolo PPPoE , consulte esta entrada de Wikipedia . Una base de datos de usuarios local puede ser utilizado para la autenticación y la autenticación RADIUS con la contabilidad opcional también se apoya.

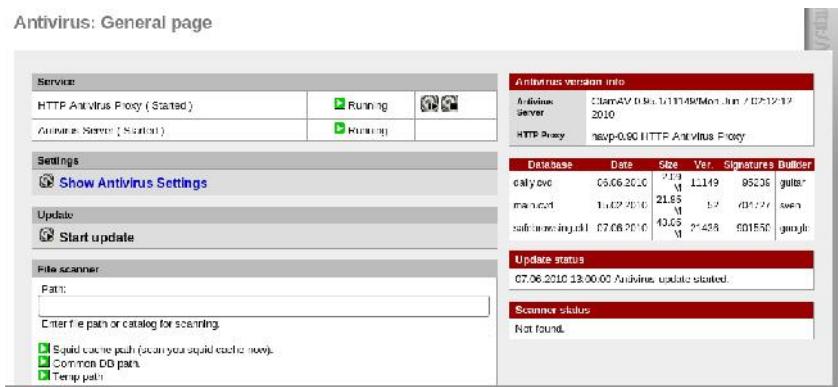
## Sistema de Deteción / Prevención de Intrusiones (IPS/IDS)

- Snort es un IDS (NIDS/IPS) o Sistema de detección de intrusiones basado en red. Implementa un motor de detección de Ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, intentos aprovechar alguna vulnerabilidad, análisis de protocolos conocidos... Todo esto en tiempo real.

Snort: Snort Alerts										
Alert Log View Settings										
Last 250 Alert Entries (Most recent entries are listed first)										
Date	Pr1	Proto	Class	Source	SPort	Destination	DPort	SID	Description	
03/28/14 18:06:55	3	TCP	Unknown Traffic	192.168.10.4	88	192.168.10.23	47074	129:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	
03/28/14 18:06:55	3	TCP	Not Suspicious Traffic	192.168.10.23	47074	192.168.10.4	88	119:4	(http_inspect) BARE BYTE UNICODE ENCODING	
03/28/14 18:06:55	3	TCP	Unknown Traffic	192.168.10.4	88	192.168.10.23	47073	129:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	
03/28/14 18:06:55	3	TCP	Not Suspicious Traffic	192.168.10.23	47073	192.168.10.4	88	119:4	(http_inspect) BARE BYTE UNICODE ENCODING	
03/28/14 18:06:55	3	TCP	Unknown Traffic	192.168.10.4	88	192.168.10.23	47072	129:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	
03/28/14 18:06:55	3	TCP	Not Suspicious Traffic	192.168.10.23	47072	192.168.10.4	88	119:4	(http_inspect) BARE BYTE UNICODE ENCODING	
03/28/14 18:06:55	3	TCP	Unknown Traffic	192.168.10.4	88	192.168.10.23	47071	129:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE	

## Gateway Antivirus

- Clam AntiVirus es un antivirus de código abierto ( GPL ) que incluye un conjunto de herramientas antivirus para UNIX, diseñado especialmente para el análisis en gateways de correo o HTTP . Proporciona una serie de utilidades que incluyen un demonio multi-hilo flexible y escalable , un escáner de línea de comandos y una herramienta avanzada para actualizaciones de bases de datos automáticas.
- Características principales:
  - Escáner de línea de comandos (Bios Security Box analiza todo el tráfico HTTP) según las reglas definidas en el Proxy Transparente.
  - Daemon rápido, multi-escala con soporte para el escaneado en tiempo real.
  - Avanzado soporte de actualización de bases de datos con soporte para actualizaciones de base de firmas de virus y firmas digitales.
  - Biblioteca de escáner de virus escrita en C.
  - Desarrollado específicamente para sistemas Linux ® y FreeBSD ®
  - Bbase de datos de virus actualizada varias veces al día.
  - Soporte integrado para varios formatos de archivo, incluyendo ZIP , RAR , TAR, gzip , bzip2 , OLE2 , Gabinete , CHM, BinHex , SIS y otros.
  - Soporte integrado para casi todos los formatos de archivo de correo.
  - Soporte integrado para los ejecutables ELF y archivos ejecutables portátiles comprimido con UPX , FSG , Mujer pequeña, NsPack , WWPack32 , MEW , Upack y ofuscado con SUE , Y0da Cryptor y otros.



Antivirus: General page

**Service:**

HTTP Antivirus Proxy ( Started )	Running
Antivirus Server ( Started )	Running

**Settings**

Show Antivirus Settings

**Update**

Start update

**File scanner**

Path:

Enter the path or catalog for scanning.

Squid cache path (scans your squid cache now).

Common DB path

Temp path

**Antivirus version info**

Antivirus Server	ClamAV 0.96.1/11149/Mon,Jun 7 07:21:17 2010
HTTP Proxy	http://0.0.0.0:8080/HTTP_Antivirus_Proxy

**Database**

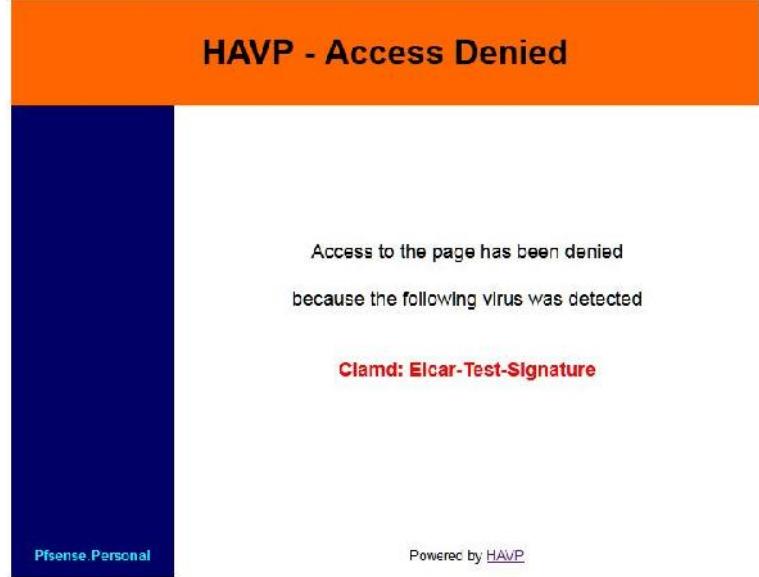
Database	Date	Size	Ver.	Signatures	Builder
clamav.cvd	05.06.2010	2.13M	1.149	65.36	gutte
main.cvd	14.07.2010	21.65M	1.149	401.24	gutte
signatureenginel	07.06.2010	43.45M	2.458	601.550	gutte

**Update status**

07.06.2010 13:00:00: Archive update started.

**Scanner status**

Not found.



**HAVP - Access Denied**

Access to the page has been denied because the following virus was detected

**Clamd: Elcar-Test-Signature**

**Pisense Personal**

Powered by [HAVP](http://HAVP)

## Informes y Monitorización

### Status: System logs: Firewall

Has activado el modo de pantalla completa

System Firewall DHCP Portal Auth IPsec PPP VPN Load Balancer OpenVPN NIP Settings

Action Time Source IP Address Source Port Destination Port Protocol Protocol Flags Quantity

Pass Block Reject

Interlace Destination IP Address

Desired Port

Protocol

Filter

Matches regular expression. Proceeds with exclamation (!) as first character to exclude match.

Normal View | Dynamic View | Summary View

Last 50 firewall log entries.Max(50)

Act	Time	IF	Source	Destination	Proto
✗	Nov 27 11:39:58	RADIOKAPIF	192.168.1.16	255.255.255.255:5678	UDP
✗	Nov 27 11:39:58	RADIOKABLE	0.0.0.0:5378	255.255.255.255:5678	UDP
✗	Nov 27 11:39:58	RADIOKADL	0.0.0.0:5570	255.255.255.255:5670	UDP
✗	Nov 27 11:39:59	ORANGE	0.0.0.0:68	255.255.255.255:67	UDP
✗	Nov 27 11:39:59	ORANGE	192.168.2.1:67	255.255.255.255:68	UDP
✗	Nov 27 11:39:59	RADIOUKAEL	192.168.1.16:18/56/8	255.255.255.255:5678	UDP
✗	Nov 27 11:40:03	RADIOKABLE	192.168.1.16:175:5678	255.255.255.255:5578	UDP
✗	Nov 27 11:40:07	ORANGE	0.0.0.0:68	255.255.255.255:67	UDP
✗	Nov 27 11:40:07	ORANGE	192.168.2.1:67	255.255.255.255:68	UDP
✗	Nov 27 11:40:09	RADIOKAPIF	213.0.3.88:50192	192.168.0.47:9443	TCP:PA
✗	Nov 27 11:40:12	RADIOKABLE	0.0.0.0:5378	255.255.255.255:5578	UDP
✗	Nov 27 11:40:14	ORANGE	0.0.0.0:68	255.255.255.255:67	UDP
✗	Nov 27 11:40:14	ORANGE	192.168.2.1:67	255.255.255.255:68	UDP
✗	Nov 27 11:40:14	ORANGE	0.0.0.0:68	255.255.255.255:67	UDP
✗	Nov 27 11:40:14	ORANGE	192.168.2.1:67	255.255.255.255:68	UDP
✗	Nov 27 11:40:16	RADIOKABLE	192.168.1.16:138:5678	255.255.255.255:5578	UDP
✗	Nov 27 11:40:16	RADIOKABLE	0.0.0.0:5578	255.255.255.255:5578	UDP
✗	Nov 27 11:40:16	RADIOKABLE	192.168.1.16:172:5678	255.255.255.255:5578	UDP
✗	Nov 27 11:40:16	RADIOKAPIF	192.168.1.16:137:5678	255.255.255.255:5578	UDP
✗	Nov 27 11:40:18	ORANGE	0.0.0.0:68	255.255.255.255:67	UDP
✗	Nov 27 11:40:10	ORANGE	192.168.2.1:67	255.255.255.255:68	UDP

- Gráficos RRD
- Los gráficos RRD en Bios Security Box mantienen información histórica sobre lo siguiente:
  - Utilización y rendimiento de la CPU
  - Tráfico total por IP (también de URL por IP si se ha instalado Squid Proxy)

### Estados Firewall

- Rendimiento individual para todas las interfaces
- Paquetes por segundo de todas las interfaces

### Status: DHCP leases

Has activado el modo de pantalla completa

IPaddress	MAC address	Hostname	Start	End	Online	Lease Type
192.168.0.1.6	3c:d9:2b:5e:90:72	Rafael-PC	2014/11/27 10:41:18	2014/11/27 12:41:18	online	active
192.168.0.184	00:22:77:17:a2:a5		2014/11/27 10:22:22	2014/11/27 12:22:22	online	active
192.168.0.101	c0:5f:c5:6c:2a:c5	usuario-desktop	2014/11/27 10:19:49	2014/11/27 12:19:49	online	active
192.168.0.192	00:22:54:b4:63:f3	a-Hp-Compaq-dc-900-Ultra-slim-Desktop	2014/11/27 10:10:53	2014/11/27 12:10:53	online	active
192.168.0.109	a0:d3:c1:4c:a4:21	hp	2014/11/27 10:39:18	2014/11/27 12:39:18	online	active
192.168.0.103	c0:3f:c5:6c:05:39	NUC000001	2011/11/27 10:05:25	2011/11/27 12:05:25	online	active
192.168.0.106	e0:0f:49:30:c1:2b	Usuario-PC	2011/11/27 09:32:06	2011/11/27 11:32:06	online	active
192.168.0.61	20:92:4a:20:0e:53	Javier_Gamido	n/a	n/a	online	static
192.168.0.62	00:23:18:c1:13:c5	Juan_de_Dios_Fernandez_Siller	n/a	n/a	online	static
192.168.0.63	1c:75:00:17:4c:65	Andrea_Cuesta	n/a	n/a	offline	static
192.168.0.64	f0:da:f1:59:06:83	Jose_Antonio_Pascual	n/a	n/a	online	static
192.168.0.65	00:15:47:64:8a:e7	Rafael_Canella	n/a	n/a	offline	static
192.168.0.66	6c:71:99:bf:47:87	1-14-1_Invitado_V-ja	n/a	n/a	offline	static
192.168.0.67	0c:d9:2b:60:4f:a1	Jose_Montes	n/a	n/a	offline	static
192.168.0.68	c8:90:33:1c:65:31	David_Hurtado	n/a	n/a	offline	static
192.168.0.69	bccc:7b:0a:00:92	JJANIE_LAN	n/a	n/a	online	static
192.168.0.70	c0:d9:2b:60:4f:8c	Andrea_New_PU	n/a	n/a	online	static

Show all configured leases

