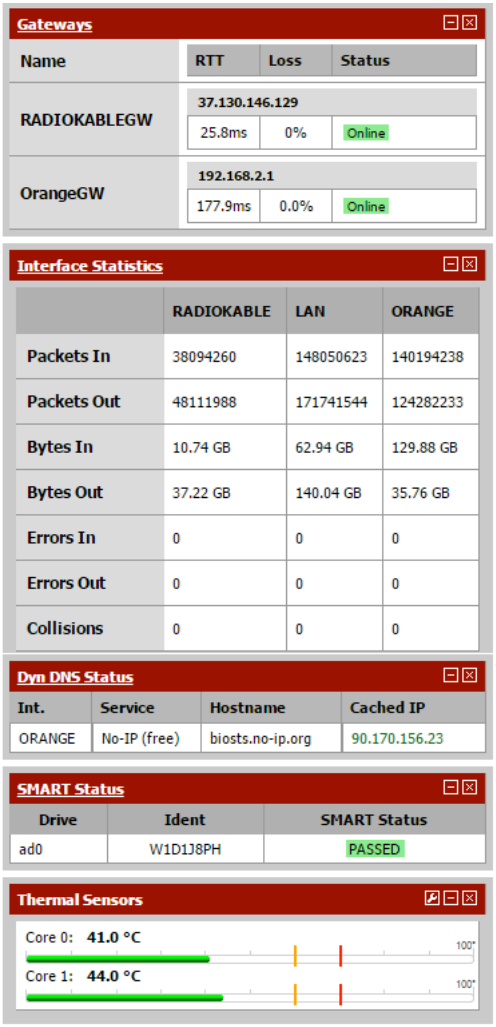
bios
technology solutions

QUÉ ES BSB

(Bios Security Box – Unified Threat Management)

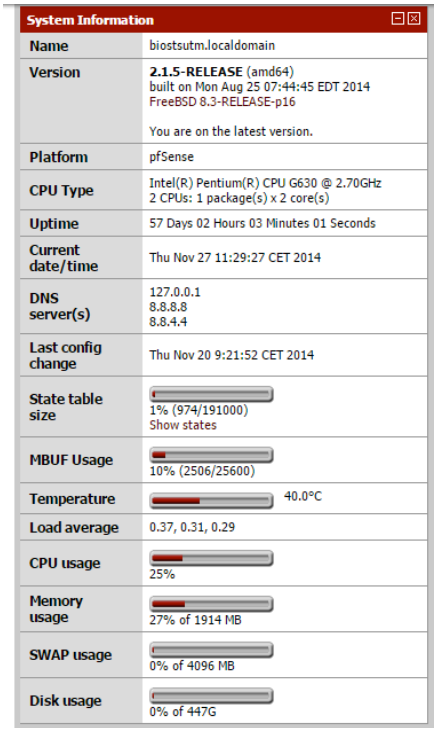
Bios Security Box

Unified Threat Management



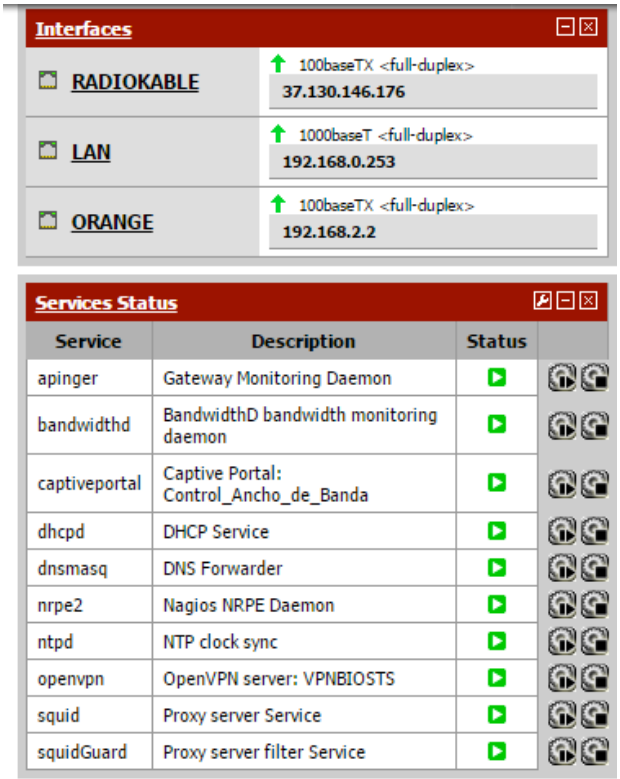
Firewall

- 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 coincidente 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.



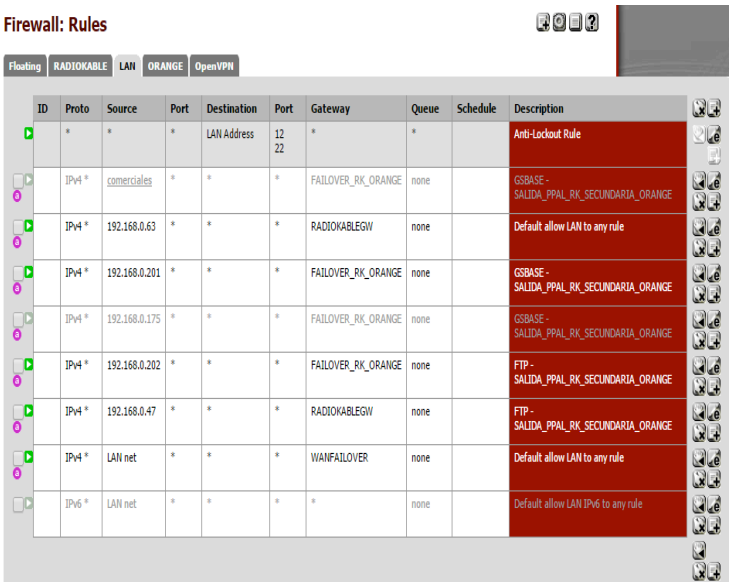
- Capa 2 Transparente: Permite agrupar interfaces y filtrar el tráfico entre ellos, incluso teniendo en cuenta un firewall IP.
- Paquete de normalización: Descripción de la documentación de grupo. Define la normalización de los paquetes para que no haya ambigüedades en la interpretación por el destino 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.

- 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.



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.

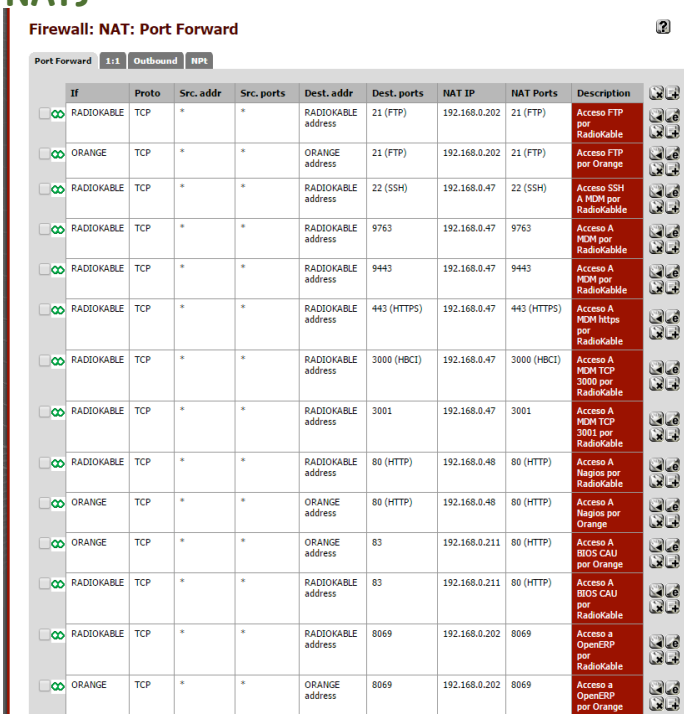


- Estatados “Sloppy” - Funciona con todos los protocolos. Menos seguimiento estricto del estado, útil en casos de enrutamiento asimétrico.
- Estado Modular: Bios Security Box generará fuertes números de secuencia inicial (ISNs) en nombre del host.
- Estado Synproxy : Conexiones Proxies TCP entrantes 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 - Útil 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.
- Advanced Outbound NAT: Permite este comportamiento predeterminado que se inutilice 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.



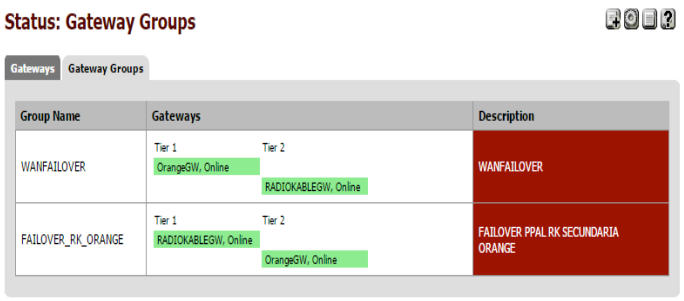
If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
RADIOKABLE	TCP	*	*	RADIOKABLE address	21 (FTP)	192.168.0.202	21 (FTP)	Acceso FTP por RadioKable
ORANGE	TCP	*	*	ORANGE address	21 (FTP)	192.168.0.202	21 (FTP)	Acceso FTP por Orange
RADIOKABLE	TCP	*	*	RADIOKABLE address	22 (SSH)	192.168.0.47	22 (SSH)	Acceso SSH A MDM por RadioKable
RADIOKABLE	TCP	*	*	RADIOKABLE address	9763	192.168.0.47	9763	Acceso A MDM por RadioKable
RADIOKABLE	TCP	*	*	RADIOKABLE address	9443	192.168.0.47	9443	Acceso A MDM por RadioKable
RADIOKABLE	TCP	*	*	RADIOKABLE address	443 (HTTPS)	192.168.0.47	443 (HTTPS)	Acceso A MDM https por RadioKable
RADIOKABLE	TCP	*	*	RADIOKABLE address	3000 (HBCI)	192.168.0.47	3000 (HBCI)	Acceso A MDM TCP 3000 por RadioKable
RADIOKABLE	TCP	*	*	RADIOKABLE address	3001	192.168.0.47	3001	Acceso A MDM TCP 3001 por RadioKable
RADIOKABLE	TCP	*	*	RADIOKABLE address	80 (HTTP)	192.168.0.48	80 (HTTP)	Acceso A Nagios por RadioKable
ORANGE	TCP	*	*	ORANGE address	80 (HTTP)	192.168.0.48	80 (HTTP)	Acceso A Nagios por Orange
ORANGE	TCP	*	*	ORANGE address	83	192.168.0.211	80 (HTTP)	Acceso A BIOS CAU por Orange
RADIOKABLE	TCP	*	*	RADIOKABLE address	83	192.168.0.211	80 (HTTP)	Acceso A BIOS CAU por RadioKable
RADIOKABLE	TCP	*	*	RADIOKABLE address	8069	192.168.0.202	8069	Acceso a OpenERP por RadioKable
ORANGE	TCP	*	*	ORANGE address	8069	192.168.0.202	8069	Acceso a OpenERP por Orange

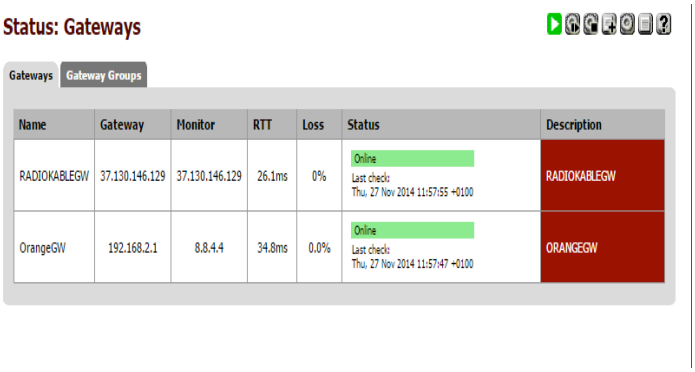
DNS DINÁMICO

- 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 conmutación 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.
- 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:

- 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: Después 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:

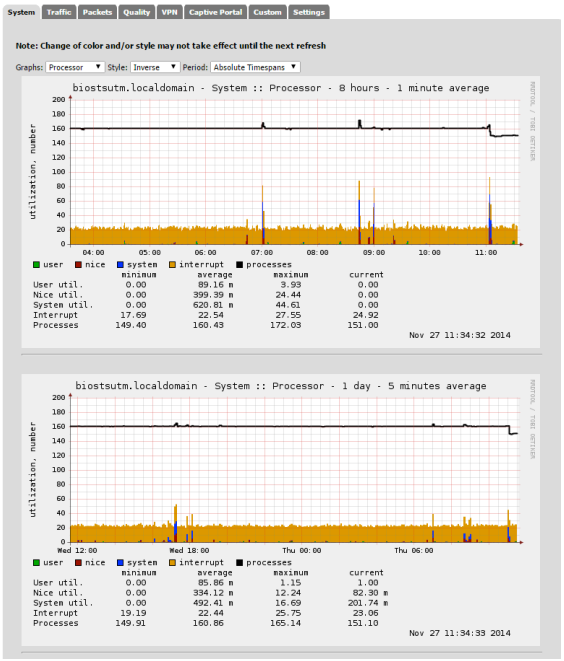
- Forzado re-autenticación
- Capaz de enviar actualizaciones a los usuarios conectados según las normas definidas.
- Autenticación RADIUS MAC: Permite al portal cautivo autenticar a un servidor RADIUS utilizando la dirección MAC del cliente como el nombre de usuario y contraseña.

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

Alta Disponibilidad

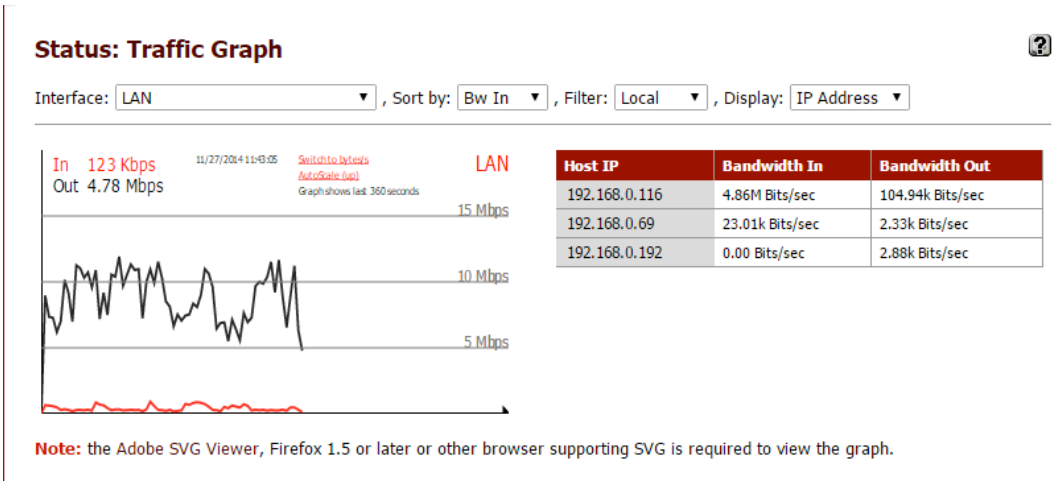
- CARP : Permite la conmutación por error de hardware. Dos o más servidores de seguridad (UTM) se pueden configurar como un grupo de conmutación por error . Si una interfaz falla en la UTM primaria, esta se desconecta por completo, pasando a ser la UTM secundaria.



- 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

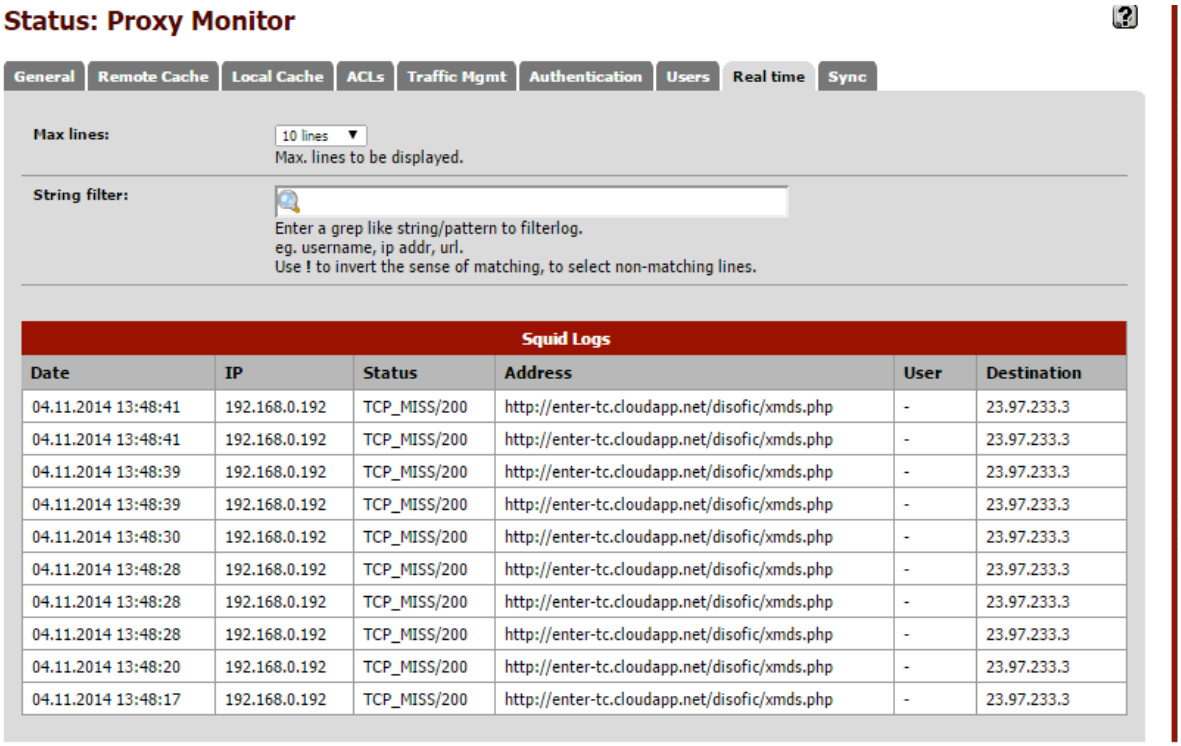


- La información histórica es importante, pero a veces es más importante ver la información en tiempo real.
- Gráficos SVG están disponibles en Bios Security Box; muestran el rendimiento en tiempo real para cada interfaz .
- Pantalla de colas: Proporciona una visualización en tiempo real del uso de colas 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.
- 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.



Status: Proxy Monitor

General | Remote Cache | Local Cache | ACLs | Traffic Mgmt | Authentication | Users | Real time | Sync

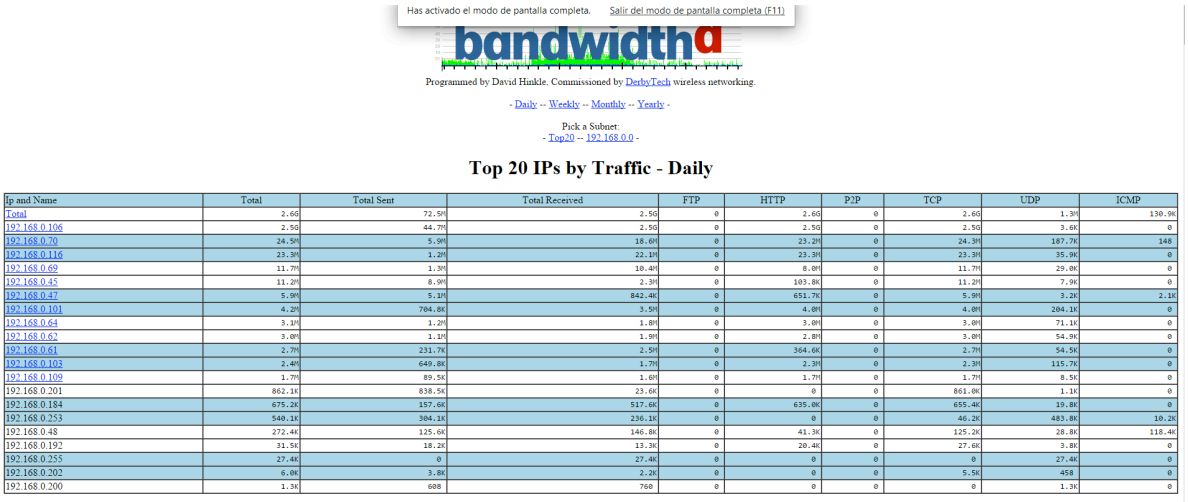
Max lines: 10 lines
Max. lines to be displayed.

String filter:
Enter a grep like string/pattern to filterlog.
eg. username, ip addr, url.
Use ! to invert the sense of matching, to select non-matching lines.

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

- 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



Has activado el modo de pantalla completa. Salir del modo de pantalla completa (F11)

bandwidthd

Programmed by David Hinkle. Commissioned by DerbyTech wireless networking.

- Daily -- Weekly -- Monthly -- Yearly -

Pick a Subnet:
- Top20 -- 192.168.0.0 -

Top 20 IPs by Traffic - Daily

Ip and Name	Total	Total Sent	Total Received	FTP	HTTP	P2P	TCP	UDP	ICMP
Total	2.6G	72.5M	2.5G	0	2.6G	0	2.6G	1.3M	130.9K
192.168.0.106	2.5G	44.7M	2.5G	0	2.5G	0	2.5G	3.6K	0
192.168.0.70	24.5M	5.9M	18.6M	0	23.2M	0	24.3M	187.7K	148
192.168.0.116	23.3M	1.2M	22.1M	0	23.3M	0	23.3M	35.9K	0
192.168.0.69	11.7M	1.3M	10.4M	0	8.0M	0	11.7M	29.0K	0
192.168.0.45	11.2M	8.9M	2.3M	0	103.8K	0	11.2M	7.9K	0
192.168.0.47	5.9M	5.1M	842.4K	0	651.7K	0	5.9M	3.2K	2.1K
192.168.0.101	4.2M	704.8K	3.5M	0	4.0M	0	4.0M	204.1K	0
192.168.0.64	3.1M	1.2M	1.8M	0	3.0M	0	3.0M	71.1K	0
192.168.0.62	3.0M	1.1M	1.9M	0	2.8M	0	3.0M	54.9K	0
192.168.0.61	2.7M	231.7K	2.5M	0	364.6K	0	2.7M	54.5K	0
192.168.0.103	2.4M	649.8K	1.7M	0	2.3M	0	2.3M	115.7K	0
192.168.0.109	1.7M	89.5K	1.6M	0	1.7M	0	1.7M	8.5K	0
192.168.0.201	862.1K	838.5K	23.6K	0	0	0	861.0K	1.1K	0
192.168.0.184	675.2K	157.6K	517.6K	0	635.0K	0	655.4K	19.8K	0
192.168.0.253	540.1K	304.1K	236.1K	0	0	0	46.2K	483.8K	10.2K
192.168.0.48	272.4K	125.6K	146.8K	0	41.3K	0	125.2K	28.8K	118.4K
192.168.0.192	31.5K	18.2K	13.3K	0	20.4K	0	27.6K	3.8K	0
192.168.0.255	27.4K	0	27.4K	0	0	0	0	27.4K	0
192.168.0.202	6.0K	3.8K	2.2K	0	0	0	5.5K	458	0
192.168.0.200	1.3K	608	760	0	0	0	0	1.3K	0

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..)

Servidor PPTP

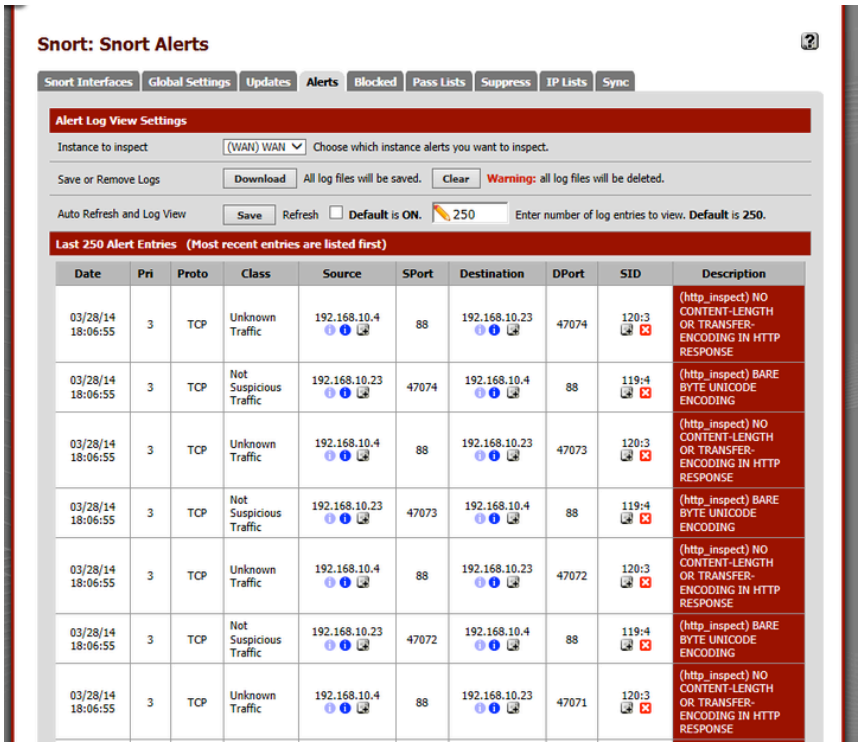
- PPTP fue una opción popular VPN debido a que casi todos los sistemas operativos ha construido en un cliente PPTP , incluyendo cada versión de Windows desde Windows 95 OSR2.

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.

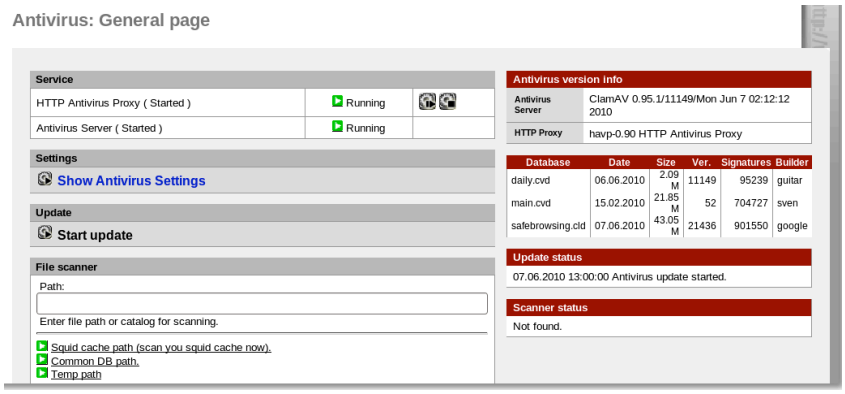
Sistema de Deteción / Prevención de Intrusiones (IPS/IDS)

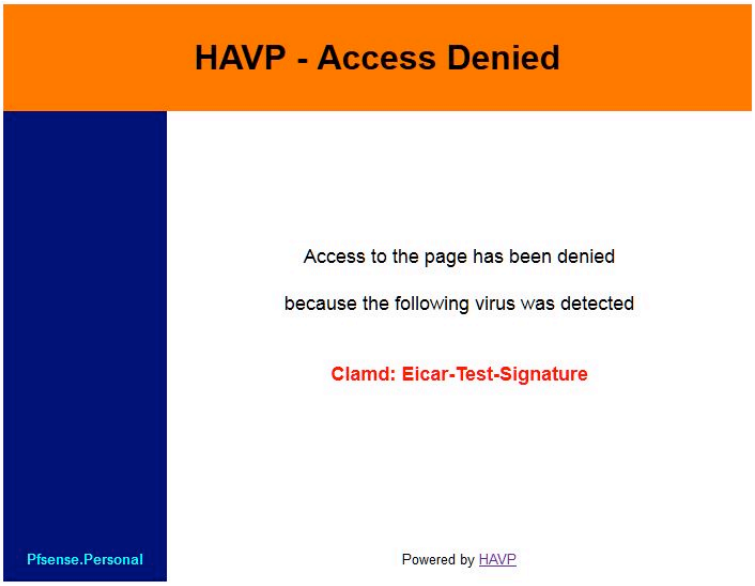
- Snort es un IDS (NIDS/IPS) o Sistema de detección de intrusiones basado en red. Implementa un motor de detección de Ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida como patrones que corresponden a ataques, barridos, intentos aprovechar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



Gateway Antivirus

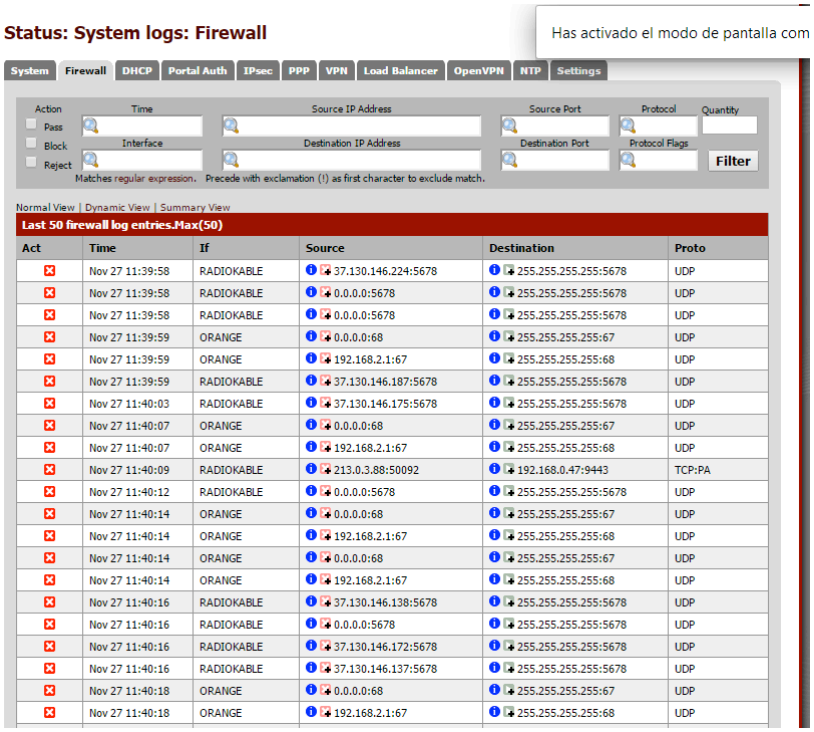
- Clam AntiVirus es un antivirus de código abierto (GPL) que incluye un conjunto de herramientas antivirus para UNIX, diseñado especialmente para el análisis en gateways de correo o HTTP . Proporciona una serie de utilidades que incluyen un demonio multi-hilo flexible y escalable , un escáner de línea 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.





Informes y Monitorización

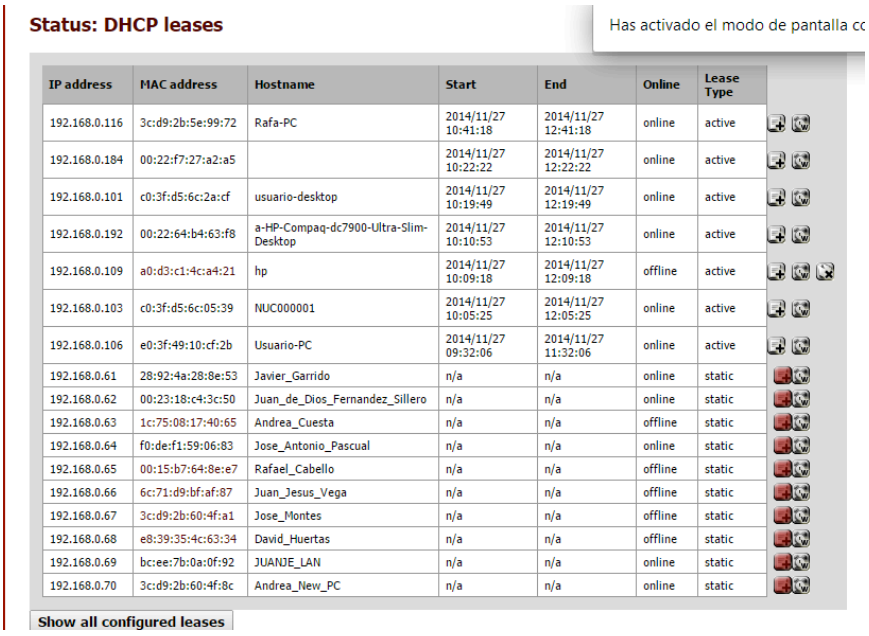
- Gráficos RRD
- Los gráficos RRD en Bios Security Box mantienen información histórica sobre lo siguiente:
- Utilización y rendimiento de la CPU
- Tráfico total por IP (también de URL por IP si se ha instalado Squid Proxy)



– Estados Firewall

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

- Los tiempos de respuesta de pasarela de la interfaz WAN (s) de ping.
- Colas de Tráfico en sistemas con modulación del tráfico habilitados



WWW.BIOS-TS.ES

www.bios-ts.es
Email: info@bios-ts.es

Tel. 902 879 620

CÓRDOBA | GRANADA | MÁLAGA | SEVILLA |