

SERVIDOR PROXY-CACHÉ

Servicios que ofrece:

1. Filtrado de contenidos web.
2. Proxy caché.
3. Cortafuegos.
4. Antivirus
5. Servidor DHCP.
6. Balanceo de carga.
7. Servidor Web para Intranets.
8. Administración gráfica.

Hardware necesario:

No son necesarios grandes requisitos de hardware para esta plataforma, con lo cual puede ser implementado sin problemas en hardware de servidor de bajo coste.

Como mínimo ha de contar con 2 interfaces de red, ya que actuará de pasarela entre Internet y la red interna filtrando todo el tráfico entre ambas.

Software:

Sobre el hardware de servidor se instalará el sistema operativo **GNU/Linux**, concretamente la distribución **Ubuntu Server** en su última versión. Sobre esta base se instalará el siguiente software:

- Plataforma **Ebox**.
- **Squid** para servicios de proxy.
- **ClamAV** antivirus.
- **Dansguardian** para filtrado web.
- **Iptables** para los servicios de cortafuegos.
- Servidor Web **Apache** con el módulo para https.
- Servidor de bases de datos **Mysql**.
- Servidor **DHCP**.
- Módulo de **PHP** para Apache.

Funcionamiento:

El servidor irá ubicado entre la puerta de enlace de acceso a Internet y la red interna, de esta forma todo el tráfico hacia ó desde Internet será filtrado según la política correspondiente. En primer lugar el cortafuegos aceptará o impedirá que ciertas aplicaciones tengan acceso a Internet denegando o aceptando el acceso de ciertos puertos. En principio lo más sencillo a nivel de administración es denegar el acceso hacia o desde Internet a todos los puertos, y después ir creando reglas según las necesidades.

El **servicio de proxy caché** mejora el acceso a Internet ya que alberga en el disco del servidor aquellas páginas que han sido visitadas recientemente, así cuando esa misma página vuelve a ser solicitada se sirve la ubicada en la caché del disco, optimizando el ancho de banda sobre todo en entornos con un volumen de tráfico elevado. El inconveniente está en páginas con actualizaciones frecuentes, por ejemplo páginas de cotizaciones bursátiles, en estos casos habrá que establecer reglas específicas para ellas evitando que sean cacheadas por el servidor.

El **filtrado web** nos permite denegar el acceso a ciertas páginas según varios criterios:

- Por **contenido**: nos permite denegar el acceso a ciertas webs si su contenido coincide con las palabras clave que previamente establezcamos.
- Por tipos de contenidos **MIME**: denegando la descarga de ficheros de audio o vídeo.
- Por **extensión** del fichero a descargar.
- Por **dominios**: denegará el acceso a aquellos dominios que establezcamos. También permite todo lo contrario, es decir, deniega el acceso absolutamente a todo excepto aquellos dominios previamente establecidos.

El servidor Proxy funciona de forma **transparente**, es decir, no es necesario configurar los navegadores de las máquinas para que lo usen, ya que ahora el servidor funcionará como la pasarela de acceso a Internet obligando a todo el tráfico a que sea filtrado.

El **cortafuegos** funciona en conjunción con el servicio de filtrado web y el servicio de **antivirus**, así nos permite establecer reglas de acceso o denegación a ciertos servicios de Internet. De esta manera tenemos un conjunto que nos permite establecer a qué servicios se dará acceso, permitiéndonos por ejemplo cortar el acceso a ciertas aplicaciones como los programas p2p, un filtrado a nivel del protocolo http, y por último un filtro antivirus de todo el tráfico.

Como ya vimos anteriormente, no es necesario cambiar ningún parámetro en las máquinas clientes, ya que de forma transparente el servidor proxy actuará como la pasarela de acceso a Internet. Pero para aquellos entornos donde los clientes necesiten recibir los parámetros de conexión (ips, puertas de enlace, dns), el servidor cuenta con un servicio de **DHCP**, centralizándose todas las tablas de ip,s asignadas a todos los clientes.

También es posible disponer de **varias pasarelas de salida a Internet**, esto nos permite establecer qué pasarela actuará como primaria y cual como alternativa en caso de fallo de la principal (redundancia), también nos permite balancear la carga entre las dos pasarelas sobre todo en aquellos entornos donde el tráfico hacia Internet es intensivo.

Por último, todas estas funcionalidades se gestionan de forma fácil e intuitiva mediante un **entorno gráfico basado en web**, este servicio se ofrece mediante el servidor web seguro ubicado en el mismo servidor.

Desde cualquier cliente dentro de la red se puede acceder a la página de administración. Mediante la introducción de credenciales de acceso se accede a la parametrización de los diferentes servicios, así como ver el estado de los mismos.

Funcionalidades de ebox:

Ebox es una plataforma que integra todos los servicios anteriores y nos permite su administración de forma fácil y cómoda como ya se ha visto. Hecharemos un vistazo a las funcionalidades necesarias para la tarea que nos interesa a través de varias capturas de pantalla.

Para acceder a la interfaz de administración es necesario introducir una contraseña de administrador:



La siguiente captura es la **pantalla principal** que aparece al acceder al panel de administración, donde se observa a la izquierda los enlaces a los servicios que se pueden configurar, en el centro tenemos información sobre las interfaces de red instaladas, y a la derecha el estado de los diferentes servicios.



Dashboard
Configure widgets

Network Interfaces:

- eth0**
Status: up, link ok
MAC address: 08:00:27:ef:0d:0e
IP address: 10.0.2.15
Tx bytes: 2.44 KB
Rx bytes: 48.83 KB
- eth1**
Status: down, link ok
MAC address: 08:00:27:26:ec:56
Tx bytes: 0 B
Rx bytes: 0 B
- eth2**
Status: down, link ok
MAC address: 08:00:27:a1:ef:13
IP address: 192.168.100.9
Tx bytes: 0 B
Rx bytes: 0 B
- eth3**

Module Status:

Network	Running	
Firewall	Running	
Antivirus	Running	Restart
Apache	Running	
VoIP	Running	Restart
Certification Authority	Running	
DHCP	Disabled	
DNS	Disabled	
Backup	Running	Restart
Events	Disabled	
IDS	Running	Restart
Jabber	Running	Restart
Logs	Running	Restart
Mail	Running	Restart
Mail Filter	Running	Restart
Monitor	Disabled	
NTP	Disabled	
VPN	Disabled	
Printer Sharing	Disabled	
File Sharing	Running	Restart
Software Management	Disabled	
HTTP Proxy	Running	Restart
Traffic Shaping	Disabled	
User Corner	Disabled	
Users and groups	Running	
Web Server	Disabled	

1. En primer lugar podemos **configurar las diferentes interfaces de red** de forma estática o dinámica, incluso asociando interfaces virtuales para servir direcciones ip adicionales:

Network interfaces [\(show help\)](#)

eth0

Name:

Method:

External:

IP address:

Netmask:

2. Configuraremos los servidores **DNS**:

Name server resolver [\(show help\)](#)

Adding a new name server

Name server:

IP address of the DNS server that eBox will use to resolve names

Name server resolver list

Name server	Action
10.0.2.3	

3. Podemos configurar un **servidor DHCP** para que los clientes obtengan los parámetros de red de forma automática. Para ello necesitamos al menos una interfaz configurada de forma estática, así en el menú dhcp configuraremos el servicio:

DHCP [\(show help\)](#)

Service configuration

Choose a static interface to configure:

Default gateway:

Search domain:

Primary nameserver:

Secondary nameserver:

Optional

DHCP ranges





Interface IP address: 10.37.129.3
Subnet: 10.37.129.0/24
Available range: 10.37.129.1 - 10.37.129.254

4. **Balaceo de carga:** permite a los ordenadores de la red usar varias conexiones a Internet de forma transparente, de forma que la carga se distribuya automaticamente entre ellas. Definimos tantos routers como sea necesario para establecer una configuración multirouter con balanceo de carga, también establecemos los pesos de cada uno (proporción de paquetes que cada uno enviará).

Gateways [\(show help\)](#)

Gateway list

[Add new](#)

Name	IP Address	Interface	Upload	Download	Weight	Default	Action
router-warp	192.168.45.1	eth1	1000 Kb/s	1000 Kb/s	10	✓	 
backup-router	192.168.45.4	eth1	200 Kb/s	200 Kb/s	5	✗	 

Una vez configurados los routers, activamos el balanceo de carga. Aquí también podemos establecer reglas para que un determinado tráfico se encamine por un router determinado.

Balance Traffic [\(show help\)](#)







Traffic balancing

Enable:

[Change](#)

Multigateway rules

[Add new](#)

Enabled	Interface	Source	Destination	Service	Gateway	Action
✓	any	Any	Any	www	main-router	  
✓	any	Any	Any	ssh	backup-router	  

5. **Cortafuegos:** permite establecer reglas de filtrado que se encargarán de determinar si el tráfico de un servicio local o remoto es aceptado o no.

Filtering rules from Internal networks to eBox

[Add new](#)

Decision	Source	Service	Description	Action
↑	Any	http	--	🗑️✎️⬇️
↑	Any	Mail system	--	🗑️✎️⬆️⬇️
↑	Any	ipp	--	🗑️✎️⬆️⬇️
↑	Any	samba	--	🗑️✎️⬆️⬇️
✖️	Any	ldap	--	🗑️✎️⬆️⬇️
↑	Any	ntp	--	🗑️✎️⬆️⬇️
↑	Any	dns	--	🗑️✎️⬆️⬇️
↑	Any	lftp	--	🗑️✎️⬆️⬇️
↑	Any	dhcp	--	🗑️✎️⬆️⬇️
↑	Any	ssh	--	🗑️✎️⬆️

6. **Proxy:** El primer paso es establecer una **política global de acceso**. Podemos establecer la opción de “**proxy transparente**” para evitar tener que configurar cada navegador, y un **tamaño de caché** para albergar en disco las páginas de acceso más reciente. También podemos establecer qué dominio/s quedan excluidos de la caché (sitios web cuyo contenido es modificado frecuentemente).

HTTP Proxy [\(show help\)](#)

General Settings

Transparent Proxy:

Note that you cannot proxy HTTPS transparently. You will need to add a firewall rule if you enable this mode.

Port:

Cache files size (MB):

Default policy:

- Always allow
- Filter
- Always deny
- Authorize and allow
- Authorize and filter
- Authorize and deny

requests will go through the content filter and they might be rejected if the content is not

Cache exemption

[Add new](#)

Domain	Exempt domain from caching	Action
myorganization.com	✔️	🗑️✎️

7. **Filtrado de contenidos:** Para configurar las opciones de filtrado en “Perfiles de Filtrado” podemos usar la configuración del perfil *por defecto*.

Filter profiles [\(show help\)](#)
[Add new](#)

Search

Filter group	Configuration	Action
default		
IT		
sales		

10 Page 1

Tenemos varias opciones de filtrado:

- Por **dominio**: Prohibiendo el acceso a ciertos dominios de una lista, o bien aceptando todos los accesos excepto esa lista.
- Por **extensión del fichero** a descargar.
- Por tipo de contenidos **MIME**: Denegando la descarga de todos los ficheros de audio o vídeo.

Domain filter settings

Block not listed domains:
If this is enabled, any domain which is not allowed in the Domains list section below will be forbidden.

Block sites specified only as IP:
[Change](#)

Domains rules
[Add new](#)

Search

Domain	Policy	Action
myorganization.com	Always allow	

10 Page 1

Domains lists files
[Add new](#)

Search

Description	Categories	File	Action
shalla blacklist		shalla_blacklist Download	

10 Page 1

Hardware recomendado:

Servidor HP ML110G5.

Características del equipo:

Procesador, sistema operativo y memoria	
Tipo de procesador	Procesador Intel® Core™ 2® E7400
Velocidad del procesador	2,80 GHz
Número de procesadores	1 procesador
Núcleo de procesador disponible	Dual
Memoria caché interna	3 MB de caché de nivel 2
Chipset	Chipset Intel® 3200
Memoria	800 MHz de memoria DDR2 PC2-6400 sin búfer
Memoria de serie	1 GB (1 x 1 GB) de memoria estándar
Bus frontal del procesador	Bus frontal a 1.066 MHz
Memoria máxima	8 GB
Ranuras de memoria	4 ranuras DIMM
Unidades internas	
Unidades internas	1 disco duro SATA de 3,5" y 250 GB, sin conexión en caliente
Velocidad de la unidad de disco duro	7.200 rpm
Controlador de almacenamiento	Controlador SATA de 6 puertos integrado HP con RAID integrado (4 puertos para discos duros)
Ranuras de expansión	Ranuras de expansión: Ranura 1: PCI de 32 bits/33 MHz a 3,3 V; Ranura 2: Conector PCI-Express x8 con enlace x1; Ranura 3: Conector PCI-Express x8 con enlace x1; Ranura 4: Conector PCI-Express X8 con enlace x8
Unidades ópticas	Unidad DVD-ROM
Características del sistema	
Formato	Torre Micro ATX (4U)
Chipset	Chipset Intel® 3200
Interfaz de red	Adaptador de servidor NC105i PCI-Express Gigabit Ethernet

	integrado
Puertos de E/S externos	Paralelo - 0; serie - 1; dispositivo señalador (ratón, PS2) - 1; gráficos - 1; teclado (PS2) - 1; USB - 8 en total (4 posteriores, 2 en panel frontal, 2 internos (uno para conectividad con cinta USB)); Red RJ-45 (Ethernet) -1; gestión: Puerto de gestión remota HP ProLiant G5 Lights-Out 100c (opcional)
Ranuras de expansión	Ranuras de expansión: Ranura 1: PCI de 32 bits/33 MHz a 3,3 V; Ranura 2: Conector PCI-Express x8 con enlace x1; Ranura 3: Conector PCI-Express x8 con enlace x1; Ranura 4: Conector PCI-Express X8 con enlace x8
Tipo de fuente de alimentación	Fuente aliment. de 365 vatios
Requisitos de alimentación	De 90 a 132 VCA, de 180 a 264 VCA, de 47 a 63 Hz
Sistemas operativos compatibles	Microsoft® Windows® Server; Red Hat Enterprise Linux (RHEL); SUSE Linux Enterprise Server (SLES); Netware
Medidas del producto (P x A x L)	17,5 x 42,6 x 36,7 cm
Peso del producto	10,8 kg
Cumplimiento de estándares del mercado	Cumple con ACPI V3.0a; Cumple con PCI 2,3; Admite PXE; Admite WOL; Cumple con IPMI 2.0; Certificaciones del logotipo Microsoft®; Certificaciones del logotipo RedHat Enterprise Linux; Certificaciones del logotipo SUSE Linux Enterprise Server; USB 2.0
Gestión de seguridad	Contraseña de encendido; Contraseña configur.; Bloqueo USB
Garantía	1 años en piezas, 1 años en mano de obra, 1 años de asistencia en domicilio