FIREWALL DE APLICACIONES PROXY SQUID

Armando Carvajal, Ing. Sistemas Unincca, Especialista en software para redes de computadores Uniandes, Master en seguridad de la Informacion universidad Oberta de Catalunya,
e-mail: armando.carvajal@globalteksecurity.com

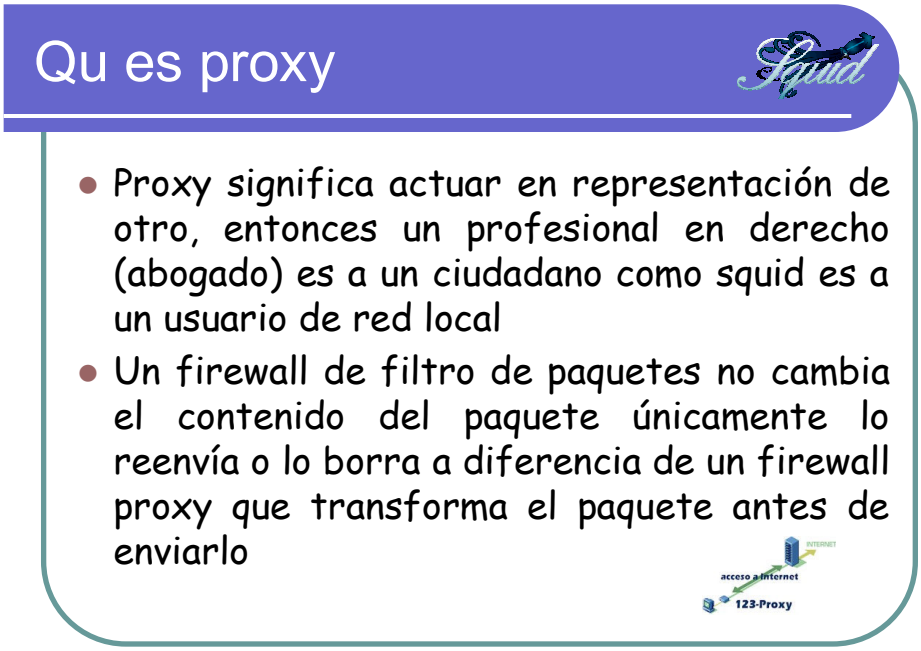
DEFINICIÓN DE FIREWALL DE APLICACIONES PROXY

Un Firewall es un conjunto de limitaciones de acceso para hacer nuestros servidores más seguros frente al mundo exterior. Hay dos clases de firewall, los de filtros de paquetes y los de aplicaciones. A los firewall de filtros de paquetes se les llama firewall de nivel de red, pero a los firewall de tipo proxy se les denomina firewall de aplicaciones debido a que estos servicios están por encima del nivel de red en el modelo OSI de la ISO.

Existen muchos programas firewall de tipo proxy para Linux algunos son:

- Active guardian (http://www.activeguardian.com)
- Apache mod_proxy (http://www.apache.org)
- Delegate (http://wall.etl.go.jp/delegate)
- SQUID (http://squid.nlanr.net)

Proxy significa actuar en representación de otro, entonces un profesional en derecho (abogado) es a un ciudadano como squid es a un usuario de red local, es decir un Firewall de filtro de paquetes no cambia el contenido del paquete únicamente lo reenvía o lo borra a diferencia de un firewall proxy que transforma el paquete antes de enviarlo.



El cliente de la red local generalmente debe ser configurado antes de que este pueda usar el servidor proxy, el servidor proxy se sitúa en el medio entre Internet o la red externa y la red local entonces el proxy actúa como un relevo “Internet relay” de acceso a Internet. El servidor proxy recibe los requerimientos de los clientes y los reenvía hacia Internet.

El servidor proxy mantiene un cache en disco duro de los documentos que accedieron últimamente a Internet de algún tráfico específico, para cuando un usuario de la red local llame a un documento que fue consultado éste deberá estar en el cache y el servidor web no deberá traer nuevamente el documento; obviamente hay datos que no se llevan a cache como las páginas web generadas por scrips cgi (Common gateway interface) y los mensajes de error que el servidor web envía a los clientes.

La idea desde el punto de vista telemático es disminuir la utilización del ancho de banda por accesos a Internet, los accesos se pueden limitar dependiendo de la parametrización por medio de las listas de control de acceso.

A menudo a los proxys se les llama “Gateway de aplicaciones”, un “proxy transparente” trabaja de la mano con un firewall de filtro de paquetes para permitir otros servicios diferentes al acceso http.

Página web

- A menudo a los proxys se les llama “Gateway de aplicaciones”, un “proxy transparente” trabaja de la mano con un firewall de filtro de paquetes para permitir otros servicios diferentes al acceso http.
- El software “SQUID” es un servidor proxy para servicios de Internet, este puede ser configurado como Proxy genérico o como “Transparent proxy”

El software “SQUID” es un servidor proxy para servicios de Internet, este puede ser configurado como Proxy genérico o como “Transparent proxy”.

La página web del grupo de desarrollo de SQUID es http://www.squid-cache.org

Una deficiencia del proxy genérico es que se debe configurar una aplicación proxy por cada servicio de red como ftp, correo, web, news, etc.

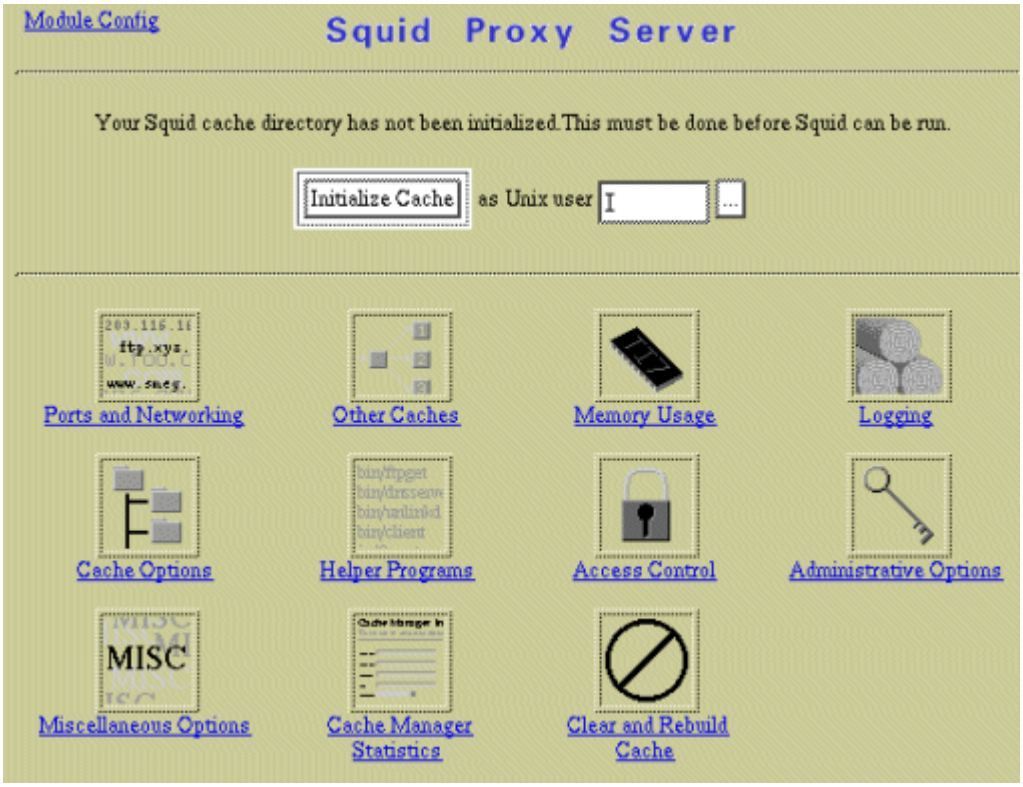
Squid no soporta protocolos de datos “streaming” como Real Audio o Real video.

Squid no soporta los protocolos de correo POP, IMAP y NNP.

CONFIGURACIÓN DEI FIREWALL DE APLICACIONES PROXY SQUID:

La configuración del servidor Linux como un servidor de Firewall de aplicaciones proxy se realiza a través de la interface web de Linux “webmin”.

Tome la opción servers, Squid Proxy Server:



Antes de poder trabajar con el servidor proxy Squid, es necesario inicializar la cache del servidor Proxy, con lo cual necesitamos definir un usuario con el cual se ejecute el servidor Proxy. Para ello creamos el usuario "proxy" y el grupo "proxy " (Ambos creados por el sistema webmin). El mismo debe poseer como shell /bin/false.

Después ingresaremos a "Administrative Options" y verificaremos que el usuario y grupo seleccionados sean los correctos.

Ingresamos a "Cache Options" y definimos el directorio donde almacenaremos los archivos de cache de Squid "Cache Directory”, el tamaño del cache y los directorios de primer nivel y segundo nivel, que es la forma que Squid utiliza para administrar él cache. El directorio donde almacenar los archivos puede ser el directorio por omisión de Squid (/usr/local/squid/cache) o aquel que definamos nosotros. El directorio debe ser creado previamente para poder trabajar con Squid. Si se desean utilizar mas de un directorio para almacenar el Cache, estos deben ser creados de a uno por vez.
Una vez realizados estos pasos podemos inicializar él cache con el botón "Initialize Cache" o "Clear and Rebuild Cache".

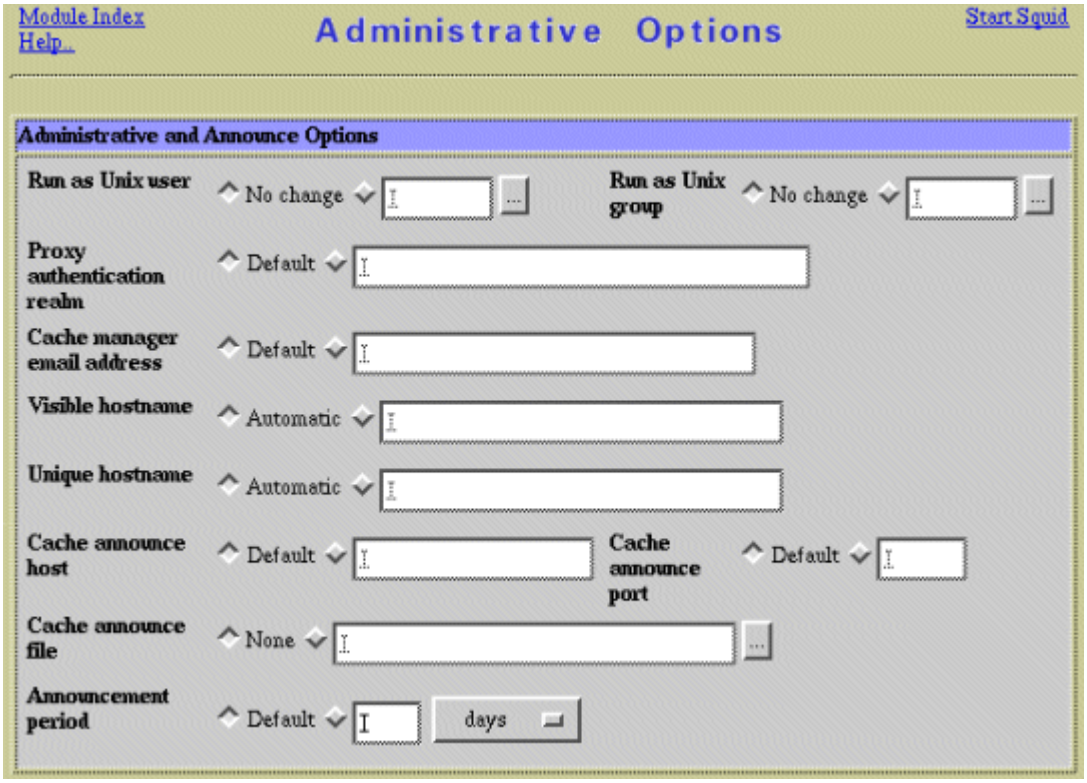
Para hacer esto mismo en forma manual se debería digitar:

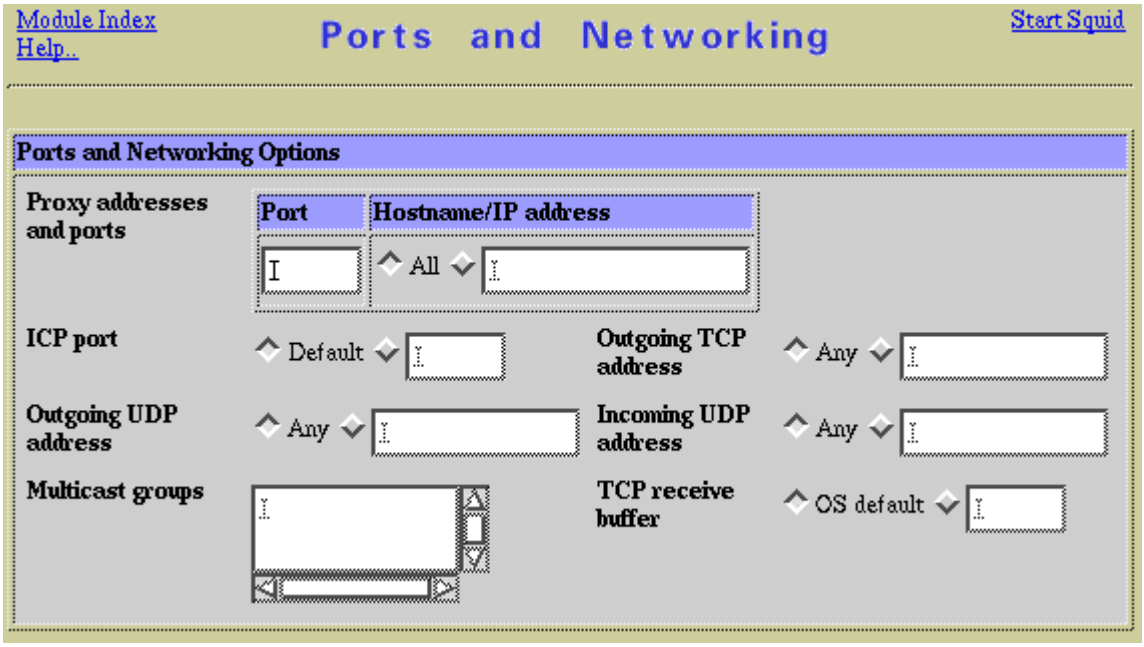
```
# /etc/init.d/squid stop
# squid –f /etc/squid/squid.conf -z
# /etc/init.d/squid start
```

El menú de configuración de Squid incluye las siguientes opciones:

Configuración de puertos y direcciones sobre las que se dan los servicios de proxy	**Ports and Networking**

Los parámetros que esta interface modifica se encuentran en el archivo **/usr/local/squid/etc/squid.conf** pero podría estar en otro sitio pues esto varía según las versiones, siendo generalmente el directorio /etc/squid.





Revisemos algunos parámetros del archivo squid.conf:

http_port: Configura el puerto lógico sobre el cual el servidor proxy funcionara. Si en vez de ser el puerto **3128** lo queremos cambiar por el puerto **8080**, entonces quedaría como **http_port 8080**.

Se puede configurar el proxy para que trabaje con 2 puertos lógicos:

http_port 3128 8080

cache_mem: Es la cantidad de memoria que va a ser utilizada para guardar objetos se lleven a cache por el servidor. no incluye los procesos SQUID que se están ejecutando. El valor por omisión es 8 Mb.

cache_mem 8Mb

maximum_object_size: El tamaño máximo que podrán ocupar los archivos que sean cacheados a disco. Es decir que no serán guardados en disco aquellos archivos que sean mayor a un determinado tamaño . El valor por omisión es 4096 Kb.

maximum_object_size 4096 KB

cache_dir: Es el directorio en el cual se almacenara el cache . Este puede encontrarse en otro filesystem de ser necesario.

cache_dir /usr/local/squid/cache 100 16 256

En donde /usr/local/squid/cache es el directorio por omisión, 100 significa la cantidad máxima de espacio que se almacenará y 16 son los subdirectorios de primer nivel y 256 los de 2 nivel para el cache.

cache_access_log: Mantiene un registro de aquellos clientes que accedieron al cache

cache_access_log /usr/local/squid/logs/cache.log

pid_filename: En este archivo se indica cual es el pid (Process Identification) con el cual se esta ejecutando el servidor SQUID .

pid_filename /usr/local/squid/logs/squid.pid

debug_options : Indica el nivel de debug que se va a ejercer sobre el proxy . Se puede configurar según el nivel de log que se requiera o la calidad del mismo . Al ejecutarlo de la sgte. manera

debug_options ALL,1

En este caso haremos un log de todo el sistema con un nivel 1 que es el mas bajo, siendo el nivel mas alto de log el 9.

reference_age: Es el tiempo máximo que un archivo permanecerá en el cache. Después de esto el archivo es eliminado del cache, el valor por omisión es un mes .

reference_age 1 month

cache_efective_user: Es el usuario con el cual se guardaran los documentos en el disco.

cache_efective_user nobody

cache_efective_group: Es el grupo con el cual se guardaran los documentos en el servidor .

cache_efective_group nobody

visible_hostname : Si en los mensajes de error desea que aparezca el nombre del servidor.

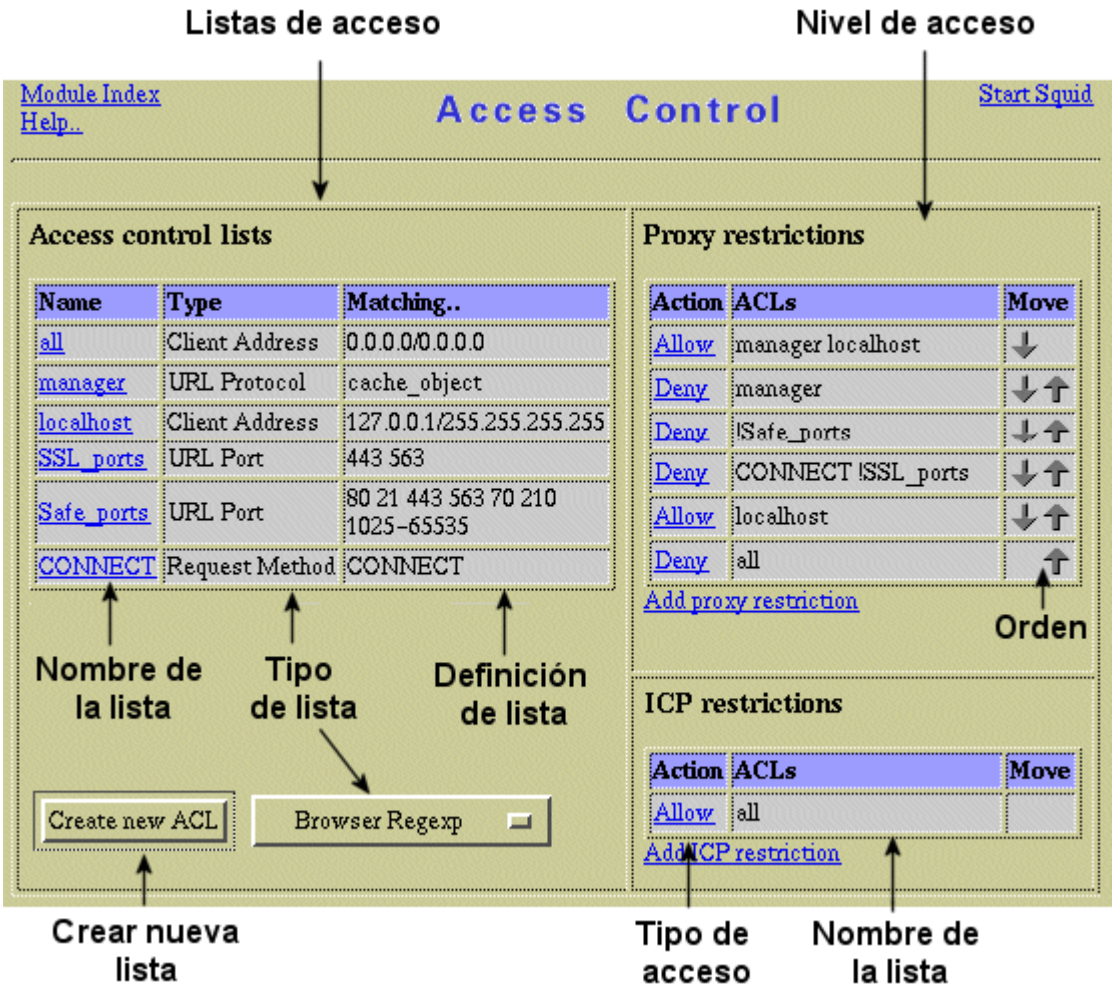
visible_hostname squid.sco.com

Listas de control de acceso:

Se puede limitar el acceso a los usuarios de la red local hacia Internet, o hacia determinadas páginas o servidores web.

Para ello se utiliza el comando acl, que son las listas de acceso que nos limitaran el acceso a Internet.

El límite impuesto a los usuarios se compone de 2 comandos, **http_access** y **acl**.



Con **acl** se construye la lista de direcciones IP, direcciones WEB o aquello que sea requerido para después utilizar el **http_access** y denegar o autorizar el acceso a los diferentes recursos.

La sintaxis genérica es:

acl <nombre_acl> <**tipo_acl**> <dirección>

Para controlar puertos:
acl <nombre_acl> **port** <numero puerto>

Para controlar url:
acl <nombre_acl> **url_regex** <expresión_regular o archivo>

Para controlar el acceso por tiempo:
acl <nombre_acl> **time** <Abreviatura del día> <h1:m1-h2:m2>

Donde las abreviaturas del día son:

S-sunday (Domingo)
M-Monday (Lunes)
T-Tuesday (Martes)
W-Wednesday (Miércoles)
H-Thursday (Jueves)
F-Friday (Viernes)
A-Saturday (Sabado)

Con **http_acces** <**allow**/**deny**> <nombre_del_acl> impondremos un orden de reglas, el orden en que aparezcan es el orden de ejecución de las reglas.

Allow significa “se permite” y ***deny*** significa “denegar o prohibir”.

Por ejemplo vamos a limitar el acceso a aquellos usuarios que se encuentren en las direcciones IP entre 10.10.1.5 hasta la dirección 10.10.1.10.

El nombre de la lista de acceso será “ventas” y negaremos el acceso a dichas direcciones:
acl ventas 10.10.1.5-10.10.1.10/255.255.255.255
http_access deny ventas

Ahora limitaremos el acceso al dominio playboy.com:
acl playboy **dstdomain** playboy.com
http_access deny playboy

Creemos un acl que agrupe varios puertos:
acl puertos_seguros **port** 80 21 23 25 110 114 443 563 1025-65535
http_access allow puertos_seguros

Ahora una lista que agrupe fechas de lunes a viernes durante las horas 8AM a 6PM:
acl horas_de_trabajo **time** M-F 08:00-18:00
http_access allow horas_de_trabajo

Configuración de acceso de usuarios:

También podemos configurar el servidor proxy para que permita el acceso al sistema de solo aquellos usuarios que hayan iniciado sesión en el proxy.

Crear una lista con "External Auth" y valor REQUIRED, Nivel de acceso Allow

En la pantalla de configuración principal de Squid ir a "Helper Programs -> Custom authentication Program" e indicar ahí algunas de las opciones de autenticación.

Los métodos de autenticación disponibles son:

Servidor de Dominio Samba/Microsoft:

/usr/lib/squid/smb_auth -W DOMINIO

Servidor LDAP:

/usr/lib/squid/squid_ldap_auth -b dc=lacositarica,dc=com -u cn -s sub 1.2.3.4

Archivo de claves

/usr/lib/squid/nsca_auth /etc/squid.d/claves

Analizaremos caso por caso el como verificar la correcta conexión a los distintos servicios

Servidor de Dominio:

 # /usr/lib/squid/smb_auth -W DOMINIO -d usuario clave

La única diferencia radica en la autenticación del usuario bajo el sistema de controlador de dominio, en el que en el directorio de \\NETLOGON del usuario debemos crear el archivo proxyauth que contenga solamente la palabra "Allow" y con permisos 444.

Además deberemos agregar en el archivo /usr/lib/squid/smb_auth.sh las siguientes líneas

SAMBAPREFIX=/usr;
export SAMBAPREFIX;

Servidor LDAP:

 # /usr/lib/squid/squid_ldap_auth -b dc=lacositarica,dc=com -u cn -s sub 1.2.3.4 usuario clave

Archivo de claves

Para crear el archivo de claves digite:

 # htpasswd -c /etc/squid.d/claves usuario
 # htpasswd /etc/squid.d/claves usuario2

Edite /etc/squid.d/squid.conf y edite la línea ncsa_auth para que permita validar los usuarios contra un password:

authenticate_program /usr/sbin/ncsa_auth /etc/squid.d/claves

Cree un ACL y autorice la autenticación:

acl password proxy_auth REQUIRED

http_access allow password

¿Que pasaría si el authenticate_program apuntara a /etc/shadow ?, es decir:

authenticate_program /usr/sbin/ncsa_auth /etc/shadow

Como bloquear el acceso a Messenger:

Messenger es un servicio que permite la funcionalidad P2P para que dos usuarios intercambien archivos o hagan chat. Este servicio cambia de puertos con frecuencia y no ha sido fácil bloquearlo en forma automática. Para bloquearlo en forma permanente se debe utilizar un ACL de tipo MIME:

acl MSN **req_mime_type** -i ^application/x-msn-messenger$

http_access **deny** MSN

```
acl Safe_ports port 591         # filemaker

acl Safe_ports port 777         # multiling http

acl CONNECT method CONNECT

##### Block messenger logins

acl msnlogin dstdomain nexus.passport.com

http_access deny msnlogin

deny_info TCP_RESET msnlogin

##### Block MSN Messenger

acl msnmessenger url_regex -i gateway.dll

http_access deny msnmessenger

##### Block MSN online chat

acl msnchathttp url_regex -i ^http://chat\.

acl msnchathttp url_regex -i ^http://.*chat.*

http_access deny msnchathttp
```

```
#### Blocking Adware
acl adware url_regex -i ^http://.*lzio\.com.*
http_access deny adware
http_reply_access deny adware

##### Block messenger web sites
acl msnoverhttp url_regex -i e-messenger
acl msnoverhttp url_regex -i ^http://.*messenger.*\.com
acl msnoverhttp url_regex -i ^http://.*messenger.*\.ca
acl msnoverhttp url_regex -i ^http://.*messenger.*\.us
acl msnoverhttp url_regex -i ^http://.*messenger.*\.info
acl msnoverhttp url_regex -i ^http://.*messenger.*\.cn
acl msnoverhttp url_regex -i ^http://.*messenger.*\.org
acl msnoverhttp url_regex -i ^http://.*messenger.*\.net
acl msnoverhttp url_regex -i ^http://.*messenger.*\.biz
acl msnoverhttp url_regex -i ^http://.*messenger.*\.fi
#acl msnoverhttp url_regex ^http://.*msg.*\.com
acl msnoverhttp url_regex ^http://.*msg.*\.ca
acl msnoverhttp url_regex ^http://.*msg.*\.us
acl msnoverhttp url_regex ^http://.*msg.*\.info
acl msnoverhttp url_regex ^http://.*msg.*\.cn
acl msnoverhttp url_regex ^http://.*msg.*\.org
acl msnoverhttp url_regex ^http://.*msg.*\.net
acl msnoverhttp url_regex ^http://.*msg.*\.biz
acl msnoverhttp url_regex ^http://.*msg.*\.fr
acl msnoverhttp url_regex -i ^http://.*\.AIM.*
acl msnoverhttp url_regex -i ^http://.*AIM\..*
acl msnoverhttp url_regex -i ^http://.*wbmsn.*\.com
acl msnoverhttp url_regex -i ^http://.*wbmsn.*\.ca
acl msnoverhttp url_regex -i ^http://.*wbmsn.*\.us
acl msnoverhttp url_regex -i ^http://.*wbmsn.*\.info
acl msnoverhttp url_regex -i ^http://.*wbmsn.*\.cn
acl msnoverhttp url_regex -i ^http://.*wbmsn.*\.org
acl msnoverhttp url_regex -i ^http://.*wbmsn.*\.net
```

```
acl msnoverhttp url_regex -i ^http://.*wbmsn.*\.biz
acl msnoverhttp url_regex -i ^http://.*wbmsn.*\.fr
acl msnoverhttp url_regex ^http://64\.12\.163\.136
http_access deny msnoverhttp

##### AIM / MSN domains
acl baddomains dstdom_regex -i .*\.blue\.aol\.com
acl baddomains dstdom_regex -i .*\.icq\.com
http_access deny baddomains

##### Downloads
acl download rep_mime_type ^.*video.*
acl download rep_mime_type ^.*audio.*
http_reply_access deny download

##### Block AOL and YAHOO
acl aolyahoo dstdomain login.oscar.aol.com
acl aolyahoo dstdomain pager.yahoo.com
acl aolyahoo dstdomain shttp.msg.yahoo.com
acl aolyahoo dstdomain update.messenger.yahoo.com
acl aolyahoo dstdomain update.pager.yahoo.com
http_access deny aolyahoo

##### Mime blocking
##### Blocking reqested mine types
acl mimeblockq req_mime_type ^application/x-msn-messenger$
acl mimeblockq req_mime_type ^app/x-hotbar-xip20$
acl mimeblockq req_mime_type ^application/x-icq$
acl mimeblockq req_mime_type ^.*AIM.*
acl mimeblockq req_mime_type ^application/x-comet-log$
acl mimeblockq req_mime_type ^application/x-pncmd$


##### Blocking sent mime types
```

```
acl mimeblockp rep_mime_type ^application/x-msn-messenger$
acl mimeblockp rep_mime_type ^app/x-hotbar-xip20$
acl mimeblockp rep_mime_type ^application/x-icq$
acl mimeblockp rep_mime_type ^.*AIM.*
acl mimeblockp rep_mime_type ^.*AIM/HTTP
acl mimeblockp rep_mime_type ^application/x-comet-log$
acl mimeblockp rep_mime_type ^application/x-pncmd$
acl mimeblockp rep_mime_type ^application/x-chaincast$


##### Setting Access controls
http_access deny mimeblockq
http_reply_access deny mimeblockp


##### Streaming players
acl useragent browser -i ^.*NSPlayer.*
acl useragent browser -i ^.*player.*
acl useragent browser -i ^.*Windows-Media-Player.*
http_access deny useragent
```

Como bloquear el bajar archivos con extensión .exe:

acl EXE **urlpath_regex** -i \.gif$

http_access **deny** EXE

Laboratorio:

Objetivo:

Configurar SQUID como "TRANSPARENT PROXY"

Prerrequisitos:

Suponga que el servidor tiene dos interfaces de red la eth1 con IP válido 200.93.178.2 para acceso a Internet, adicionalmente se cuenta con la eth0 como gateway de usuarios con la IP 192.168.11.254

Se deben tener las siguientes reglas:

a) Los gerentes, subgerentes y los funcionarios de sistemas pueden tener acceso no restringido a Internet, sus IP están desde la dirección 192.168.11.15 al 192.168.11.17
b) Los usuarios del área administrativa con IPs del 192.168.11.51 y 192.168.11.52 pueden salir a Internet desde las 7:00AM hasta las 12:00M a los sitios definidos en la lista autorizados
c) Los usuarios del área de producción con IPs del 192.168.11.110 y 192.168.11.111 pueden salir a Internet desde las 13:00PM hasta las 18:00PM a los sitios definidos en la lista autorizados
d) La lista de los sitios autorizados son: www.unixgroup.com.co www.mvaonline.com www.tarantella.com.co www.tarantella.com www.linux.org y www.unincca.edu.co

Las reglas según la nomenclatura ACL del archivo /etc/squid/squid.conf serían:

```
acl IPGerencias         src 192.168.11.15-192.168.11.17/255.255.255.255
acl IPAdministrativo    src 192.168.11.51-192.168.11.52/255.255.255.255
acl IPProduccion        src 192.168.11.110-192.168.11.111/255.255.255.255
acl MANIANA             time 07:00-12:00
acl TARDE               time 07:00-12:00
acl SitiosAutorizados   urlpath_regex   www.google.com   www.unixgroup.com.co
www.sco.com.co www.mvaonline.com www.asogas.org.co www.norgas.com.co

http_access   allow   localhost
http_access   allow   IPGerencias
http_access   allow   IPAdministrativo   MANIANA   SitiosAutorizados
http_access   allow   IPProduccion   TARDE   SitiosAutorizados
```

Es importante que la regla http_access deny all este desactivada

Ahora en el explorador indique el servidor proxy y prueba la navegación.

Paso 1.Configure los acl de squid en el archivo /etc/squid/squid.conf

Se debe definir el nombre del servidor proxy con capacidad de dominios virtuales:

```
httpd_accel_host virtual
```

Ahora debe indicar el número del puerto que realmente usa el servidor web:

```
httpd_accel_port 80
```

Debemos indicarle a squid que funcione como servidor acelerador httpd local y como servidor proxy:

httpd_accel_with_proxy on

Configure Squid para que busque el host:

httpd_accel_uses_host_header on

NOTA: NUNCA ACTIVE LA OPCIÓN HTTP_ACCEL_SINGLE_HOST ON

Paso 2.Active el servidor como un Gateway

Active su servidor como un Gateway adicionando la variable IPFORWARDING=yes en el archivo /etc/sysconfig/network, esto también se puede hacer por webmin

Paso 3.Habilite el firewall de filtro de paquetes para redireccionar el puerto 80

Con Netfilter/iptables:

Permitir todos los paquetes de la interfaz local
iptables –A INPUT –i lo –j ACCEPT

Habilitar conexión a servidor Web
iptables -A INPUT -p tcp --dport 80 -j ACCEPT

Habilita la red local a salir hacia internet por la red valida 200.93.178.2
iptables -t nat -A POSTROUTING -j SNAT –s 192.168.1.0/24 --to 200.93.178.2

Redireccionar el tráfico del puerto 80 al dedicado a squid 3128 suponiendo que la tarjeta de lan es eth0:

iptables -t nat -A PREROUTING –i eth0 -p tcp -–dport 80 –j REDIRECT -–to-port 3128

Nota: Se asume que la eth0 es la red LAN

Evite que el servidor squid sea utilizado por personas externas a la organización, para ello use las siguientes reglas:

```
# ******************************************************
# squid = 3128 - Squid proxy cache
# ******************************************************
iptables -A INPUT -i eth1 -p tcp --dport 3128     -j DROP
iptables -A INPUT -i eth1 -p udp --dport 3128     -j DROP
iptables -A INPUT -i eth1 -p tcp --dport 3130     -j DROP
iptables -A INPUT -i eth1 -p udp --dport 3130     -j DROP
iptables -A INPUT -i eth1 -p tcp --dport 4827     -j DROP
iptables -A INPUT -i eth1 -p udp --dport 4827     -j DROP
```

Reportes de SQUID con SARG

Se descarga la versión 2.2.2 de SARG del sitio http://sarg.sourceforge.net

Descárguela en el directorio /tmp

Procedimiento de instalación:

1. cd /tmp
2. tar zxvf sarg-x.y.z.tar
3. cd sarg-x.y.z
4. ./configure
5. make
6. make install

Para generar los reportes se debe usar el comando sarg, para mayor información digite en la consola de Linux el comando #man sarg.

Ejemplos de generación de informes:

Informe general con resolución de nombres. Si desea el informe por direcciones IP quite la opción -n

#sarg –o /root/squid-reports/ -f /var/log/squid/access.log -n

Informe de un usuario en especial

#sarg –o /root/squid-reports/ -f /var/log/squid/access.log –u *usuario*

Nota: Webmin permite hacer estos reportes sin bajar a la línea de comandos.

Bibliografía

- www.squid-cache.org
- The definitive guide, Duane Wessels, Enero de 2004, O'Reilly
- Web Caching, Duane Wessels, Junio 2001, O'Reilly

Para mejorar esta ayuda por favor escribanos a armando.carvajal@globalteksecurity.com