By Eduardo Casarero y Pablo Scheveloff
eduardo dot casarero at informaticaavanzada dot com dot ar
pablo at atdt dot com dot ar

Guia de Instalacion y Configuracion Basica, Sistema Operativo Slacware 10.2, Dansguardian 2.9.7.1, squid 2.5.STABLE13.

Squid (en Slackware 10.2)

-Bajar el paquete desde
http://www.linuxpackages.net/download.php?id=8917

-Instalar el paquete
installpkg squid-2.5.STABLE13-i486-1maew.tgz

-Crear directorio cache
/usr/sbin/squid –z

-Poner el script de Squid en rc.local para el inicio automático
En /etc/rc.d/rc.local poner:
/usr/bin/RunCache

-Archivos de configuración
Están en etc/squid/
.squid.conf : Archivo principal de configuración

Configurar las IP de quienes pueden navegar:
acl our_networks src A.B.C.D/Mask
http_access allow our_networks
http_access allow localhost

Nota: en caso de que solo el dansguardian pueda navegar solo tiene que tener acceso a traves del squid 127.0.0.1 que es el locahost.

-Logs
En /var/lib/squid/
. squid.out
y en /var/lib/squid/logs/
. access.log, cache.log, store.log

-Modo Debug
/usr/sbin/squid –d 10

Herramientas para Reportes: Sarge

Nota: Hay muchos mas parámetros de configuración, esta breve guia no pretende ser un instructivo de configuración de Squid, sino una breve descripción para poner en marcha el Dansguardian.

By Eduardo Casarero y Pablo Scheveloff
eduardo dot casarero at informaticaavanzada dot com dot ar
pablo at atdt dot com dot ar

DansGuardian

-Bajar el paquete desde
http://www.slackware.com/~alien/slackbuilds/dansguardian (versión para Slackware)
sino desde http://dansguardian.org/?page=download2

-Instalar el paquete
installpkg dansguardian-2.9.x.x-i486-1.tgz (Slackware)

-Cambiar permisos de ejecucion del script de inicio del DansGuardian
En /etc/rc.d/ hacer un *chmod 755 rc.dansguardian*

-Iniciar el servicio de DansGuardian
/etc/rc.d/rc.dansguardian start (para el inicio automático ubicar esta línea en rc.local) verificar la configuración del proxy, dado que si el proxy no esta online, el dansguardian no iniciara. Por default busca el proxy en localhost:3128

Nota: Comentar las 2 listas de más abajo que se encuentran en */etc/dansguardian/lists/weightedphraselist* ya que contienen demasiadas listas para control de contenido y no dejan iniciar el servicio error "More than 60 links from this node!" no es arbitraria la eleccion, la lista japonesa es una de las mas largas. Sin embargo pueden comentarse otras depende de la configuracion que se necesite.

#.Include</etc/dansguardian/lists/phraselists/pornography/weighted_japanese>
#.Include</etc/dansguardian/lists/phraselists/pornography/weighted_malay>

-Archivos de configuración: etc/dansguardian/

dansguardian.conf:
Archivo principal de configuración
dansguardianf1.conf:
Archivo de configuración para el grupo 1 por default es el grupo que usa para todos los usuarios. Si se utiliza algún tipo de autenticación para identificar usuarios por grupos, por cada nuevo grupo tiene que haber un dansguardianfX.conf (X=nro de grupo)

/lists:
Todo lo relacionado a los filtros, bloqueos y excepciones (Ver mas adelante)
/authplugins:
ident, ip o proxy-basic
/contentscanners:
Configuración del plugin de AV (Clam AV)
/downloadmanagers:
fancy o default

-Archivos de idiomas para las plantillas html de denegación de pagina en el dansguarian.conf por default esta 'ukenglish'
/usr/share/dansguardian/languages

-Logs
/var/log/dansguardian/access.log

By Eduardo Casarero y Pablo Scheveloff
eduardo dot casarero at informaticaavanzada dot com dot ar
pablo at atdt dot com dot ar

Archivos de configuración

/etc/authplugins/

/etc/dansguardian/authplugins/

ident.conf se utiliza cuando el plugin de indentd esta instalado en los clientes.

proxy-basic.conf se utiliza cuando el squid es el encargado de hacer la autenticacion

ip.conf se utiliza cuando la autenticacion es por la direccion ip de origen, en este archivo se guarda la referencia al fichero que contiene la lista de ips y el grupo al que pertenecen

/etc/dansguardian/contenscanners

clamdscan.conf tiene el parametro ClamD UNIX domain socket que sale de la configuracion del Clamav, para la version 0.88.3 este parametro es: clamdudsfile='/var/run/clamav-milter/clamd.sock'. Ademas estan las listas de excepciones al scaneo.

Nota: Para que el Scanning de virus funcione hay que tener en cuenta que el clamav tiene que poder leer y escribir los archivos temporales del dansguardian, por lo que deberian ser ejecutados con el mismo user. Por defecto el dansguardian corre con user nobody y el clamAV con user clamav.

/etc/dansguardian/downloadmanagers

default.conf
fancy.conf

Depende de la configuracion cuando dansguardian tiene que bajar archivos muy grandes puede enviarle al navegador una senial de progreso como fancy.conf que usa javascript para mostrar una barra con el % de descarga. Utiliza el formato plugin y depende de cada navegador.

/etc/dansguardian/lists/

/etc/dansguardian/lists/authplugins/ipgroups :
contiene el listado de ips y su asignacion a los grupos

/etc/dansguardian/lists/blacklists
contiene todas las urllists para bloquear por dominio.

/etc/dansguardian/lists/phraselist
contiene las listas de frases para el escaneo de contenidos.

/etc/dansguardian/lists/bannedextensionlist:
Extensiones de archivos que pueden ser potenciales virus. Y por lo tanto los bloquea.

/etc/dansguardian/lists/bannediplist:
contiene las ip para las cuales se bloquea el acceso a www.

/etc/dansguardian/lists/bannedmimetypelist:
tipos mime baneados.

/etc/dansguardian/lists/bannedphraselist:
contiene la lista de listas de frases a utilizar por el escaneo de contenidos, aca se pueden habilitar o no listas de frases para abarcar mas o menos contenidos a bloquear

/etc/dansguardian/lists/bannedregexpurllist:
Banned URLs based on Regular Expressions

By Eduardo Casarero y Pablo Scheveloff
eduardo dot casarero at informaticaavanzada dot com dot ar
pablo at atdt dot com dot ar

/etc/dansguardian/lists/bannedsitelist
contiene las listas de sites bloqueados y demas herramientas como ventanas horarias, etc (falta revisar)

/etc/dansguardian/lists/bannedurlist
contiene listas de url bloqueadas, no incluyen el site completo sino alguna parte.

/etc/dansguardian/lists/contentregexplist
Content modifying Regular Expressions, permite modificar el contenido de las www antes de mandarselo al navegador asi remover javascript, cookies, popups, windows resizing, flash objetcs.

/etc/dansguardian/lists/exceptionextensionlist
exception file extension list, extensiones permitidas (document types .css .html .shtml .asp .php image types .bmp .jpeg)

/etc/dansguardian/lists/exceptionfilesitelist : contiene una lista de sitios de los cuales se puede descargar cualquier archivo sin que la extension sea banneada

/etc/dansguardian/lists/exceptioniplist :
contiene una lista de las ip de los host con navegacion libre.

/etc/dansguardian/lists/exceptionmimetypelist:
unblocked text/web document types and images types

/etc/dansguardian/lists/exceptionphraselist:
contiene listas de palabras que si son detectadas omiten el escaneo de contenido.

/etc/dansguardian/lists/exceptionregexpurllist:
tiene una lista de excpciones al las expresiones regulares para url, si se detecta una exception es permitida la url

/etc/dansguardian/lists/exceptionsitelist
dominios y .tld para permitir libremente

/etc/dansguardian/lists/exceptionurllist
url permitidas

/etc/dansguardian/lists/filtergrouplist
listado de usuarios para asignacion a grupos (solo cuando se utiliza algun metodo de autenticacion)

/etc/dansguardian/lists/greyurllist
permite desbloquear parte de un sitio, grey tienen mas importancia que las banned, un ejemplo de uso es cuando se necesita habilitar algun sitio en particular, pero sin deshabilitar el filtro de contenido. o cuando se quiere permitir una parte del sitio y bloquear el resto.

/etc/dansguardian/lists/pics opciones para filtro de contenido de imágenes.

/etc/dansguardian/lists/urlregexplist
Permite configurar la modificacion de url por medio de expresiones regulares sirve para los redireccionamientos, etc.

By Eduardo Casarero y Pablo Scheveloff
eduardo dot casarero at informaticaavanzada dot com dot ar
pablo at atdt dot com dot ar

Reportes:

En http://ip-server/cgi-bin/dglog.pl hay una herramienta para analisis de logs (http://www.tiger.org/technology/dg/) según el desarrollador no esta portado a la version 2.9, lo haran cuando el producto este en STABLE.

Otra herramienta:
En /var/www/cgi-bin/dg-log-parser-0.03.pl genera un reporte que es puesto en /var/www/htdocs/ despues de ejecutarse el script deja un archivo con el formato Mes-dia-anio.hmtl con el parseo del log del dia.