Instituto Superior de Formación Docente
"Dr. J. Alfredo Ferreira"
Bartolomé Mitre 956 – C.P.: W3196AKX

Email: ifdferreiraesquina@yahoo.com.ar

www.isfdjaferreira.wordpress.com

Esquina, Corrientes.

Ministerio de Educación
Provincia de Corrientes

D.G.E.S
DIRECCIÓN GENERAL DE EDUCACIÓN SUPERIOR

"Experiencia Técnica: Resguardo, Restauración y Configuración del Servidor Escolar Linux Debian TopSchool V03, ante eventualidades y otras aplicaciones prácticas"

Año: 2011/2012

Conectar Igualdad

Autor: Ing. Ricardo Dal Lago

Índice

Introducción.

En este material, se pretende dar respuestas a los interrogantes que pueden surgirles a los administradores de red de las instituciones educativas alcanzadas por “Conectar Igualdad”, en adelante CI. Como se podrá observar, los títulos son preguntas, que se responderán en función a la experiencia técnica afrontada en este trabajo por el autor. No solamente se limita al servidor Debian, sino también a encarar cuestiones técnicas propias de los comandos utilizados para lograr ciertos objetivos de las configuraciones. Se documentó la experiencia de resguardo y restauración del servidor Debian TopSchool v03, pero también se encaran cuestiones que hacen a la personalización de los diversos servicios que ofrece este servidor, y que de éstos dependerá una optima administración de toda la red escolar. Además se enfocan también cuestiones que hacen a la ejecución de comandos necesarios en Linux, para alcanzar la configuración deseada. También se realiza una explicación de las tareas a realizar por el administrador para la migración de equipos provenientes de otros ISFDs, se explica un tema no menor, que es la restauración del servidor escolar Ubuntu, que si bien corresponde a una familia de servidores educativos anterior a la TopSchool v3, no está demás en líneas generales explicar el método de restauración necesario ante una eventualidad. También se explica cómo gestionar la restauración de los sistemas operativos de las netbooks educativas, y se propone un método experimentado por el autor, para restablecer el sistema operativo de éstas, cuando la tabla de particiones ha sido modificada y todo el disco haya sido formateado por un uso inadecuado de los alumnos. Este método ha surgido en función de la necesidad de restablecer netbooks dañadas por mal uso, si bien el administrador puede enviar a garantía estos equipos, el autor lo solucionó personalmente utilizando el método que aquí se desarrolla, y evitando así el envío innecesario de equipos a garantía, considerando el tiempo que esto demora, y a veces las soluciones no son las esperadas, este método fue compartido con los demás administradores de la provincia de Corrientes, y se consideró fue considerado un aporte por la Coordinación Jurisdiccional de CI.

¿Cómo generar la imagen original del servidor escolar?

El servidor instalado en el ISFD, viene con un manual de backups (resguardo) y restauración. Inicialmente se pensó que alcanzaba con la lectura de este material, que si bien fue necesaria no fue suficiente, a la hora de efectuar las pruebas de restauración. Un principio de resguardo de información establece que el resguardo no sirve de nada, si no se efectúa una restauración del mismo. Por ejemplo, de nada serviría tener una copia de un archivo de trabajo en una unidad de almacenamiento X (X puede ser un DVD, un CD, un pendrive, etc.), si no se tiene la certeza a ciencia cierta de que esa copia realmente funciona y es legítima y exacta del archivo original. Es por ello que se consideró sumamente necesaria la pronta restauración del backup original. El backup se estructura en tres partes que se detallan a continuación:

1. Backup del host: es el resguardo de los archivos de la máquina servidora y se realiza sobre las particiones: SDA1 que representa el sector de booteo del servidor y contiene los archivos de arranque de la máquina con sus ficheros de configuración, y SDA2 que contiene al sistema operativo del servidor, es una partición cifrada del tipo LVM2. SDA1 tiene una capacidad de 512 MB; SDA2 de 31 GB aproximadamente.
2. Backup de la máquina de servicios: es el resguardo de la máquina virtual de servicios, es decir sin ella el sistema operativo no serviría de nada para los propósitos de la red escolar, ya que para trabajar se necesita acceder a los servicios que vienen integrados en esta máquina virtual; para ser más claro, es como trabajar desde el servidor, pero conectados virtualmente a otra máquina.
3. Backup del TDSERVER (Significa Theft Deterrent Server, es el servidor de seguridad que administra los dispositivos de la red): Es el resguardo del sistema de seguridad y obviamente de todos sus datos, contenidos en una base de datos.

Se va a omitir explicar cómo se realizan estos tres backups, ya que esta información está explicada en la documentación suministrada por el soporte técnico del servidor, y no representa ningún aporte repetir la misma, ya que consiste en pasos que deben efectuarse sobre el servidor y está bien detallado. Lo importante es especificar las cuestiones fundamentales de la política de backup y destacar lo más importante a tener en cuenta en la práctica de este tipo de sistemas.

La partición SDA3 (431 GB de capacidad) es la que alberga los contenidos educativos suministrados con el servidor, y además almacena los resguardos realizados. Todos los resguardos realizados, inclusive los automáticos de la máquina de servicio y del tdserver se almacenan en SDA3.

Debido a que se detectó que la imagen original que viene en el servidor tenía errores de generación; es decir, el gestor de software que generó la imagen original del servidor lo hizo con errores; aunque en el momento de la generación no se advirtió esta situación ya que las leyendas indicaban que todo estaba bien. Siguiendo con el principio de backup enunciado anteriormente, al restaurar el resguardo estos errores fueron detectados y corregidos. El aporte que el autor realiza a la generación del backup, es la realización del mismo a través de una herramienta alternativa a la que viene originalmente, que es una versión de clonezilla live 64 con más opciones que la que trae el servidor. Es decir, la generación original según explica la documentación se debe realizar con un DVD que viene para tal fin; debido a que el backup efectuado de esta manera causó inconvenientes, es decir que no representó una buena copia del servidor; se buscó otra manera de hacerlo; es por eso que se propone que para futuros backups, se trabaje con un pendrive booteable (un pendrive preparado para arrancar el servidor leyendo este dispositivo), con este pendrive se accede a la herramienta clonezilla live 64 y se genera el backup sobre las particiones SDA1 y SDA2 (partición cifrada LVM2, que se monta desde /dev/pve1/root). Este backup se almacenará en otra unidad USB conectada al servidor, obviamente que deberá ser otro pendrive con capacidad superior a 4 GB, para tener idea la imagen del host pesa aproximadamente 5.3GB. Aquí es fundamental que antes de comenzar a generar el archivo de backup, se tilde la opción “-fsck-src-part”, de lo contrario se producirá un error por omitir la comprobación fsck sobre la partición cifrada LVM2. Esto es fundamental, y es el motivo que causó problemas con el DVD original al realizar la imagen. **Este inconveniente ya fue informado a referente de la empresa EXO que brinda soporte al servidor. Esta empresa acordó con el autor, enviar de cortesía un disco externo con la totalidad de las imágenes del servidor, de tal manera de tener una copia sin problemas de todo el disco rígido, reconociendo los problemas que le fueron informados y detallados durante los meses de diciembre de 2011 y enero de 2012. Se ha logrado una muy buena**

retroalimentación con EXO, ya que al informarle de este inconveniente en el ISFD de Esquina, también le sirve a ellos como disparador al considerar que puede estar sucediendo lo mismo en otras instituciones, y han reconocido que el ISFD es el primer establecimiento del país que los alerta de esta cuestión. Además se les informó que este inconveniente también se ha presentado en la Escuela Normal de Libertador.

Luego de realizar la imagen se puede salvaguardar además una copia en SDA3, pero lo ideal por política de backup es que todos los resguardos se guarden off-site, es decir fuera de la institución, esto es así porque si en algún momento sucede algún siniestro sobre el servidor, teniendo los backup en otro lado, se podrá levantar fácilmente todo el sistema utilizando los resguardos realizados.

¿Cómo restaurar Linux TopSchool?

Una vez que se tienen los respaldos en el DVD original del servidor, que fue creado con la documentación suministrada por EXO, se procede a levantar la imagen original, luego sobre ella se customizará toda el host y la interfaz de servicios, luego se vuelve a crear el backup de la máquina de servicio y del tdserver para que contenga los cambios realizados dentro de la partición de datos más grande la SDA3, luego con el clonezilla live 64 se genera la imagen de la SDA1 del SDA2, siguiendo lo explicado en el punto anterior, es decir almacenándolas en un pendrive lo suficientemente grande como para que quepan, después se podrá guardarlas en la SDA3.

A la hora de restaurar la máquina de servicio, debe existir la carpeta /var/lib/vz/storage/backups, que contiene los backups del servidor, en realidad esa carpeta es un enlace (sería como un acceso directo a otra carpeta que está físicamente en otro lado), a la carpeta de backup que está en la partición de datos más grande SDA3, como se explicó previamente. Esto tiene sentido, si lo pensamos desde el punto de vista que solo se backupea (se resguarda) la carpeta SDA1 y SDA2, si el backup quedaría dentro de SDA2, el resultado sería un backup demasiado grande que contendría a los sucesivos resguardos, entonces al representar la carpeta /var/lib/vz/storage/backups solo un acceso directo a SDA3 que es la partición que efectivamente contiene los backups, nos da la certeza de que las imágenes que se generen sobre SDA1 y SDA2 van a ser relativamente de tamaños considerables, es decir no va a existir mucha variación en

cuanto a tamaño entre dos imágenes sucesivas que se realicen. Para explicarlo de otro modo, las imágenes resguardadas sobre SDA1 y SDA2 no van a ser muy grandes, deberían pesar entre 5.3 a 5.6GB; otro punto a tener en cuenta antes de realizar un backup de la máquina de servicio, es la cache del squid, es la que almacena las búsquedas de navegación y puede llegar a pesar demasiado y a influir en el tamaño del backup. El autor garantiza este hecho porque le ha sucedido con otro servidor, donde el tamaño de la cache llegó a influir en un 70% en el tamaño de la imagen. Esta cache se almacena en la virtual de servicios y se aloja en la carpeta /var/spool/squid. Es por ello que es conveniente vaciar esta carpeta que guarda el cache de navegación del servicio de squid, antes de realizar un backup, de tal modo que no se resguarde el cache ocupando espacio adicional.

Es importante considerar el uso de clonezilla 64 bits, de lo contrario, si se utiliza clonezilla 32 bits (el mismo que se usa para gestionar backups de las netbooks), no se podrá tener control de root sobre la partición montada, debido a que es un sistema de 64bits. Se Hace esta aclaración porque ambas versiones son parecidas, pero no son iguales, se deben seguir las mismas opciones de restauración que las utilizadas para las netbooks, el origen sería el pendrive que se generó con la imagen, y el destino el disco rígido, seteando las 3 particiones SDA1, SDA2, SDA3.

Luego de culminado el proceso de restauración se reinicia, se accede a la interfaz de host con el usuario “topadmin” y se elige la opción de reconfigurar las placas de red, luego se levanta la imagen del tdserver y como para poder restaurar la interfaz de servicios es necesario que exista la carpeta /var/lib/bz/storage/share, que en realidad es también un acceso directo que apunta a una carpeta en la partición SDA3, se debe crear esta carpeta, pero para ello es necesario tener permisos de root en el host, entonces se reinicia. Se entra con el clonezilla de nuevo y se elige la opción del promt y se hace:

sudo bash

mount /dev/pve1/root /mnt

cd /

cd /mnt/var/lib/vz/storage

mkdir share

Listo, la próxima vez que se reinicia ya se podrá levantar el backup de la interfaz de servicio, la que escuchará luego de ser restaurada, y ya se podrá acceder a través del navegador al webmin colocando la siguiente URL (Localizador Único de Recurso): localhost:1000. La dirección IP (protocolo de internet) de la máquina de servicios es 172.16.0.1 y del tdserver: 172.16.0.2.

Antes de reiniciar, se borra la password de root:

cd /mnt/etc/

vi shadow

Ahí adentro con el editor "vi" se borran todos los caracteres del password de root que está encriptado, sería algo así:

root:!e@ye76$59309kmfjhf:1500.7823:::

quedando de esta manera:

root::1500.7823:::… más o menos eso

Luego, se debe salir del "vi" guardando los cambios para lo que se tipea

"wq" + ENTER

Es posible antes de reiniciar, crear una password de root, para lo cual se hace:

/# chroot /mnt passwd root

(luego se ingresa el nuevo password dos veces y debería salir lo siguiente):

Password update successfully

Para verificar se puede mirar con el comando "more" el archivo shadow dentro de /mnt/etc/

y ahí se vería que la password ya fue modificada y que está encriptada obviamente.

Además se puede editar el archivo /etc/gdm/gdm.conf con el editor “vi”, obviamente que logueado como root, se busca la directiva [security] AllowRoot=false, cambiando false por true y guardando el archivo, se le da la posibilidad al usuario de ingresar al host como usuario root, pero solo root del host. Si bien por razones de seguridad esta opción viene deshabilitada, no es que se esté buscando atentar contra la seguridad, sino solamente hacer el sistema más flexible para gestionar carpetas y configuraciones en el host, por ejemplo crear los accesos directo de la suite de ofimática OpenOffice, y ponerlos a disposición del usuario topadmin en su escritorio. Se debe tener en cuenta que esta suite de ofimática no viene instalada para el usuario topadmin, y con solo crear los accesos directos y colocarlos en el escritorio del mencionado usuario, ya estará disponible para que pueda utilizarlos. Por propósitos de gestión del servidor es muy necesario tener habilitado este paquete.

Se deja en claro también que no se habilita el modo gráfico del usuario root para loguearse constantemente, sabiendo que no es del todo seguro, se lo hace solo por principios de facilitar la gestión de carpetas, y se le dará el uso más limitado posible. En la realización normal de las actividades del administrador de red frente al server escolar, se va a estar trabajando logueado en el GDM como topadmin, y solo se logueará como root en contadas ocasiones, que la labor lo requiera. Además el usuario topadmin, es el administrador de la máquina de servicios, esto es importantísimo rescatarlo, ya que le da muchísimas herramientas para gestionar toda la configuración de los servicios disponibles a través de la máquina virtual de servicios, que es en definitiva la que comanda la red escolar, el host si bien es importante porque sostiene toda la infraestructura, pasa a ocupar un segundo lugar de importancia, en el momento que el lector se va involucrando en las diversas configuraciones y posibilidades administrativas que proporciona la máquina virtual de servicios. Es decir, un segundo lugar desde un punto de vista de los servicios que ofrece la máquina virtual.

Luego de esa última configuración mencionada se reinicia la máquina y se restaura la interfaz de servicios utilizando el backup respectivo generado previamente, una vez hecho esto, se debería poder acceder desde el icono del escritorio a dicha interfaz, o bien desde el navegador tipeando en la barra de navegación: http://172.16.0.1:10000 (IP y puerto donde se presta el servicio)

Con la clave generada del usuario root, no solo se puede ahora loguear el usuario desde el entorno gráfico como root, sino además puede loguearse

en el webmin, ¡pero ojo!, debe manejarse con cuidado esta cuestión, ya que si se toca más de la cuenta, puede quedar no operativa la red, y será necesario comenzar desde cero el proceso de restauración. Lo único que se debería hacer es configurar, la posibilidad de que los demás usuarios puedan montar y ejecutar binarios desde la partición de datos SDA3, una vez hecho esto se guarda todo y se sale.

Por último, es importante dejar customizada (personalizada) la configuración del booteo de la máquina, para ello, en este punto se puede ingresar ya desde una consola como root, o desde el modo gráfico a la carpeta /grub. Pero primero se debe explicar que en realidad la carpeta grub está físicamente en la partición SDA1 y por defecto está montada como una carpeta más en el sistema de archivos de la partición SDA2, eso es lo que en realidad sucede. Por lo tanto para tener una idea acabada de la ubicación de SDA1, si alguien está trabajando desde afuera en una consola de alguna distribución Linux del tipo live cd, puede montar SDA1 en alguna carpeta utilizando el comando “mount”, y luego deberá editar allí un archivo llamado menu.lst. Se podrá comentar la línea de password que contiene la contraseña encriptada (cifrada) de las opciones del gestor de arranque grub, y alargar el período de tiempo que muestra el contador antes de comenzar el booteo de la partición linux del. En el caso que se ha probado se le ha dado 45 segundos al usuario para que elija que hacer al bootear, antes de comenzar a levantar la partición SDA2 que contiene al linux Debian TopSchool.

¿Cómo hacer para customizar la lista de páginas filtradas?

Si es un servidor Ubuntu se debe mirar el squid, editando los archivos que se han llamado palabra_denegar, web_denegar y web_permitir dentro de /etc/squid.

Squid es un programa que tiene implementadas las funciones de un servidor proxy, y una cache de navegación web, es decir mantiene una memoria de las páginas que se navegan y que son solicitadas por los usuarios, de tal manera de minimizar las búsquedas repetitivas de DNS de los sitios que se almacenan en esa cache, esto ayuda a mejorar la velocidad de navegación web, ya que efectivamente se efectúa la búsqueda cuando el sitio no está en la caché. Además el squid agrega seguridad, restringiendo el tráfico que pasa por la red.

Dansguardian es otro de los servicios que viene con el servidor Linux Debian TopSchool, este es un filtro directo que se ubica entre el cliente Web (navegador web) y el Servidor Proxy Squid. Dansguardian acepta conexiones en el puerto 8080 y se conecta a squid en el puerto 3128. Por lo tanto, es importante que no haya otro servicio utilizando el puerto 8080. DansGuardian además de ubicarse entre el navegador web del cliente y el proxy, intercepta y modifica la comunicación entre ambos. De esta forma facilita la tarea de filtrado de páginas visitadas por el usuario desde el equipo cliente, cuya utilización puede ser de especial interés en el aula para los propósitos educativos de CI, e incluso en el propio domicilio.

Ahora se explicará a grandes rasgos como filtrar contenidos con dansguardian. Si es un server TopSchool hay que entrar por ssh a la carpeta /etc/dansguardian/lists/blacklists y ahí adentro hay subcarpetas ordenadas por categorías, por ej. socialnetwork, mail, chat, etc. y dentro de cada una de estas subcarpetas se debe editar con el "vi" los archivos que guardan las configuraciones: domains y url, editando según corresponda, hay que recordar que para guardar los cambios introducidos con el "vi" al editar los archivos, después de loguearse por ssh, hay que hacer sudo bash para adquirir privilegios de root en la máquina de servicios. Luego se debe reiniciar dansguardian para que los cambios impacten en la red, por lo tanto hay que volver a levantarlo al servicio desde /etc/init.d, haciendo "./dansguardian restart", de este modo se refrescan los cambios, el "./" que se puede ver es imprescindible que esté y que no se omita, de lo contrario no se reiniciará el servicio. Una vez reiniciado, se podrá probar desde una netbook conectada a la red local, los filtros configurados desde las listas de dansguardian. Es importante también saber que existen listas de excepciones que permiten omitir los filtros establecidos, así como también una lista de IPs (direcciones de internet) que se pueden omitir completamente del filtrado, no es muy aconsejable que esta lista sea muy larga, ya que no se aplica ningún filtro sobre esas IPs, pudiendo los usuarios acceder a cualquier sitio prohibido por su contenido para el resto de los clientes de la red.

¿Cómo configurar sarg para squid y dansguardian?

Sarg es el generador de reportes de navegación que viene con squid, es decir el encargado de generar los informes de todas las páginas que han sido visitadas por los usuarios de la red escolar. El reporte brinda varias

características que permiten visualizar como navegan las distintas IPs, es decir las diferentes máquinas que están conectadas a la red. Esto es importante para evaluar la navegación y el uso que se le está dando al enlace de internet conectado al servidor. En el archivo de configuración se tienen diversas opciones que permiten personalizar bastante los reportes generados por sarg.

Para generar un informe:

- Se deberá editar el archivo /etc/squid/sarg.conf y comentar language English (se trató de dejarlo seteado a Spanish) pero no funcionó, el mensaje de error dice que no se puede abrir el archivo, ese menaje se visualiza al correr el sarg), es por ello que directamente se comentó la línea del lenguaje.
- Correr “sudo sarg”, generará el informe en /var/www/squid-reports/.

Hay varias opciones, hay una que es para reemplazar dentro de sarg, el url de donde debe tomar los archivos de logs para generar el informe, es decir en el archivo de configuración sarg.conf, por defecto se toman los logs del squid, y se verá una línea que indica de donde obtiene los logs: /var/log/squid/access.log, esto puede cambiarse por /var/log/dansguardian/acess.log, para que tome los logs del dansguardian, o bien se puede proporcionar el directorio directamente al ejecutar el comando, haciendo: “sudo sarg –l /var/log/squid/access.log” (se obtiene el reporte en base al log de squid), o bien, ·sudo sarg –l /var/log/dansguardian/access.log” (se obtiene el log en base al log de dansguardian). El reporte puede visualizarse desde la máquina de servicios a través del webmin, desde donde también se puede generar el informe seleccionando la opción correspondiente. Hay que recordar que todo lo que sea la máquina de servicios, se debe gestiona solamente con el usuario topadmin, ya sea para loguearse a la máquina vía ssh, o bien para configurar algo en particular desde webmin.

¿Cómo hacer para colocar excepciones a las páginas filtradas?

Al deshabilitar el filtrado de Hotmail, no se podía desde la LAN ingresar de todas maneras al correo, entonces fue necesario agregar el url “mail.live.com” al archivo de excepciones de sitios del dansguardian, que se llama exceptionsitelist. Esto podría ser útil para otro caso que pueda presentarse.

¿Cómo hacer para filtrar facebook con https?

El filtrado de facebook que hace dansguardian con el manejo de las listas negras, no soluciona la cuestión de que alguien ingrese a través de https://www.facebook.com, es decir utilizando en la url del navegador el protocolo https (http con seguridad), si lo hace de esta forma, dansguardian ni se entera, y se podría ingresar a facebook, o a cualquier sitio que esté en la lista negra, pero que también permita el ingreso por https. Es notable como un sitio que está siendo filtrado por dansguardian, deja de estarlo al agregar una simple letra "s" al final de "http". Esta situación queda salvada con el firewall de Linux. Obviamente el firewall de la interfaz de servicios, es por ello que se debe loguear a la máquina de servicio a través de ssh con el usuario topadmin. Una vez que se ingresa y se le da los permisos de root, se debe ir a editar el archivo /etc/iptables.up.rules, ahí dentro con el editor "vi" se agregan las siguientes reglas para filtrar facebook:

#filtro face

iptables -A FORWARD -s 0/0 -d 69.0.0.0/8 -p tcp --dport 443 -j REJECT

iptables -A FORWARD -s 69.0.0.0/8 -d 0/0 -p tcp --dport 443 -j REJECT

iptables -A FORWARD -s 0/0 -d 204.0.0.0/8 -p tcp --dport 443 -j REJECT

iptables -A FORWARD -s 204.0.0.0/8 -d 0/0 -p tcp --dport 443 -j REJECT

iptables -A FORWARD -s 0/0 -d 66.0.0.0/8 -p tcp --dport 443 -j REJECT

iptables -A FORWARD -s 66.0.0.0/8 -d 0/0 -p tcp --dport 443 -j REJECT

Luego se guarda todo y se sale. Ahora al abrir el navegador e ingreso a la interfaz de servicios, hay que dirigirse a Network Configuration y ahí dentro a Firewall de Linux, luego se debe aplicar la configuración para que las reglas que se agregaron al firewall desde la consola con el editor "vi", tengan efecto, cuando se clickea aplicar cambios, si hubiera un error de sintaxis el administrador vería un mensaje en pantalla desde esta sección, de lo contrario, si todo va bien, los cambios se aplicarían y devolvería la interfaz del firewall desde webmin sin inconvenientes, donde se observaría que se agregaron correctamente al firewall las reglas enunciadas anteriormente. Acá hay que tener cuidado, debido a que estas reglas se

agregaron pero al reiniciar el sistema se borrarán, es decir que funciona como una memoria volátil, pues persisten mientras dure la volatilidad del servidor por decir así, no sería válido decir la durabilidad de la sesión, ya que si cierro sesión y abro otra nueva, estas reglas siguen estando activas. En resumen, estas reglas agregadas estarán activas hasta antes del próximo reinicio, y ya no más. Es por ello que se debe crear un archivo de firewall dentro de la carpeta /etc/init.d. Para esto desde la consola donde se tiene la sesión abierta con la virtual de servicios, hay que posicionarse en esta ubicación y hacer "vi firewall.sh". El "vi" abre un proyecto de archivo vacío, ya que no existe un archivo con ese nombre en esa ubicación, el cual será editado agregando las reglas antes mencionadas, otra alternativa es copiar y pegar tal cual está, todo el contenido en /etc/iptables.up.rules, que como se vio antes, incluye las reglas que se agregaron, pero en este caso en particular, solo se agregaron las reglas de filtrado de facebook. Una vez que se lo customiza (personaliza) a gusto y necesidad, ya que puede haber por supuesto muchas otras reglas que se deseen agregar, se lo guarda y se sale del editor. Ahora se le debe dar permiso de ejecución, para esto se hace: "chmod + firewall.sh", además hay que decirle a linux que lo cargue al inicio, esto se hace con el siguiente comando: "update-rc.d firewall.sh defaults 80". Para probar el script se puede aplicar dentro de /etc/init.d/, el siguiente comando: "bash firewall.sh"; a partir de esta ejecución se verá si todo anduvo bien o existen errores los que deberán corregirse si aparecen, editando este archivo. Una vez que se agregó el archivo al arranque de linux, el script se va a ejecutar cada vez que el sistema arranque, y cada vez que se desee agregar o sacar algo del firewall será necesario solamente editar el archivo.

Una cuestión a resaltar, es que en la configuración de squid se ha definido una subred de profesores, de tal manera que éstos tengan acceso a páginas que para los alumnos estén filtradas. Es decir que si bien esta subred estaría contenida en los filtros de dansguardian, squid le permitiría acceder a páginas que para todos los demás en la red estarían siendo filtradas. Para esto se definió el archivo web_permitir. No se ha podido darle la funcionalidad deseada a la regla explicada previamente. Se trabajó con la documentación del servidor escolar Linux Ubuntu, con la versión 3.0 de squid, tal vez este es el motivo por el cual la regla no funciona, es decir, al asignar a una netbook una IP del rango de docentes, se le aplica el mismo filtrado que a los demás, y el mismo squid no deja acceder a estos sitios que estarían permitidos solo para los docentes, hay que considerar que Linux Debian TopSchool viene con la versión 2.7.9 de squid, este motivo

puede ser el que genere la no funcionalidad de la regla. Para paliar esta situación, se puede dar permiso a cada IP de profesor, a acceder a la red obviando el dansguardian, es decir, que naveguen sin filtros, pero de todos modos es preferible lograr con el soporte técnico resolver esta cuestión, ya que no es la mejor solución que existan usuarios que naveguen sin restricción alguna, pues no todos estos usuarios tienen la misma visión de la navegación.

Otra consideración importante es la que hace al firewall, las IPs que puedan navegar sin restricciones, es decir que estén en el exceptioniplist del dansguardian, no se salvan de ser controladas por el firewall, por lo tanto el firewall aplicará sus reglas independientemente de la configuración del dansguardian. Un ejemplo sería, un profesor que esté en la lista exceptioniplist del dansguardian e intente entrar vía https al facebook, el firewall rechazará la conexión.

¿Qué archivos se deberán resguardar una vez realizada la configuración inicial de la máquina de servicio?

Lo ideal no es salvar archivos puntuales, aunque es una alternativa. Debería hacerse un backup de la máquina de servicios como primera medida. Independientemente de esto, habría que solicitar al soporte técnico que provea el asesoramiento respecto del software de acceso a la máquina de servicios, ya que es archi conocida la incomodidad que supone trabajar con una máquina virtual de servicios, solamente vía ssh y solamente editando archivos con el editor “vi”. Es decir, un software que en base a las necesidades detectadas durante esta experiencia, al menos permita al administrador acceder a un navegador de archivos y poder copiar a gusto y paladar las carpetas que contienen a los ficheros de configuración, como también la edición de archivos utilizando un editor gráfico como el gedit.

Algunas de las carpetas a salvar serían por ejemplo:

/etc/squid

etc/dansguardian

/etc/init.d

Se editó además el archivo de configuración de dansguardian: /etc/dansguardian/dansguardian.conf, seteando el lenguaje español. Dentro del dansguardian hay una carpeta “language” que tiene todos los lenguajes, se ingresó a spanish y ahí dentro se editó template.html seteando el mail

de administrador, que en este caso es el mail del autor de este documento; de este modo las alertas de dansguardian informarán a los usuarios que se encuentren con un mensaje de página filtrada, que le envíen un mail al administrador de la red, y que el acceso al sitio está restringido.

También en el archivo de configuración del squid, se seteó el mail del administrador en la directiva cache_mgr.

¿Cómo hacer para limitar la cantidad de clientes que utilicen el navegador en la red de forma concurrente?

Una necesidad podría ser limitar la cantidad de alumnos que navegan al mismo tiempo en la red escolar, para configurar esto, se debe setear la opción "maxip" del danguardian.conf y obviamente reiniciando dansguardian, recordar que el archivo de configuración es: /etc/dansguardian/dansguardian.conf. Y el demonio de ejecución que se debe reiniciar se ubica en: /etc/init.d/ y se llama dansguardian

¿Cómo hacer para arrancar o parar un servicio desde la interfaz de servicios una vez logueado en ssh, en Linux TopSchool?

Una vez ubicado en la raíz de /etc/init.d/ "./samba stop" por ejemplo, si se pretende correr el firewall: "bash firewall.sh". Esta forma de operación que se utiliza para parar o arrancar un servicio, obviamente que es extensible al host del servidor, aunque no se trabaje sobre el host para configurar la red escolar, sino solamente sobre la virtual de servicios. Con esto se ve que es extensible para cualquier consola de una distribución Linux Debian.

¿Cómo hacer para habilitar que el usuario root se loguée en la interfaz gráfica?

Si bien esto ya fue comentado previamente, no está demás expresarlo en forma independiente en otro apartado debido a la importancia que tiene. Una vez logueado en la interfaz gráfica como topadmin, presionar CTRL+Alt +F1, se abrirá una terminal Unix, aquí se debe loguear como root, una vez hecho esto, ingresar a /etc/gdm, luego con el "vi" editar el archivo gdm.conf y buscar la línea donde está seteada la variable que permite loguearse con GDM al usuario root, la misma dice: AllowRoot=false, reemplazar false por true, salvar los cambios y la próxima vez que se pretenda loguear desde GDM como root debería funcionar. Este es uno de los modos de hacer esto, otra posibilidad es iniciar el servidor desde el pendrive booteable con

clonezilla live 64, montar la partición SDA2 desde su punto de montaje /dev/pve1/root (partición de sistema cifrada LVM2), y desde el punto de montaje que elija, por ejemplo puede ser /mnt, ingresar a /mnt/etc/gdm, editando luego gdm.conf y haciendo lo que se explicó previamente.

¿Cómo hacer para poder hermanar una máquina que viene de otro colegio?

Se deberá enviar al soporte técnico del servidor:

1) Número de serie del Servidor.

2) Versión de sistema operativo del Servidor:

A) Si la versión del sistema operativo es Debian, se necesitará además el archivo versión.txt & TOPSCHOOLID.txt; archivos que se encuentran dentro del directorio de usuario “topadmin”

B) Si la versión del sistema operativo fuese Ubuntu, se necesitará lo siguiente:

Descargar el siguiente archivo en el escritorio del usuario “admsrv”:

http://www.exo.com.ar/emails/Z/topschool/diagnostics/gen.zip

Descomprimir el archivo en el escritorio para poder continuar.

Presionar “Alt+F2” y dentro del cuadro de dialogo escriba “gnome-terminal” y presionar la tecla “Enter” para continuar.

En la nueva ventana de trabajo escribir lo siguiente:

chmod +x generador.sh y presionar la tecla “Enter” para continuar.

sudo ./generador.zip y presionar la tecla “Enter”. El sistema le solicitará el ingreso de la contraseña del usuario “admsrv”, luego de ingresarla se debe presionar “Enter” para dar inicio al proceso.

El proceso anterior se obtiene como resultado un archivo .zip que se almacenará en el “Escritorio” del usuario, el mismo se debe remitir al soporte técnico del servidor.

3)Los Special Number (S/N o N/E) de los equipos bloqueados y dispuestos a migrar al nuevo Servidor.

El Special Number podrá extraerse de la pantalla de bloqueo de la netbook, es un número que consta de 40 dígitos separados por un guion medio.

Es necesario que se aclare el Special Number y el Nro. De serie del Servidor de destino para avanzar con el proceso respetando los puntos anteriores.

¿Cómo hacer para restaurar el server Ubuntu en una PC de escritorio ante una eventualidad en la cual el servidor quede no operativo?

Si bien el soporte técnico no desea que se realice el clonado de servidores, no se puede dejar de lado la realidad, que es bien distinta, y los riesgos a los que está expuesto el servidor educativo, hacen necesaria la generación de una política de resguardo y restauración del servidor y de una posible máquina que lo reemplace, en caso de que surja la pérdida del mismo, o el daño físico de alguna de sus partes que lo deje no operativo. Si bien es más difícil que esto suceda, aquí se trata de exponer un poco como se haría el restablecimiento del servidor en una máquina, que por llamarla de alguna manera se podría decir un “servidor de emergencia”, el cual estaría operativo, solamente por el tiempo que dure la reparación del servidor original.

Para llevar adelante la restauración, se deberá preparar una máquina con dos placas de red LAN del tipo Ethernet 10/100 Mbps, podría ser la placa integrada que traen las máquinas en general, y otra placa PCI que se agregue.
Se deberá levantar la imagen del pendrive o del DVD, dependiendo de donde se tenga el backup, y luego se debe editar el archivo /etc/init.d/share_net (que es el firewall del server), se debe cambiar eth0 por eth2 y eth1 por eth3, luego también se cambiará esto en la configuración de red de webmin y por último se reiniciará el sistema, la placa superior (la integrada onboard) de arriba es eth2, a la cual se conectará la WAN, y la de abajo que es la eth3 (PCI) se conectará a la LAN del servidor.

En este punto se puede hacer una comparación respecto al Linux Debian TopSchool, ya que en Ubuntu como se ve es mucho más sencillo personalizar las configuraciones, ya que al no tener la máquina de servicios del TopSchool, directamente se trabaja sobre el host, además los servidores escolares Ubuntu no traen instalado por defecto el dansguardian, la mayoría trabajan solamente con squid.

¿Cómo hacer para restablecer el sistema operativo y arreglar el gestor de arranque de las netbook con Windows Seven?

Si se tiene el pendrive booteable con clonezilla, se debe iniciar con el mismo e ir siguiendo los pasos de restauración que indica la interfaz de dicho Linux, eligiendo respectivamente lo que se desea restaurar, por lo general la partición SDA2 de Windows es la que a menudo se tiende a restaurar porque es la más utilizada por los alumnos. Es decir que se debe elegir la partición origen que es SDA5 (partición de backup integrada en las netbooks), luego se elige lo que se va a restaurar Windows o Linux, si se elije Linux, luego se deberá elegir como partición destino la SDA1, en cambio si se elije Windows, se deberá elegir como partición destino la SDA2. Esto se puede utilizar si la partición SDA5 no ha sido borrada, ya que si SDA5 no existe o está dañada, esto indica que el alumno metió mano a la tabla de particiones.

En caso de que no se cuente con el pendrive booteable con clonezilla live, y además no se cuente con la partición de recuperación que traen los equipos (la SDA5):

1) Con muchísima paciencia, generar con norton ghost una imagen de cada partición de una netbook que funcione correctamente, esto lleva su tiempo, mientras uno realiza otra actividad seguramente.
2) Borrar la tabla de partición completa de la netbook dañada, en el caso que al autor le tocó trabajar, el alumno ya había hecho estragos con la tabla, y se utilizó la herramienta Acronis Disk Director Suite.
3) Una vez borradas las particiones, con el mismo software enunciado en el punto anterior: mirar en una netbook que funcione correctamente, el tamaño de cada partición y su tipo, esta netbook puede ser la misma utilizada previamente para hacer las imágenes en el punto 1).
4) Ingresar de nuevo con Acronis Disk Director a la netbook dañada, y crear la tabla de partición, respetando los tipos de partición existente y su tamaño, información que se obtuvo en el punto 3). Luego con Norton Ghost, bajar las imágenes en el orden correspondiente y en los sectores correspondientes.
5) Una vez que se bajaron todas las imágenes reiniciar booteando con el pendrive booteable de windows seven, ingresar a la consola de recuperación, puede que en este paso se vea un mensaje de error de driver del disco, omitir y continuar.

Hay que fijarse cual es la parición de Windows Seven, cual es la

letra que representa la unidad; en la que se trabajó era la “D”, entonces escribir:

D:\>bootrec /rebuildBcd
D:\>bootrec /fixboot
D:\>bootrec /fixmbr

Cada uno de estos tres pasos pide confirmación.

6) Ingresar con el software Special Fdisk 2000 y setear la partición llamada Sistema, que es la de Windows, como activa, esto es necesario hacer para que efectivamente bootée el gestor de arranque.
7) Hasta acá se hizo andar Windows Seven sin gestor de arranque y totalmente original, ahora lo que hay que hacer es bootear con el pendrive de ubuntu 11.04, elegir la opción de arrancar ubuntu sin instalación, luego de levantar la interfaz gráfica dirigirse a terminal (consola) y escribir: “sudo bash” (para que permita ejecutar todo sin restricciones de permisos) “fdisk –l” (muestra las particiones que se tienen, recordar que estas netbooks vienen con Windows Seven y con Ubuntu), en este caso sucedió que la de Ubuntu se llama SDC1, si este es el caso, escribir “mount /dev/sdc1 /mnt”, de este modo se le está diciendo al sistema operativo que monte en la carpeta /mnt del sistema, la partición SDC1 que es la de Ubuntu de la netbook.

   Ahora faltaría regenerar el gestor de arranque grub, escribir “grub-install --root-directory=/mnt/ /dev/sdc1”, luego de correr este comando sin problemas, reiniciar y se debería visualizar ya el gestor de arranque que traen las netbooks educativas, funcionando todo normalmente.

   Gracias a esto el autor comprendió que en la partición /dev/sdc5 está la imagen que traen las netbooks incorporadas para restaurar, es un clonezilla que pesa 8.3 Gigas. Los pasos al autor le funcionaron correctamente, pero tuvo que trabajar arduamente en ello, lleva tiempo pero es algo que vale la pena hacerlo al menos una vez para ser consientes de que existen otras formas alternativas de restaurar la imagen de estos equipos. **Todo esto fue compartido con el foro de administradores de Corrientes y ha sido reconocido por el Coordinador Jurisdiccional de CI como un buen aporte**.

Es muy importante destacar que estos pasos hay que realizarlos en el caso de que no se tenga la imagen SDA5 en el disco de la netbook, y se deba restaurar desde cero todas las imágenes y la tabla de partición. Obviamente

que si se tiene en el disco de la netbook la partición SDA5, y solo está dañado el gestor de arranque, el administrador podrá restaurarlo rápidamente con el pendrive de clonezilla live como se indicó al principio de este apartado.

Bibliografía consultada.

- http://www.forosdelweb.com/f41/bloquear-https-www-facebook-com-con-ipcop-706454/
- http://www.rolandovera.com/2008/03/22/debian-como-hacer-un-script-que-arranque-automaticamente-durante-el-arranque-del-sistema/
- http://recursostic.educacion.es/observatorio/web/es/software/software-general/524-dansguardian-filtro-de-contenidos
- http://sliceoflinux.com/2009/02/23/como-saltarse-squid-yo-dansguardian/
- http://dansguardian.org/downloads/detailedinstallation2-spanish.html
- https://lists.ourproject.org/cgi-bin/mailman/listinfo/referticsar-general
- http://www.taringa.net/posts/linux/8603931/Uso-de-la-Terminal-en-Debian_Ubuntu-y-derivados.html
- http://blog.debian.org.sv/?p=30
- http://es.wikipedia.org/wiki/Wiki
- http://dansguardian.org/downloads/detailedinstallation2-spanish.html