IMPLEMENTACION SCRIPT PARA FIREWALL

1 INTRODUCCION

El siguiente documento esta diseñado para que los Administradores de red de la Provincia de Santa Fe implementen en los servidores del Plan Conectar Igualdad políticas de seguridad. En este caso implementaremos reglas para el filtrado de paquetes (FIREWALL), el Script presentado esta diseñado para evitar el uso de algunas aplicaciones que saltean las políticas de seguridad necesarias dentro de las Instituciones Educativas.

2 BACKUP

IMPORTANTE: Antes de realizar cualquier modificación en el Servidor Escolar, es obligación del Administrador de Red realizar un back up correcto y funcional del mismo

3 IMPLEMENTACION

3.1 La implementación esta dividida en dos, para los servidores Ubuntu y para los servidores Debian virtualizados. De ahora en adelante los llamaremos UBUNTU y DEBIAN respectivamente. Según el modelo de servidor con el que se cuenta en la institución se deben seguir los pasos correspondientes. Cuando figuren los 2 servidores son pasos comunes a seguir.

3.2 Instalación de archivo. Como primer paso debemos copiar el archivo firewall.sh dentro del servidor en el cual se va a realizar la implementación. El archivo de configuración del script puede ser descargado de la plataforma de Administradores de red.

DEBIAN:

Descargar el archivo de la Plataforma de administradores desde un navegador de Internet y guardar el archivo "firewall.sh" en /home/topadmin

El entorno de trabajo de Debian es distinto ya que el mismo se encuentra virtualizado, la descarga del archivo se realizo en servidor anfitrión y no en el de servicios como necesitamos, entonces lo que debemos hacer es pasar el archivo descargado dentro del servidor de servicios, que es el encargado de manejar las comunicaciones entre la red interna e Internet. Para ello debemos seguir los siguientes pasos.

3.2.1 Abrir una consola (teminal), al abrir la consola ya nos encontramos en el directorio /home/topadmin del servidor anfitrión.

3.2.2 Copiar el archivo dentro del servidor de servicios, para ello debemos ejecutar el siguiente comando

```
# scp firewall.sh servicios:/tmp
```

La ejecución de este comando nos pedirá la clave correspondiente al topadmin, al momento de ingresarla el archivo se copiara dentro de la carpeta /tmp del servidor de sevicios.

3.2.3 Loguearse dentro del servidro de servicios

```
# ssh servicios
```

En este momento nos encontramos logueados en el servidor de servicios dentro del directorio raiz "/".

UBUNTU:

Descargar el archivo de la Plataforma de administradores desde un navegador de Internet y guardar el archivo "firewall.sh" en /home/admsrv

Abrir una consola (teminal), al abrir la consola ya nos encontramos en el directorio /home/admsrv

UBUBTU y DEBIAN:

Necesitamos ahora pasar a root para poder instalar los archivos necesarios

```
# sudo -i
```

Una vez que somo root crearemos dentro del directorio /etc el directorio firewall donde guardaremos el archivo de configuración para implementar el firewall

```
# mkdir /etc/firewall
```

Movemos el archivo firewall.sh que se encuentra en /home/topadmin dentro del directorio /etc/firewall

DEBIAN:

```
# mv /tmp/firewall.sh /etc/firewall
```

UBUNTU:

```
# mv /home/admsrv/firewall.sh /etc/firewall
```

Cambiamos los permisos de ejecucion del archivo firewall.sh, le necesitamos dar permiso de ejecución

```
# chmod 700 /etc/firewall/firewall.sh
```

3.3 Edición del archivo del firewall

UBUBTU y DEBIAN:

Cambiamos al directorio del firewall

```
# cd /etc/firewall
```

Antes implementar el firewall debemos hacer unos ajustes al script ya que no todos los servidores cuentan con la misma configuración, para ello necesitamos editar el archivo firewall.sh utilizando cualquier editor de texto como ser vi, nano, etc..

3.3.1 Abrimos el archivo firewall.sh para modificarlo

```
# nano firewall.sh
```

En caso de no ejecutarse nano, se puede utilizar

```
# vi firewall.sh
```

Buscamos y Configuramos las siguientes variables acorde a nuestro servidor.

DEFAULT_EXTIF: Es la interface utilizada para conectarse a internet
DEFAULT_INTIF: Es la interface utilizada para conectarse a red interna
DANSGUARDIAN: Variable que especifica si el DansGuardian se encuentra instalado y en funcionamiento

* Para conocer la configuracion de nuestro servidor, basta con dentro de la consola en el servidor de servicios ejecutar el comando "ifconfig" lo que devolverá las interfaces que tenemos, aquella que tenga como ip 172.16.0.x sera la DEFAULT_INTIF y por descarte la otra sera DEFAULT_EXTIF

* Para conocer si nuestro servidor DEBIAN tiene dansguardian ejecutándose basta con ejecutar el comando "/etc/init.d/dansguardian restart" con permisos administrativos (sudo -i) y si responde a este comando es que lo tenemos, si no, no.

Una vez configuradas las variables guardamos el archivo y procederemos a la prueba del script, para

ello ejecutamos el siguiente comando

```
# ./firewall.sh start
```

Luego de ejecutarse el firewall, todo trafico https debe quedar bloqueado. En este momento se debe realizar las pruebas de conectividad desde la red interna hacia Internet. Verificar la navegación web. En caso de falla reiniciando el equipo volvemos a la normalidad.

La ejecución por primera vez del script creará dentro del directorio /etc/firewall un nuevo directorio llamado permitidos, en este directorio definiremos los dominios a habilitar para tráfico HTTPs

NOTA: Si el usuario ya está usando script del firewall, la ejecución del mismo migrará la configuración actual, al nuevo formato. **(Ver punto 2.4)**

3.4 Habilitación de dominios HTTPs

UBUBTU y DEBIAN:

Cambiamos al directorio del firewall donde crearemos los archivos para habilitar los dominios con permiso de acceso HTTPs

```
# cd /etc/firewall/permitidos
```

Dentro del directorio permitidos, podemos crear varios archivos dentro de los mismo se pueden especificar dominios para acceso HTTPs, Estos archivos deben tener extensión ".conf".
Por ejemplo si queremos habilitar el uso de gmail.com, podemos crear una archivo llamado "gmail.conf", dentro del archivo debemos agregar las siguientes lineas

```
# Habilitacion Gmail
accounts.google.com
mail.google.com
```

Tener en cuenta que se debe agregar un dominio por renglon, además que muchos servidores HTTPs utilizan distintos dominios como por ejemplo gmail, que se autentica en accounts.google.com y luego cambia al dominio mail.google.com para acceder a los correos.

También se pueden especificar direcciones IP en lugar de dominios y redes /25 a /30

Dentro del archivo se pueden agregar lineas con # a modo de comentario las cuales no serán procesadas.

Una vez creado el archivo debemos ejecutar el firewall para que se carguen la nuevas reglas, para ello ejecutamos el siguiente comando

```
# ./firewall.sh restart
```

Dentro del directorio permitidos puedo tener muchos archivos ".conf" los cuales serán cargados al momento de iniciar o reiniciar el firewall, en caso de necesitar desactivar algunos de los sitios con acceso HTTPs simplemente renombramos el archivo cambiando le la extensión y re-ejecutamos el firewall.

3.5 Configuración final (implemntación en el arranque)

DEBIAN:

Entrar en el directorio /etc

```
# cd /etc
```

Editar el archivo rc.local

nano rc.local

Una vez dentro del archivo agregamos la siguiente linea, la cual debe quedar antes que la linea que dice "exit 0"

/etc/firewall/firewall.sh start &

Salimos del archivo grabando los cambios

UBUNTU:

Entrar en el directorio /etc/network

cd /etc/network

Editar el archivo interfaces

nano interfaces

Agregar o reemplazar en la interface de Internet el siguiente parámetro

post-up /etc/firewall/firewall.sh start &

Salimos del archivo grabando los cambios

3.6 Finalización de implementación

UBUBTU y DEBIAN:

Debemos desactivar el firewall que se ejecuta en el momento que se activa el servidor webmin, ya que este reemplaza la implementacion del nuevo firewall.

Para ello nos debemos loguear en el servidor webmin con nuestro navegador.
Una vez logueados nos dirigimos hacia la opción Networking (Menu Izquierdo), luego a Linux Firewall. Una vez dentro buscamos el boton que dice Activate at boot, seleccionamos No y cliqueamos en Activate at Boot. Puede ser que los menues y/o botones se encuentren en castellano

3.7 Verificación de la implementación

Para corroborar que nuestras nuevas políticas de control de paquetes están siendo implementadas correctamente solo basta con ingresar al terminal, localizarnos sobre el servidor de servicios y como administradores (sudo -i) ejecutamos el siguiente comando

/etc/firewall/firewall.sh status

La salida de este comando debe mostrar las reglas de firewall aplicadas, la ejecución de este comando dependiendo de la conexión de Internet puede llegar a demorar unos minutos

4 PROBLEMAS

4.1 Al querer ejecutar el archivo firewall.sh, salta el siguiente error:

"/bin/bash^M: bad interpreter: No such file or directory"

Solución: Reconvertir el archivo a formato unix ejecutar el siguiente comando

#dos2unix firewall.sh

5 FUNCIONES

5.1 Esta versión del firewall genera 2 archivos ips_habilitadas y redes_habilitadas ambos en el directorio /etc/squid. Estos archivos se deberán utilizar en la configuración del squid para permitir conexiones https a los dominios permitidos y/o habilitados en la configuración del firewall.