Universidad de La Laguna

Práctica 07. Una configuración sencilla de Firewall con `IPtables`

1. MV para el firewall

Instanciar una MV en el IAAS de la ULL para implementar el Firewall. Activar dos interfaces de red, una de ellas en una red interna (DOCINT1). Dejaremos la primera interfaz en la red DOC1 para el acceso exterior.

2. Configurar las interfaces de red del firewall

Como estamos trabajando en el IAAS de la ULL debemos establecer la IP de esta interfaz DOC1 por DHCP (especificarlo en la configuración de red: /etc/network/interfaces). La segunda interfaz la podemos poner en una red de clase C para direccionamiento falso: por ejemplo, 192.168.X.0/24 (cada alumno trabajará con una clase C distinta, eligiendo el número X). Asignarle la dirección "1", ya que será nuestra "default gateway" para la red interna.

3. Asignar máquina virtual “cliente” como cliente

Crear y poner una IP fija en una máquina virtual "cliente" en la red especificada anteriormente. Recordar que la interfaz de red configurada en en IAAS debe estar en la misma "Red interna" que una de las interfaces del Firewall. Asignar la ruta por defecto a la IP del firewall para que el tráfico saliente se dirija por él. Instalar un navegador en modo texto para hacer pruebas (por ejemplo links).

4. Configurar el Firewall

Implementar un script para la configuración del firewall de forma que:

1. Tenga política por defecto ACCEPT para la cadena OUTPUT y DROP para INPUT y FORWARD
2. Permita conectividad total desde la interfaz de loopback (lo) para hacer pruebas desde la consola del firewall
3. Acepte conexiónes desde la red interna a los puertos 80 (web) y 22 (servicio SSH en el FW)
4. Crear una cadena "custom" denominada "SERVICES" para la gestión de los servicios anteriores
5. Permita el tráfico a una impresora a todo el rango IP de la clase C especificada en la red interna

C/ Padre Herrera s/n
38207 La Laguna
Santa Cruz de Tenerife. España

T: 900 43 25 26

ull.es

5. Configuración de un proxy

Para permitir la navegación por internet de los clientes de la red interna, vamos a implementar un proxy transparente. Lo primero es especificar las reglas para redirigir el puerto 80 (tráfico normal de la web) a un puerto donde se ejecute el proxy. Por ejemplo, el 8080. Esto incluye trabajar con las tablas de NAT (redirigir puertos es un tipo de NAT: DNAT).

Una vez tengamos redirigido el puerto 80 de nuestra red interna al puerto 8080 del firewall, podemos instalar un proxy transparente para dar servicio de navegación a los clientes de la red interna. Podemos utilizar Squid Cache para esto. Aquí tienen una Guía rápida de configuración de Squid