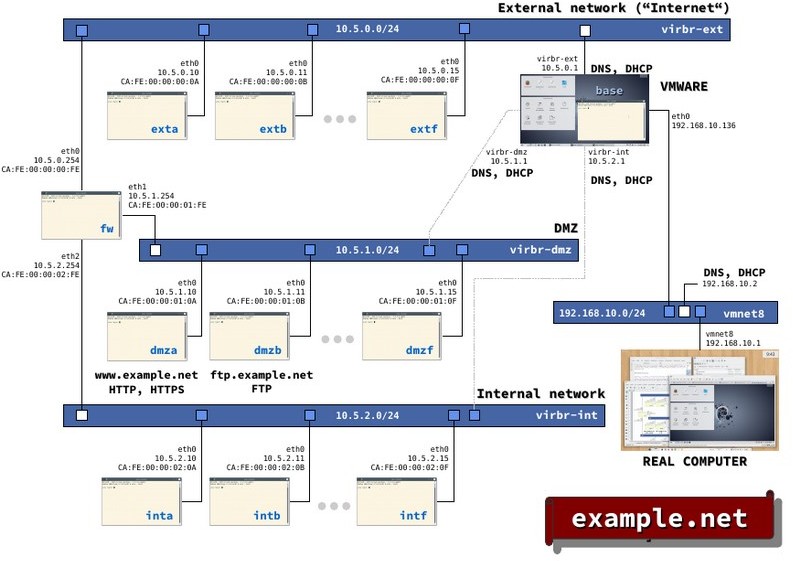
TAREA 2 Cortafuegos IPTABLES PARA UNA RED

Partimos de una red corporativa bastante completa como la de la imagen y de un conjunto de especificaciones de filtrado de tráfico y trataremos de construir el script iptables que configure el cortafuegos de acuerdo con las especificaciones para NETinVM con todas las máquinas virtuales que contiene y el esquema de la red siguiente:



Una vez confeccionado y depurado el script construido tendremos que ejecutarlo manualmente o bien insertarlo en procedimiento de arranque automático del cortafuegos, que es lo habitual. Esta operación dependerá de la distribución GNU/Linux que se utilice por lo que es conveniente consultar la documentación de la distribución instalada para realizar correctamente este automatismo.

Limpieza inicial de las tablas

En primer lugar, procederemos a limpiar las tablas de reglas anteriores residuales de modo que partimos de cero en la configuración del cortafuegos. En la construcción de las reglas iremos numerando cada regla pada podernos referir a ella con

precisión. No obstante, esta numeración no puede aparecer en el script que se ponga en ejecución.

1 . iptables —F

1. iptables —X
2. iptables —Z
3. iptables -t nat —F
4. iptables -P INPUT DROP
5. iptables -P OUTPUT DROP
6. iptables -P FORWARD DROP
7. iptables -t nat -P PREROUTING DROP
8. iptables -t nat -P POSTROUTING DROP

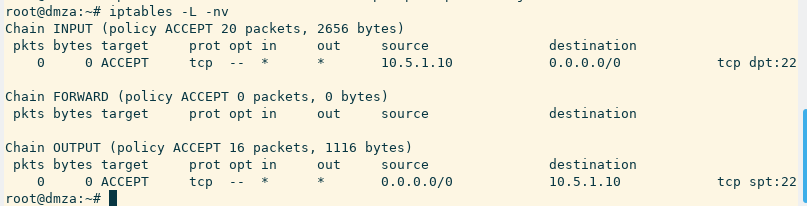
Las reglas 1 a 4 limpian las tablas y limpian los contadores de tráfico. Las reglas 5 a 7 establecen la política de destino por defecto (su target), que establecen en DROP, es decir, por defecto se denegará en las tablas INPUT, OUTPUT y FORDWARD todo el tráfico que no esté expresamente permitido. Las tablas 8 y 9 hacen la misma operación, pero en la tabla NAT para las cadenas PREROUTING Y POSTROUTING.

Permitir ssh hacia dmza

El script continuaría con las siguientes dos reglas (números 10 y 11), que permitirían el tráfico de ida y vuelta hacia/desde el puerto 22 de dmza que tiene por dirección IP 10.5.1.10.

1. iptables -A INPUT -s 10.5.1.10 -p tcp --dport 22 -j ACCEPT
2. iptables -A OUTPUT -d 10.5.1.10 -p tcp -sport 22 -j ACCEPT





Prevención de suplantaciones

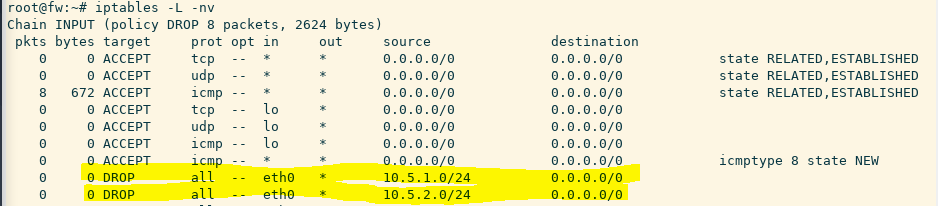
Ahora vamos a rechazar todo el tráfico que venga por eth0 (Internet y/o red externa) con direcciones IP de origen 10.5.1.0/24 puesto que estas direcciones acceden al FW por eth1 (la red DMZ). Si un paquete de estas características llega por eth0 es que es una suplantación y estamos sufriendo un ataque que deberemos rechazar.

De modo semejante tendríamos que gestionar que por eth0 vinieran paquetes con direcciones IP del tipo 10.5.2.0/24 que se corresponden con la red interna (LAN) y, que, por tanto, no pueden venir más que de eth2.

Estos dos ataques de suplantación los bloquearemos con las dos siguientes reglas:

1. iptables -A INPUT -i eth0 -s 10.5.1.0/24 -j DROP
2. iptables -A INPUT -i eth0 -s 10.5.2.0/24 -j DROP





Análisis del tráfico FTP

Seguidamente permitiremos el tráfico FTP desde la red LAN (interna, visible por eht2) hasta el servidor FTP que gestiona las conexiones FTP que se encuentra en la DMZ (visible por eth1) en

la dirección 10.5.1.11. Las conexiones FTP pueden utilizar los puertos 20 y 21 y la conexión es de tipo TCP. Estableceremos las dos nuevas siguientes reglas:

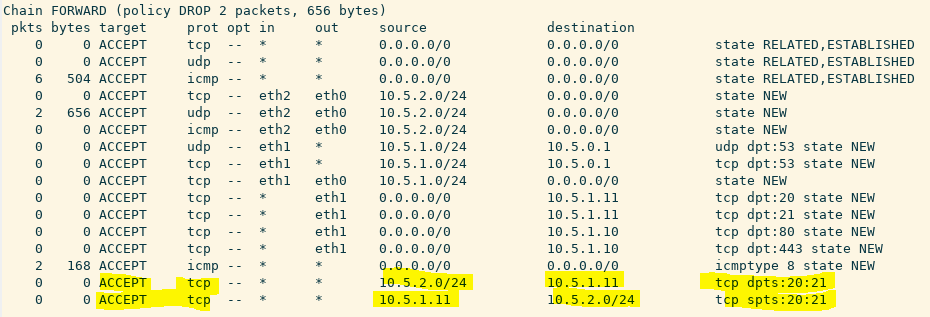
1. iptables -A FORWARD -s 10.5.2.0/24 -d 10.5.1.11 -p tcp –dport

20:21 -j ACCEPT



15. iptables -A FORWARD -s 10.5.1.11 -d 10.5.2.0/24 -p tcp --sport 20, 21 -j ACCEPT





Obsérvese que en este caso las reglas se ejecutan en la cadena FORDWARD ya que es un tráfico que no tiene ni origen ni destino en FW sino en sistemas ajenos a él y que por tanto tendrá que enrutar.

Ejercicios: Completar las reglas de iptables siguientes:

1.- Tráfico entre la LAN y la DMZ

En primer lugar, permitiremos hacer ping desde la LAN hasta la red DMZ (reglas 16 y 17), lo que especificaremos mediante la opción —p icmp, que es el protocolo que utiliza ping en la cadena FORDWARD ya que será tráfico enrutado entre dos redes.

En segundo lugar, permitiremos todo el tráfico desde inta en la LAN hasta cualquier sistema de la red DMZ, lo que puede ser necesario para hacer tareas de administración desde el sistema del administrador (reglas 18 y 19)

1. Escribe aquí la regla 16

iptables -A FORWARD -s 10.5.2.0/24 -d 10.5.1.10 –p icmp –j ACCEPT

1. Escribe aquí la regla 17

Iptables -A FORWARD -s 10.5.1.10 -d 10.5.2.0/24 -p icmp -j ACCEPT

1. Escribe aquí la regla 18

iptables -A FORWARD -s 10.5.2.10 -d 10.5.1.0/24 -j ACCEPT

1. Escribe aquí la regla 19

iptables -A FORWARD -d 10.5.2.10 -s 10.5.1.0/24 -j ACCEPT

2.- Tráfico entre Internet y la DMZ

Ahora vamos a definir el tráfico permitido dirigido al servidor web en la DMZ (10.5.1.10) que provenga desde Internet (red WAN 10.5.0.1/24). Si el servidor web es accesible por http tendremos que abrir el puerto 80, mientras que si es accesible por https el puerto relacionado es el 443. Abriremos los dos puertos para accesos por http y https, Deberemos tener en cuenta que los protocolos http y https están encapsulados sobre tcp por lo que no permitiremos el tráfico UDP hacia estos puertos especificando restrictivamente el protocolo con la opción —p tcp. Además, como viene siendo habitual, tendremos que permitir el tráfico bidireccional.

1. Escribe aquí la regla 20

iptables -A FORWARD -p tcp –i eth0 –o eth1 –dport  80 -j ACCEPT

iptables -A FORWARD -p tcp –i eth0 –o eth1 –dport  443 -j ACCEPT

1. Escribe aquí la regla 21

iptables -A FORWARD  –i eth0 –o eth1 –p  tcp --sport 80 -j  ACCEPT

iptables -A FORWARD  –i eth0 –o eth1 -p tcp --sport 443 -j  ACCEPT

1. Escribe aquí la regla 22

iptables -A FORWARD -p tcp –i eth1 –o eth0 --dport 80:443 -j ACCEPT

1. Escribe aquí la regla 23

iptables -A FORWARD -p tcp –i eth0 –o eth1 --dport 80:443 -j ACCEPT

3.- Tráfico de navegación entre LAN y WAN

Por último, permitiremos que los usuarios de la LAN o red interna puedan navegar por internet mediante http y https de modo que se puedan realizar conexiones desde el interior hacia el exterior, pero que se impidan las conexiones que se intenten desde el exterior contra el interior, protegiendo a los sistemas de la LAN o red interna de ataques desde la WAN o red externa.

Para llevar a cabo esto, tendremos que gestionar la inspección de estado de paquetes de modo que se permita la entrada de paquetes desde la WAN a la LAN, pero exclusivamente aquellos que estén relacionados con una conexión previamente abierta por algún usuario de la LAN. (-m state --state NEW, ESTABLISHED,RELATED)

1. Escribe aquí la regla 24

iptables -A FORWARD -p tcp –i eth2 –o eth0 -m state –state NEW,ESTABLISHED, RELATED –dport 80 -j ACCEPT

1. Escribe aquí la regla 25

iptables -A FORWARD -p tcp –i eth0 –o eth2 -m state –state ESTABLISHED, RELATED –dport 80 -j ACCEPT

1. Escribe aquí la regla 26

Iptables -A FORWARD -p tcp -i eth2 –o eth0 –m state –state NEW, ESTABLISHED, RELATED --dport 443 -j ACCEPT

1. Escribe aquí la regla 27

Iptables -A FORWARD -p tcp -i eth0 –o eth2 –m state –state ESTABLISHED, RELATED --dport 443 -j ACCEPT