[Cod.: CC481 Curso: Administración de Redes]
[Tema: Firewall – Parte I]
[Prof.: Manuel Castillo]

Laboratorio dirigido 8.1

Firewall en Linux - iptables

Instrucciones:

1. Fecha de entrega será antes del **domingo a las 23:59**.
2. El formato de entrega será *pdf*.
3. El laboratorio tendrá una puntuación sobre 20.
4. Para los laboratorios de servicios se deberá realizar capturas de cada paso que se están llevando a cabo. Además de realizar un **videotutorial** al final que muestre la correcta implementación de nuestro servicio.
5. La primera hoja será para la portada que se especificará, el número de laboratorio, nombre y apellidos de los integrantes, nombre asignatura y el escudo de la UNI.
6. La segunda página será el índice. Donde se deberá tener en cuenta la página de cada Actividad.
7. Las citas y extracciones realizadas de Internet se deberán especificar. No se corregirá el laboratorio en caso de copiar y pegar fragmentos sin especificar.
8. Utilizar letra clara y adecuada a un documento técnico con tamaño 12 y márgenes superior e inferior de 3 cm y laterales de 2,5 cm.
9. Se corregirá la claridad y exactitud de la pregunta, en ningún caso se expondrán fundamentos no preguntados, además de la claridad del documento.
10. En las actividades realice una captura de pantalla mínimo por actividad para verificar su autoría.

0. Antecedentes

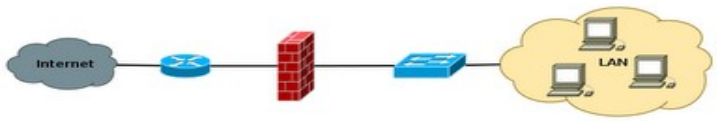
En este laboratorio vamos a trabajar la conexiones entre máquinas (por lo que tenemos que tener otra máquina virtual activa). Trabajaremos la conexión entre máquinas virtuales como red interna por lo que la configuración es como hemos venido haciendo hasta ahora.

Realizar un snapshot de nuestra máquina ya que vamos a trabajar dos laboratorios parecidos para que nos queden claros los conceptos.

Trabajaremos con una nueva máquina CentOS o Ubuntu Server.

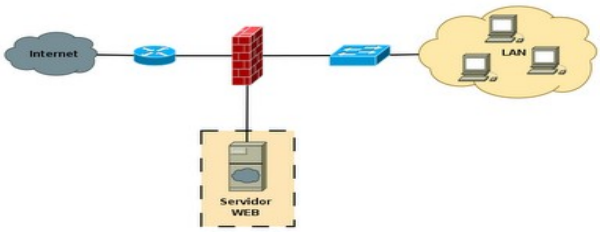
1. Introducción

Un *firewall* es, por lo general, un *software* o *hardware*, a través del cual nos conectamos a una red como Internet, y que sirve como filtro sobre el tráfico que por él pasa, en ambas direcciones, y que en un momento dado puede rechazar cierto tráfico en alguna de las direcciones.

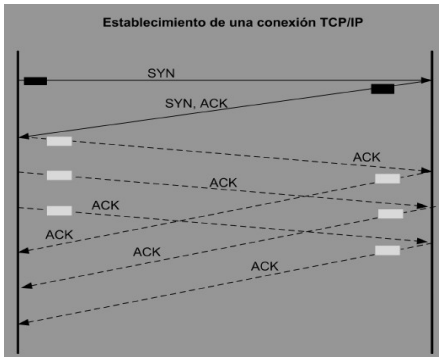


Eso quiere decir que, mediante un *firewall*, podemos detectar el tráfico no deseado hacia nuestros sistemas, y en general, los posibles ataques de que seamos objeto. De esta manera podremos aislar nuestros equipos del exterior, permitiendo nuestro uso de Internet de manera absolutamente normal pero minimizando en lo posible la probabilidad de padecer las consecuencias de un ataque.

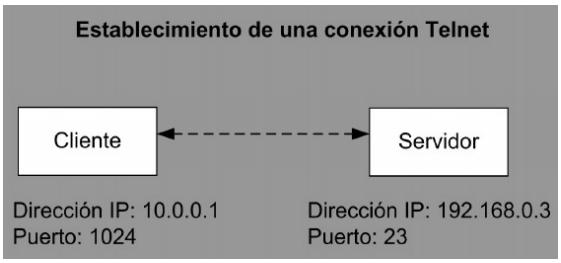
Es frecuente también que se necesite exponer algún servidor a Internet (como es el caso de un servidor web, un servidor de correo, etc...), y en esos casos obviamente en principio se debe aceptar cualquier conexión a ellos.



1. Según el siguiente esquema (donde se ilustra como ocurre una conexión TCP), ¿qué tipo de paquetes podría inspeccionar un encaminador con filtrado de paquetes para poder controlar los intentos de conexión? ¿Y para identificar las respuestas?



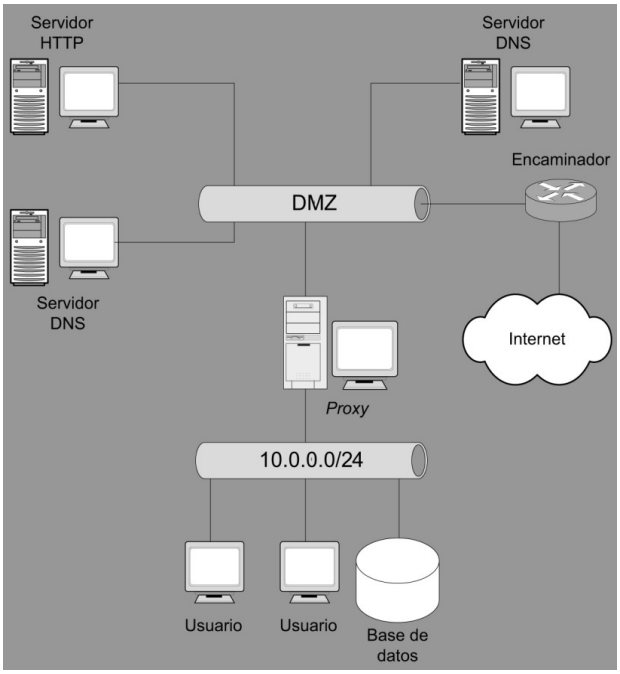
2. A partir de la siguiente figura, donde se observa una conexión Telnet realizada desde el cliente hacia el servidor. Si suponemos que el servidor 192.168.0.3 es el servidor Telnet de la red interna, ¿cómo se pueden bloquear las conexiones destinadas a éste, exceptuando las procedentes del sistema 10.0.0.1?



3. Según la siguiente política de seguridad, ¿cómo impediríais que se hicieran conexiones a servidores HTTP externos que funcionan sobre un puerto distinto del 80?

Regla	Acción	Origen	Puerto de origen	Destino	Puerto de destino	Indicador	Descripción
1	Rechaza	10.0.0.0	*	*	80	TCP	Rechaza cualquier conexión a servidores HTTP
2	Permite	10.0.0.0	*	*	*	TCP	Permite conexiones TCP de salida
3	Permite	*	*	10.0.0.1	80	TCP	Permite conexiones HTTP entrantes
4	Permite	*	*	10.0.0.2	25	TCP	Permite conexiones SMTP entrantes
5	Permite	*	*	10.0.0.3	53	UDP	Permite conexiones DNS entrantes
6	Rechaza	*	*	10.0.0.0	*	*	Rechaza cualquier otra conexión a la red interna

4. ¿Por qué no encontramos la base de datos de la siguiente figura dentro de la zona desmilitarizada?

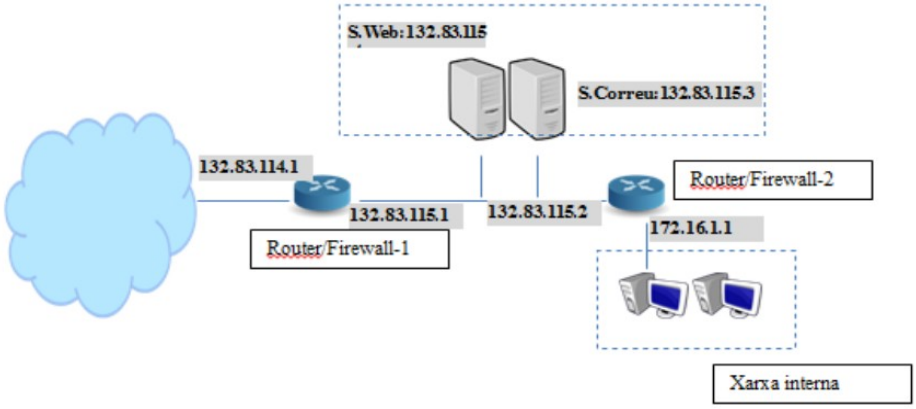


5. Defina con sus propias palabras el concepto de zona desmilitarizada (DMZ).
6. Defina los términos *choke router* y *bastion host*, utilizando tus propias palabras. Dibuja el esquema de una DMZ que incluya un *bastion host* y un *choke router*.
7. La red de computadores de una empresa dispone de estaciones de trabajo y de tres servidores. Las estaciones de trabajo que utiliza el personal, tienen direcciones en el rango 192.0.2.0/24. Los tres servidores corporativos son accesibles públicamente: un servidor DNS con dirección 203.0.113.1, un servidor de correo saliente y entrante (servicios SMTP y POP3) con dirección 203.0.113.2, y un servidor que da los servicios de HTTP, HTTPS y FTP con dirección 203.0.113.3. Desde las estaciones sólo se puede acceder a servicios HTTP y HTTPS del exterior (además de los servidores corporativos), y desde el exterior no se puede acceder a las estaciones.
   - Explique cómo sería la configuración de esta red con una DMZ con dos sistemas cortafuegos y escriba, con el formato de los ejemplos visto en clase, las reglas de filtrado de cada cortafuegos.

8. Realice una pequeña presentación de 5-7 transparencias, formato PDF, que sirva para explicar en que consiste lo siguiente:
   - El proyecto Hogwash. En esta presentación hay que resolver, como mínimo, lo siguiente: Qué es y para qué sirve. Cuáles son sus componentes. Qué tipos de ataques distribuidos puede detectar. Un ejemplo de cómo lo hace por un tipo en concreto de ataque distribuido. Un ejemplo de donde se podría ubicar en una red.
   - Explique la principal diferencia, en cuanto a la seguridad, entre el uso de una zona desmilitarizada (DMZ) y una arquitectura de cortafuegos dual-homed. Haga un esquema de cada una de las opciones, indicando donde se coloca la red interna, los servidores y Internet.
   - Define qué es un equipo de decepción (o honeypot) y relaciona su utilidad con los procesadores de eventos. Así mismo responde las mismas preguntas expuestas en el 1. Proyecto Hogwash.

CASO PRÁCTIO 1 – Escenario real

En esta actividad vamos a ver un ejemplo real de cómo realizar un diseño de seguridad para nuestra red. Para ello tenga en mente el siguiente esquema:



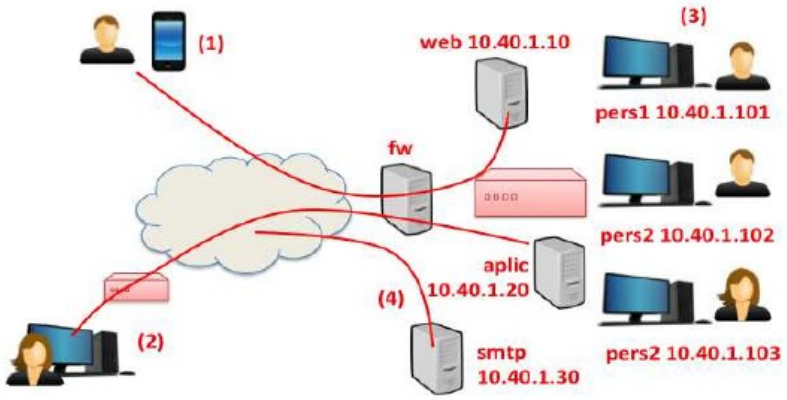
A partir del esquema anterior diseñe las reglas de configuración de los dos routers/firewalls considerando que son equipos Linux y que utilizan *iptables*.

1. Configuración de las reglas del Router/Firewall-1:

- El servidor web puede ofrecer servicio web (HTTP y HTTPS) en todo Internet.
- El servidor de correo puede recibir y enviar correo (SMTP) desde y hacia todo Internet.
- En el servidor de correo se le puede descargar correo (POP3 e IMAP) desde todo Internet.
- Los dos servidores deben poder ser administrados mediante SSH, desde las máquinas de los dos compañeros.
- Hay que permitir el paso de paquetes ICMP desde y hacia todo Internet.
- A fin de proteger los servidores contra ataques de Syn-flooding, limitaremos las peticiones de conexión dirigidas a cada uno de los servidores a 2 por segundo.

2. Configuración de las reglas del Router/Firewall-2:
   - La máquina de la red interna puede navegar por Internet (HTTP y HTTPS) sin limitación.
   - La máquina de la red interna solo puede enviar correo (SMTP) a través del servidor de correo instalado en su casa.
   - La máquina de la red interna solo puede descargar correo (POP3 e IMAP) del servidor de correo instalado en su red .
   - Hay que evitar posibles conexiones desde el exterior a esta red interna.
   - A continuación habrá que instalar la herramienta IDS Snort, para monitorizar el tráfico y poder detectar posibles intentos o intrusiones en los servidores.
3. Describe los pedidos de *iptables* necesarias para permitir sólo el acceso a través de HTTPS y HTTP al servidor web.

CASO PRÁCTIO 2 – Escenario real



Respecto al esquema anterior:

- Vemos como los postulantes externos de nuestra empresa (1) acceden a una página web y, de esta manera, introducen información de su puesto de trabajo. Toda la información se almacena en los servidores de su departamento.
- Los gerentes de departamentos (2), cuando tienen una vacante disponible se conectan al servidor para exponer la necesidad/oferta.
- Finalmente, el RRHH (3) selecciona a los potenciales candidatos según la necesidad. Este aspecto se realiza mediante un sistema inteligente integrado que emite la resolución por correo electrónico (4) a los candidatos.

En este esquema se tiene el siguiente flujo de sistemas:

- Los candidatos se conectan por medio de HTTP al servidor 'web' LAMP que se encuentra dentro de la red.
- Los gerentes se conectan por medio de SSH al servidor.
- El personal accede al servidor, mediante el puerto TCP/21060, mediante una interfaz local en su propia estación.
- El correo electrónico se envía desde el servidor SMTP hacia el servidor correo del candidato.
- Servidores y estaciones de trabajo están dentro de una misma red LAN con direccionamiento IP 10.40.1.*. La conexión con el exterior se hace por medio de un servicio 'fw' con Linux que tiene dos interfaces de red, la interna, IP 10.40.1.1 y la externa IP 80.90.50.31.

Como se ha observado en este tema, la mejor manera de aislar los servidores de los ataques de seguridad sería, en primer lugar, ponerlos en una DMZ. Así pues, dispondrás de la máquina 'fw' y otro ordenador ('fw2') que tiene dos interfaces de red. Habilitarás la *iptables*. Haz tu propuesta de diseño de red y tablas de políticas de seguridad para las máquinas 'fw' y 'fw2', para que controlen estrictamente las conexiones indicadas en el enunciado, y muéstrales.