UT4. INSTALACIÓN Y CONFIGURACIÓN DEL CORTAFUEGOS

Módulo: Seguridad y Alta Disponibilidad

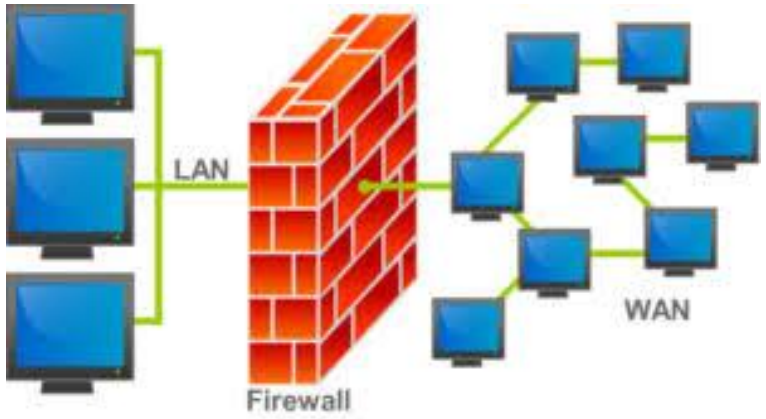
Curso 2023/2024. 2º ASIR

CONTENIDOS

- Concepto
- Características
- Ventajas e inconvenientes
- Clasificación
- Reglas de filtrado
- Registro de sucesos
- Políticas de seguridad
- Arquitecturas
- IPTables
- Instalación y configuración
- Integración con otras tecnologías

QUÉ ES

- Un firewall o cortafuegos es un sistema o grupo de sistemas que hace cumplir una política de control de acceso entre dos redes.
- Es cualquier sistema (desde un simple router hasta varias redes en serie) utilizado para separar una máquina o subred del resto, protegiéndola así de servicios y protocolos que desde el exterior puedan suponer una amenaza a la seguridad.
- El espacio protegido, denominado perímetro de seguridad, suele ser propiedad de la misma organización, y la protección se realiza contra una red externa, no confiable, llamada zona de riesgo.



CARACTERÍSTICAS

- Los cortafuegos pueden ser usados a través de una solución de hardware, es decir un dispositivo físico, o a través de un programa informático instalado en el sistema operativo del ordenador que se desea proteger.
- En entornos empresariales suele ser común la utilización de cortafuegos basados en hardware, que protegen y separan la red interna del exterior. Se sitúan en un punto determinado de la conexión entre la red interna y la red exterior.
- Sin embargo en ambientes domésticos la utilización más extendida son las soluciones por software, bien mediante programas informáticos existentes para tal fin o configurando los que incorporan los sistemas operativos. Se sitúan entre el ordenador del usuario y el resto de la red a la que pertenece.
- Éste se encarga de comprobar los intentos de conexión entrantes y salientes del ordenador o red de ordenadores, controlando el puerto, protocolo, IP, etc.

VENTAJAS DE LOS CORTAFUEGOS

- Bloquea el acceso a personas no autorizadas a redes privadas.
- Administra los accesos provenientes de Internet hacia la red privada. Sin un firewall, cada uno de los servidores propios del sistema se exponen al ataque de otros servidores en el Internet. Por ello la seguridad en la red privada depende de la "dureza" con que el firewall cuente.
- Administra los accesos provenientes de la red privada hacia Internet.
- Permite al administrador de la red mantener fuera de la red privada a los usuarios no-autorizados (tal, como, hackers , crackers y espías), prohibiendo potencialmente la entrada o salida de datos.
- El firewall crea una bitácora en donde se registra el tráfico más significativo que pasa a través el.
- Concentra la seguridad ya que centraliza los accesos.

INCONVENIENTES Y LIMITACIONES

- Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación, (una conexión PPP).
- El firewall no puede contar con un sistema preciso de SCAN para cada tipo de virus que se puedan presentar en los archivos que pasan a través de él, pues el firewall no es un antivirus. Es preciso instalar software antivirus en cada máquina.
- El firewall no puede ofrecer protección alguna una vez que el agresor lo traspasa.
- Un cortafuegos no puede proteger contra aquellos ataques cuyo tráfico no pase a través de él.
- El cortafuegos no puede proteger de las amenazas a las que está sometido por ataques internos o usuarios negligentes. El cortafuegos no puede prohibir a espías corporativos copiar datos sensibles en medios físicos de almacenamiento (discos, memorias, etc.) y sustraerlas del edificio.
- El cortafuegos no puede proteger contra los ataques de ingeniería social.
- El cortafuegos no protege de los fallos de seguridad de los servicios y protocolos cuyo tráfico esté permitido.

CLASIFICACIÓN DE LOS CORTAFUEGOS

- Según su **ubicación**:
  - Cortafuegos personales.
  - Cortafuegos para pequeñas redes SOHO (Small Office Home Office).
  - Cortafuegos corporativos.

- Tipos según su **tecnología**:
  - Filtrado de paquetes de datos.
  - Pasarelas de nivel de aplicación (proxys).
  - Inspección de estados.
  - Pasarelas de nivel de circuitos (híbridos).

CORTAFUEGOS PERSONALES

- Cortafuegos personales: Es un caso particular de cortafuegos que se instala como software en un ordenador, filtrando las comunicaciones entre él y el resto de la red. Se usa, por tanto, a nivel personal.
- Se instalan de forma residente en nuestro ordenador y permiten filtrar y controlarla conexión a la red.
- Entrante: el que controla las conexiones que "entran" en el sistema. Por ejemplo, desde el punto de vista de un servidor que muestra páginas web, un cliente que desee visualizar esa página, será una conexión entrante que deberá verificar en su tabla de reglas. Este tipo de cortafuegos es muy usado tanto en servidores como en sistemas que habitualmente actúan como clientes. Por ejemplo, todos los sistemas Windows cuentan con un cortafuegos entrante activado por defecto y la inmensa mayoría de los routers usados para establecer una conexión ADSL tienen un firewall entrante activado por defecto, que protege al ordenador interno.
- Saliente: controla las conexiones que "salen" del sistema. Está pensado en mayor medida para clientes, para comprobar hacia qué direcciones IP o qué puertos se conecta nuestro ordenador. Este tipo de cortafuegos es mucho menos usado que el entrante, aunque es más seguro, puesto que nos permite tener control total de hacia dónde intentan conectarse los programas y, por tanto, nuestros datos.

CORTAFUEGOS PARA PEQUEÑAS REDES SOHO

- SOHO es el acrónimo de Small Office-Home Office (Pequeña Oficina-Oficina en Casa).

- Es un término que se aplica para denominar a los aparatos destinados a un uso profesional o semiprofesional pero que, a diferencia de otros modelos, no están pensados para asumir un gran volumen de trabajo.

- El entorno SOHO propiamente dicho se refiere a toda la tecnología informática, a muebles funcionales, productos y servicios destinados al armado de una oficina en un ámbito doméstico.

CORTAFUEGOS CORPORATIVOS

- Es un tipo de cortafuego utilizado mayormente en sistemas interconectados de organizaciones y empresas en donde cierta cantidad de equipos podrían estar conectados en red compartiendo y accediendo a cientos de recursos simultáneamente.
- Estos sistemas tienen el objetivo de filtrar las comunicaciones en el borde de la organización.
- Debido a que todo el tráfico que circula desde la red interna hacia fuera y viceversa es elevado, estos sistemas deben ser eficientes en el manejo de todas las conexiones.
- Una de las ventajas de la utilización de estos dispositivos es que todos los equipos de la organización estarán protegidos por un único sistema, bloqueando o dejando pasar las comunicaciones que el administrador haya dispuesto para toda la organización.
- Este tipo de dispositivos puede ser de software o hardware y su costo dependerá del tamaño y prestaciones brindadas.

CORTAFUEGOS CORPORATIVOS

Los principales aspectos críticos que deberá resolver la configuración del cortafuegos en los sistemas corporativos se centrarán en las siguientes problemáticas:

- Comunes con el usuario: usurpación de la identidad e integridad de la información.
- Accesos autorizados: permitir el acceso a las direcciones de origen validadas y autorizadas.
- Aplicaciones autorizadas: permitir el acceso a las aplicaciones en función de la identidad validada.
- Filtrado de solicitudes de conexión desde nuestra red a Internet.
- Protección de los datos de identidad de nuestros usuarios en los accesos autorizados a Internet.
- Protección ante "caballos de troya", en forma de archivos Java, PostScript, etc.
- Realizar todas las funciones anteriores sin afectar a las prestaciones y funcionalidades de Internet que los usuarios internos demandan.

CORTAFUEGOS DE FILTRADO DE PAQUETES

Cortafuegos de filtrado de paquetes de datos (Packet Filter Firewalls):

- Se analiza el tráfico de la red fundamentalmente en la capa 3, teniendo en cuenta a veces algunas características del tráfico generado en las capas 2 y/o 4 y algunas características físicas propias de la capa 1. Los elementos de decisión con que cuentan a la hora de decidir si un paquete es válido o no son los siguientes:
  - La dirección de origen desde donde, supuestamente, viene el paquete (capa 3).
  - La dirección del host de destino del paquete (capa 3).
  - El protocolo específico que está siendo usado para la comunicación, frecuentemente Ethernet o IP aunque existen cortafuegos capaces de desenvolverse con otros protocolos como IPX, NetBios, etc. (capas 2 y 3).
  - El tipo de tráfico: TCP, UDP o ICMP (capas 3 y 4).
  - Los puertos de origen y destino de la sesión (capa 4).
  - El interfaz físico del cortafuegos a través del que el paquete llega y por el que habría que darle salida (capa 1), en dispositivos con 3 o más interfaces de red.

Ejemplos: Iptables en Linux y ACL's en Cisco.

CORTAFUEGOS DE FILTRADO DE PAQUETES

Ventajas:

- Rapidez, transparencia y flexibilidad.
- Proporcionan un alto rendimiento y escalabilidad y muy bajo coste, y son muy útiles para bloquear la mayoría de los ataques de Denegación de Servicio, por ello se siguen implementando como servicios integrados en algunos routers y dispositivos hardware de balanceo de carga de gama media-alta.

Inconvenientes:

- Limitada funcionalidad y su dificultad a la hora de configurarlos y mantenerlos.
- Son fácilmente vulnerables mediante técnicas de spoofing.
- No pueden prevenir contra ataques que exploten vulnerabilidades específicas de determinadas aplicaciones, puesto que no examinan las capas altas del modelo OSI.
- No son, pues, efectivos como medida única de seguridad, pero si muy prácticos como primera barrera, en la que se bloquean ciertos ataques, se filtran protocolos no deseados y se pasan los paquetes restantes a otro cortafuegos que examine las capas más altas del protocolo.

CORTAFUEGOS POR FILTRADO DE APLICACIÓN

Cortafuegos de filtrado por aplicación:

- La práctica totalidad de los cortafuegos de este tipo, suelen prestar servicios de Proxy.
- Un Proxy es un servicio específico que controla el tráfico de un determinado protocolo (como HTTP, FTP, DNS, etc.), proporcionando un control de acceso adicional y un detallado registro de sucesos respecto al mismo.
- Los servicios o agentes típicos con que cuentan este tipo de dispositivos son: DNS, Finger, FTP, HTTP, HTTPS, LDAP, NMTP, SMTP y Telnet.
- Los agentes o servicios Proxy están formados por dos componentes: un **servidor** y un **cliente**. Ambos suelen implementarse como dos procesos diferentes lanzados por un único ejecutable. El servidor actúa como destino de las conexiones solicitadas por un cliente de la red interna. El cliente del servicio proxy es el que realmente encamina la petición hacía el servidor externo y recibe la respuesta de este. Posteriormente, el servidor proxy remite dicha respuesta al cliente de la red interna.

CORTAFUEGOS POR FILTRADO DE APLICACIÓN

De esta forma estamos creando un aislamiento absoluto, creando comunicación directa entre la red interna y la externa. En el diálogo entre cliente y servidor proxy se evalúan las peticiones de los clientes de la red interna y se decide aceptarlas o rechazarlas en base a un conjunto de reglas, examinando meticulosamente que los paquetes de datos sean en todo momento correctos.

Ventajas:

- Detallados registros de tráfico (ya que pueden examinar la totalidad del paquete de datos).
- Servicio de autenticación.
- Nula vulnerabilidad que presentan ante ataques de suplantación (spoofing).
- Servicios añadidos: como caché y filtro de URL's.

Inconvenientes:

- Menor velocidad de inspección.
- Necesidad de contar con servicios específicos para cada tipo distinto de tráfico.
- Imposibilidad de ejecutar muchos otros servicios en él (puesto que escucha en los mismos puertos).

INSPECCIÓN DE ESTADOS (STATEFUL INSPECTION)

- Un cortafuegos de inspección de estados (cualquier firewall que realiza Stateful Packet Inspection –SPI-) es un firewall que realiza un seguimiento del estado de las conexiones de red (como TCP o UDP) que viajan a través de ella.

- El firewall está programado para distinguir los paquetes legítimos para diferentes tipos de conexiones. Sólo los paquetes que coincidan con una conexión conocida activa serán permitidos por el firewall, mientras que otros serán rechazados.

CORTAFUEGOS HÍBRIDOS

- Conscientes de las debilidades de los firewalls de filtrado de paquetes y de los de nivel de aplicación, algunos proveedores han introducido firewalls híbridos que combinan las técnicas de los otros dos tipos.

- Debido a que los firewalls híbridos siguen basándose en los mecanismos de filtrado de paquetes para soportar ciertas aplicaciones, aún tienen las mismas debilidades en la seguridad.

REGLAS DE FILTRADO

- Los cortafuegos funcionan filtrando las comunicaciones en ambos sentidos entre su interfaz interna (la que lo conecta a su red) y la externa.
- El mecanismo de funcionamiento para realizar este filtrado es a través de una lista de reglas.
- Las reglas, pueden ser de dos tipos; de **aceptación** y de **rechazo**. Y el rechazo se descompone **en rechazo** y **denegación**.(En iptables se corresponde con los argumentos ACCEPT, REJECT y DROP).
- La lista de reglas de entrada (del exterior hacia la red) es totalmente independiente de la lista de reglas de filtrado de salida (de la red hacia el exterior). Las distintas listas de reglas se llaman cadenas (**chains**).
- Cuando un cortafuegos **rechaza** una petición externa, envía una respuesta negativa diciendo que no acepta la comunicación, por el contrario, si **descarta** una petición, no envía ningún tipo de respuesta, es decir, que el agente externo que intentó establecer contacto, no sabrá siquiera si la máquina existe o está apagada.

REGISTRO DE SUCESOS DEL CORTAFUEGOS

- Es posible habilitar el registro de sucesos del cortafuegos como ayuda para identificar el origen del tráfico entrante y obtener información detallada acerca de qué tráfico se está bloqueando.
- Normalmente el tráfico saliente correcto no se registra.
- Algunos de los datos que se pueden recopilar en un registro de sucesos:
  - Fecha: Año, mes y día en que tuvo lugar la transacción registrada.
  - Hora: Hora, minuto y segundo en que tuvo lugar la transacción registrada.
  - Acción: OPEN, CLOSE, DROP e INFO-EVENTS-LOST (número de sucesos que ocurrieron, pero no se anotaron en el registro).
  - Protocolo: Protocolo que se utilizó para la comunicación.
  - src-ip: Dirección IP, o la dirección IP del equipo, que intenta establecer comunicación.
  - dst-ip: Dirección IP de destino de un intento de comunicación.
  - src-port: Número del puerto de origen del equipo que realizó el envío.

REGISTRO DE SUCESOS DEL CORTAFUEGOS

- dst-port: Muestra el número del puerto del equipo de destino. Una entrada dst-port se registra en forma de número entero entre 1 y 65.535. Sólo TCP y UDP muestran una entrada dst-port válida. Todos los demás protocolos muestran una entrada dst-port de guión (-).
- tamaño: Muestra el tamaño del paquete en bytes.
- tcpflags: Muestra los indicadores de control de TCP que se encuentran en el encabezado TCP de un paquete IP:
  - Ack: confirmación de campo significativo.
  - Fin: no hay más datos del remitente.
  - Psh: función de inserción.
  - Rst: restablecer la conexión.
  - Syn: sincronizar los números de secuencia.
  - Urg: campo Puntero urgente significativo

POLÍTICAS DE CORTAFUEGOS

Hay dos políticas básicas en la configuración de un cortafuegos:

- Política restrictiva: Se deniega todo el tráfico excepto el que está explícitamente permitido. El cortafuegos obstruye todo el tráfico y hay que habilitar expresamente el tráfico de los servicios que se necesiten. Esta aproximación es la que suelen utilizar las empresas y organismos gubernamentales.
- Política permisiva: Se permite todo el tráfico excepto el que esté explícitamente denegado. Cada servicio potencialmente peligroso necesitará ser aislado básicamente caso por caso, mientras que el resto del tráfico no será filtrado. Esta aproximación la suelen utilizar universidades, centros de investigación y servicios públicos de acceso a internet.

La política restrictiva es la más segura, ya que es más difícil permitir por error tráfico potencialmente peligroso, mientras que en la política permisiva es posible que no se haya contemplado algún caso de tráfico peligroso y sea permitido por omisión.

CORTAFUEGOS

Arquitecturas de cortafuegos:

- Cortafuegos de filtrado de paquetes.
- Cortafuegos Dual-Home Host.
- Screened Host
- Screened subnet (DMZ)
- Otras arquitecturas.

CORTAFUEGOS DE FILTRADO DE PAQUETES

- El modelo de cortafuegos más antiguo consiste en un dispositivo capaz de filtrar paquetes, lo que se denomina choke.
- Está basado simplemente en aprovechar la capacidad que tienen algunos routers para bloquear o filtrar paquetes en función de su protocolo, su servicio o su dirección IP.
- Los cortafuegos de filtrado de paquetes utilizan una técnica de filtrado, que consiste en una lista de órdenes ejecutadas secuencialmente a la entrada/salida de cada paquete en las interfaces de un router, con las opciones de permitir ó bloquear, por ejemplo: iptables en Linux y ACL en Cisco.
- Esta arquitectura es la más simple de implementar y la más utilizada en organizaciones que no precisan grandes niveles de seguridad, donde el router actúa como de pasarela de la subred y no hay necesidad de utilizar proxies, ya que los accesos desde la red interna al exterior no bloqueados son directos.

CORTAFUEGOS DE FILTRADO DE PAQUETES

Ventajas:

- Disponible en casi cualquier router y en muchos sistemas operativos.
- Ofrece un alto rendimiento para redes con una carga de tráfico elevada.
- Necesita pocos recursos.
- Es fácil añadir nuevos protocolos o aplicaciones.

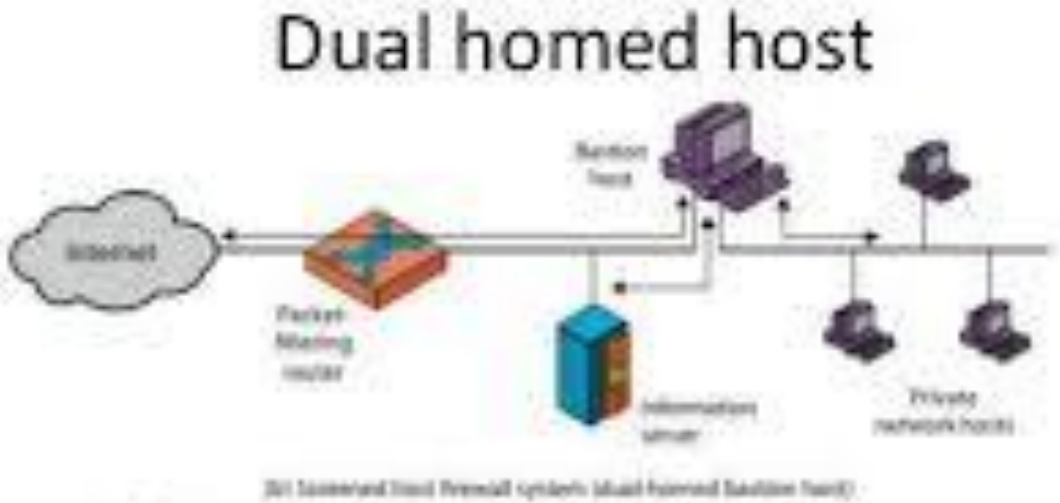
Inconvenientes:

- Las reglas de filtrado pueden llegar a ser complejas de establecer y por lo tanto, se hace difícil comprobar su corrección.
- Al procesar los paquetes de forma independiente, no se guarda ninguna información de contexto (no se almacenan históricos de cada paquete), ni se puede analizar a nivel de capa de aplicación, dado que está implementado en los routers.
- No disponen de un sistema de monitorización sofisticado.
- Es difícil de manejar la autenticación y autorización.

CORTAFUEGOS DUAL-HOMED HOST

- Una dual-homed host architecture esta construida un ordenador con dos tarjetas de red.
- Este host es capaz de enrutar paquetes IP desde una red a otra. Pero los paquetes IP de una red a la otra no son enrutados directamente. El sistema interno al Firewall puede comunicarse con el dual-homed host, y los sistemas fuera de Firewall también pueden comunicarse con él, pero los sistemas no pueden comunicarse directamente entre ellos.
- También es necesario que el IP Forwarding esté deshabilitado en el equipo: aunque una máquina con dos tarjetas puede actuar como un router, para aislar el tráfico entre la red interna y la externa es necesario que no se enruten paquetes entre ellas.
- Así, los sistemas externos `verán' al host a través de una de las tarjetas y los internos a través de la otra, pero entre las dos partes no puede existir ningún tipo de tráfico que no pase por el cortafuegos.

CORTAFUEGOS DUAL-HOMED HOST



- Packet filtering router not completely compromised
- Traffic between internet and hosts on private network has to flow through bastion host
- DMZ-CONTAINS INFO WHICH CAN BE ACCESSED FROM OUTSIDE

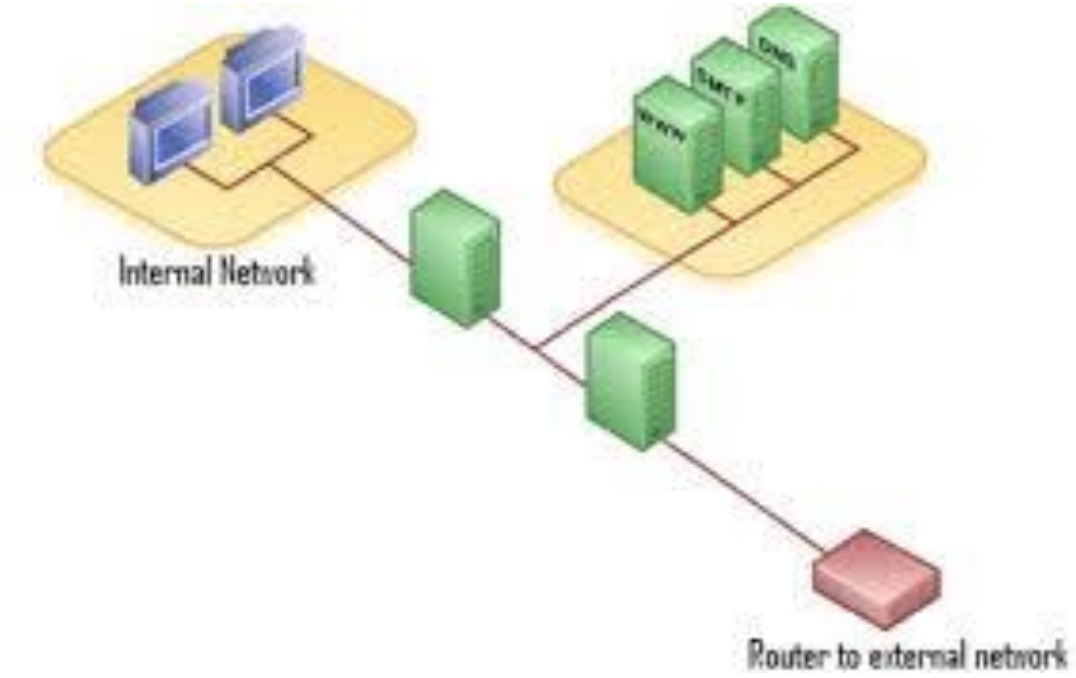
CORTAFUEGOS SCREENED HOST

- En esta arquitectura se combina un screening router con un host bastión y el principal nivel de seguridad proviene del filtrado de paquetes.
- El screening router está situado entre el host bastión y la red externa, mientras que el host bastión está situado dentro de la red interna.
- El filtrado de paquetes en el screening router está configurado de modo que el host bastión es el único sistema de la red interna accesible desde la red externa. Incluso, únicamente se permiten ciertos tipos de conexiones. Cualquier sistema externo que intente acceder a los sistemas internos tendrán que conectar con el host bastión.
- Por otra parte, el filtrado de paquetes permite al host establecer las conexiones permitidas, de acuerdo con la política de seguridad, a la red externa:
  - Permitir a otros hosts internos establecer conexiones a hosts de la red exterior para ciertos servicios.
  - Denegar todas las conexiones desde los hosts de la red interna, forzando a los hosts a utilizar los servicios proxy a través del host bastión.
- Es decir, los servicios se pueden permitir directamente vía filtrado de paquetes o indirectamente vía proxy, tanto para los usuarios internos como para los usuarios externos.

CORTAFUEGOS SCREENED SUBNET (DMZ)

- La arquitectura Screened Subnet también se conoce con el nombre de red perimetral o De-Militarized Zone (DMZ).
- En los modelos anteriores, la seguridad se centraba completamente en el host bastión, de manera que si la seguridad del mismo se veía comprometida, la amenaza se extendía automáticamente al resto de la red.
- En cambio, en este modelo se añade un nivel de seguridad en las arquitecturas de cortafuegos situando una subred (DMZ) entre las redes externa e interna, de forma que se consigue reducir los efectos de un ataque exitoso al host bastión.
- Se crea una red aislada utilizando dos routers. Todos los hosts pueden acceder a la red intermedia pero no la pueden atravesar directamente.
- La arquitectura DMZ intenta aislar la máquina bastión en una red perimétrica, de forma que si un intruso accede a esta máquina no consigue un acceso total a la subred protegida.

CORTAFUEGOS SCREENED SUBNET (DMZ)



CORTAFUEGOS SCREENED SUBNET (DMZ)

- Se emplean dos routers, exterior e interior, ambos conectados a la red perimetral donde se incluye el host bastión. También se podrían incluir sistemas que requieran un acceso controlado, como baterías de módems o el servidor de correo, que serán los únicos elementos visibles desde fuera de la red interna.
- La misión del router exterior es bloquear el tráfico no deseado en ambos sentidos, es decir, tanto hacia la red perimetral como hacia la red externa.
- El router interior bloquea el tráfico no deseado tanto hacia la red perimetral como hacia la red interna. De este modo, para atacar la red protegida se tendría que romper la seguridad de ambos routers.
- Para obtener un mayor nivel de seguridad, se pueden definir varias redes perimetrales en serie, cada una con diferentes reglas de filtrado. Situando los servicios que requieran de menor fiabilidad en las redes más externas. Un posible atacante tendría que pasar por todas y cada una de las redes perimétricas para llegar a acceder a los equipos de la red interna.

CORTAFUEGOS SCREENED SUBNET (DMZ)

- Aunque se trata de la arquitectura más segura, también pueden aparecer problemas:
  - Cuando se emplea el cortafuegos para que los servicios fiables pasen directamente sin acceder al bastión, lo que puede desencadenar en un incumplimiento de la política de seguridad.
  - La mayor parte de la seguridad reside en los routers empleados. Las reglas de filtrado sobre estos elementos pueden ser complicadas de establecer y comprobar, lo que puede desembocar en importantes fallos de seguridad del sistema.

CORTAFUEGOS. OTRAS ARQUITECTURAS

- Alternativa 1: Emplear un host bastión distinto para cada protocolo o servicio en lugar de un único host bastión. Como inconveniente se tiene la cantidad de máquinas necesarias para implementar el cortafuegos.

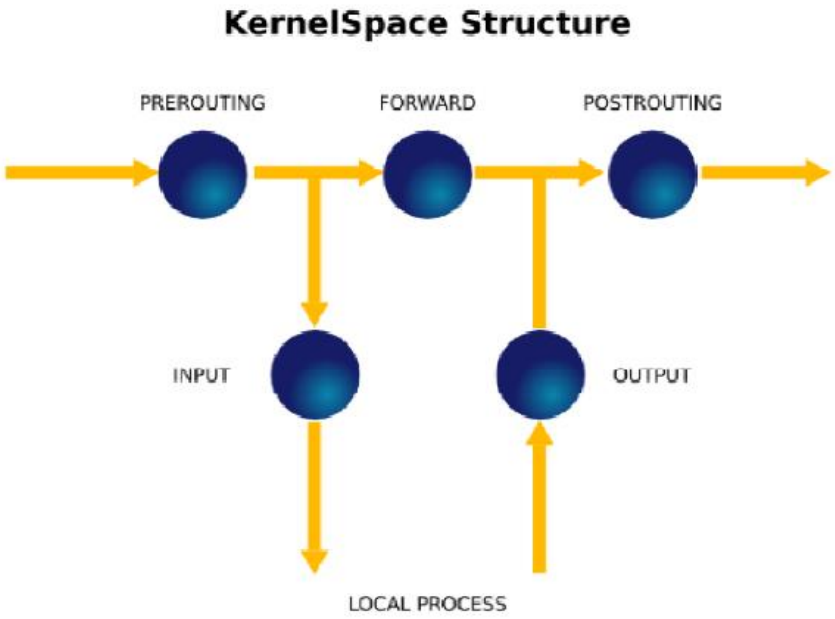
- Alternativa 2: Un único bastión, pero distintos servidores proxy para cada uno de los servicios ofrecidos.

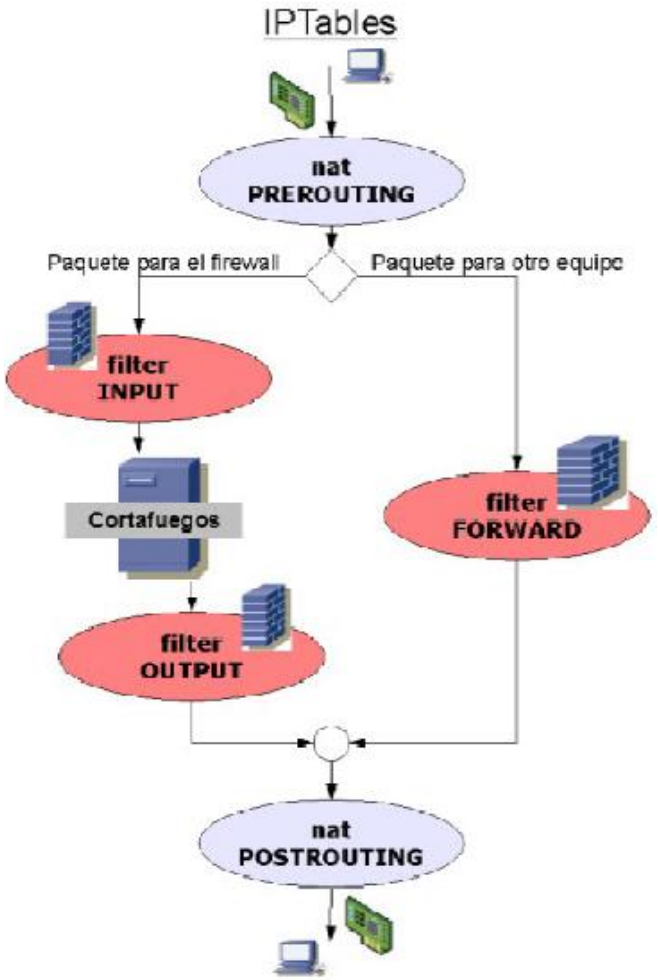
- Alternativa 3: División de la red interna en diferentes subredes, situando cortafuegos internos entre dichas zonas y la red exterior. Aparte de incrementar la seguridad, los firewalls internos son especialmente recomendables en zonas de la red desde la que no se permite a priori la conexión con Internet.

IPTABLES

- Netfilter es el sistema de filtrado de paquetes incluido a partir de las series 2.4 y 2.6 del núcleo de Linux. Iptables es el programa de línea de comandos que usamos para configurar las reglas de filtrado de paquetes en Linux.
- Las reglas de iptables están a nivel del kernel, por lo que cuando un paquete llega al equipo, dependiendo de si el paquete es para la propia máquina o para otra consulta las reglas de firewall y decide qué hacer.
- Iptables tiene dos tablas (subprogramas):
  - La tabla filter deja o no pasar los paquetes que llegan al cortafuegos.
  - La tabla nat se utiliza para modificar las direcciones IP de los paquetes.
- Esas tablas se aplican en diferentes momentos o actúan sobre paquetes con diferentes destinos, como se muestra en la figura, donde se ve un esquema simplificado del camino que recorren los paquetes cuando llegan al enrutador.

IPTABLES


KernelSpace Structure
PREROUTING
FORWARD
POSTROUTING
INPUT
OUTPUT
LOCAL PROCESS


IPTables
nat
PREROUTING
Paquete para el firewall
Paquete para otro equipo
filter
INPUT
Cortafuegos
filter
FORWARD
filter
OUTPUT
nat
POSTROUTING

IPTABLES

- En la figura también aparecen 5 cadenas (chains): PREROUTING, POSTROUTING, INPUT, OUTPUT y y FORWARD.
- La traducción de direcciones o nat puede realizarse en dos momentos:
  - en cuanto el paquete llega al firewall y antes de decidir si el destino es el propio equipo o si debe ser reenviado a otro. Este momento o cadena se denomina PREROUTING. Usado cuando queremos que nuestro equipo sea accesible como servidor web desde el exterior.
  - justo antes de que el paquete abandone el firewall, es decir, en la cadena POSTROUTING. Este es el escenario más habitual, usamos la traducción de direcciones de red para posibilitar que todos los equipos de la red local salgan a Internet compartiendo una única dirección IP pública.

IPTABLES

La tabla filter se puede usar con todos los paquetes, pero en diferentes cadenas dependiendo del destino de cada paquete:

- los paquetes cuyo destino es el propio firewall, sea desde la red interna o desde la externa, pueden ser filtrados en la cadena INPUT. De esta forma podemos controlar el tráfico que alcanza el firewall. Por ejemplo, si el único servicio que nuestro firewall ofrece es el servidor SSH, admitiremos conexiones al puerto 22 y rechazaremos todo lo demás.
- los paquetes que salen del cortafuegos, en cualquier dirección, pueden ser filtrados en la cadena OUTPUT.
- los paquetes que llegan al firewall pero cuyo destino final es otro equipo, es decir, los que deben ser reenviados, pueden ser filtrados en la cadena FORWARD. De nuevo se aplica tanto a los paquetes que entran a nuestra red como a los que salen de ella.

IPTABLES

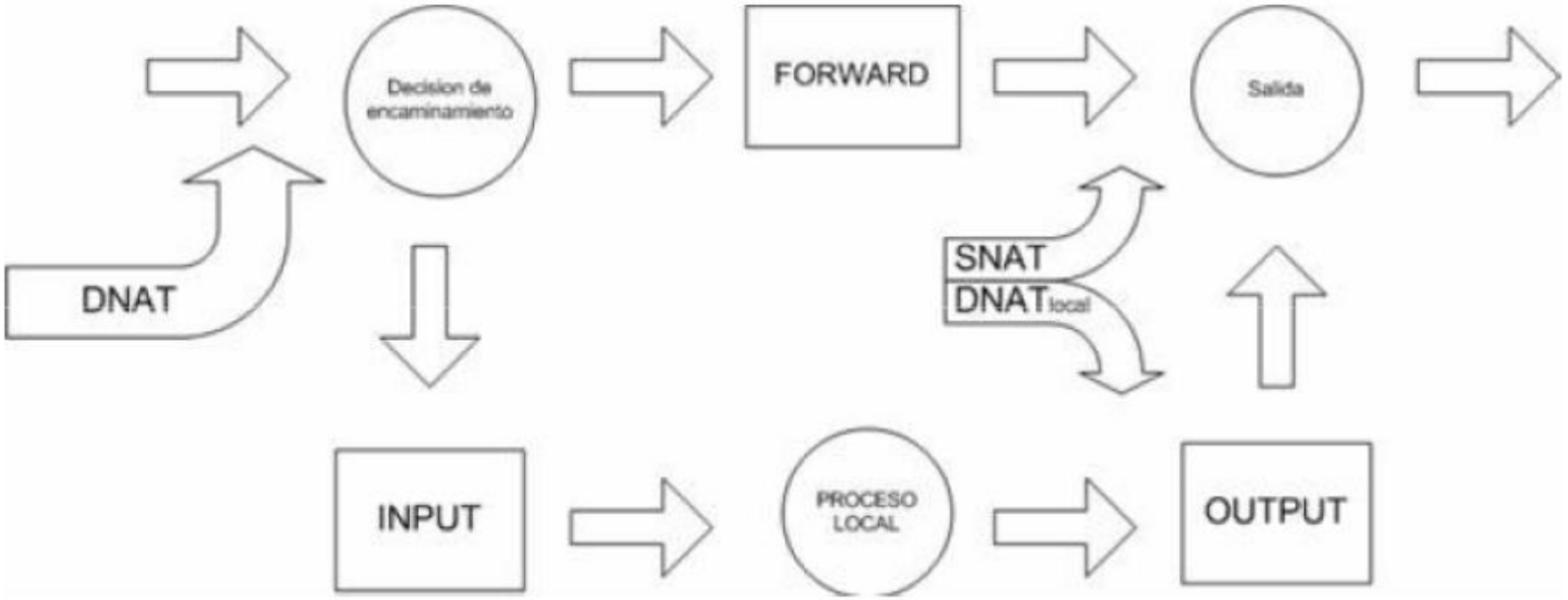
DNAT:

- Alteramos la dirección de destino del primer paquete: esto es, cambiamos la dirección a donde se dirige la conexión.
  - Antes del encaminamiento, cuando el paquete entra por el cable (PREROUTING).
  - El port forwarding , el balanceo de carga y el proxy transparente son formas de DNAT.

SNAT:

- Source NAT es cuando alteramos el origen del primer paquete, esto es, estamos cambiando el lugar de donde viene la conexión.
- Source NAT siempre se hace después del encaminamiento, justo antes de que el paquete salga por el cable (POSTROUTING).
- El enmascaramiento es una forma especializada de SNAT.

IPTABLES


Decision de encaminamiento
FORWARD
Salida
DNAT
SNAT
DNAT local
INPUT
PROCESO LOCAL
OUTPUT

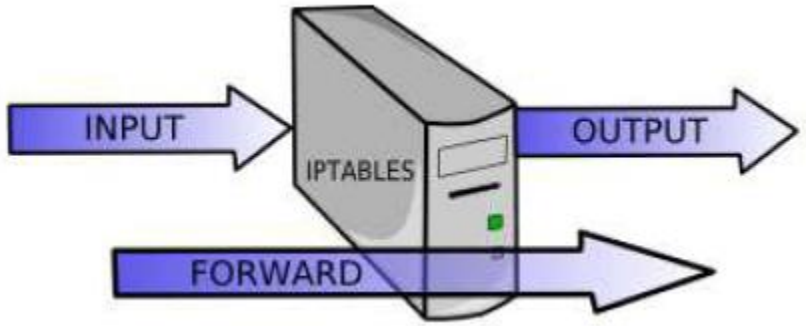
IPTABLES. SINTAXIS

Los comandos **iptables** tienen la siguiente forma:

- **iptables [-t table] -[AD] chain especificación-regla [opciones]**: con **A** se añade una regla a la cadena de reglas; con **D** se borra una regla de la cadena de reglas.
- **iptables [-t table] -I chain [numeroregla] especificación-regla [opciones]** : inserta una regla en concreto.
- **iptables [-t table] -R chain numeroregla especificación-regla [opciones]**: reemplaza una regla en concreto.
- **iptables [-t table] -D chain numeroregla [opciones]**: elimina una regla en concreto.
- **iptables [-t table] -[LFZ] [chain] [opciones]**: **L** lista todas las reglas de una cadena de reglas; **F** hace un flush, se actualiza; **Z** pone a cero los paquetes y contadores de las cadenas de reglas.

IPTABLES. SINTAXIS

- iptables [-t table] -N chain: Crea una nueva cadena de reglas (chain).
- iptables [-t table] -X [chain]: Elimina toda una cadena de reglas (chain).
- iptables [-t table] -P chain objetivo [opciones]: Establece la política para una cadena de reglas, es decir, el objetivo para la misma. Sirve como política por defecto.
- iptables [-t table] -E old-chain-name new-chain-name: renombra una cadena de reglas (chain).



IPTABLES. SINTAXIS

Parámetros para especificar reglas. Se usan al añadir, eliminar, insertar, reemplazar y concatenar comandos:

- -p, --protocol [!] protocolo: Protocolo del paquete a chequear. Se admite: tcp, udp, icmp, or all (por defecto), o un valor numérico. Con "!" se niega.
- -s, --source [!] dirección[/máscara]: Origen o fuente. La dirección puede ser un nombre de dominio, hostname, una IP de red o IP de máquina. Se suele usar el alias --src.
- -d, --destination [!] dirección[/máscara]: Destino. Se suele usar el alias –dst.
- -j, --jump objetivo: Indica el objetivo de la regla, es decir, que hacer con ella (ACCEPT, DROP, MASQUERADE, REJECT,etc)
- -i, --in-interface [!] name: Interfaz por la que se reciben los paquetes. Admite las cadenas de reglas INPUT, FORWARD y PREROUTING.
- -o, --out-interface [!] name: Interfaz por la que se envían los paquetes. Admite las cadenas de reglas FORWARD, OUTPUT y POSTROUTING.

IPTABLES. SINTAXIS

Extensiones: se puede hacer implícitamente (ej. con -p o –protocol, que indican el protocolo y automáticamente se carga el módulo del protocolo) o explícitamente, con las opciones -m o --match, seguidas del nombre del módulo de matching:

- [--sport [!] [puerto[:puerto]]]: puerto de origen
- [--dport [!] [puerto[:puerto]]]: puerto de destino.
- [--icmp-type [!] nombre_de_tipo]: tipo de mensaje ICMP (echo-request, echo-reply, time-exceeded, destination-unreachable, networkunreachable, host-unreachable, protocol-unreachable, y portunreachable).
- [--mac-source [!] address] : dirección MAC.
- [--state] estado: para el seguimiento del estado de las conexiones (INVALID, ESTABLISHED, NEW, RELATED).

IPTABLES. CREACIÓN DE SCRIPT

Borrado de reglas:

- Cuando se añade nuevas reglas al cortafuegos utilizando el comando iptables, éstas no sobrescriben las anteriores, sino que se añaden a ellas.
- Es por eso que las primeras líneas de todos los scripts de Iptables se dedican a borrar cualquier regla que pudiera existir:

```
iptables -t filter -F
iptables -t nat -F
```

- Vaciar (-F viene de "flush", tirar de la cadena) las reglas de la tabla filter y de la tabla nat.
- O bien:

```
iptables -F
iptables -t nat -F
```

IPTABLES. CREACIÓN DE SCRIPT

Política por defecto:

- Tras borrar las reglas anteriores ejecutamos la política restrictiva:

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

- La política por defecto (-P) se establece para cada cadena (INPUT, OUTPUT y FORWARD) a DROP: los paquetes que lleguen a cada una de estas cadenas serán ignorados. A no ser que otras reglas posteriores cambien esta política.
- O la política permisiva:

```
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
```

IPTABLES. CREACIÓN DE SCRIPT

Reenvío de paquetes:

- Si queremos que el firewall reenvíe todos los paquetes que le lleganpero no son para él, sino para otros equipos:

```
iptables -t filter -A FORWARD -j ACCEPT
```

o más corto, pero con el mismo efecto:

```
iptables -A FORWARD -j ACCEPT
```

(Añade una regla (-A) a la cadena 'FORWARD' de la tabla 'filter' de forma que acepte, o sea, reenvíe, todos los paquetes (-j ACCEPT)".

- Estaríamos inyectando paquetes que vienen de rangos de direcciones privadas en una red con rangos diferentes o en Internet, con lo que esas direcciones no serían válidas. Debemos hacer la traducción de direcciones:

```
iptables -t nat -A POSTROUTING -j MASQUERADE
```

(Añade una regla (-A) a la cadena 'POSTROUTING' de la tabla 'nat' para sustituir la dirección fuente de los paquetes que salen por una tarjeta de red por la IP de esa tarjeta. Para los paquetes que salen a Internet, esa IP será la dirección pública)

IPTABLES. CREACIÓN DE SCRIPT

Reenvío de paquetes:

- Por último, habría que activar el reenvío de paquetes:

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

IPTABLES. CREACIÓN DE SCRIPT

Refinamiento de reglas:

- Algunas de las reglas pueden ser más específicas, siguiendo la idea que no permitir más de lo estrictamente necesario. Por ejemplo, ni hay necesidad ni es conveniente hacer NAT en todos los adaptadores de red. Como sólo es necesario en los paquetes que van a Internet (salen por la tarjeta externa, eth1, la regla MASQUERADE podría reescribirse como:

```
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

('-o' viene de 'output').

- O utilizar variables al principio del script para sólo tener que pensar una vez cuál es la tarjeta externa y cuál la interna.

```
TARJ_EXT="eth1"
iptables -t nat -A POSTROUTING -o $TARJ_EXT -j MASQUERADE
```

IPTABLES. CREACIÓN DE SCRIPT

Refinamiento de reglas:

- Otra regla que puede mejorarse es la que reenvía todo:

```
iptables -t filter -A FORWARD -j ACCEPT
```

- Puesto que no queremos que reenvíe todo, sólo lo que llega por la tarjeta de red interna, 'eth2' en nuestro ejemplo. La regla quedaría:

```
TARJ_INT="eth2"
iptables -t filter -A FORWARD -i $TARJ_INT -j ACCEPT
```

IPTABLES. CREACIÓN DE SCRIPT

Refinamiento de reglas:

- Permitir las respuestas a los paquetes que nacen en nuestra red local:

```
iptables -t filter -A FORWARD -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

  (Aceptamos los paquetes que coinciden (-m, match, coincidir) con el estado (--state) 'ESTABLISHED,RELATED', esto es, paquetes que pertenecen o bien a conexiones ya establecidas o a conexiones relacionadas con ellas.

- De esta forma:
  - permitimos que los ordenadores de nuestra red local puedan iniciar conexiones con equipos de Internet y que las respuestas de éstos (ESTABLISHED,RELATED) lleguen a nuestros equipos.
  - no permitimos que los ordenadores del exterior inicien conexiones con PCs de nuestra red interna, evitando así muchos de los riesgos que entraña poner un equipo en Internet.

IPTABLES. CREACIÓN DE SCRIPT

Permitiendo ciertos servicios:

- Si sólo queremos permitir la navegación web y a cortar todo lo demás. Sólo reenviaremos peticiones al puerto 80. Cambiar

```
iptables -t filter -A FORWARD -i eth1 -j ACCEPT
```

por

```
iptables -t filter -A FORWARD -i $TARJ_INT -p TCP --dport 80 -j ACCEPT
```

Hemos añadido dos condiciones más, el protocolo debe ser TCP (-p TCP) y el puerto de destino tiene que ser el 80 (--dport 80).

IPTABLES. CREACIÓN DE SCRIPT

Pings:

- Para permitir pings, debemos añadir una línea como la siguiente:

```
iptables -t filter -A FORWARD -i $TARJ_INT -p ICMP --icmp-type 8 -j
ACCEPT
```

Nuestros equipos podrán hacer ping a equipos externos. Estos últimos pueden respondernos (la línea iptables -t filter -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT ya está en el script).

EJEMPLOS DE IPTABLES

- Script que no deje pasar ningún tipo de tráfico hacia y desde nuestra máquina de manera que parezca que no tenemos ningún servicio disponible.

firewall.sh

```
#!/bin/sh

# Primer script de iptables del curso de linux

# Políticas por defecto
/sbin/iptables -P INPUT DROP
/sbin/iptables -P OUTPUT DROP
/sbin/iptables -P FORWARD DROP

# Vaciando las tablas
/sbin/iptables -F
/sbin/iptables -F INPUT
/sbin/iptables -F OUTPUT
/sbin/iptables -F FORWARD
/sbin/iptables -X
/sbin/iptables -F -t nat
```

EJEMPLOS DE IPTABLES

- Líneas que permiten el acceso a los servicios locales:

firewall.sh

```
# loopback rules
/sbin/iptables -A INPUT -i lo -j ACCEPT
/sbin/iptables -A OUTPUT -o lo -j ACCEPT
```

EJEMPLOS DE IPTABLES

- Borrado de reglas anteriores, política restrictiva, acceso a los servicios locales y posibilidad de utilizar el servicio ubicado en el propio firewall:

firewall.sh

```
#!/bin/sh

# Políticas por defecto
/sbin/iptables -P INPUT DROP
/sbin/iptables -P OUTPUT DROP
/sbin/iptables -P FORWARD DROP

# Vaciando las tablas
/sbin/iptables -F
/sbin/iptables -F INPUT
/sbin/iptables -F OUTPUT
/sbin/iptables -F FORWARD
/sbin/iptables -X
/sbin/iptables -F -t nat


# loopback
/sbin/iptables -A INPUT -i lo -j ACCEPT
/sbin/iptables -A OUTPUT -o lo -j ACCEPT

# www
/sbin/iptables -A INPUT -p tcp -i eth0 --dport 80 -j ACCEPT
/sbin/iptables -A OUTPUT -p tcp -o eth0 --sport 80 -j ACCEPT
```

FUENTES

- Abad Domingo, Alfredo, "Seguridad y Alta Disponibilidad", Ed. Garceta
- "Puesta en marcha de un cortafuegos con IPTABLES", David J. Horat Flotats y Enrique Fernández Perdomo. (Arquitectura de Sistemas y Aplicaciones Distribuidas - U.L.P.G.C.)

UT4. INSTALACIÓN Y CONFIGURACIÓN DEL CORTAFUEGOS

Módulo: Seguridad y Alta Disponibilidad

Curso 2023/2024. 2º ASIR