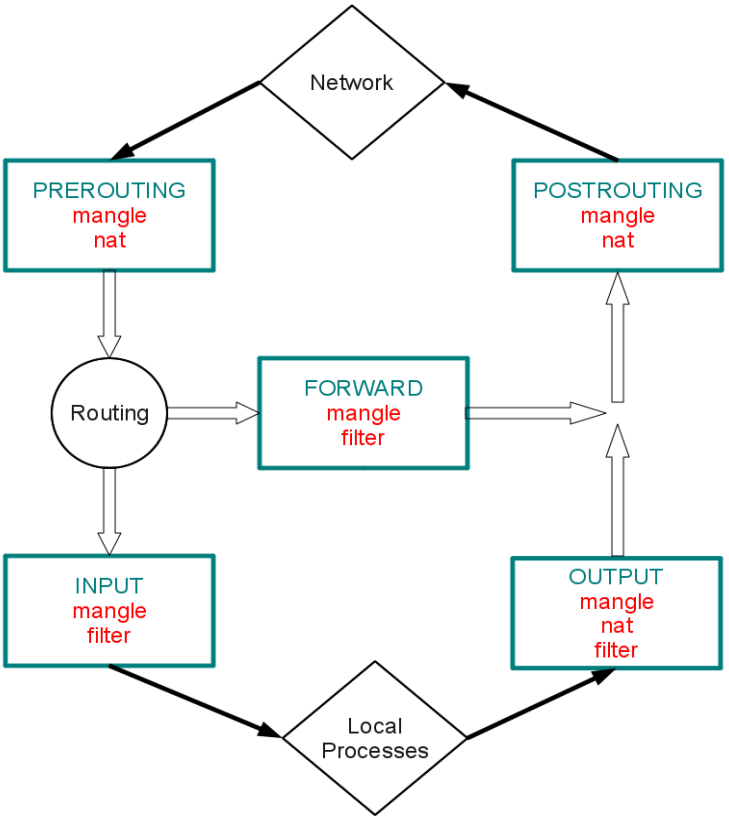
	COMUNICACIONES II	
	Ingeniería en Informática - Licenciatura en Informática Programador Universitario	Mg. Ing. Hugo Ortega Esp. Ing. Luis Ortíz
	Trabajo práctico N°10	Fecha:13/11/2025
Tema:	Seguridad	

Introducción a IPTABLES

Principales tablas y reglas

- NAT: se usa para modificar IP o puerto origen o destino
  - Prerouting: se aplica antes del ruteo
  - Postrouting: se aplica después del ruteo
- Filter: se usa para permitir o denegar cierto tráfico
  - INPUT: Tráfico entrante al equipo destinado al mismo
  - OUTPUT: Tráfico generado desde el equipo
  - FORWARD: tráfico que pasa por el equipo pero no está dirigido a el.



Principales comandos de IPtables

- -A –append → agrega una regla a una cadena.
- -D –delete → borra una regla de una cadena especificada.

- -R –replace → reemplaza una regla.
- -I –insert → inserta una regla en un lugar de una cadena.
- -L –list → muestra las reglas que le pasamos como argumento.
- -F –flush → borra todas las reglas de una cadena.
- -Z –zero → pone a cero todos los contadores de una cadena.
- -N –new-chain → permite al usuario crear su propia cadena.
- -X –delete-chain → borra la cadena especificada.
- -P –policy → explica al kernel qué hacer con los paquetes que no coincidan con ninguna regla.
- -E –rename-chain → cambia el orden de una cadena.

Condiciones principales para Iptables:

- -p –protocol → la regla se aplica a un protocolo.
- -s –src –source → la regla se aplica a una IP de origen.
- -d –dst –destination → la regla se aplica a una Ip de destino.
- -i –in-interface → la regla de aplica a una interfaz de origen, como eth0.
- -o –out-interface → la regla se aplica a una interfaz de destino.

Condiciones TCP/UDP

- -sport –source-port → selecciona o excluye puertos de un determinado puerto de origen.
- -dport –destination-port → selecciona o excluye puertos de un determinado puerto de destino.

Targets más usados

(qué hacer con el tráfico que coincide con la regla)

filter

- ACCEPT: se acepta el tráfico que coincide con la regla
- DROP : se descarta el tráfico que coincide con la regla
- REJECT: se rechaza el tráfico que coincide con la regla

nat

- DNAT: cambia dirección destino
- SNAT: cambia dirección origen
- MASQUERADE: similar a snat pero cambia la ip por la que tenga asignada una interfaz

Sintaxis

	COMUNICACIONES II	
	Ingeniería en Informática - Licenciatura en Informática Programador Universitario	Mg. Ing. Hugo Ortega Esp. Ing. Luis Ortíz
	Trabajo práctico N°10	Fecha:13/11/2025
Tema:	Seguridad	

iptables [-t table] -[AD] chain rule-specification [options]
iptables [-t table] -I chain [rulenum] rule-specification [options]
iptables [-t table] -R chain rulenum rule-specification [options]
iptables [-t table] -D chain rulenum [options]
iptables [-t table] -[LFZ] [chain] [options]
iptables [-t table] -N chain
iptables [-t table] -X [chain]
iptables [-t table] -P chain target [options]
iptables [-t table] -E old-chain-name new-chain-name

Ver estado de firewall

iptables -L -n -v

Ejemplos:

Definiendo políticas para firewall

(Qué hacer con el tráfico que no coincide con ninguna regla)

restrictivo

iptables -P INPUT DROP

iptables -P FORWARD DROP

iptables -P OUTPUT DROP

permisivo

iptables -P ACCEPT

iptables -P FORWARD ACCEPT

iptables -P OUTPUT ACCEPT

El tráfico tcp que pasa por el firewall (que entra y sale) hacia el puerto 80 y que es enviado a la IP 211.34.149.2 será aceptado.
iptables -t filter -A FORWARD -p tcp --dport 80 -d 211.34.149.2 -j ACCEPT

El tráfico que venga de la red 192.168.10.0/24 será enviado por la interfaz eth0 con la misma IP. Es decir, le daremos acceso a internet. (El ip4.forward debe estar activado y eth0 es la interfaz a la cual tendremos acceso a internet).
iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o eth0 -j MASQUERADE
El tráfico tcp que viene por la interfaz eth0 con destino 2022 será enviado a la IP 192.168.0.111 al puerto 22.

	COMUNICACIONES II	
	Ingeniería en Informática - Licenciatura en Informática Programador Universitario	Mg. Ing. Hugo Ortega Esp. Ing. Luis Ortíz
	Trabajo práctico N°10	Fecha:13/11/2025
Tema:	Seguridad	

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 2022 -j DNAT --to
192.168.0.111:22
# No permitimos que al firewall lleguen paquetes que usamos al hacer ping. Es decir,
no permitimos que hagan ping al firewall.
iptables -t filter -A INPUT -p ICMP --icmp-type echo-request -j DROP
# El ping llega pero no permitimos al firewall devolver el ping.
iptables -t filter -A OUTPUT -p ICMP --icmp-type echo-reply -j DROP
```

Casos prácticos

1. Explique qué hace cada una de estas reglas y todas en su conjunto

caso 1

```
iptables -F
iptables -X
iptables -Z
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -s 192.168.22.143 -j ACCEPT
iptables -A INPUT -s 231.45.34.234 -p tcp --dport 3306 -j ACCEPT
iptables -A INPUT -s 80.37.45.194 -p tcp --dport 20:21 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 1:1024 DROP
iptables -A INPUT -p udp --dport 1:1024 DROP
hemos permitido anteriormente).
iptables -A INPUT -p tcp --dport 3306 -j DROP
iptables -A INPUT -p tcp --dport 10000 DROP
iptables -A INPUT -p udp --dport 10000 DROP
```

caso 2

```
iptables -F
iptables -X
```

	COMUNICACIONES II	
	Ingeniería en Informática - Licenciatura en Informática Programador Universitario	Mg. Ing. Hugo Ortega Esp. Ing. Luis Ortíz
	Trabajo práctico N°10	Fecha:13/11/2025
Tema:	Seguridad	

```
iptables -Z
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to
192.168.3.2:80
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to
192.168.3.2:443
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -i eth1 -s 192.168.10.0/24 -j ACCEPT
iptables -t nat -A POSTROUTING -s 192.168.3.0/24 -o eth0 -j
MASQUERADE
iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -o eth0 -j
MASQUERADE
echo 1 > /proc/sys/bnet/ipv4/ip-forward
iptables -A FORWARD -s 192.168.3.2 -p tcp --dport 3306 -d
192.168.10.3:3036 -j ACCEPT
iptables -A FORWARD -s 192.168.10.5 -d 192.168.3.2 -p tcp --sport 3306 -j
ACCEPT
iptables -A FORWARD -s 192.168.10.0/24 -d 192.168.3.0/24 -p tpc --sport
3389 -j ACCEPT
iptables -A FORWARD -s 192.168.3.0/24 -d 192.168.10.0/24 -j DROP
iptables -A INPUT -i eth2 -s 192.168.3.0/24 -j DROP
iptables -A INPUT -i eth0 -s 0.0.0.0 -p tcp --dport 1:1024 -j DROP
iptables -A INPUT -i eth0 -s 0.0.0.0 -p udp --dport 1:1024 -j DROP
iptables -A INPUT -p tcp --dport 10000 -j DROP
iptables -A INPUT -p udp --dport 10000 -j DROP
```

Práctica

1. Revise usando el comando nmap cuales son los puertos que tiene escuchando en su equipo
2. Cree una regla que bloquee el acceso desde afuera a SSH
3. Pruebe y luego borre las reglas
4. Cree una regla que permita el acceso a ssh desde la pc de uno de sus compañeros y no desde el resto
5. Pruebe y luego borre
6. Cree una regla que re envíe el tráfico que llega con puerto destino 22 hacia el puerto 4222 de la misma ip
7. Cree una regla que desvíe el tráfico que llega al puerto 80 de su equipo al puerto 8080 de otro equipo (para que podría usarse una regla así?)

	COMUNICACIONES II	
	Ingeniería en Informática - Licenciatura en Informática Programador Universitario	Mg. Ing. Hugo Ortega Esp. Ing. Luis Ortíz
	Trabajo práctico N°10	Fecha:13/11/2025
Tema:	Seguridad	

Uso de funciones hash para validar integridad de archivos

Funciones ejemplo:
md5sum
sha1sum

1. En linux cree una carpeta con algunos archivos de texto
2. Generar hash correspondiente a los archivos de la carpeta y guardarlos en el archivo hash.md5 **md5sum * >hash.md5**
3. Analise el contenido del archivo hash.md5
4. Checkear integridad md5sum -c hash.md5
5. Modifique el contenido de uno de los archivos y repita el checkeo

Generación de claves públicas y privadas cifrado y firma de mensajes usando GnuPG

- Generar juegos de claves gpg --gen-key
- Listar claves gpg -k
- Exportar claves gpg -output [archivo destino] **--export [ID de a clave pública]**
- Subir clave pública a servidor de claves **gpg --send-keys --keyserver [Dirección del servidor] [ID de la clave pública]**
- Importar clave desde archivo **gpg --import [Archivo de la clave pública]**
- O importar desde servidor de claves **gpg --keyserver [Dirección del servidor] --recv-keys [ID de la clave]**
- Cifrar con clave pública **gpg —encrypt —recipient [ID de la clave] [Archivo]**
- Descifrado con clave privada **gpg -d [Archivo]**
- Firmar archivo **gpg -u [ID de la clave privada] --output [Archivo resultante] --sign [Archivo para firmar]**
- Verificar firma **gpg --verify [Archivo]**

1. Escriba la secuencia de pasos detallados para:
   a. Generar un conjunto de claves públicas y privadas rsa, exportar a archivo la pública, importarla en otro equipo, cifrar un archivo de texto y luego para descifrarlo usando la clave privada
   b. Generar un conjunto de claves públicas y privadas rsa, exportar a archivo la pública, firmar un documento con la privada y en otro equipo importar la clave pública desde archivo y verificar la firma del documento.

	COMUNICACIONES II	
	Ingeniería en Informática - Licenciatura en Informática Programador Universitario	Mg. Ing. Hugo Ortega Esp. Ing. Luis Ortíz
	Trabajo práctico N°10	Fecha:13/11/2025
Tema:	Seguridad	

Referencias

https://linux.die.net/man/8/iptables
https://sospedia.net/tutorial-basico-de-iptables/
https://www.linuxito.com/seguridad/793-tutorial-basico-de-iptables-en-linux
https://www.redeszone.net/gnu-linux/iptables-configuracion-del-firewall-en-linux-con-iptables/
https://www.genbeta.com/desarrollo/manual-de-gpg-cifra-y-envia-datos-de-forma-segura