

---

**SMIX M7- UF3**

**PRACTICA 4**  
**PROXY SQUID EN LINUX**

**EDUARD LARA**

# ÍNDICE

---

- ❖ Firewall.
  - ❖ Características.
  - ❖ Concepto de DMZ
  - ❖ Clasificación
- ❖ NAT
  - ❖ Cisco
  - ❖ Linux
- ❖ ACL
  - ❖ Cisco
  - ❖ Linux
- ❖ Proxy

# FIREWALL O CORTAFUEGOS

---

- Internet Security:
    - **Social engineering:** pretending to be a legitimate system administrator (access by social means)
    - **War dialing:** search modems that answer to your requests so you may get introduced into the corporate network
    - **Denial-of-service attack:** overwhelm a network/computer in such a way that legitimate users can not use it
    - **Session hijacking, spoofing, ...**
    - **Protocol-based attacks:** take advantage of known weakness in network services
    - **Host attacks:** attack a particular OS or in how the system is set up and administered
    - **Password guessing**
    - **Eavesdropping:** stealing all kind of information (e.g.; e-mail messages, files, passwords, ...)
-

# FIREWALL O CORTAFUEGOS

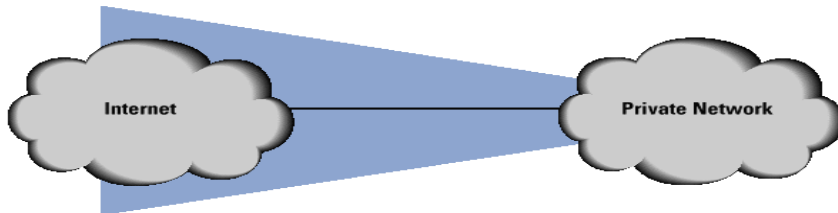
---

- Internet Security:
    - **Denial-of-service (DoS) attack:** impedir el acceso a un servicio
      - Generar peticiones de conexión (segmentos TCP con SYN activo) y no contestar al SYN+ACK del servidor. Agotamos la cola de clientes en proceso de petición de servicio
    - **Spoofing:** hacerse pasar por quien no es:
      - Red privada con esquema de direcciones @IP<sub>base</sub>. Desde fuera de la red accede alguien con @IP origen perteneciente a la red privada (@IP<sub>base</sub>)
    - **Session hijacking:** robar una sesión TCP en curso y hacerse pasar por esa sesión (normalmente acompañada de DoS para hundir la máquina del cliente o del servidor)
-

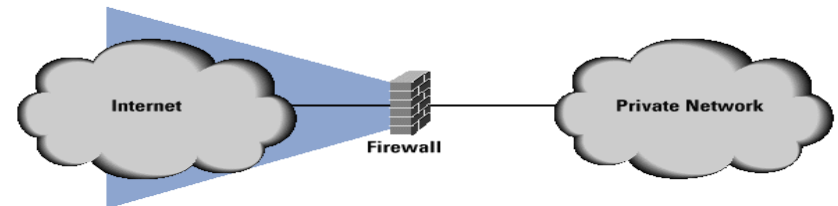
# FIREWALL O CORTAFUEGOS

- ❖ Un firewall o cortafuegos es un dispositivo que separa una red que se desea proteger, de otra de donde pueden venir ataques de seguridad (Internet), y usa una política activa de seguridad.
- ❖ Está situado entre dos redes por donde todo el tráfico debe pasar (checkpoint).
- ❖ El tráfico puede ser controlado, puede ser autenticado en el dispositivo y todo el tráfico puede ser registrado

Zona de riesgo de una red privada no protegida



Zona de riesgo de una red privada protegida



# FIREWALL O CORTAFUEGOS

---

Un firewall debe permitir que:

- ❖ Cada host en una red privada puede acceder a cualquier recurso de Internet
- ❖ Evitar que un host de Internet puede atacar a cualquier host de la red privada.



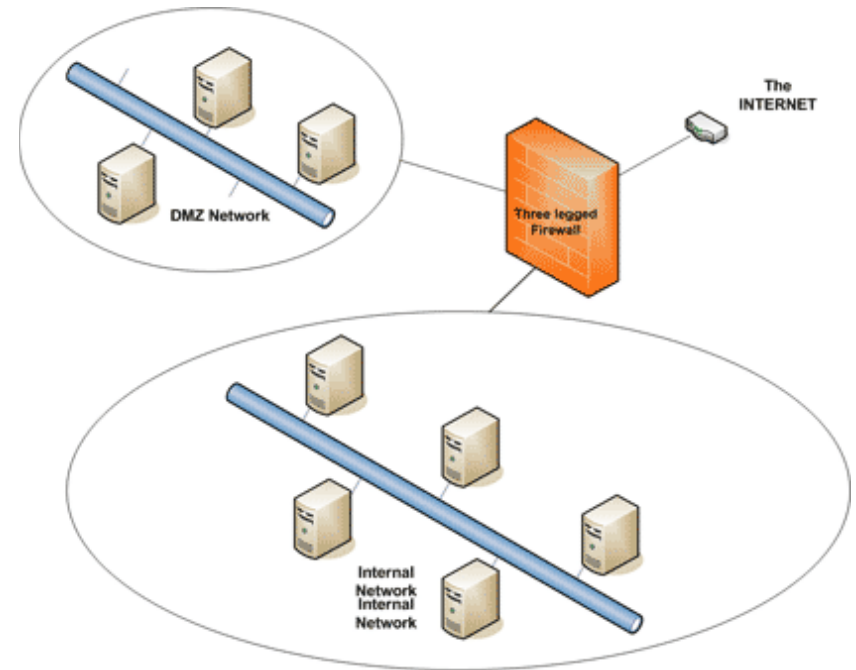
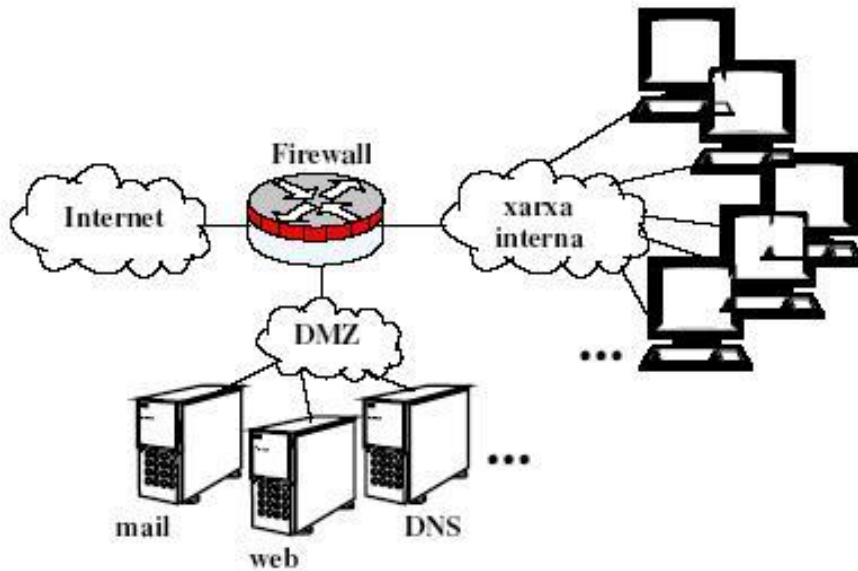
# **ZONA DMZ**

## **(DE-MILITARIZED ZONE)**

---

- ❖ DMZ es un término militar que se utiliza para identificar una zona neutral entre dos bandos en conflicto.
- ❖ En la zona DMZ están los servidores que se desean que sean accesibles desde el exterior.
- ❖ Generalmente el firewall restringe el acceso desde el exterior a la DMZ, y sólo permite a algunos puertos de los servidores.

# ZONA DMZ (DE-MILITARIZED ZONE)



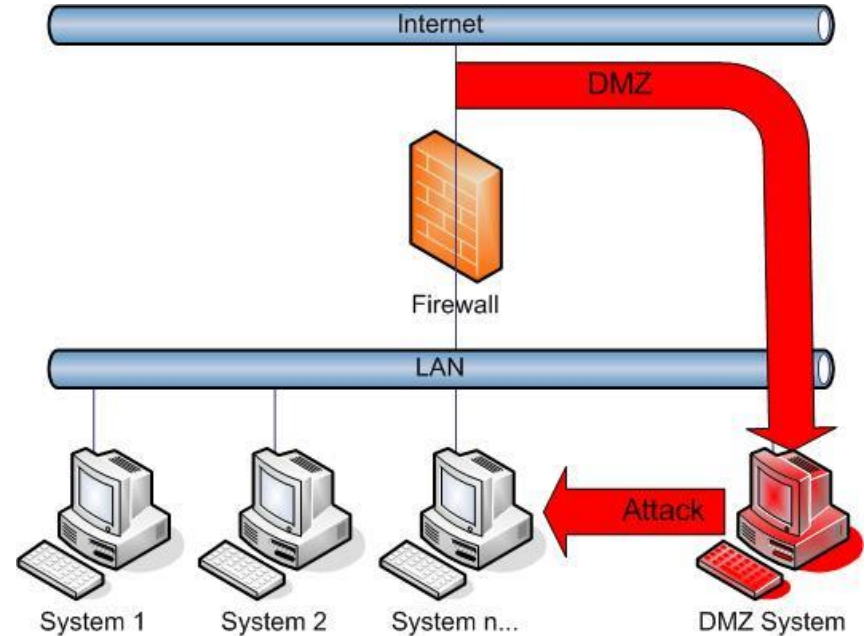
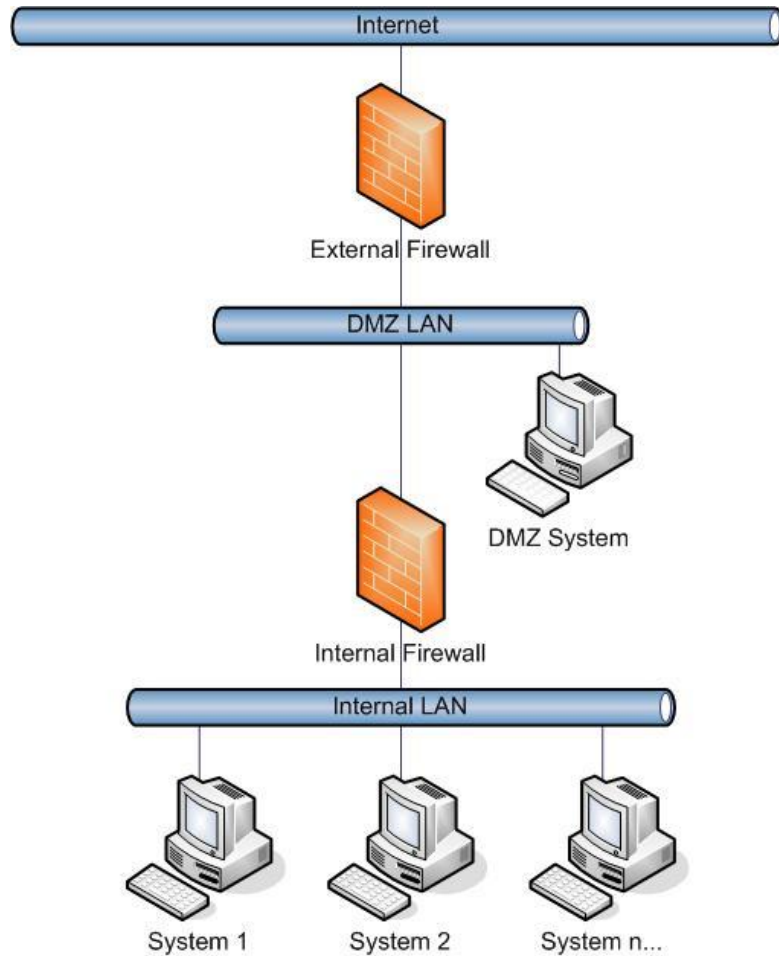
DMZ: De-Militarized Zone →  
Red interna con servidores  
públicos

MZ: Militarized Zone →  
Red Interna

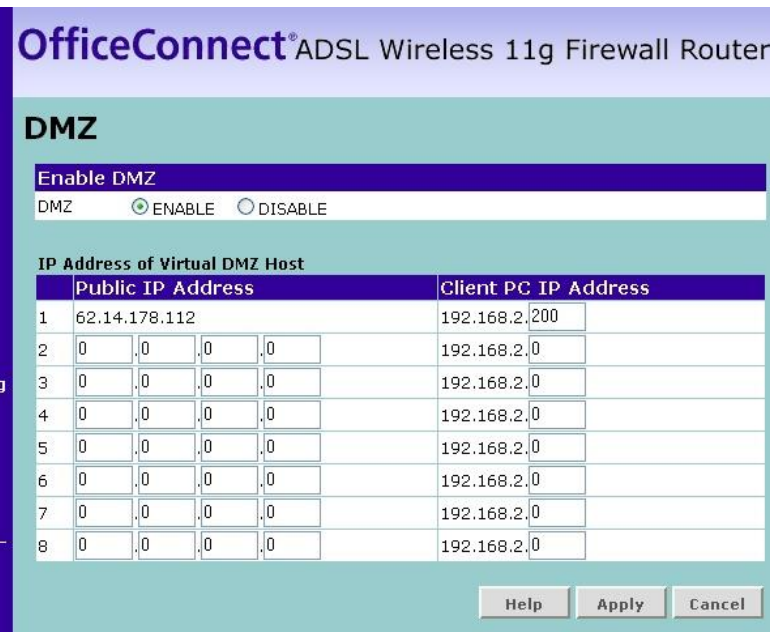
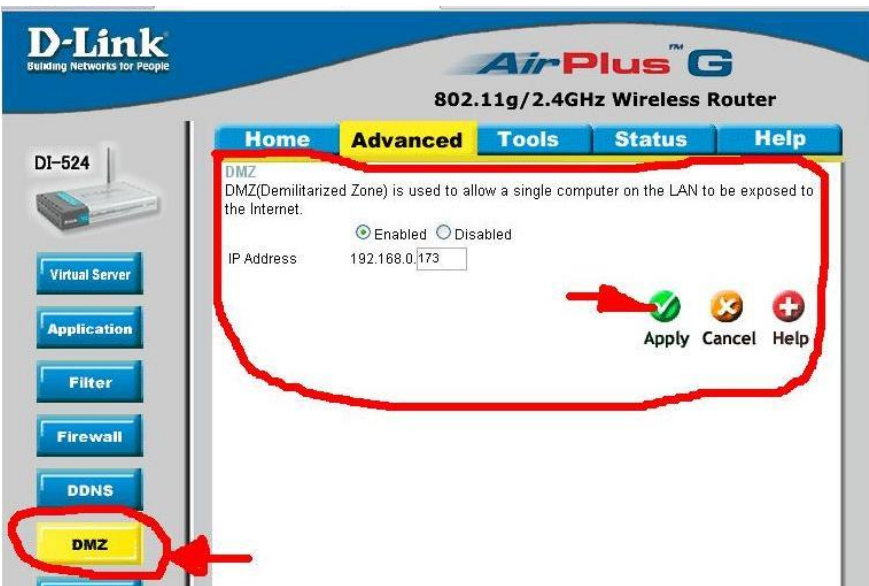




# ZONA DMZ (DE-MILITARIZED ZONE)



# ZONA DMZ (DE-MILITARIZED ZONE)



# ZONA DMZ (DE-MILITARIZED ZONE)

**LINKSYS**  
A Division of Cisco Systems, Inc.

**Applications & Gaming**

Setup | Wireless | Security | Access Restrictions | Applications & Gaming

Port Range Forward | DMZ

**DMZ**

☐ Enable ☒ Disable

DMZ Host IP Address: 10.34.121.0

Save Settings Cancel Changes

---

**Security**

Status | Internet | LAN | Wireless | Security | Device

**DMZ Host**

The ADSL Gateway will forward from the WAN to the DMZ host computer any IP packets that do not appear in the **Virtual Servers** table.

To activate the DMZ host, enter the computer's IP address and press **Apply**.

To deactivate the DMZ host, clear the IP address field and press **Apply**.

DMZ host IP address:

Apply

SonicWALL - Administration for 0006B1224F3C - Windows Internet Explorer

File Edit View Favorites Tools Help

Links Brian's Ski Epic Brian@HomeTz170 Codeblaze

Go PageRank 522 blocked Check Settings

https://192.168.123.1/main.html

Home Bonjour

**SONICWALL** COMPREHENSIVE INTERNET SECURITY™

System | Network

Network > Interfaces Setup Wizard... Clear Statistics ?

Interface Settings

| Name | Zone | IP Address    | Subnet Mask   | IP Assignment | Status               | Comment               | Configure |
|------|------|---------------|---------------|---------------|----------------------|-----------------------|-----------|
| LAN  | LAN  | 192.168.123.1 | 255.255.255.0 | Static        | 100 Mbps full-duplex | Default LAN           |           |
| WAN  | WAN  | 64.81.247.148 | 255.255.255.0 | Static        | 100 Mbps full-duplex | Default WAN           |           |
| OPT  | DMZ  | 192.168.124.1 | 255.255.255.0 | Static        | 100 Mbps full-duplex | DMZ - by Brian Wilson |           |
| WLAN | WLAN | 172.16.31.1   | 255.255.255.0 | Static        | 54 Mbps half-duplex  | Default WLAN          |           |

Edit Interface OPT - Windows Internet Explorer

https://192.168.123.1/editInterface\_2.html

Interface Traffic Statistics

General Advanced

**Interface 'OPT' Settings**

Zone: DMZ

IP Assignment: Static

IP Address: 192.168.124.1

Subnet Mask: 255.255.255.0

Comment: DMZ - by Brian Wilson

Management: ☐ HTTP ☐ HTTPS ☐ Ping ☐ SNMP ☐ SSH

User Login: ☐ HTTP ☐ HTTPS

☐ Add rule to enable redirect from HTTP to HTTPS

Status: The configuration has been updated.

# CATEGORIAS DE FIREWALLS

---

- Hay diferentes tipos de firewalls, desde los más sencillos que simplemente filtran según las @ IP o puertos, hasta otros que son capaces de seguir y filtrar según el estado de las conexiones y el tipo de mensajes del nivel de aplicación.
  - Categorías de firewalls
    - 1) Packet filtering
    - 2) Circuit gateways
    - 3) Application gateways or proxy servers
    - 4) Hybrid firewalls: Combinación de las tres categorías anteriores
-

# PACKET FILTERING

---

- ❖ El firewall observa y filtra los paquetes que no cumplen ciertas condiciones.
- ❖ Trabajan a nivel IP/TCP y toman decisiones basándose en las cabeceras de los paquetes (direcciones IP, nº de puertos, otras opciones de los paquetes)
- ❖ El filtrado se hace con listas de control de acceso (Access Control List, ACL).

# CIRCUIT GATEWAYS

---

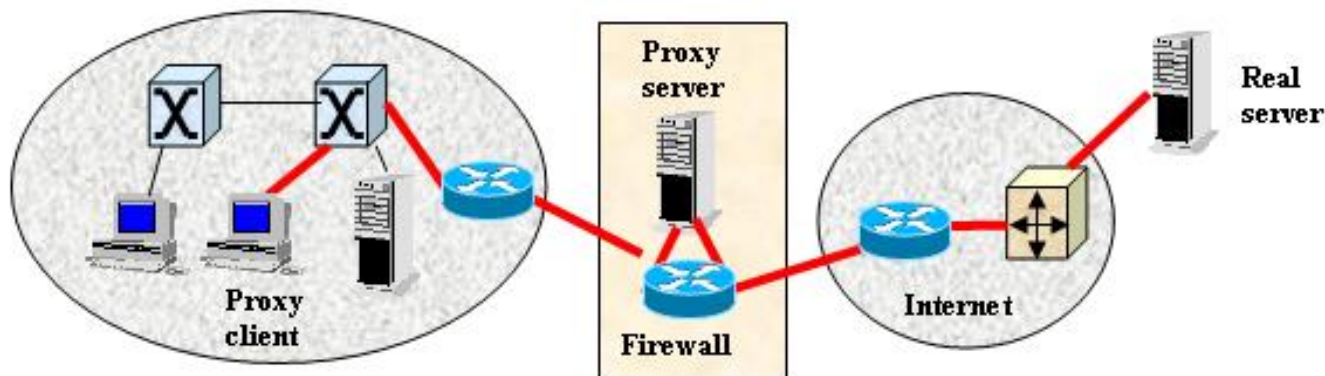
- ❖ En las redes internas que utilizan direcciones privadas, el firewall utiliza NAT para que los hosts de la red interior puedan acceder al exterior.
- ❖ Operan ocultando direcciones de la red (por ejemplo NAT)
- ❖ Previenen conexiones directas entre redes.



# PROXY SERVERS

---

- ❖ Operan a nivel de aplicación y pueden examinar el contenido de la aplicación
- ❖ El proxy server actúa como un intermediario para el cliente





# HYBRID FIREWALLS

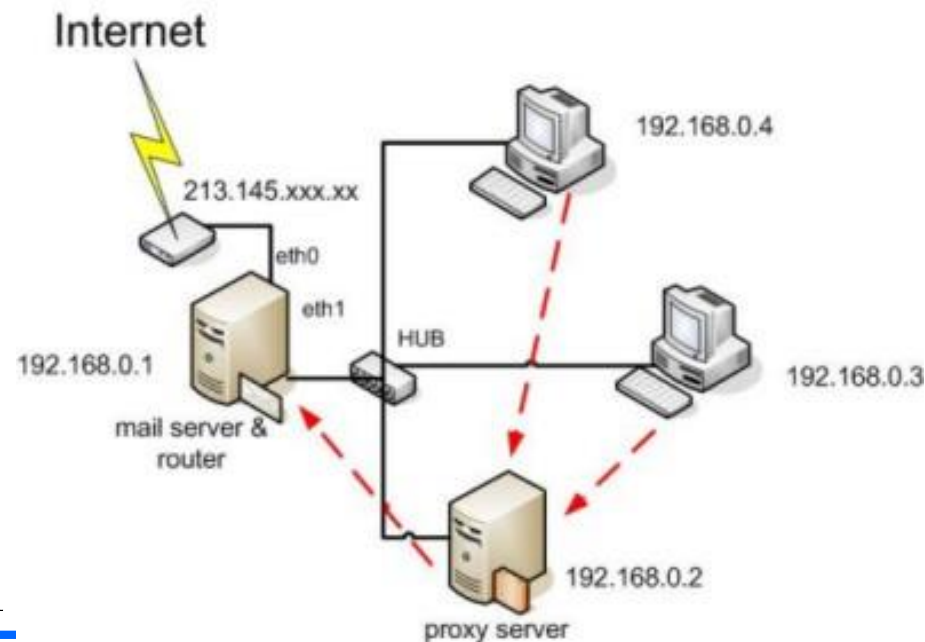
---

- Hybrid firewalls:
    - Mezcla de firewalls
  - Añadidos en los Firewalls:
    - User authentication (e.g. certificates)
    - Firewall-to-firewall encryption (e.g. VPNs since the firewall acts as a VPN end-point)
    - Content screen devices (virus scanning, URL screening)
    - Flow control to deliver QoS (e.g limit the amount of network bandwidth per connection)
-

# FUNCIONALIDADES ADICIONALES EN LOS FIREWALLS

---

- ❖ Autenticación de usuarios ( certificados)
- ❖ Encriptación Firewall-a-firewall (en VPNs donde el firewall actúa como un punto final VPN)
- ❖ Detección Content screen devices (virus scanning, URL screening)
- ❖ Control de flujo a entregar QoS (limita la cantidad de ancho de banda por conexión).



# INTRODUCCIÓN NAT

---

- ❖ NAT es una de las soluciones que ha evitado el colapso del direccionamiento IPv4 de Internet.
  - ❖ Otras soluciones que han evitado la escasez de direcciones IPv4:
    - Introducción de la máscara en las tablas routing
    - La división en subredes (1985-Subnetting)
    - La división en subredes de longitud variable (1987-VLSM)
    - El enrutamiento interdominio sin clase (1993-CIDR)
    - Las direcciones IP privadas
    - La traducción de direcciones de red (NAT)
-

# DIRECCIONES IP PRIVADAS

---

- ❖ Son direcciones útiles para terminales o hosts de la parte interna de la red, que no tienen direcciones públicas.
- ❖ Son direcciones reservadas para que cualquiera las utilice de forma interna.
- ❖ Los paquetes que contienen a estas direcciones no son enrutables a través de Internet.

| Clase | Prefijo CIDR   | Rango                         |                         |
|-------|----------------|-------------------------------|-------------------------|
| A     | 10.0.0.0/8     | 10.0.0.0 - 10.255.255.255     | 1 dirección clase A     |
| B     | 172.16.0.0/12  | 172.16.0.0 - 172.31.255.255   | 16 direcciones clase B  |
| C     | 192.168.0.0/16 | 192.168.0.0 - 192.168.255.255 | 256 direcciones clase C |

---

# INTRODUCCIÓN NAT

---

- ❖ NAT (Network Address Translation) (RFC 1631)
- ❖ NAT es un software especializado que se ejecuta en un firewall o router fronterizo
- ❖ Permite la conservación de direcciones IP públicas asignadas a grandes redes, permitiendo la utilización de direcciones IP privadas en sus redes internas.
- ❖ NAT realiza la traducción de direcciones privadas internas a direcciones IP públicas para poder acceder a internet desde una intranet
- ❖ El mecanismo debe ser transparente a los usuarios finales
- ❖ Compatibilidad con firewalls y con seguridad en Internet

# INTRODUCCIÓN NAT

**Internet Connection Configuration**

**Configure WAN IP Settings**

Enter information provided by your ISP to configure WAN IP settings.

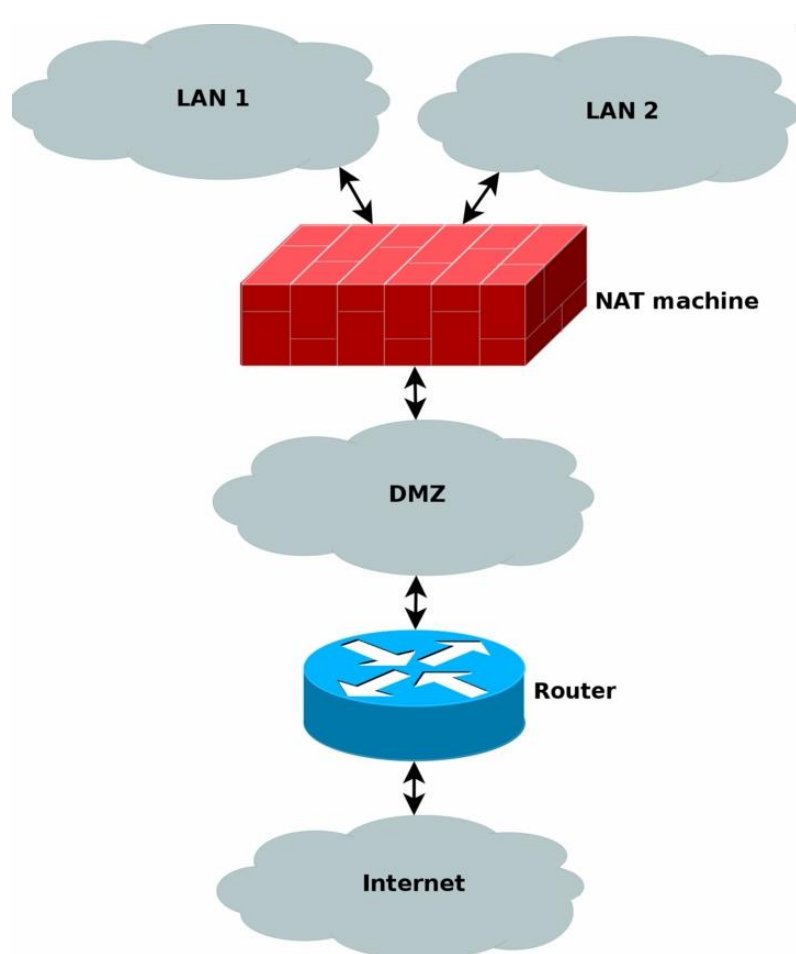
- ☒ Enable/Disable the Access Concentrator:
- ☒ Obtain an IP address automatically
- ☐ Use the following IP address: WAN IP Address:
- ☒ Enable NAT
- ☒ Add Default Route

**NAT -- Virtual Servers Setup**

Virtual Server allows you to direct incoming traffic from WAN side (identified by Protocol and External port) to the Internal server with private IP address only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum 32 entries can be configured.

| Server Name | External Port Start | External Port End | Protocol | Internal Port Start | Internal Port End | Server IP Address | Remove                   |
|-------------|---------------------|-------------------|----------|---------------------|-------------------|-------------------|--------------------------|
| emule       | 4662                | 4662              | TCP      | 4662                | 4662              | 168.192.1.3       | <input type="checkbox"/> |
| emule       | 4672                | 4672              | UDP      | 4672                | 4672              | 168.192.1.3       | <input type="checkbox"/> |
| emule       | 4661                | 4661              | TCP      | 4661                | 4661              | 168.192.1.2       | <input type="checkbox"/> |
| emule       | 4671                | 4671              | UDP      | 4671                | 4671              | 168.192.1.2       | <input type="checkbox"/> |
| Emule       | 4670                | 4670              | UDP      | 4670                | 4670              | 168.192.1.4       | <input type="checkbox"/> |
| Emule       | 4660                | 4660              | TCP      | 4660                | 4660              | 168.192.1.4       | <input type="checkbox"/> |
| AZAREUS     | 6881                | 6881              | TCP      | 6881                | 6881              | 168.192.1.2       | <input type="checkbox"/> |
| ARES        | 25140               | 25140             | TCP      | 25140               | 25140             | 168.192.1.3       | <input type="checkbox"/> |
| BITSPIRIT   | 6881                | 6881              | TCP      | 6881                | 6881              | 168.192.1.3       | <input type="checkbox"/> |

# INTRODUCCIÓN NAT



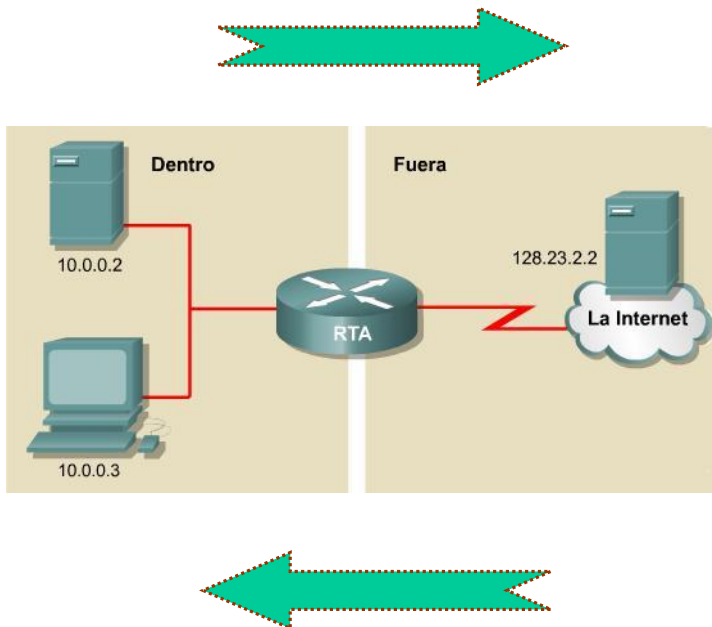
Redes internas con direccionamiento IP privado

NAT configurado en los routers fronterizos, traduce las direcciones privadas del tráfico interno enviado al exterior.

NAT permite que las empresas puedan direccionar sus hosts con direcciones privadas y tener acceso a Internet (redes públicas)  
Sin NAT los hosts privados no podrían acceder a Internet, puesto que los routers fronterizos de los ISP lo impedirían

# PROCESO NAT

NAT se compone de dos procesos:

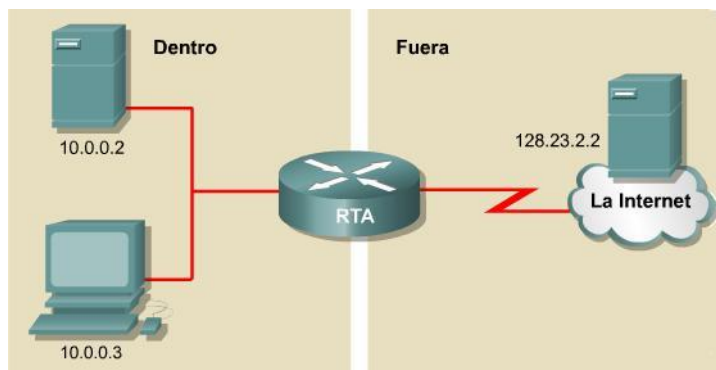


❖ Un paquete se enruta hacia fuera de su red privada. Se traduce su **dirección IP fuente privada** por una dirección IP pública enrutable, contratada con el ISP.

❖ Un paquete entra en la red privada en respuesta a datagramas anteriores. Se traduce su **dirección IP destino pública** a una dirección interna privada para su entrega dentro de la red.



# PROCESO NAT



Red privada interna = 10.0.0.0

Las estaciones no pueden acceder a Internet con estas direcciones, puesto que los routers fronterizos impiden que el tráfico privado se envíe al exterior.

IP router proporcionada ISP = 83.45.66.3

1) Dentro → Internet (Traducción en la fuente)

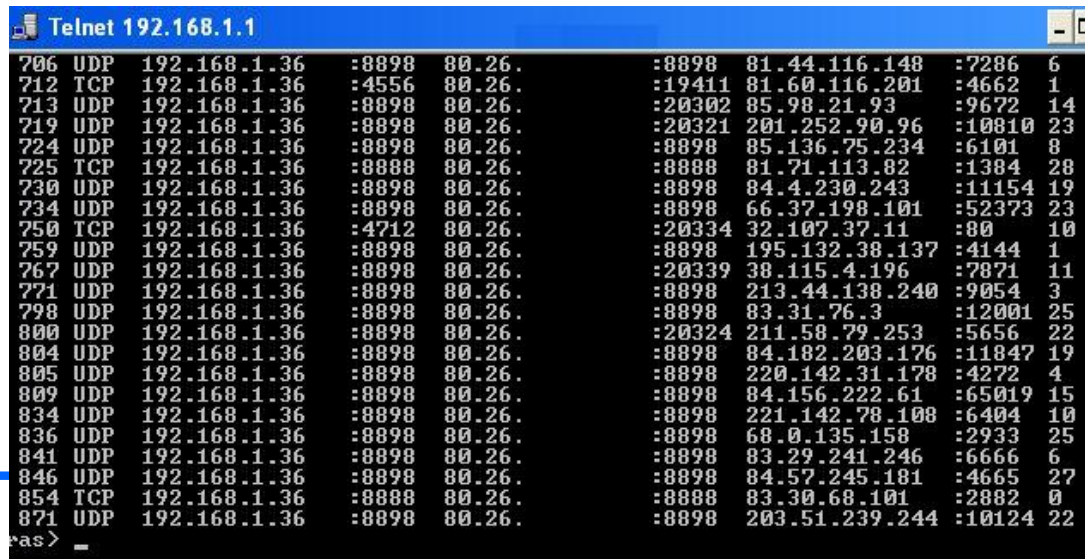
|                |                   |            |         |
|----------------|-------------------|------------|---------|
| Dentro → RTA   | 10.0.0.2          | 128.23.2.2 | Payload |
| RTA → Internet | <b>83.45.66.3</b> | 128.23.2.2 | Payload |

2) Internet → Dentro (Traducción en el destino)

|                |            |                 |         |
|----------------|------------|-----------------|---------|
| Internet → RTA | 128.23.2.2 | 83.45.66.3      | Payload |
| RTA → Dentro   | 128.23.2.2 | <b>10.0.0.2</b> | Payload |

# TABLA NAT

- ❖ El router mantiene una Taula NAT con las direcciones privadas y sus correspondientes direcciones públicas asignadas
- ❖ Una entrada en la tabla NAT está activa mientras la conexión está activa.



The image shows a Telnet session window titled "Telnet 192.168.1.1". The window displays a list of NAT table entries. Each entry consists of a sequence number, a protocol (UDP or TCP), a local IP address, a local port, an outside IP address, an outside port, and a timeout value.

| Seq | Protocol | Local IP     | Local Port | Outside IP | Outside Port | Timeout                  |
|-----|----------|--------------|------------|------------|--------------|--------------------------|
| 706 | UDP      | 192.168.1.36 | :8898      | 80.26.     | :8898        | 81.44.116.148 :7286 6    |
| 712 | TCP      | 192.168.1.36 | :4556      | 80.26.     | :19411       | 81.60.116.201 :4662 1    |
| 713 | UDP      | 192.168.1.36 | :8898      | 80.26.     | :20302       | 85.98.21.93 :9672 14     |
| 719 | UDP      | 192.168.1.36 | :8898      | 80.26.     | :20321       | 201.252.90.96 :10810 23  |
| 724 | UDP      | 192.168.1.36 | :8898      | 80.26.     | :8898        | 85.136.75.234 :6101 8    |
| 725 | TCP      | 192.168.1.36 | :8888      | 80.26.     | :8888        | 81.71.113.82 :1384 28    |
| 730 | UDP      | 192.168.1.36 | :8898      | 80.26.     | :8898        | 84.4.230.243 :11154 19   |
| 734 | UDP      | 192.168.1.36 | :8898      | 80.26.     | :8898        | 66.37.198.101 :52373 23  |
| 750 | TCP      | 192.168.1.36 | :4712      | 80.26.     | :20334       | 32.107.37.11 :80 10      |
| 759 | UDP      | 192.168.1.36 | :8898      | 80.26.     | :8898        | 195.132.38.137 :4144 1   |
| 767 | UDP      | 192.168.1.36 | :8898      | 80.26.     | :20339       | 38.115.4.196 :7871 11    |
| 771 | UDP      | 192.168.1.36 | :8898      | 80.26.     | :8898        | 213.44.138.240 :9054 3   |
| 798 | UDP      | 192.168.1.36 | :8898      | 80.26.     | :8898        | 83.31.76.3 :12001 25     |
| 800 | UDP      | 192.168.1.36 | :8898      | 80.26.     | :20324       | 211.58.79.253 :5656 22   |
| 804 | UDP      | 192.168.1.36 | :8898      | 80.26.     | :8898        | 84.182.203.176 :11847 19 |
| 805 | UDP      | 192.168.1.36 | :8898      | 80.26.     | :8898        | 220.142.31.178 :4272 4   |
| 809 | UDP      | 192.168.1.36 | :8898      | 80.26.     | :8898        | 84.156.222.61 :65019 15  |
| 834 | UDP      | 192.168.1.36 | :8898      | 80.26.     | :8898        | 221.142.78.108 :6404 10  |
| 836 | UDP      | 192.168.1.36 | :8898      | 80.26.     | :8898        | 68.0.135.158 :2933 25    |
| 841 | UDP      | 192.168.1.36 | :8898      | 80.26.     | :8898        | 83.29.241.246 :6666 6    |
| 846 | UDP      | 192.168.1.36 | :8898      | 80.26.     | :8898        | 84.57.245.181 :4665 27   |
| 854 | TCP      | 192.168.1.36 | :8888      | 80.26.     | :8888        | 83.30.68.101 :2882 0     |
| 871 | UDP      | 192.168.1.36 | :8898      | 80.26.     | :8898        | 203.51.239.244 :10124 22 |

The prompt "as>" is visible at the bottom left of the window.

# TIPOS TRADUCCIONES NAT

---

| CISCO                 |                 |
|-----------------------|-----------------|
| NAT estático          | Para servidores |
| NAT Dinámico          | Para hosts      |
| NAT por puertos (PAT) | Para hosts      |

| LINUX      |                         |
|------------|-------------------------|
| DNAT       | Para servidores         |
| SNAT (PAT) | Para hosts o terminales |

---

# NAT ESTÁTICO

---

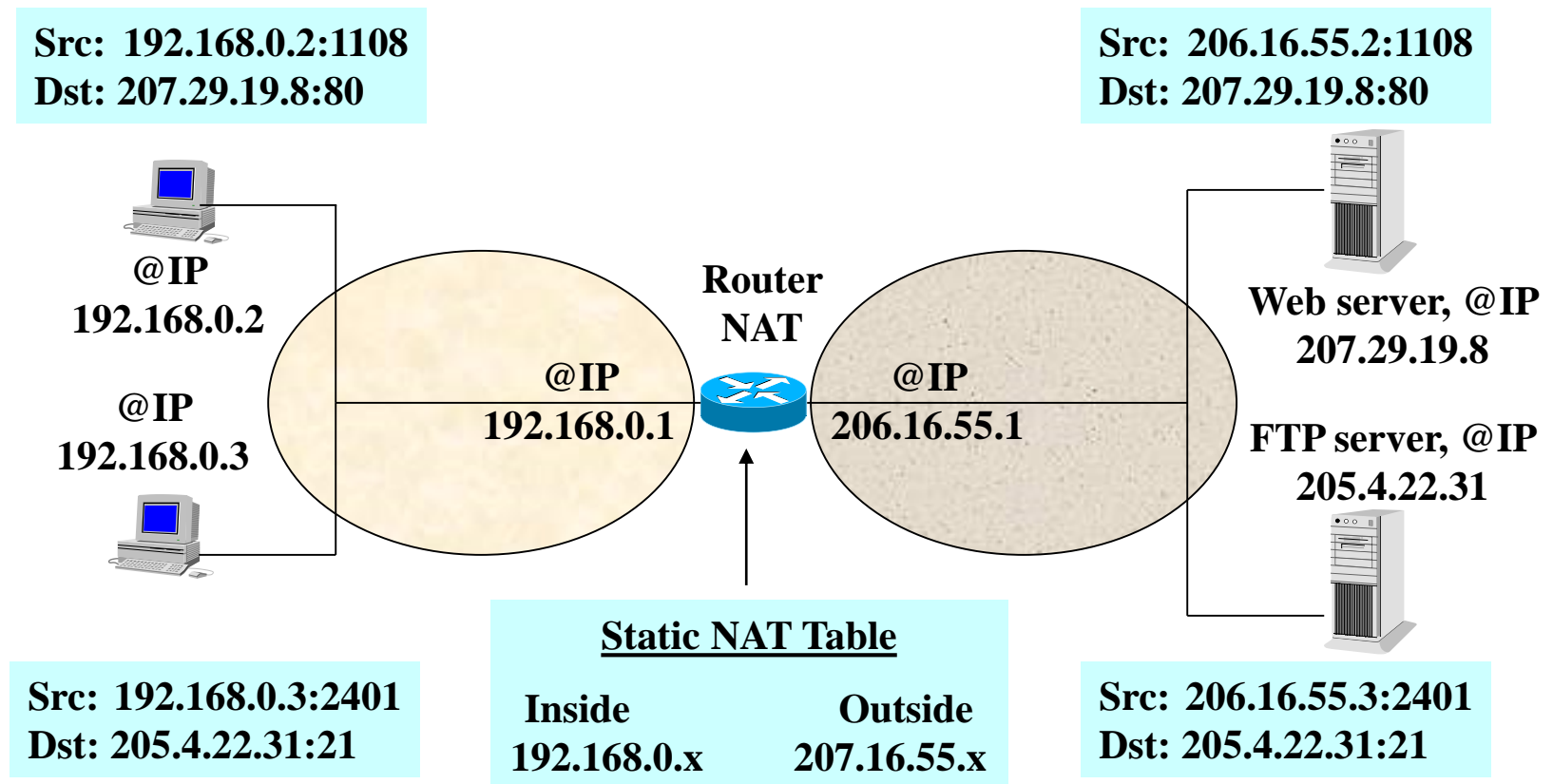
- ❖ Permite una asociación fija y única entre una @ privada interna y una @ pública global en el router.
- ❖ Permite publicar la @ privada interna de un servidor en el router para que pueda ser accedido desde el exterior.

| @ Local origen | @ Pública origen |
|----------------|------------------|
|----------------|------------------|

- Es útil para servidores de empresas o dispositivos de networking que deban tener una dirección fija que sea accesible desde Internet.
- Se necesitan tantas @ públicas como servidores queremos que puedan ser accedidos desde Internet.

# NAT ESTÁTICO

- NAT estático:** consiste en substituir la parte de host de la @IP privada en el host de la @IP pública



# NAT ESTÁTICO EN CISCO

---



**R#** configure terminal

**R(config)#** ip nat inside source static 10.1.1.1 198.3.4.1

**R(config)#** interface e0

**R(config-if)#** ip nat inside

**R(config-if)#** exit

**R(config)#** interface s0

**R(config-if)#** ip nat outside

**R(config-if)#** exit

**R(config)#** exit

---

# NAT DINÁMICO

---

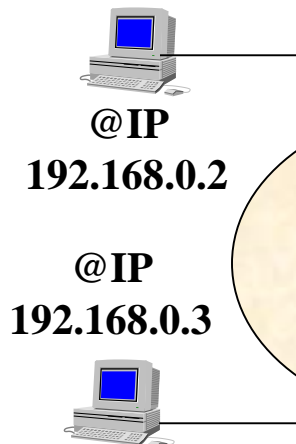
- ❖ Permite asignar a cada @ privada interna, una dirección de entre un conjunto (pool) de direcciones IP públicas, que no esté en uso (asignación dinámica).
- ❖ Cuando un host deja de acceder a Internet, otro puede reutilizar la misma @ pública.
- ❖ La asignación de una IPnat depende de las @ disponibles dentro del pool. Será totalmente diferente en cada conexión individual.
- ❖ Es normal utilizar un pool con menos direcciones que el número de máquinas a conectar. Cuando se utilizan todas las IPnat, la siguiente petición es rechazada por parte del router NAT.

# NAT DINAMICO

- **NAT dinámico (Por pool de @IP):**
  - tenemos un pool de direcciones públicas y asignamos @IP privada con @IP pública

Src: 192.168.0.2:1108  
Dst: 207.29.19.8:80

Src: 206.16.55.2:1108  
Dst: 207.29.19.8:80



Router  
NAT

@IP  
192.168.0.1

@IP  
206.16.55.1

Web server, @IP  
207.29.19.8

FTP server, @IP  
205.4.22.31

Src: 192.168.0.3:2401  
Dst: 205.4.22.31:21

Src: 206.16.55.3:2401  
Dst: 205.4.22.31:21

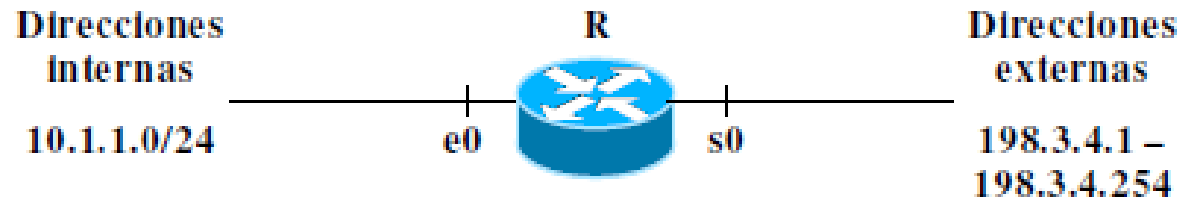
## Static NAT Table

| Inside                   | Outside     |
|--------------------------|-------------|
| 192.168.0.2              | 207.16.55.4 |
| 192.168.0.3              | 207.16.55.5 |
| Pool: 207.16.55.4 ... 15 |             |



# NAT DINÁMICO

---



```
R# configure terminal
R(config)# ip nat pool xc 198.3.4.1 198.3.4.254 netmask 255.255.255.0
R(config)# access-list 2 permit 10.1.1.0 0.0.0.255
R(config)# ip nat inside source list 2 pool xc
R(config)# interface e0
R(config-if)# ip nat inside
R(config-if)# exit
R(config)# interface s0
R(config-if)# ip nat outside
R(config-if)# exit
```

# NAT POR PUERTOS (PAT)

---

- ❖ Permite la traducción simultánea de varias direcciones IP privadas internas con una sola dirección IP pública.
- ❖ Para ello utiliza los números únicos de puerto TCP/UDP para distinguir entre las traducciones.
- ❖ En la tabla NAT se encuentra la correspondencia entre la tupla (@ privada, puerto local) y la tupla (@ pública, puerto externo).

| TABLA NAT      |                     |                  |                       |
|----------------|---------------------|------------------|-----------------------|
| @ Local origen | Puerto Local origen | @ Pública origen | Puerto externo origen |

---

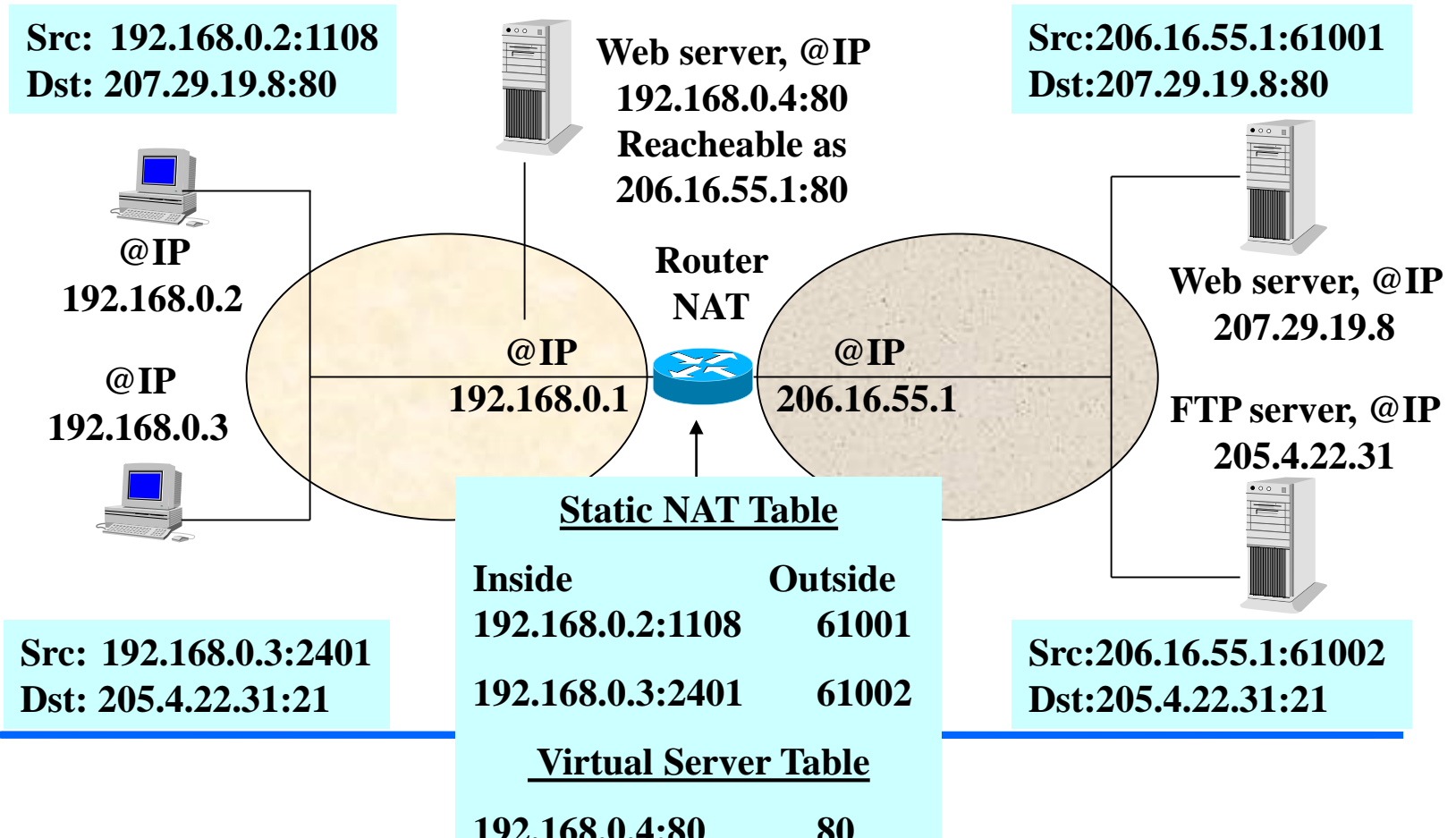
# NAT POR PUERTOS (PAT)

---

- ❖ Número total de puertos =  $2^{16} = 65.536$
  - ❖ N° máximo de puertos internos que se pueden traducir a una misma dirección externa = 4000.
  - ❖ No se usan los puertos de 0-1024. Se utilizan los puertos de rango superior (puertos efímeros).
  - ❖ PAT comienza asignando desde el 1° puerto disponible. Cuando no hay más puertos (4000), PAT utiliza la próxima dirección IP, empezando nuevamente por el primer puerto disponible.
  - ❖ Este proceso continúa hasta que no haya puertos ni direcciones IP externas disponibles.
-

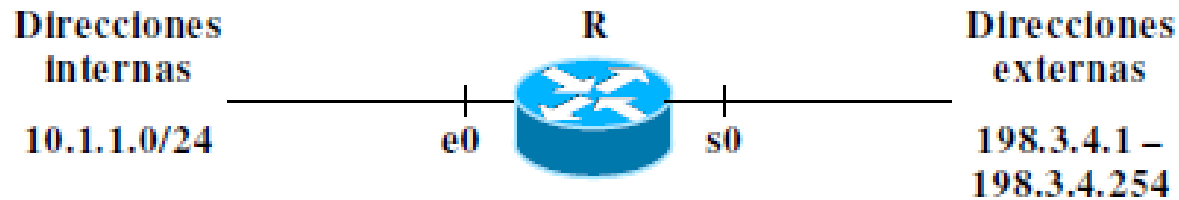
# NAT POR PUERTOS (PAT)

- **NAT dinámico (PAT: Port Address Translation):**
  - el router tiene una sólo @IP pública, y elige un nuevo puerto origen y mapea las @IP privadas a partir del puerto designado



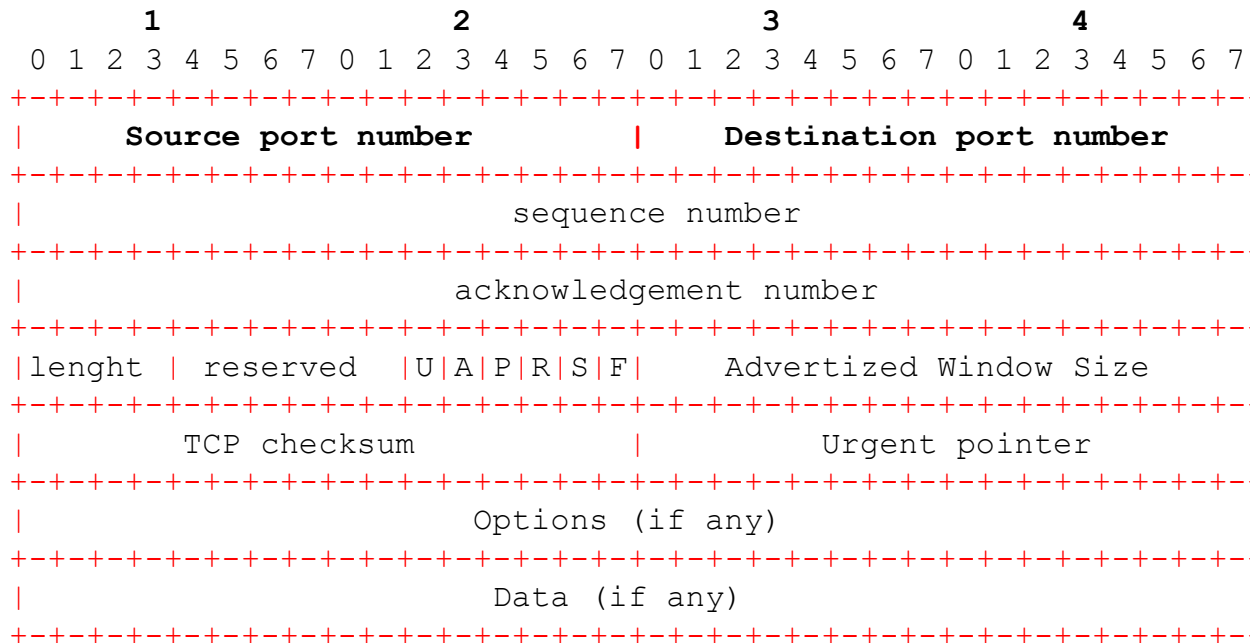
# NAT POR PUERTOS EN CISCO

---



```
R# configure terminal
R(config)# ip nat pool xc 198.3.4.1 198.3.4.254 netmask 255.255.255.0
R(config)# access-list 2 permit 10.1.1.0 0.0.0.255
R(config)# ip nat inside source list 2 pool xc overload
R(config)# interface e0
R(config-if)# ip nat inside
R(config-if)# exit
R(config)# interface s0
R(config-if)# ip nat outside
R(config-if)# exit
```

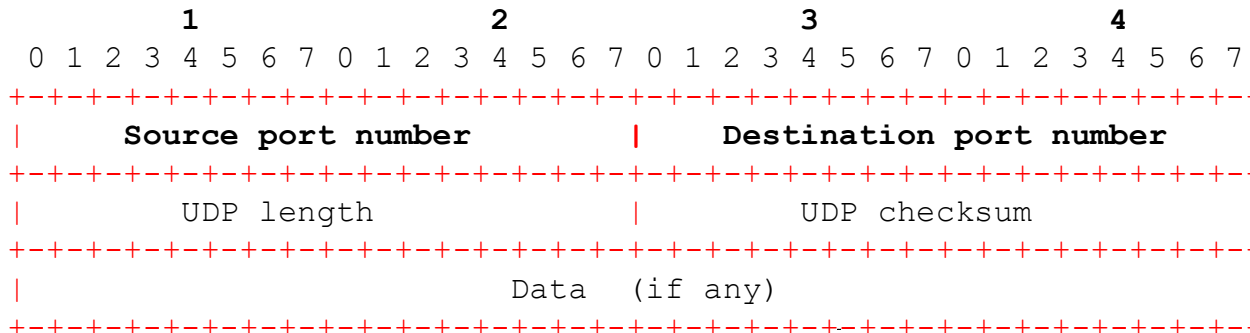
# NAT POR PUERTOS (PAT)



NAT por  
puertos es  
válido para:

TCP

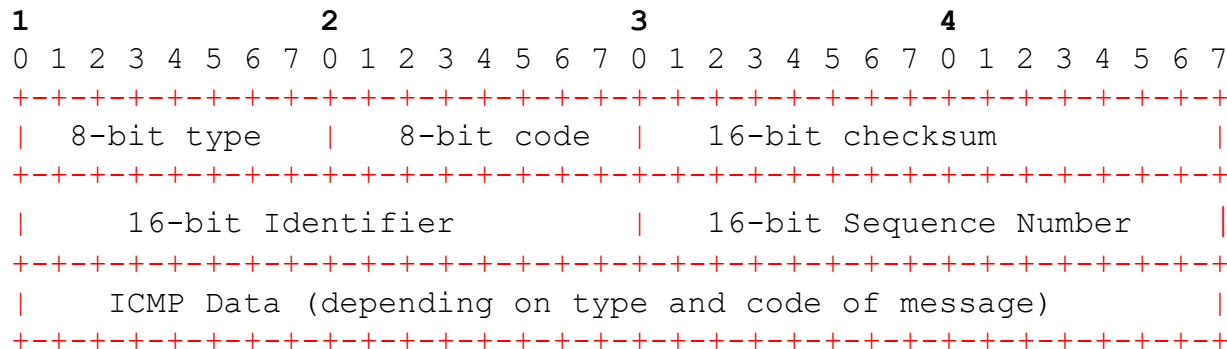
Ambos  
tienen  
puertos



UDP

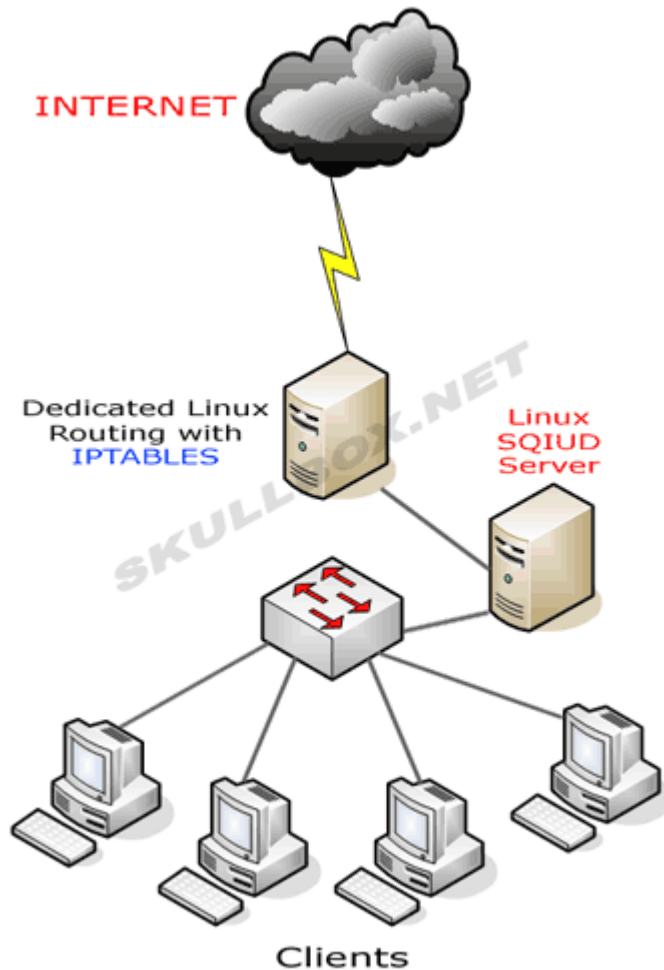
# NAT POR PUERTOS (PAT)

- ❖ ¿Cómo es que un ping puede ser traducido por PAT si no utiliza el concepto de puerto TCP/UDP?
- ❖ Los paquetes ICMP tienen el campo *identifier* que lleva un número arbitrario que sirve para relacionar *request/reply*. Este campo se utiliza en la tabla NAT de forma análoga al puerto.



## Formato mensaje ICMP Request/Replay (ping)

# NAT EN LINUX



- ❖ La comanda IPTABLES se utiliza en linux para la configuración de un *firewall*.
- ❖ IPTABLES permite realizar la programación de servicios NAT



# NAT EN LINUX

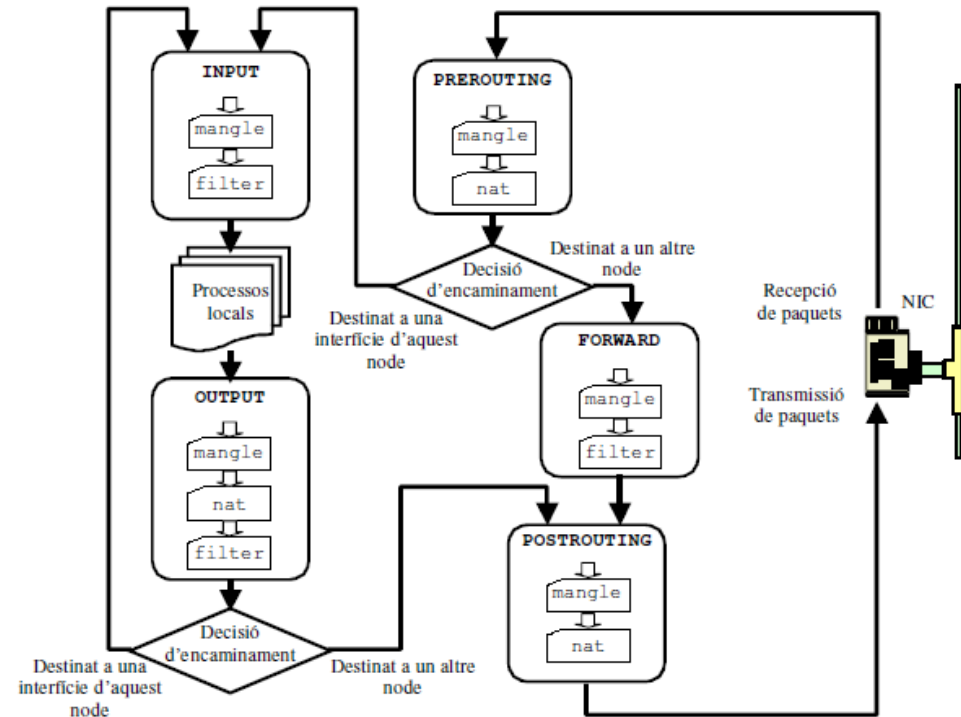
---

Existen dos modalidades:

- ❖ DNAT (Destination Network Address Translation) → Conexiones iniciadas fuera de la red. Por tanto lo primero que se hace es una traducción del destino. En CISCO este concepto se corresponde con NAT estático
- ❖ SNAT (Source Network Address Translation) → La Conexiones iniciadas dentro de la red. Este concepto en CISCO se corresponde con NAT dinámico por puertos.

# FUNCIONAMIENTO IPTABLES DE LINUX

- ❖ La comanda iptables permite agregar reglas en diferentes etapas (o *chains*) del nivel IP de la máquina linux: PREROUTING, FORWARD, POSTROUTING, INPUT y OUTPUT.
- ❖ Cuando un paquete atraviesa una de estas etapas, el nivel IP examina qué reglas se ajustan al paquete para su procesamiento.
- ❖ Las reglas se almacenan en 3 tipos de tablas: mangle, filter y nat.



# NAT EN LINUX.

## EJEMPLO DNAT-NAT ESTÁTICO

---

### Etapas en el camino de routing



```
Definición de un DNAT → iptables -t nat -A  
PREROUTING -p tcp -i eth0 -d 200.10.10.5 --dport ssh  
-j DNAT --to-destination 192.168.1.2
```

Todo paquete TCP con servicio ssh que entre por la interficie eth0 con destino 200.10.10.5, se traducirá esa dirección destino por la dirección 192.168.1.2, que es la dirección interna privada del servidor ssh.

200.10.10.5 → Dirección pública externa del servidor ssh

192.168.1.2 → Dirección privada interna del servidor ssh

---

# NAT EN LINUX.

## EJEMPLO SNAT- PAT

---

### Etapas en el camino de routing



Definición de un SNAT → `iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 200.10.10.5`

Todo paquete que salga por la interficie eth0, se le traducirá su dirección privada origen por la dirección pública 200.10.10.5 para que pueda circular por Internet

# VENTAJAS NAT

---

- ❖ Permite ahorrar @ IP públicas.
  - ❖ Es más económico porque se contratan menos @ al ISP.
  - ❖ Añade seguridad a la red: La entrada/salida de la red está controlada por el router NAT. Los ordenadores de la red local no son vistos desde la red externa o Internet.
  - ❖ NAT y el uso de direcciones privadas elimina la necesidad de reasignar nuevas direcciones cuando se cambia a un nuevo ISP, ahorrando tiempo y dinero.
  - ❖ El mecanismo NAT es transparente para ambos sistemas (usuario y servidor).
  - ❖ Compatibilidad de NAT con firewalls y con seguridad en Internet.
-

# DESVENTAJAS NAT

---

- ❖ NAT aumenta el retardo de los routers. Se introducen retardos en la conmutación de rutas debido a la traducción de @ IP.
- ❖ Además como NAT modifica cabecera IP habrá que recalcular el checksum IP y el encabezado TCP también.
- ❖ Pérdida de la posibilidad de rastreo IP de extremo a extremo. Difícil rastrear paquetes que sufren cambios en la dirección del paquete al atravesar saltos NAT. Esto dificulta la labor de los hackers.
- ❖ NAT causa una pérdida en la funcionalidad en aplicaciones que impliquen el envío de información de @ IP dentro de los datos del paquete IP (IP embebidas).

# PROTOCOLOS SENSIBLES A NAT

---

- NAT modifica cabecera IP → recalcular el checksum IP y TCP
- Protocolos que llevan embebida la @IP → también debe ser modificada → ALG (Application-Level Gateway)
  - ICMP: "Destination unreachable messages" llevan @IP embebidas
  - Comandos FTP llevan @IP embebidas como "strings" (cambiarlas además implica que cambia la longitud del segmento TCP)
  - SNMP (Simple Network Management Protocol)
  - NetBIOS over TCP/IP (NBT)
  - NAT + Firewalls + IPsec
  - DNS, Kerberos, X-Windows, remote-shell, SIP, ... (ver Internet Draft "Protocol Complications with the IP Network Address Translation")

# LISTAS DE ACCESO

---

- ❖ Los Routers se sirven de listas de control de acceso (ACL) para identificar/filtrar el tráfico que pasa por sus interfícies.
  - ❖ Una ACL se puede definir por cada interfície (eth0, s0), protocolo (IP, IPX) y sentido (entrada/salida).
  - ❖ Permite filtrar según los parámetros:
    - Direcciones IP origen o destino.
    - Puertos TCP/UDP origen o destino.
    - Protocolos IP: tcp, udp, icmp, ip
-



# LISTAS DE ACCESO

---

- ❖ Una ACL es un listado secuencial de condiciones de permiso o prohibición que indica el tipo paquete que podrá acceder o salir del router.
  - ❖ Si hay definida una ACL en una interficie, todos los datagramas se comparan con las reglas de esa ACL, de forma secuencial y ordenada.
  - ❖ Cuando el datagrama cumple alguna reglas, se deja de comprobar el resto y se toma la acción pertinente: aceptar o descartar el datagrama.
  - ❖ Si el datagrama no coincide con ninguna regla, existe una última regla en toda lista de acceso, una denegación implícita, que lo descartará.
-

# LISTAS DE ACCESO EN CISCO.

## ACLS ESTANDAR

---

En los routers CISCO existen muchos tipos de listas de acceso. De entre todas, las siguientes filtran paquetes IP:

❖ Estándar (1-99): Comprueban la dirección origen de los paquetes que solicitan enrutamiento.

```
Router(config)# access-list #id {deny/permit}
{@IPsource WildcardMask | host @IPsource | any}
```

→ Crea lista de acceso

```
Router(config-if)# ip access-group acl# {in | out} →
```

Asigna la acl sobre la interficie deseada de entrada o de salida

---

# LISTAS DE ACCESO EN CISCO.

## ACLs EXTENDIDAS

---

❖ Extendidas (100-199): Permiten comprobar la dirección origen, destino, protocolos específicos, y números de puertos de cada paquete.

```
Router(config)# access-list #id {deny/permit}  
protocol {ip/tcp/icmp/udp}  
{@IPsource WildcardMask | host @IPsource | any}  
{@IPdest WildcardMask | host @IPdest | any}  
[{eq/geq/leq/gt} portdest] → Crea lista de acceso
```

```
Router(config-if)# ip access-group acl# {in | out}
```

---

# LISTAS DE ACCESO EN CISCO.

## CONCEPTO DE WILDCARD

---

- ❖ La wildcard mask es una mascara especial de 32 bits que usada en la definición de las listas de acceso de los routers CISCO.
  - ❖ Identifica los bits de una @ IP han de ser verificados por una ACL
  - ❖ Sirve para crear filtros: decidir que direcciones IP son aceptadas o rechazadas.
  - ❖ La Wildcard funciona al revés de la máscara IP:
    - "0" indica que hay que comprobar el bit correspondiente en la dirección IP.
    - "1" indica que el bit puede ser ignorado.
-

# LISTAS DE ACCESO EN CISCO.

## EJEMPLOS DE WILDCARD

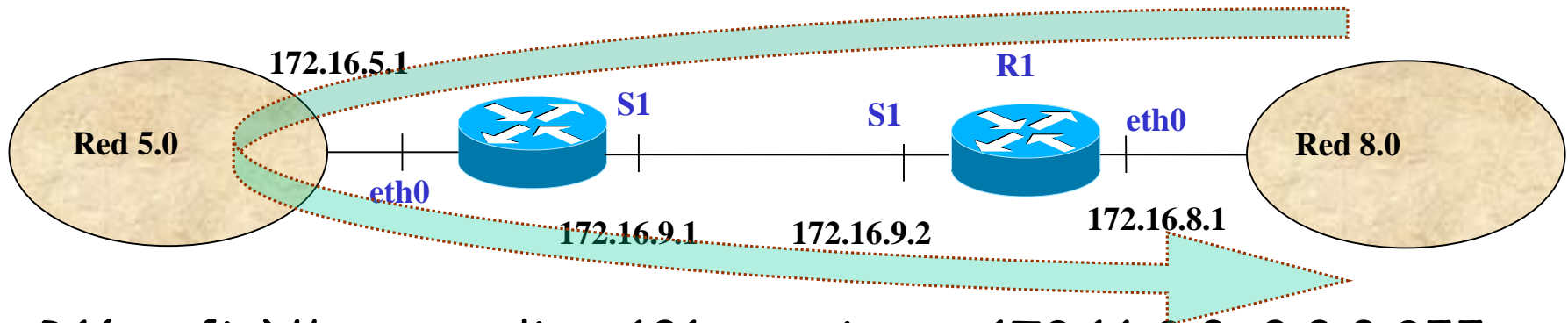
---

- ❖ Red clase C: 192.34.16.0 /24 → Wildcard Mask:  
**0.0.0.255**
  - ❖ Casos especiales:
    - ❖ Host en concreto 145.34.5.6 → Wildcard Mask:  
0.0.0.0 (Se comprobarán todos los bits de la @IP).  
Se puede substituir la tupla @IP wildcardmask por  
**host 145.34.5.6**
    - ❖ Cualquier host → Wildcard Mask:  
255.255.255.255 (No se comprobará ningún bit).  
Se puede substituir la tupla @IP wildcardmask por  
**any**
-

# LISTAS DE ACCESO EN CISCO.

## EJEMPLO

Aceptar conexiones web desde la red 8 al servidor 172.16.5.32 y denegar el acceso a la red 8 de cualquier otro servicio IP.



```
R1(config)# access-list 101 permit tcp 172.16.8.0 0.0.0.255  
172.16.5.32 0.0.0.0 eq 80  
→ En eth0 in o S1 out  
R1(config)# access-list 102 permit tcp 172.16.5.32 0.0.0.255  
172.16.8.0 0.0.0.0 gt 1023  
→ En eth0 out o S1 in
```

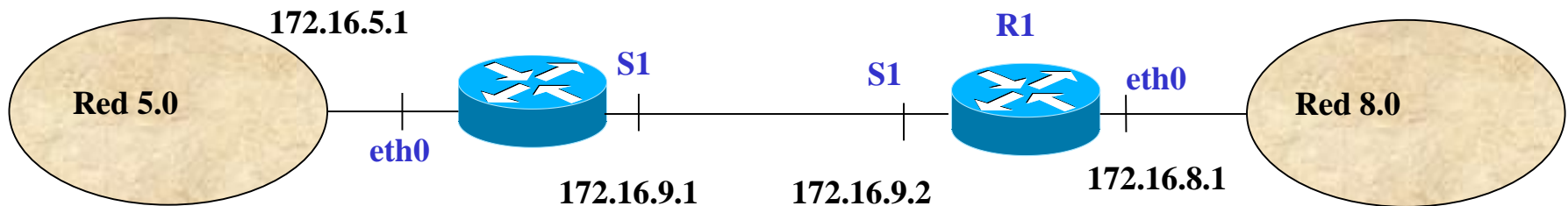
# LISTAS DE ACCESO EN CISCO.

## EJEMPLO

La denegación implícita de las últimas líneas de las listas de acceso 101 y 102 nos asegura que cualquier otro tipo de tráfico diferente al que se ha especificado va a poder ser denegado. No va a ser posible que desde el exterior accedan a cualquier otro servicio de la red 8.

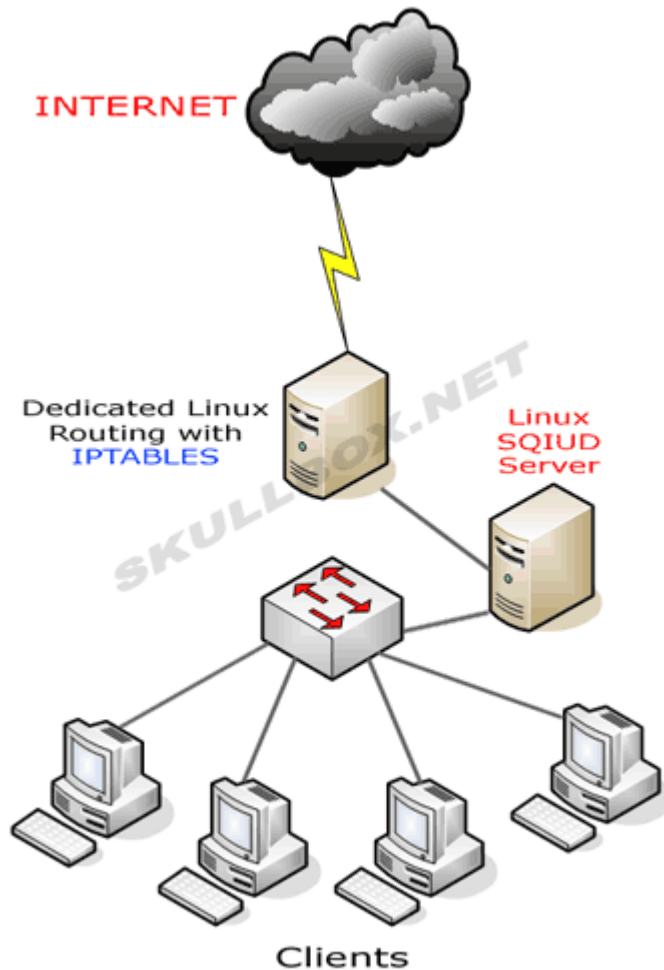
```
R1(config)# access-list 101 deny any any  
R1(config)# access-list 102 deny any any
```

} No son necesarias



# FIREWALL EN LINUX

---



❖ La comanda IPTABLES se utiliza en linux para la configuración de un *firewall*.

❖ IPTABLES permite realizar la programación de Listas de Acceso

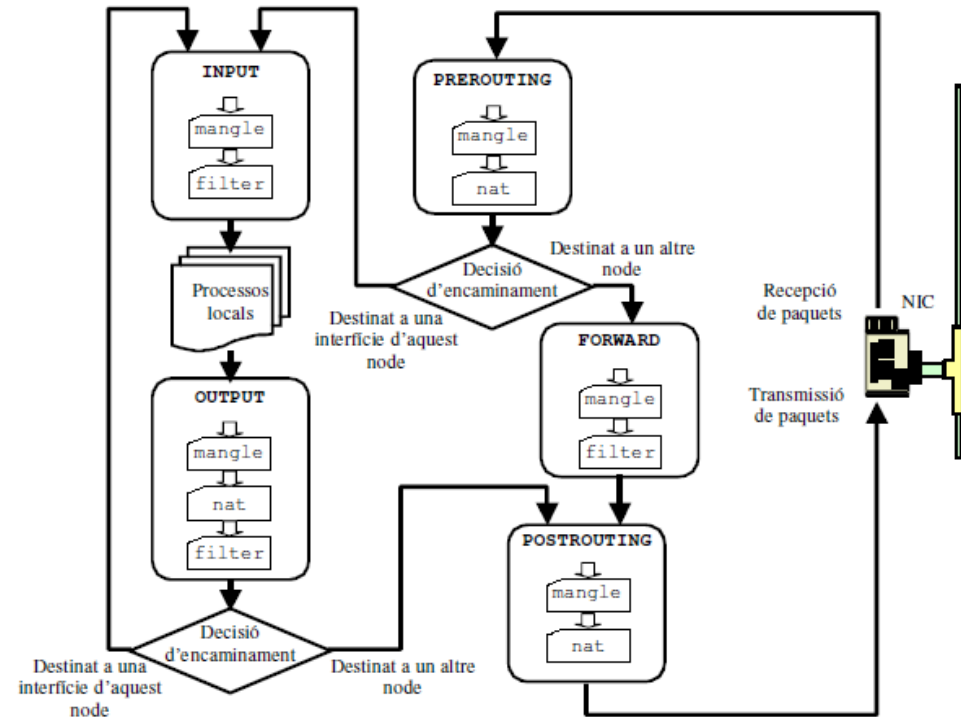


# FUNCIONAMIENTO IPTABLES DE LINUX

❖ La comanda iptables permite agregar reglas en diferentes etapas (o *chains*) del nivel IP de la máquina linux: PREROUTING, FORWARD, POSTROUTING, INPUT y OUTPUT.

❖ Cuando un paquete atraviesa una de estas etapas, el nivel IP examina qué reglas se ajustan al paquete para su procesamiento.

❖ Las reglas se almacenan en 3 tipos de tablas: mangle, filter y nat.



# LISTAS DE ACCESO EN LINUX.

## EJEMPLO

---

### Etapas en el camino de routing



Definición de reglas ACL →

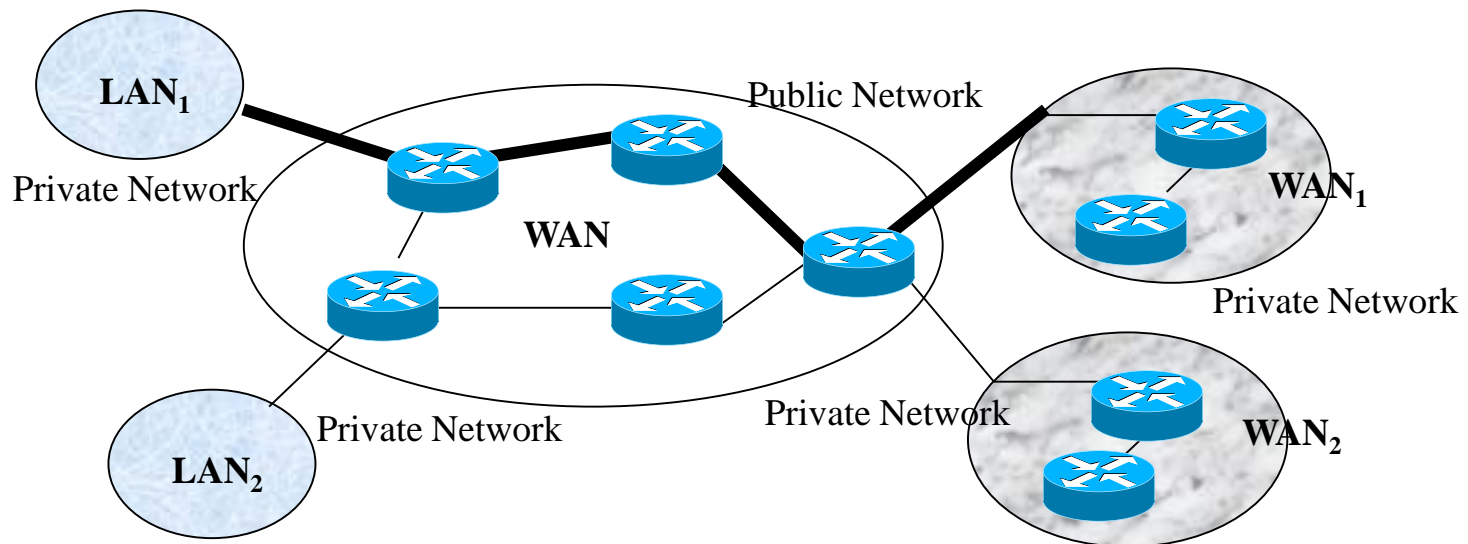
```
iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT
```

```
iptables -A FORWARD -i eth0 -o eth1 -m state -state  
ESTABLISHED,RELATED -j ACCEPT
```

Se permite el paso de todo paquete que entra por eth0 y sale por eth1.  
Se permite el paso de todo paquete que entra por eth1 y sale por eth0  
siempre que sea una conexión ya iniciada o establecida.

# VPN

- Definición de VPN (Virtual Private Network):
  - ◇ Red privada interconectadas a través de redes públicas usando líneas dedicadas semi-permanentes o permanentes (generally tunnels)
  - ◇ Circuitos Virtuales para el transporte de tráfico privado donde el circuito virtual es una conexión entre dos dispositivos tal que la ruta y el ancho de banda son asignados dinámicamente



# VPN

---

- **Construcción de VPNs:**

- VPNs convencionales

- *WANs dedicadas*: usa líneas dedicadas de una red pública WAN (FR, ATM, ...) usando PVCs (Permanent Virtual Circuits)
    - *Dial Networks*: permite conexiones bajo demanda usando PSTN
    - Los circuitos virtuales son dependientes de la tecnología (ATM o FR) y puede ofrecer QoS dependiendo de la tecnología
    - No usan Internet: alto coste debido al alquiler de las líneas dedicadas

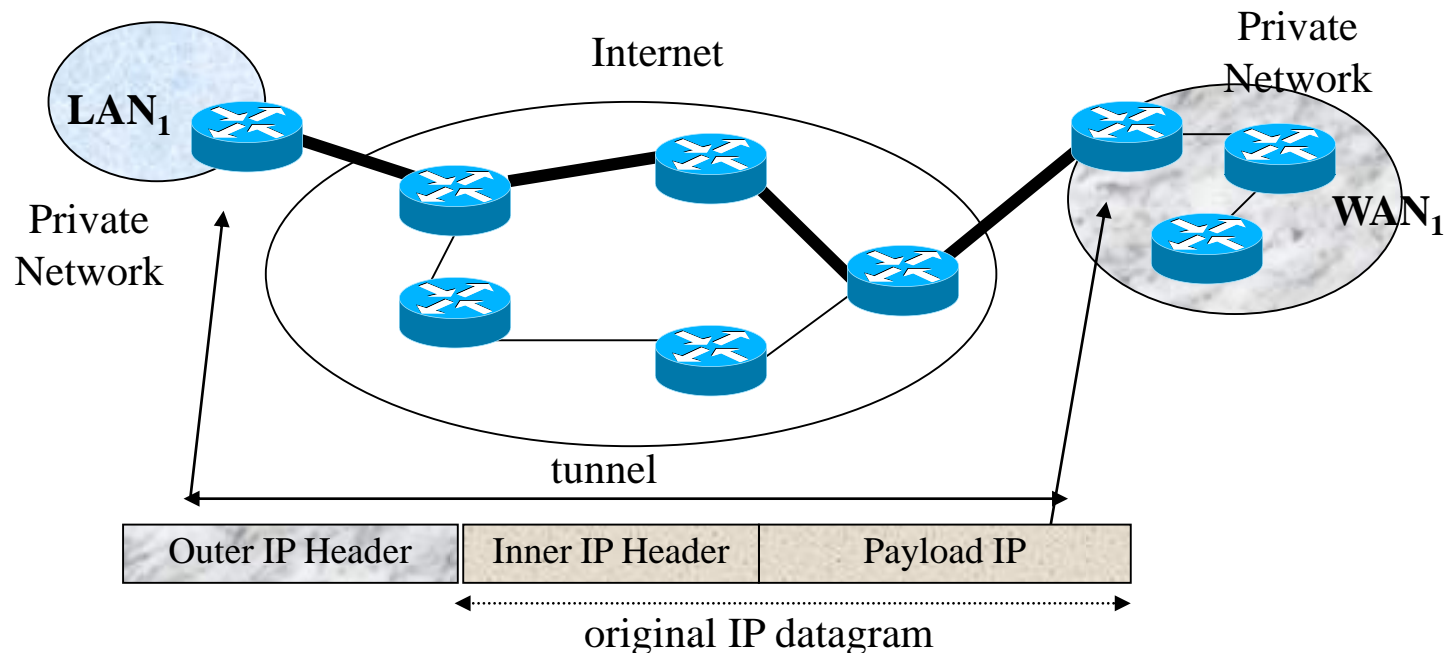
- Internet VPNs

- El contenido del circuito VPN es independiente del backbone IP
    - contrato del VPN usando una ISP que te asigna una/varias @IP o una Intranet con @IP privadas + NAT para acceder a Internet
    - El circuito virtual no puede depender de la tecnología → necesita que el protocolo IP esconda la tecnología de nivel de enlace ("Tunneling")

- 
- Posibles requisitos: seguridad (e.g. IPsec) y QoS

# TUNNELING

- Técnica que esconde la tecnología de nivel inferior, proporcionando un circuito virtual enrutable en Internet entre dos puntos de red (Edge points)
- El backbone IP se usa como si fuese una tecnología de nivel de enlace (point-to-point link)



# TUNNELING

---

- **IP-within IP (RFC 2003)**
  - IP outer header considerations
    - **ToS:** copied from inner header
    - **DF flag:**
      - **If set in the inner header:** then is set in the outer header
      - **If NOT set in the inner header:** then may or may not be set in the outer header
    - **TTL:** set to an appropriate value for the tunnel
      - The inner TTL is NOT decremented
      - The inner TTL is decremented in the router entry point before being encapsulated
      - The inner TTL is NOT decremented when decapsulating the datagram in the exit point
    - **Source IP address:** the address of the entry of the tunnel
    - **Destination IP address:** the address of the exit point of the tunnel
  - ICMP messages from inside the tunnel: depending on the ICMP message the entry point (encapsulator) MAY use this message to create a new ICMP message to the originator of the datagram

# TUNNELING

- **Características de las VPNs usando tuneles**
  - Multiplexa varios tuneles VPNs entre dos puntos extremos IP (VPN-ID para identificar que VPNs hay en el tunel)
  - Protocolo de señalización para establecer y negociar el tunel
  - Seguridad de los Datos: e.g IPsec (authentication and encryption)
  - Transporte Multiprotocolo (el protocolo debe ser identificado)
  - Secuenciamiento de tramas equivalente a líneas dedicadas de nivel 1 o 2
  - MTU grandes como cualquier protocolo de nivel de enlace (evitar fragmentación)
  - Minimización del overhead de la cabecera del tunnel para se capaz de llevar tráfico sensible al retardo (latencias y jitter): problemas en entornos móviles con poco ancho de banda
  - Control de flujo y de la congestión (redes con pérdidas como las redes vía radio con bajo buffering): hoy sólo se usa en canales de control y no en canales de datos
  - ~~Garantizar QoS y gestión de Tráfico (shaping, scheduling ...)~~

# TUNNELING

---

- Tuneles deben asegurar seguridad:
  - ◇ **Autenticación:** consiste en asegurar que los datos recibidos son de quien dicen ser
  - ◇ **Control de acceso:** consiste en prevenir que usuarios no autorizados accedan a la red privada
  - ◇ **Confidencialidad:** consiste en prevenir que los usuarios lean y copien datos
  - ◇ **Integridad de los datos:** consiste en estar seguro que nadie modifica los datos



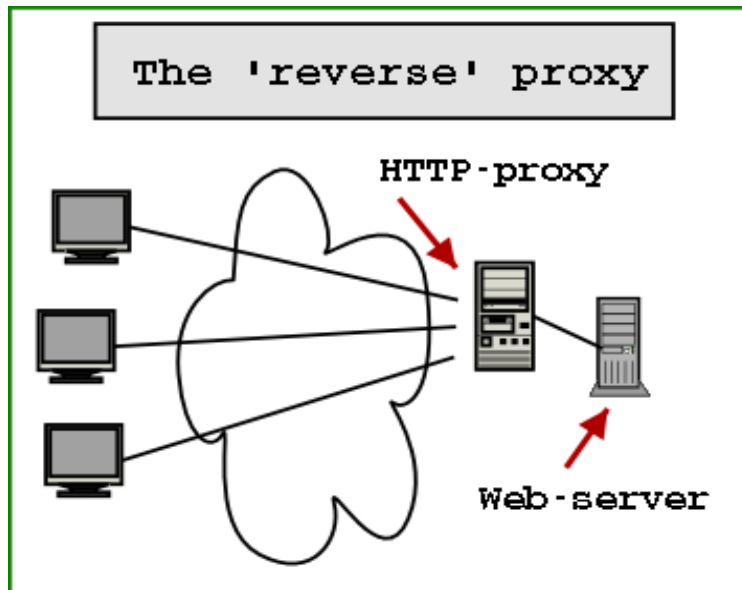
# TUNNELING

---

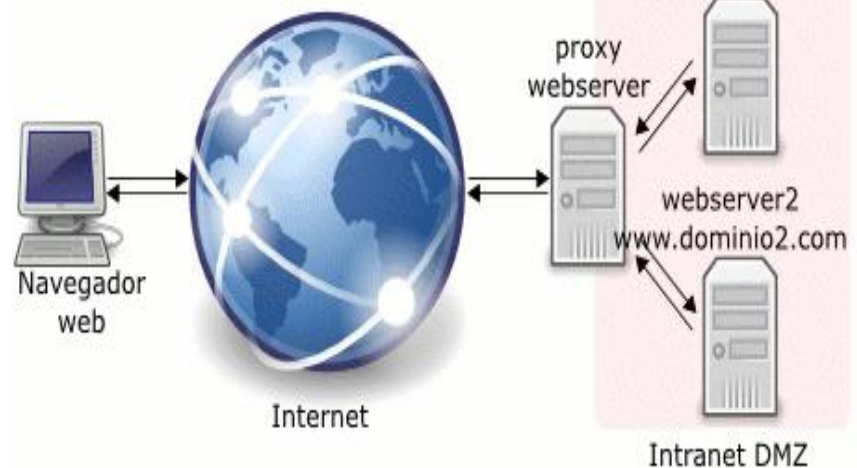
- **Protocolos de tunneling**
  - L2F (CISCO): (RFC 2341)
  - L2TP: Layer 2 Tunneling Protocol (RFC 2661)
  - PPTP: Point-to-Point Tunneling Protocol (RFC 2637)
  - GRE: Generic Routing Encapsulation (RFC 1701)
  - IP/IP: IP over IP (RFC 2003)
  - IPsec (RFC 2475)
  - MPLS: Multi-Protocol Label Switching (RFC 2917)
  - MPOA (Multi-Protocol Over ATM)

# REVERSE PROXY

Un *reverse proxy* es un servidor proxy instalado en el domicilio de uno o más servidores web. Todo el tráfico entrante de Internet y con el destino de uno de esos servidores web pasa a través del servidor proxy.



Esquema de proxy inverso http



# VENTAJAS PARA INSTALAR UN REVERSE PROXY

---

- ❖ Seguridad: el servidor proxy es una capa adicional de defensa y por lo tanto protege los servidores web.
  - ❖ Cifrado / Aceleración SSL: cuando se crea un sitio web seguro, habitualmente el cifrado SSL no lo hace el mismo servidor web, sino que es realizado por el "reverse proxy", el cual está equipado con un hardware de aceleración SSL (Security Sockets Layer).
  - ❖ Distribución de Carga: el "reverse proxy" puede distribuir la carga entre varios servidores web. En ese caso, el "reverse proxy" puede necesitar reescribir las URL de cada página web (traducción de la URL externa a la URL interna correspondiente, según en qué servidor se encuentre la información solicitada).
-

# Proxys

---

- SQUID Proxy server
- Microsoft ISA Server
- Microsoft Proxy Server

# PROXY SQUID

---

- ❖ Es un software de referencia como servidor proxy-cache de web, muy popular en Ubuntu
- ❖ Desarrollo en los años 1990, se le considera muy completo y robusto.
- ❖ Software libre bajo licencia GPL, incluido en distribuciones GNU/Linux.
- ❖ Aunque orientado principalmente a HTTP y HTTPS soporta también otros protocolos como FTP e incluso Gopher. Implementa cifrado SSL/TLS tanto en la conexión al servidor web como a los navegadores y cualquier cliente web que lo soporte.

# PROXY SQUID

---

- ❖ Mejora el rendimiento de las conexiones de empresas y particulares a Internet guardando en caché peticiones recurrentes a servidores web y DNS (caché transparente)
- ❖ Acelera el acceso a un servidor web determinado (aceleración HTTP) y la caché de consultas DNS
- ❖ Realiza filtrados de tráfico: filtración de contenido y control de acceso por IP y por usuario.
- ❖ Al iniciar Squid da origen a un número configurable (5, de modo predefinido a través del parámetro `dns_children`) de procesos de búsqueda en servidores DNS, cada uno de los cuales realiza una búsqueda única en servidores DNS, reduciendo la cantidad de tiempo de espera para las búsquedas en servidores DNS.

# PRACTICA 4: PROXY SQUID EN LINUX

---

**Paso 1.** Actualiza los paquetes de tu sistema. Todos los comandos deben ser ejecutados como el usuario root:

**sudo apt update**

**sudo apt upgrade**

**Paso 2.** Instalar el proxy Squid en Ubuntu 20.04 es fácil porque ya está disponible en los repositorios de Ubuntu 20. Confirme esto con el siguiente comando:

**sudo apt-cache policy squid**

```
marta@marta-virtual-machine:~$ sudo apt-cache policy squid
squid:
  Instalados: (ninguno)
  Candidato: 4.10-1ubuntu1.5
  Tabla de versión:
    4.10-1ubuntu1.5 500
      500 http://es.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages
      500 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages
      100 /var/lib/dpkg/status
    4.10-1ubuntu1 500
      500 http://es.archive.ubuntu.com/ubuntu focal/main amd64 Packages
```

# PRACTICA 4: PROXY SQUID EN LINUX

---

Paso 3. Instala el servidor proxy squid a través de aptitude:

**sudo apt install squid**

```
marta@marta-virtual-machine:~$ sudo apt install squid
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  libdbi-perl libecap3 squid-common squid-langpack
Paquetes sugeridos:
  libclone-perl libmldbm-perl libnet-daemon-perl
  libsql-statement-perl squidclient squid-cgi squid-purge
  resolvconf smbclient winbind
Se instalarán los siguientes paquetes NUEVOS:
  libdbi-perl libecap3 squid-common squid-langpack
0 actualizados, 5 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 3.670 kB de archivos.
Se utilizarán 15,7 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Paso 4. Comprueba el comando del paso 2:

```
marta@marta-virtual-machine:~$ sudo apt-cache policy squid
squid:
  Instalados: 4.10-1ubuntu1.5
  Candidato: 4.10-1ubuntu1.5
  Tabla de versión:
  *** 4.10-1ubuntu1.5 500
    500 http://es.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages
    500 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages
    100 /var/lib/dpkg/status
  4.10-1ubuntu1 500
    500 http://es.archive.ubuntu.com/ubuntu focal/main amd64 Packages
```



# PRACTICA 4: PROXY SQUID EN LINUX

---

## Paso 5. Comprueba el estado del proxy Squid:

```
marta@marta-virtual-machine:~$ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: active (running) since Sun 2022-03-06 15:41:21 CET; 8min ago
     Docs: man:squid(8)
  Main PID: 12985 (squid)
    Tasks: 4 (limit: 2173)
   Memory: 15.5M
    CGroup: /system.slice/squid.service
            └─12985 /usr/sbin/squid -sYC
              └─12987 (squid-1) --kid squid-1 -sYC
                └─13015 (logfile-daemon) /var/log/squid/access.log
                  └─13019 (pingr)
```

## Paso 6. Para el servicio del proxy y comprueba de nuevo su estado:

**sudo systemctl stop squid**      **sudo systemctl enable squid**  
**sudo systemctl status squid**

```
marta@marta-virtual-machine:~$ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
   Active: deactivating (stop-sigterm) since Sun 2022-03-06 15:50:26 CET; 21s ago
     Docs: man:squid(8)
  Main PID: 12985 (squid)
    Tasks: 3 (limit: 2173)
   Memory: 15.1M
    CGroup: /system.slice/squid.service
            └─12985 /usr/sbin/squid -sYC
              └─12987 (squid-1) --kid squid-1 -sYC
                └─13015 (logfile-daemon) /var/log/squid/access.log
```

# PRACTICA 4: PROXY SQUID EN LINUX

---

**Paso 7.** El archivo de configuración del proxy predeterminado de Squid se encuentra en `/etc/squid/squid.conf`. El archivo ya tiene una serie de configuraciones que funcionan al mínimo, pero podemos modificarlas según nuestras preferencias. Primero, crea una copia de seguridad del archivo original.

**`sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.orig`**

```
marta@marta-virtual-machine:~$ cd /etc/squid/  
marta@marta-virtual-machine:/etc/squid$ ls  
conf.d  errorpage.css  squid.conf  squid.conf.orig
```

**Paso 8.** Ahora podemos realizar nuestra configuración personalizada en `/etc/squid/squid.conf` → **`sudo nano /etc/squid/squid.conf`**

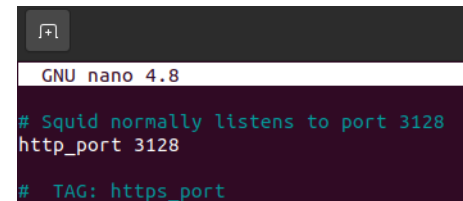
```
marta@marta-virtual-machine: /etc/squid  
GNU nano 4.8 squid.conf  
# WELCOME TO SQUID 4.10  
# -----  
#  
# This is the documentation for the Squid configuration file.  
# This documentation can also be found online at:  
#   http://www.squid-cache.org/Doc/config/  
#  
# You may wish to look at the Squid home page and wiki for the  
# FAQ and other documentation:  
#   http://www.squid-cache.org/  
#   http://wiki.squid-cache.org/SquidFaq  
#   http://wiki.squid-cache.org/ConfigExamples
```

# PRACTICA 4: PROXY SQUID EN LINUX

---

## Parámetro http\_port

**Paso 9.** Busca la línea `http_port` en `squid.conf`. Averigua cual es el puerto tcp predeterminado de Squid.



```
GNU nano 4.8
# Squid normally listens to port 3128
http_port 3128
# TAG: https_port
```

Busca mediante comandos, los puertos que están en uso y si alguno coincide con el de squid.

**sudo lsof -i -P -n | grep LISTEN**

```
marta@marta-virtual-machine:/etc/squid$ sudo lsof -i -P -n | grep LISTEN
systemd-r  656 systemd-resolve  13u  IPv4  32516      0t0  TCP 127.0.0.53:53 (LISTEN)
cupsd      722      root        6u   IPv6  36473      0t0  TCP [::1]:631 (LISTEN)
cupsd      722      root        7u   IPv4  36474      0t0  TCP 127.0.0.1:631 (LISTEN)
squid     13728    proxy      12u   IPv6  97112      0t0  TCP *:3128 (LISTEN)
```

# PRACTICA 4: PROXY SQUID EN LINUX

---

## Parámetro cache\_mem

**Paso 10.** El parámetro `cache_mem` establece el tamaño de la memoria cache de squid, necesarios para:

- Objetos en tránsito.
- Objetos frecuentemente utilizados (Hot).
- Objetos negativamente almacenados en el caché.

Busca cual es el valor predeterminado de `cache_mem`?

Que memoria caché se esta usando?

```
GNU nano 4.8
#      cache, see memory_cache_shared.
#Default:
# cache_mem 256 MB
```

```
GNU nano 4.8
# TAG:
cache_mem      (bytes)
#      NOTE: THIS PARAMETER DOES NOT
#      IT ONLY PLACES A LIMIT ON
```

# PRACTICA 4: PROXY SQUID EN LINUX

---

**Paso 11.** Bloquearemos el tráfico basándose en algunas palabras clave en el servidor proxy Squid. Crearemos un archivo que contenga las palabras claves sport, marca y as. Queremos impedir la conexión a páginas que contengan estas palabras.

**sudo nano /etc/squid/keywords.squid**

```
GNU nano 4.8 keywords.squid
sport
marca
as
```

**Paso 12.** Utilizaremos el nombre del archivo para crear una regla ACL para denegar el tráfico. Edita squid.conf para crear acl y denegar la regla.

**acl keywords url\_regex -i "/etc/squid/keywords.squid"**  
**http\_access deny keywords**

```
GNU nano 4.8 squid.conf
#
acl keywords url_regex -i "/etc/squid/keywords.squid"
http_access deny keywords
#
# Recommended minimum Access Permission configuration:
#
```

# PRACTICA 4: PROXY SQUID EN LINUX

Paso 13. Reinicia squid

**sudo systemctl restart squid**

Paso 14. Ir a ajustes de Firefox, y configura el navegador para que acceda a Internet a través del proxy squid.

Configuración de conexión

Configurar acceso proxy a Internet

- ☐ Sin proxy
- ☐ Autodetectar configuración del proxy para esta red
- ☐ Usar la configuración del proxy del sistema
- ☒ Configuración manual del proxy

Proxy HTTP 127.0.0.1 Puerto 3128

☒ Usar también este proxy para HTTPS

Proxy HTTPS 127.0.0.1 Puerto 3128

Host SOCKS Puerto 0

☐ SOCKS v4 ☒ SOCKS v5

☐ URL de configuración automática del proxy

Recargar

Ayuda Cancelar Aceptar

# PRACTICA 4: PROXY SQUID EN LINUX

---

**Paso 15.** Accede a las siguientes paginas web y comprueba que pasa:

www.marca.com

www.as.com

www.sport.es



# PRACTICA 5. INSTALACIÓN PROXY EN W10 (NO HACER)

---

## Objetivo

- ❖ Instalación del servidor Freeproxy para la conexión a Internet.
- ❖ Configuración de servidor proxy para que impida la conexión a páginas que contengan la palabra "Sport".
- ❖ Además el servidor creará un log de conexiones para que sea posible ver qué ip ha navegado a qué sitio y se crearán usuarios de conexión de manera que para cada conexión se nos pida un nombre de usuario y password



# PRACTICA 5. INSTALACIÓN PROXY EN W10 (NO HACER)

---

1. Instalar freeproxy
  2. Abrir el Centro de Control
  3. Clic en IP Service
  4. definir el nombre del servicio Ej. Internet
  - 4.1 Service. escoger Web Server
  - 4.2 Listening Port, definir el puerto o dejarlo como esta Ej(3128)
  - 4.3 LocalBinding, seleccionas la tarjeta de red (192.168.0.1)
  5. Done
- En la configuración del navegador, poner la ip del server(192.168.0.1) y el puerto con el que trabajas ej. 80 o 3128 o el que hayas elegido
-

# PRACTICA 5. INSTALACIÓN PROXY EN W10 (NO HACER)

---

## Descripción del Programa FreeProxy 3.92:

FreeProxy es un [servidor](#) con soporte para HTTP, SMTP, POP, FTP over HTTP, TCP Tunneling, NNTP y SOCKS5. Funciona con una amplia gama de clientes incluyendo navegadores, ICQ, MSN Messenger y muchos otros. Entre las funciones disponibles se encuentran: autenticación de usuario tanto para una base de datos interna de usuarios o un [dominio](#) de Windows, amplios informes, permisos para acceder a los recursos, [filtro](#) de URL, filtro de direcciones IP, marcación a demanda, interfaz ASAPI, ... Incluye un pequeño [servidor Web](#) y puede ser ejecutado como un servicio.