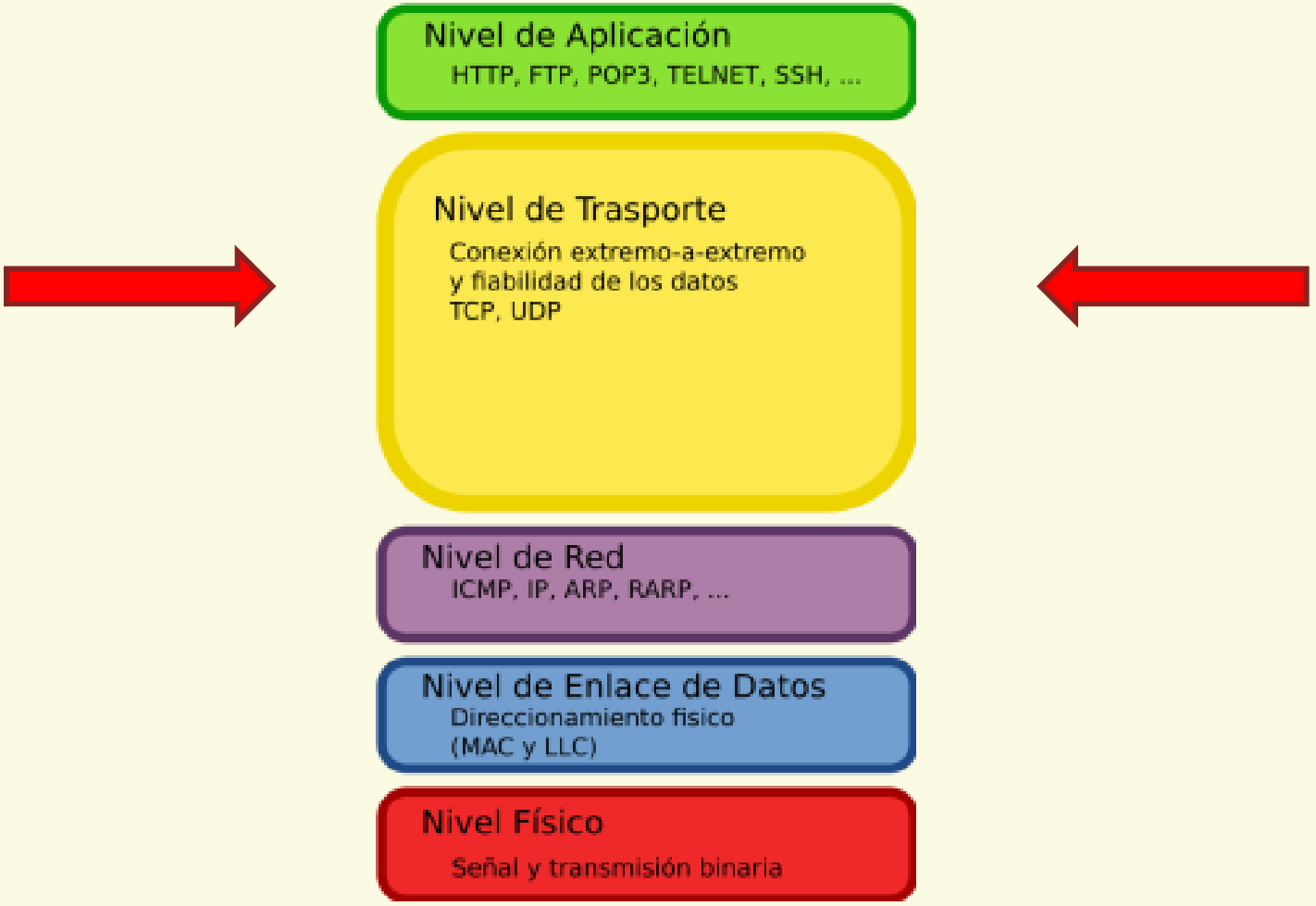
4. NIVEL DE TRANSPORTE

Planificación y Administración de Redes ASIR1

CONTENIDOS

1. Introducción
2. Función de la capa de transporte
3. Concepto de puerto
4. Tablas NAT
5. Protocolos de nivel de transporte: TCP / UDP
6. Cortafuegos (Firewall)
7. Formato de los paquetes
8. Herramientas

1. Introducción



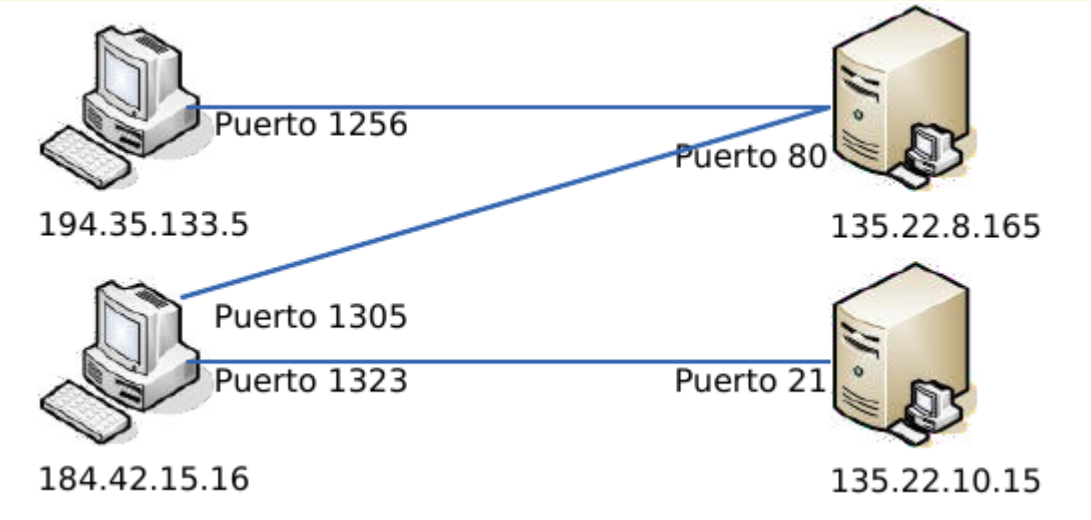
2. Función de la capa de transporte

La **capa de transporte** del modelo de referencia OSI o TCP/IP es la encargada de proporcionar un transporte de datos confiable de la máquina origen a la máquina destino, independientemente de la red o redes físicas en uso.

La capa de transporte proporciona una serie de servicios directamente a la capa de aplicación

3. Concepto de puerto

Un **puerto** es el valor que se usa, en el modelo de la capa de transporte, para distinguir entre las múltiples aplicaciones que se pueden conectar al mismo host o puesto.



3. Concepto de puerto

Cada aplicación que se comunique en un equipo lo hará a través de un puerto:

- Las aplicaciones servidoras habilitan puertos de escucha para aceptar conexiones de aplicaciones cliente.

- Las aplicaciones cliente se conectarán a las aplicaciones servidoras en sus puertos de escucha mediante sus propios puertos de salida.

3. Concepto de puerto

Para numerar los puertos asociados a una dirección IP se utilizan 16 bits, por lo que cada IP dispone de 2^{16}=65.536 puertos distintos (65.535 descontando el puerto 0)

Cualquier aplicación puede operar en cualquier puerto, aunque existen algunos predefinidos para las aplicaciones más usadas. Son los puertos “bien conocidos” (*well known ports*)

- Del 1 al 1023: puertos bien conocidos. S.O.
- Del 1024 al 49151: puertos registrados. Aplicaciones
- Del 49152 al 65535: puertos efímeros

3. Concepto de puerto

Algunos de los puertos de escucha más habituales son:

- HTTP: 80
- HTTPS: 443
- FTP:
  - 21 (canal de comandos)
  - 20 (canal de datos - modo activo)
  - Puertos seleccionados en el servidor para el canal de datos cuando se usa el modo pasivo o en el cliente si es modo activo
- TELNET: 23
- SSH: 22
- POP3: 110
- IMAP: 143
- SMTP: 25
- POP3 sobre TLS/SSL: 995
- IMAP sobre TLS/SSL: 993

3. Concepto de puerto

La lista completa puede consultarse en:

https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Otros puertos de aplicaciones interesantes son:

- Terminal Server (Windows): 3389
- VNC: 5900
- OpenVPN: 1194

3. Concepto de puerto

Comandos útiles para trabajar con puertos:

- Windows
  - netstat –n: muestra las conexiones de datos establecidas
  - netstat –A –n: muestra las conexiones y los puertos en escucha en el sistema

3. Concepto de puerto

```
λ netstat -an

Conexiones activas

  Proto  Dirección local        Dirección remota       Estado
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49157          0.0.0.0:0              LISTENING
  TCP    127.0.0.1:8307         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:49178        127.0.0.1:49179        ESTABLISHED
  TCP    127.0.0.1:49179        127.0.0.1:49178        ESTABLISHED
  TCP    192.168.1.4:139        0.0.0.0:0              LISTENING
  TCP    192.168.1.4:49173      108.160.163.38:80      ESTABLISHED
  TCP    192.168.1.4:49187      128.121.22.143:443     ESTABLISHED
  TCP    192.168.1.4:49535      193.149.88.31:443      ESTABLISHED
  TCP    192.168.1.4:49537      157.56.192.98:443      ESTABLISHED
  TCP    192.168.1.4:49594      78.31.9.100:443        ESTABLISHED
  TCP    192.168.1.4:53026      173.194.34.196:443     ESTABLISHED
  TCP    192.168.1.4:53070      173.194.41.30:443      ESTABLISHED
  TCP    192.168.1.4:53071      54.240.187.206:1935    ESTABLISHED
  TCP    192.168.1.4:53608      173.194.41.238:443     ESTABLISHED
  TCP    192.168.1.4:53771      31.13.83.8:443         ESTABLISHED
  TCP    192.168.1.4:53861      173.194.34.207:80      TIME_WAIT
  TCP    192.168.1.4:53864      173.194.41.246:443     ESTABLISHED
  TCP    192.168.1.4:53868      173.194.34.192:80      ESTABLISHED
  TCP    192.168.1.4:53869      173.194.41.194:80      ESTABLISHED
  TCP    192.168.1.4:53871      173.194.41.224:443     ESTABLISHED
```

Proto: protocolo utilizado para la comunicación

Dirección local: dirección del equipo local origen de la comunicación

Dirección remota: dirección del equipo remoto destino de la comunicación

Estado: estado de la comunicación en cada momento (LISTENING, ESTABLISHED, CLOSE_WAIT, CLOSED, TIME_WAIT

3. Concepto de puerto

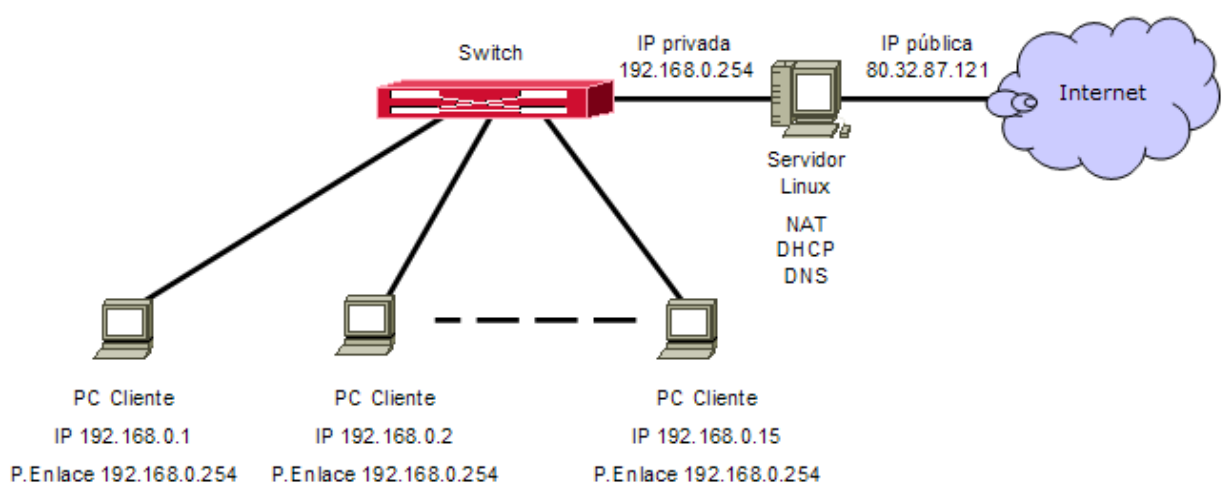
Comandos útiles para trabajar con puertos:

- Linux
  - netstat –inet -n: muestra las conexiones de datos establecidas
  - netstat –ltn: muestra los puertos en escucha en el sistema
  - sudo netstat –ltnp: muestra los puertos en escucha en el sistema y los procesos que han abierto esos puertos.

4. Tablas NAT

Los routers NAT (Network Address Translation) permiten que redes de ordenadores utilicen un rango de direcciones especiales (IPs privadas) y se conecten a Internet usando una única dirección IP (IP pública)

Con esto se consigue usar una única dirección IP y no una IP para cada máquina



PETICIÓN
Origen 192.168.0.1
Destino 8.8.8.8

PETICIÓN TRADUCIDA
Origen 80.32.87.121
Destino 8.8.8.8

4. Tablas NAT

Los routers NAT utilizan los puertos para funcionar.

- Si un paquete atraviesa routers normales no cambia la IP ni los puertos de origen y destino.
- Cuando hay un router NAT, los paquetes que pasan de LAN a WAN cambian la IP y el puerto de origen por la IP WAN del router.
- En las tablas NAT se guardan las direcciones de los equipos que están conectados al router NAT. Esta tabla se rellena cuando llegan paquetes de LAN a WAN.
- También se pueden añadir entradas a la tabla de forma manual → servidor en la parte LAN (DNAT)

4. Tablas NAT

- NAT estático. Una dirección privada y una pública

- NAT dinámico. Muchas direcciones privadas y varias públicas

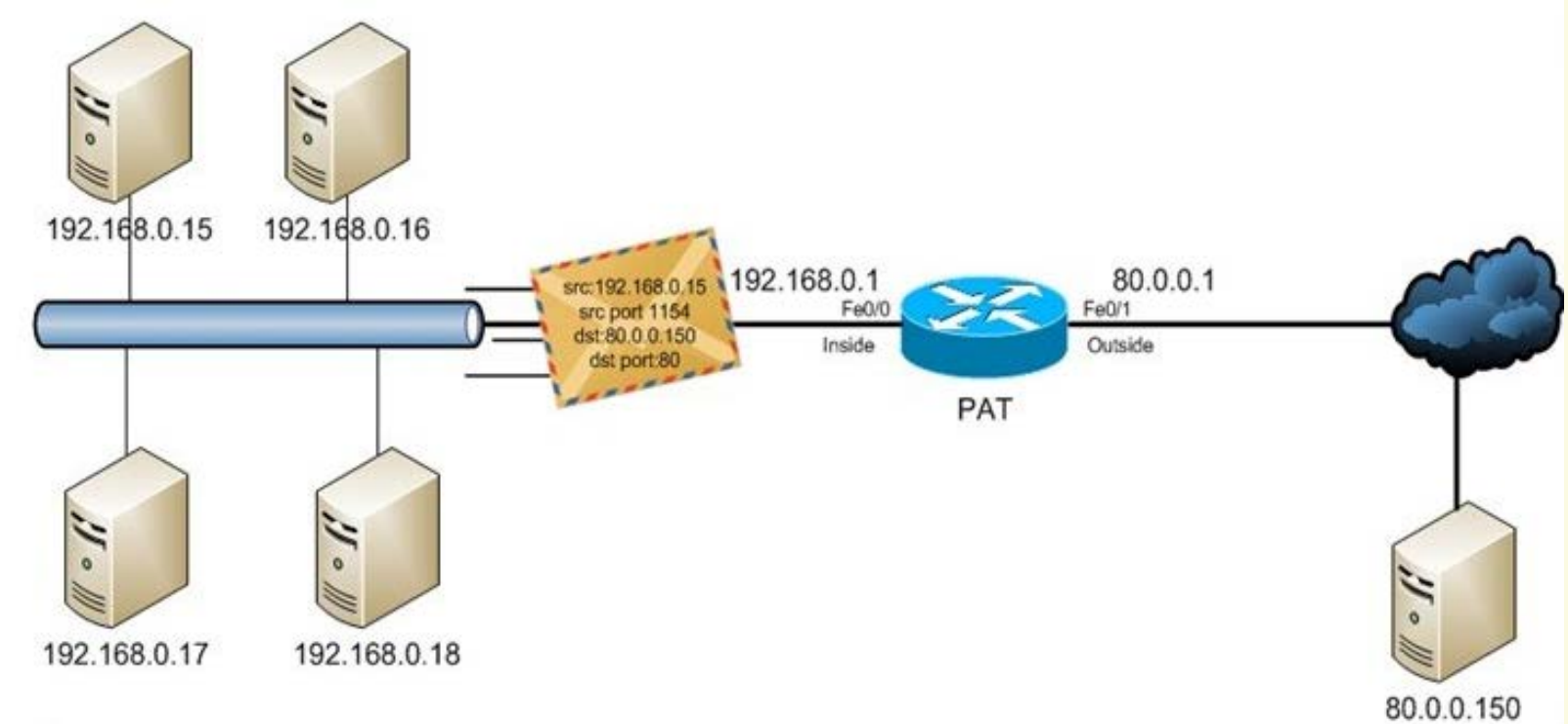
  Recuerda, esta tabla se va rellenando cuando llegan paquetes de LAN a WAN.

- NAT sobrecargado. Muchas direcciones privada y una pública → PUERTOS

  Realmente se trata de PAT (Port Address Translation)

  NAT + PAT

4. Tablas NAT


192.168.0.15
192.168.0.16
src:192.168.0.15
src port 1154
dst:80.0.0.150
dst port:80
192.168.0.1
Fe0/0
Inside
PAT
80.0.0.1
Fe0/1
Outside
192.168.0.17
192.168.0.18
80.0.0.150

4. Tablas NAT

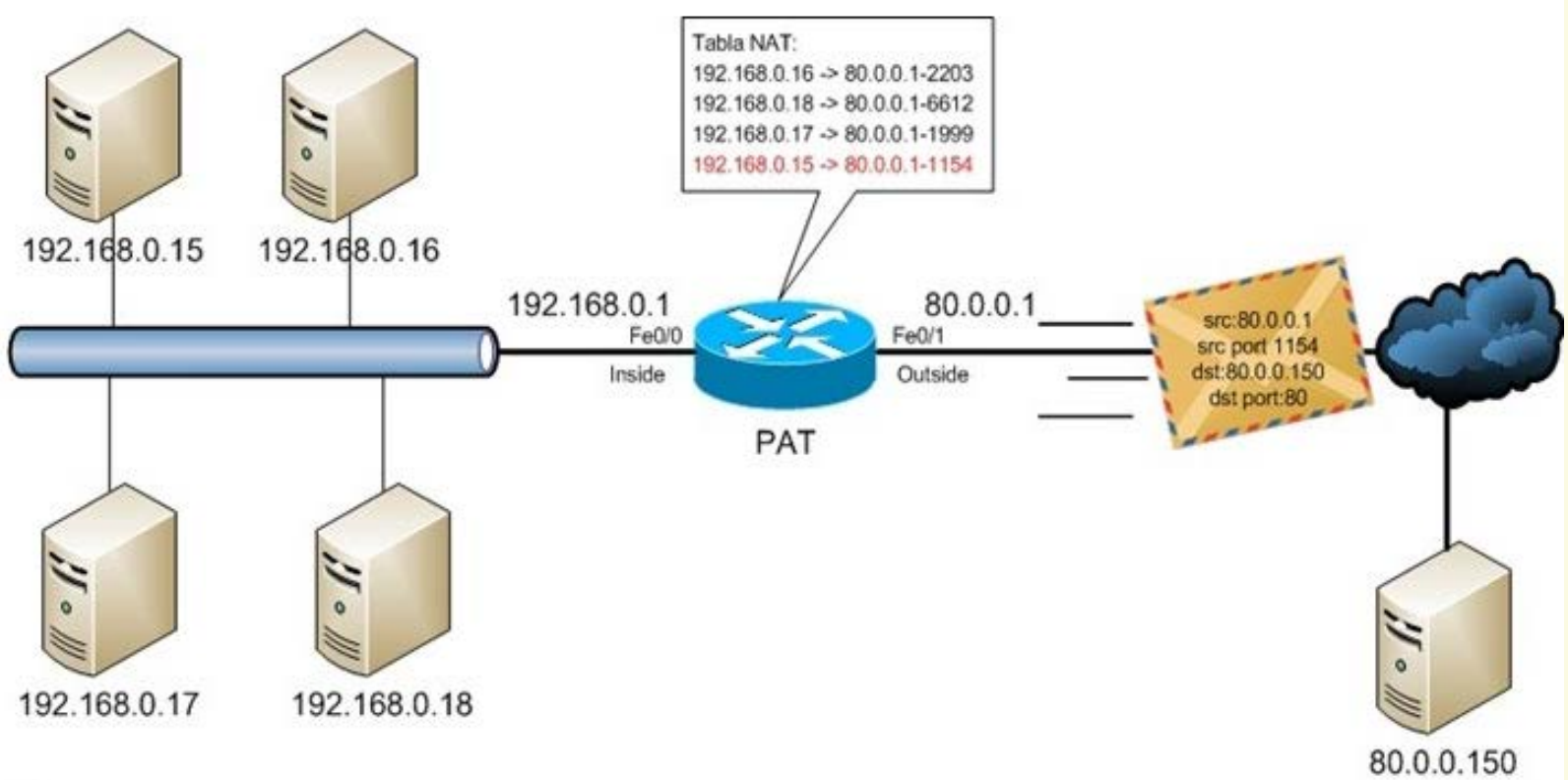
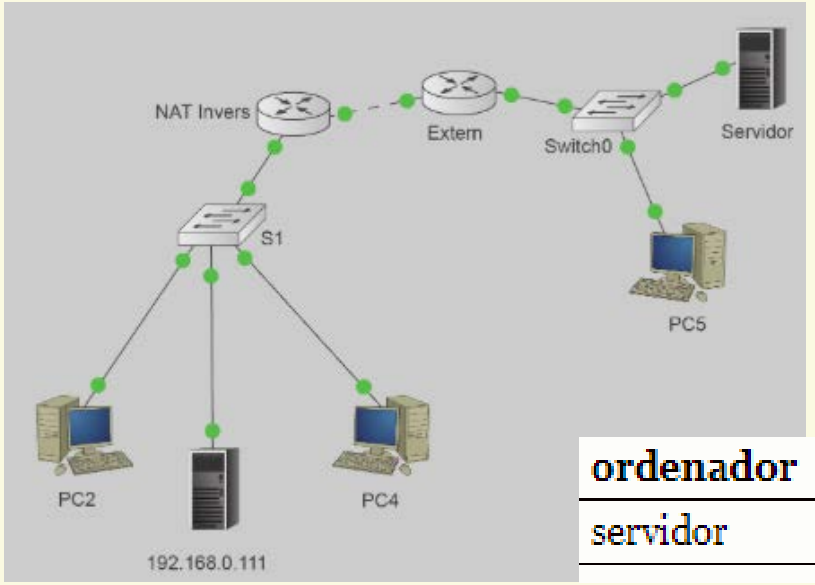


Tabla NAT:
192.168.0.16 -> 80.0.0.1-2203
192.168.0.18 -> 80.0.0.1-6612
192.168.0.17 -> 80.0.0.1-1999
192.168.0.15 -> 80.0.0.1-1154
192.168.0.15
192.168.0.16
192.168.0.1
Fe0/0
Inside
80.0.0.1
Fe0/1
Outside
PAT
src:80.0.0.1
src port 1154
dst:80.0.0.150
dst port:80
192.168.0.17
192.168.0.18
80.0.0.150

4. Tablas NAT

- DNAT (Destination Network Address Translator) o NAT inverso. Se usa para hacer visible públicamente en Internet un ordenador de una red local.

  Ejemplo: acceder a un servidor web en su red doméstica desde la red de su puesto de trabajo



ordenador	dirección privada	dirección pública
servidor	192.168.0.111	68.54.32.26

5. Protocolos de nivel de transporte: TCP y UDP

La capa de transporte puede ofrecer dos tipos de servicio:

- **TCP**: Servicio de transporte **orientado a conexión**:
  - Requiere las fases de establecimiento de la conexión, transferencia de datos y liberación
  - Diseñado para proporcionar un flujo de bytes confiable de extremo a extremo a través de redes distintas y no confiables
  - Aplicaciones usuales que utilizan este servicio son: HTTP (Web), FTP (transferencia de ficheros), SMTP (envío de emails), SSH (acceso remoto), etc.

5. Protocolos de nivel de transporte: TCP y UDP

La capa de transporte puede ofrecer dos tipos de servicio:

- **UDP**: Servicio de transporte **no orientado a conexión**:
  - Permite que las aplicaciones envíen datagramas IP encapsulados sin establecer una conexión
  - No proporciona confirmación de entrega ni control de flujo: los paquetes pueden perderse, duplicarse o desordenarse
  - Aplicaciones usuales que utilizan este servicio son: DHCP (adquisición automática de configuración de red), DNS (resolución de direcciones IP), VoIP (Voz sobre IP), videoconferencia, streaming...

6. Cortafuegos (Firewalls)

Cortafuegos: dispositivo o aplicación (HW, SW o una combinación de ambos) diseñada para bloquear el acceso no autorizado de tráfico entrante o saliente a/de una red, permitiendo al mismo tiempo comunicaciones autorizadas.

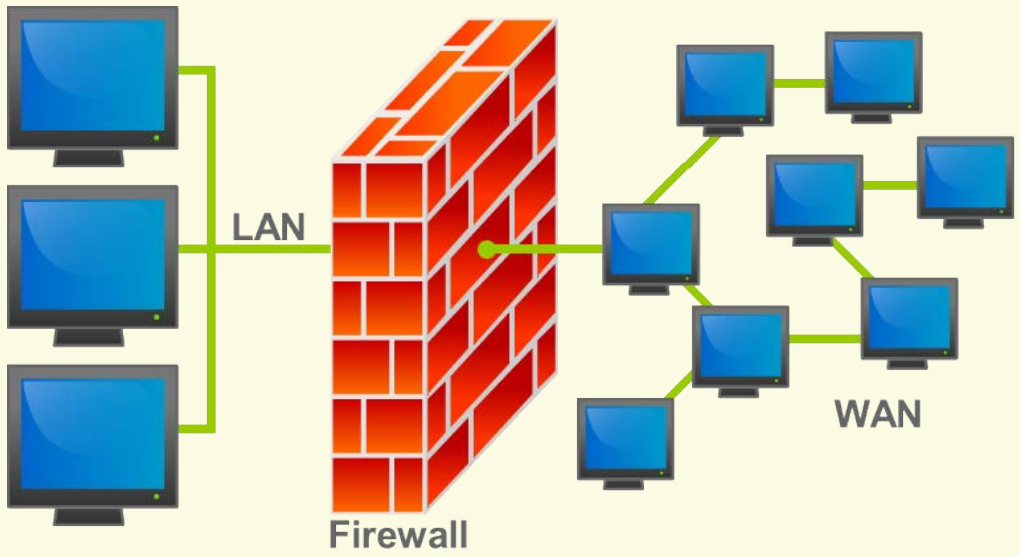
Este trabajo lo realiza sobre la base de un conjunto de normas y otros criterios.

Ejemplos:

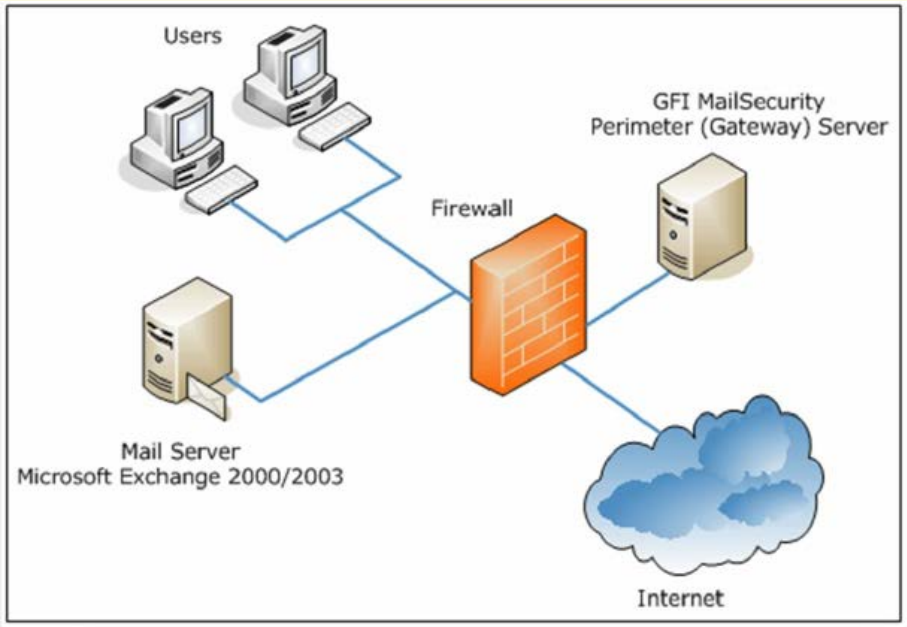
- Permitir las conexiones al puerto 80
- Bloquear todas las conexiones que vengan de la dirección 76.45.3.4
- Permitir las conexiones al puerto 443 de la red 77.6.0.0
- Bloquear todas las salidas

6. Cortafuegos (Firewalls)

Se utilizan para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet. Todos los mensajes que entren o salgan de la red privada pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados (reglas)



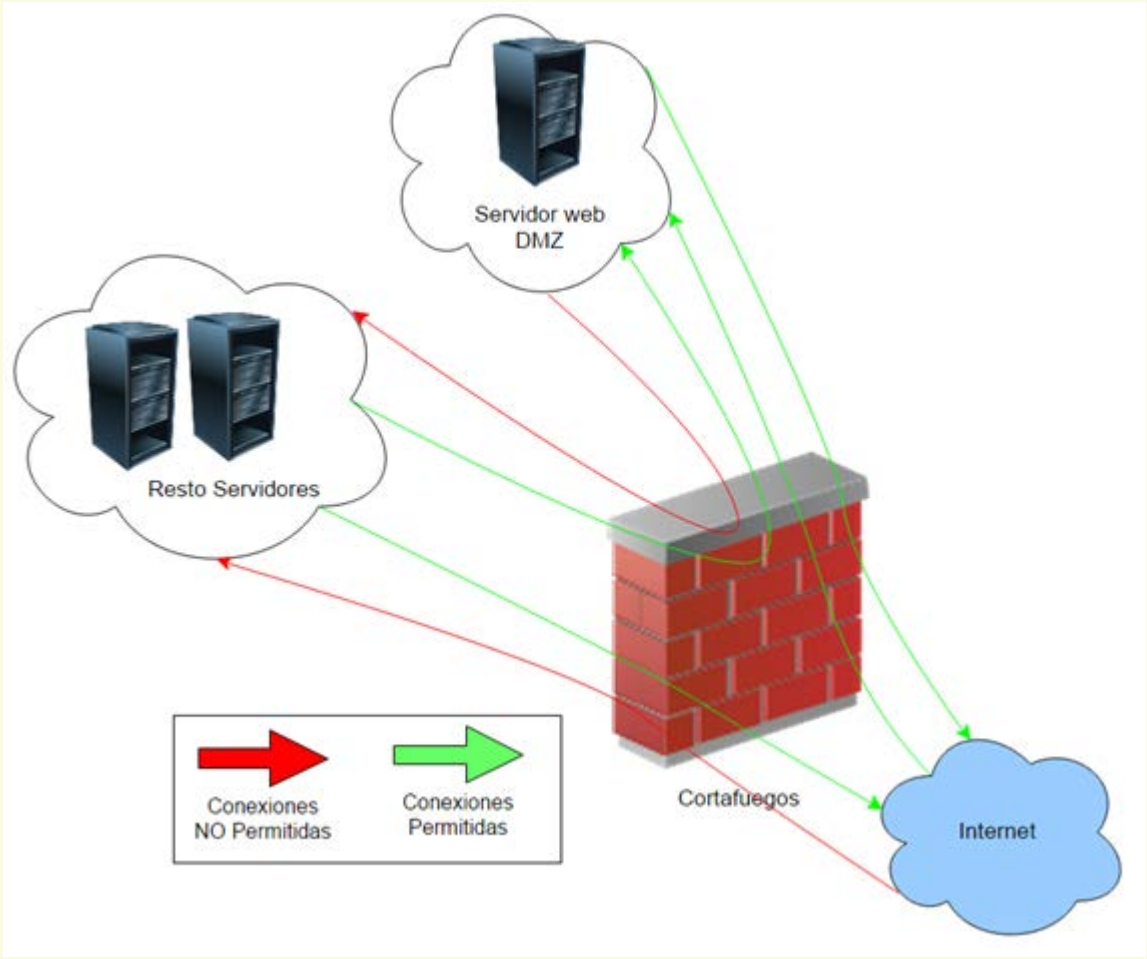
6. Cortafuegos (Firewalls)



Regla básica de cualquier cortafuegos: el bloqueo de puertos no autorizados (bloqueo a nivel 4)

También es frecuente conectar el cortafuegos a un tercer ámbito, llamado Zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

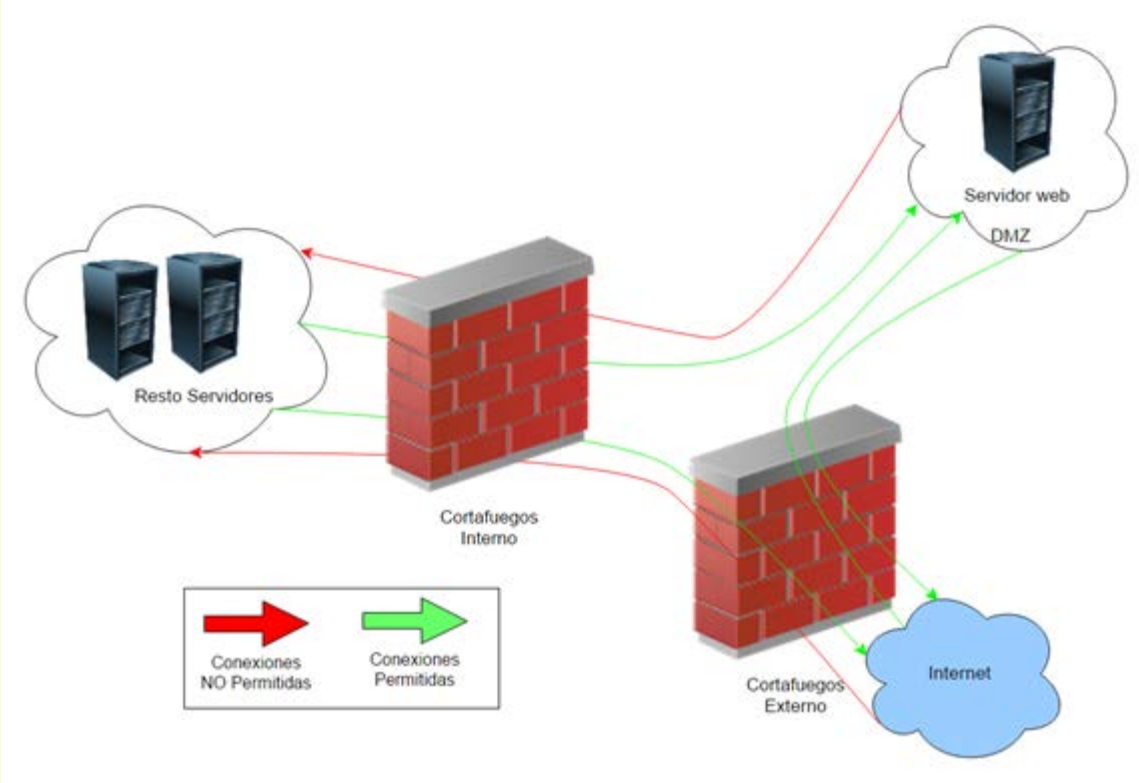
6. Cortafuegos (Firewalls)



DMZ con un único firewall.

Un fallo en la seguridad del firewall compromete toda la red.

6. Cortafuegos (Firewalls)



DMZ con doble firewall.

Nos asegura un nivel más alto de seguridad en la red interna

6. Cortafuegos (Firewalls)

Políticas de cortafuegos

- **Permisiva:** se permite todo el tráfico excepto el que esté explícitamente denegado.

- **Restrictiva:** se deniega todo el tráfico excepto el que está explícitamente permitido. Es la que se suele utilizar en empresas y organismos gubernamentales ya que es más segura.

7. Formato de los paquetes

La estructura de un segmento TCP es:

+	**Bits** 0 - 3	4 - 7	8 - 15	16 - 31
0	Puerto Origen			Puerto Destino
32	Número de Secuencia			
64	Número de Acuse de Recibo (ACK)			
96	Longitud cabecera TCP	Reserva-do	Flags	Ventana
128	Suma de Verificación (Checksum)			Puntero Urgente
160	Opciones + Relleno (opcional)			
...	Datos			

7. Formato de los paquetes

Puerto de origen (16 bits): identifica el puerto a través del que se envía

Puerto de destino (16 bits): identifica el puerto del receptor

Número de secuencia (32 bits): sirve para comprobar que ningún segmento se ha perdido, y que llegan en el orden correcto

Número de acuse de recibo (ACK) (32 bits): Si el flag ACK está puesto a activo, entonces este campo contiene el número de secuencia del siguiente paquete que el receptor espera recibir

7. Formato de los paquetes

Longitud de la cabecera TCP (4 bits): especifica el tamaño de la cabecera TCP en palabras de 32 bits. Este campo es necesario porque el campo Opciones de la cabecera es de tamaño variable. Mínimo 5. Máximo 15

Reservado (4 bits): bits reservados para uso futuro, deberían ser puestos a cero

Ventana (16 bits): Es el tamaño de la ventana de recepción, que especifica el número de bytes que el receptor está actualmente esperando recibir

7. Formato de los paquetes

Bits de control (flags) (8 bits): son 8 flags o banderas. Está "activa" con un 1 o "inactiva" con un 0. Algunos son:

ACK – Acknowledge: si está activo entonces el campo con el número de acuse de recibo es válido (sino es ignorado)

URG- Urgent: si está activo indica que el campo Puntero Urgente marca los datos que son urgentes

RST – Reset: si llega a 1, termina la conexión sin esperar respuesta y reinicializa la conexión

SYN – Synchronize: activa/desactiva la sincronización de los números de secuencia

FIN: activo indica que no hay más datos a enviar por parte del emisor, esto es, este paquete es el último de la conexión

7. Formato de los paquetes

Suma de verificación (checksum) (16 bits): verifica la integridad tanto de la cabecera como de los datos

Puntero urgente (16 bits): si el flag URG está activo este campo indica que hay datos marcados como prioritarios dentro del campo Datos. Estos se colocan al principio y este campo indica el último byte de datos marcados como "urgentes"

Opciones (número de bits variable): campos opcionales. Su longitud ha de ser múltiplo de 32 bits (si es menor, se rellena con ceros al múltiplo más cercano)

Datos (número de bits variable): es la parte con los datos del paquete TCP. Pueden ser datos de cualquier protocolo del nivel de aplicación. Los más comunes son HTTP, Telnet, SSH, FTP, ...

7. Formato de los paquetes

La estructura de un datagrama UDP es:

+	Bits 0 - 15	16 - 31
0	Puerto origen	Puerto destino
32	Longitud del Mensaje	Suma de verificación
64	Datos	

Cabecera UDP: consta de 4 campos de los cuales 2 son opcionales (puerto origen y suma de verificación)

Los campos de los puertos fuente y destino son campos de 16 bits que identifican el proceso de origen y recepción

7. Formato de los paquetes

Como UDP carece de estado y el origen UDP no solicita respuestas, el puerto origen es opcional. En caso de no ser utilizado, el puerto origen debe ser puesto a cero

A los campos del puerto destino le sigue un campo obligatorio que indica el tamaño en bytes del datagrama UDP incluidos los datos. El valor mínimo es de 8 bytes. El campo de la cabecera restante es una suma de comprobación de 16 bits

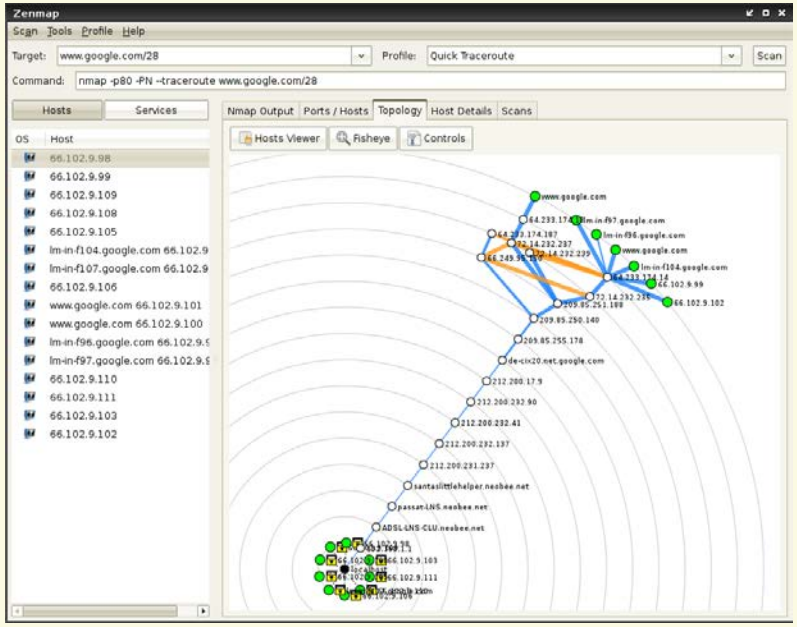
El checksum también es opcional, aunque generalmente se utiliza en la práctica

8. Herramientas

- **netstat:** Permite ver los puertos que nuestro equipo tiene abiertos

- **nmap:** permite ver los puertos que otro equipo tiene abiertos. Es extremadamente potente y dispone de numerosas opciones para realizar distintos tipos de sondeos o escaneos.

Tiene una aplicación grafica asociada conocida como **Zenmap**



8. Herramientas

- **Cortafuegos:** bloquea el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

- **Proxy:** equipo o software intermediario que hace peticiones a distintos servidores (generalmente páginas web) en representación del equipo que se halla detrás de proxy haciendo uso de él.

- **VPN (Virtual Private Network):** permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Permite que un equipo envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

PRÁCTICAS

1. Ejercicios prácticos relacionados con los conceptos vistos
2. Análisis de los puertos empleados en conexiones de datos
3. Análisis de puertos de escucha
4. Configuración de tablas NAT en router
5. Modificación de puertos de escucha en servicios de red habituales (FTP)
6. Configuración de cortafuegos