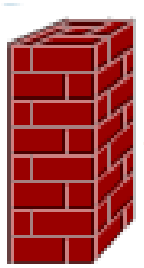
Firewalls (cortafuegos)

Concepto

- Cortafuegos = Firewall
- Un firewall es un programa o dispositivo que recibe el tráfico de red y decide si lo permite o lo bloquea en función de unas reglas.
- Los firewalls los podemos encontrar:
  - En los equipos finales, para protegerlos. Por ejemplo, firewall de Windows.
  - En la red, protegiendo los accesos entre los diferentes segmentos → trabajaremos con este tipo.

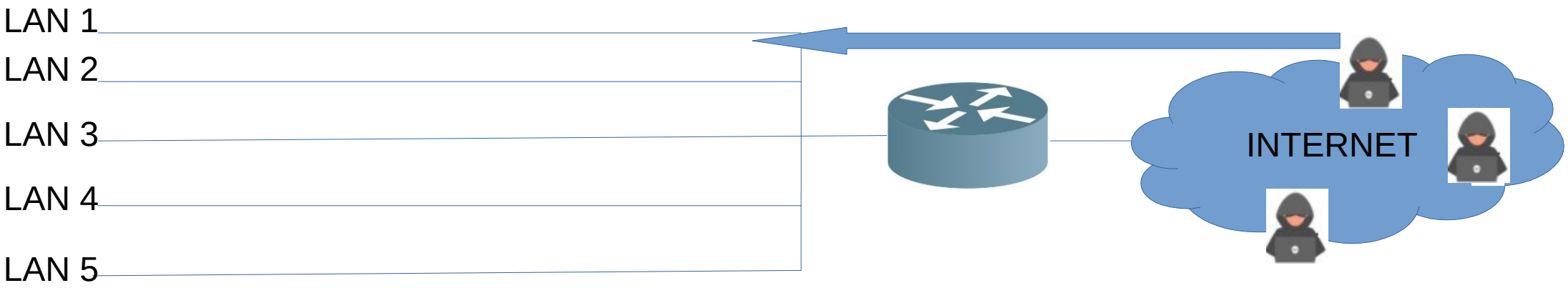
Firewalls (I)

- A nivel de red, un firewall es un elemento fundamental de protección.
- Se encarga de robustecer las redes frente a los ataques → seguridad perimetral.
- En la red, un firewall dispone de interfaces en los diferentes segmentos de red.
- Intercepta todo el tráfico entre las redes y decide si lo deja pasar o no.



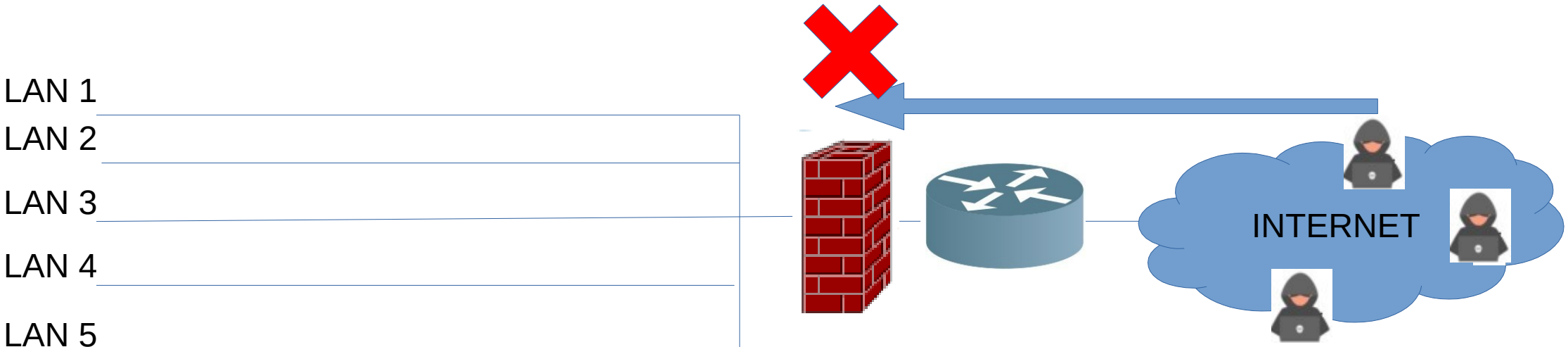
Redes no protegidas

- Los sistemas operativos y las aplicaciones desplegados sobre ellos tienen fallos de seguridad.
- ¿Qué ocurriría si conectamos las rede internas e Internet sin ningún tipo de filtro?



Protección mediante firewall

- El firewall actúa de filtro, revisando cada paquete de red y decidiendo si debe dejarlo pasar o no.



Firewalls- inspección

- El flujo que sigue es:
  - El firewall recibe el tráfico por alguna de sus interfaces
  - Comprueba si ese tráfico encaja en alguno de los patrones que tiene configurados
  - En cuanto cumple uno de ellos, ejecuta la regla asociada
  - Si no cumple ningún patrón, se ejecuta la regla por defecto.

Firewalls – tipos de políticas

- Precisamente, en función de la regla por defecto existen:
  - Políticas restrictivas: se deniega todo salvo lo explícitamente permitido en las reglas → regla por defecto DENY ALL
  - Políticas permisivas: se permite todo, salvo lo explícitamente denegado → ALLOW ALL
- Las políticas permisivas no son recomendadas. Deben emplearse cortafuegos con reglas de DENY ALL por defecto.

Firewalls – filtrado

- Existen firewalls que trabajan en diferentes capas: Ethernet, IP, aplicación, …
- Los más utilizados filtran en capa 3. Las reglas se pueden configurar en función de:
  - IP origen y/o destino
  - Puerto origen y/o destino
  - Si la conexión se realiza mediante una VPN

Firewalls – Ejemplo

Origen | Destino | Puerto | Acción | Traza

Firewall | NAT | IPS | Anti-Spam & Mail | Anti-Virus & URL Filtering | SSL VPN | IPSec VPN | QoS | Desktop

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON
1		* Any	* Any	* Any Traffic	NBT	drop	- None	* Policy Targets
2		test_host01	cluster01	* Any Traffic	TCP http TCP ssh	accept	Log	* Policy Targets
3		test_net01	test_host01	* Any Traffic	TCP ftp	accept	- None	* Policy Targets
4		* Any	* Any	* Any Traffic	* Any	drop	Log	* Policy Targets

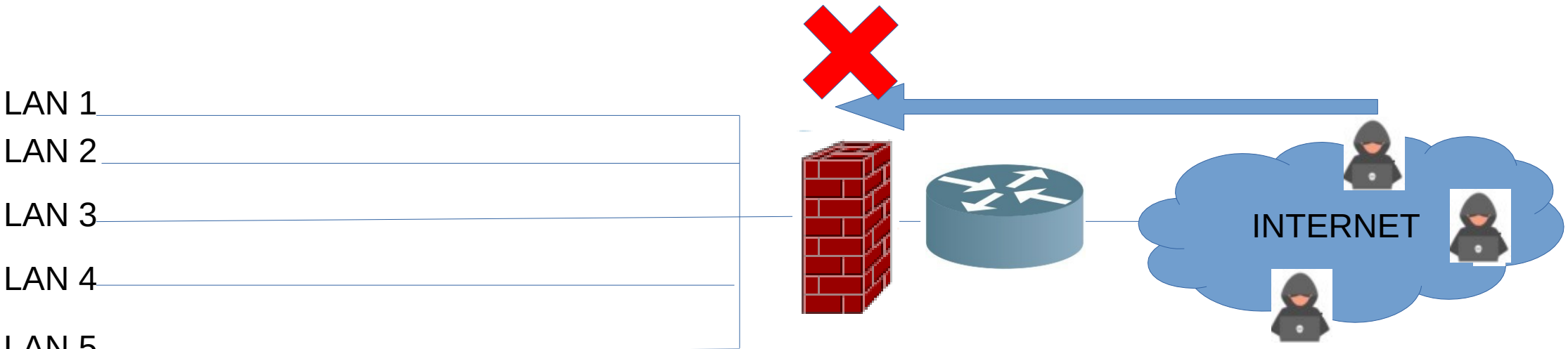
- Si es tráfico Netbios, da igual origen o destino, lo rechazamos.
- Si es una conexión desde el equipo *test_host01* al equipo *cluster01* de tipo http o ssh lo dejamos pasar, y registramos el acceso en el log
- Si es una conexión desde la subred *test_net01* al host *test_host01* para ftp, lo dejamos pasar
- En cualquier otro caso, el firewall bloqueará el tráico de red

Firewalls – tipos de firewall

- Podemos encontrar firewalls:
  - Software: software sobre algún sistema operativo.
    - Pfsense
    - Ipfire
    - Iptables
  - Appliances: dispositivos hardware dedicados, fabricados específicamente para funcionar como cortafuegos.
    - Checkpoint
    - Palo alto
    - Fortinet

Firewalls – configuraciones: Internet

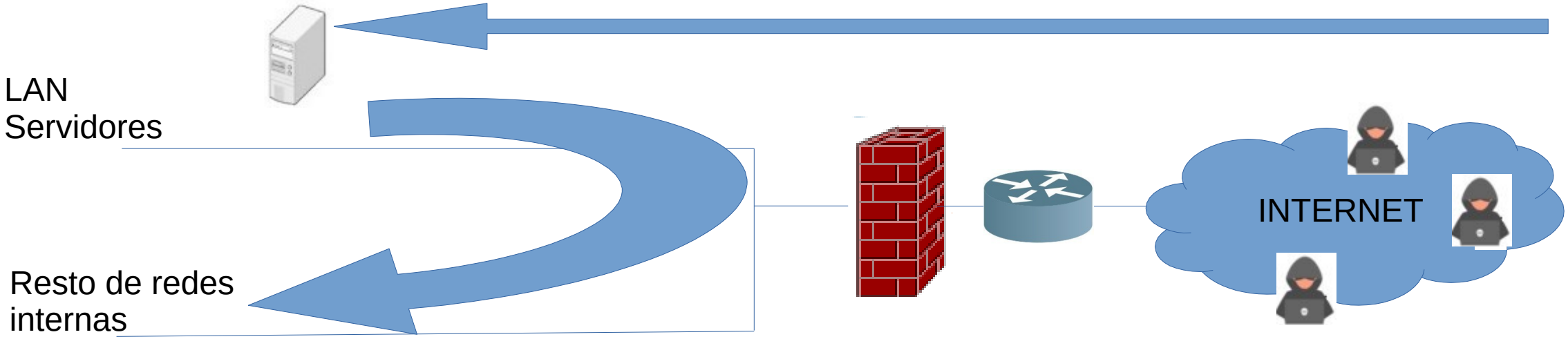
- Una configuración muy habitual es la de un firewall que protege nuestras redes de Internet.
- Permitiremos el tráfico saliente (Desde nuestras redes a Internet), pero no entrante.



Firewalls – configuraciones: DMZ (I)

- Hay muchas ocasiones en las que, dentro de nuestra red, tenemos los servidores que ofrecen servicios hacia Internet → email, web, ...
- En este caso, es necesario configurar en el firewall reglas que permitan conexiones entrantes hacia esos servicios.
- Pero las aplicaciones tienen vulnerabilidades.
- Si un atacante logra acceder a una de las máquinas que aloja uno de esos servicios → puede acceder a cualquier otra de nuestra red, ya que no hay filtro.

Firewalls – configuraciones: DMZ (II)

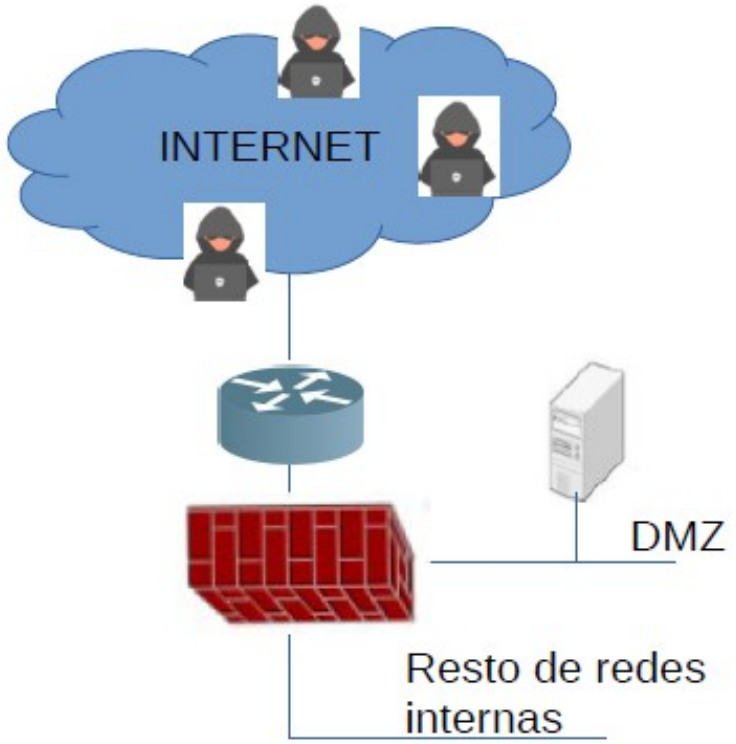


- Si un atacante logra acceder a una de las máquinas que aloja uno de esos servicios → puede acceder a cualquier otra de nuestra red, ya que no hay filtro.

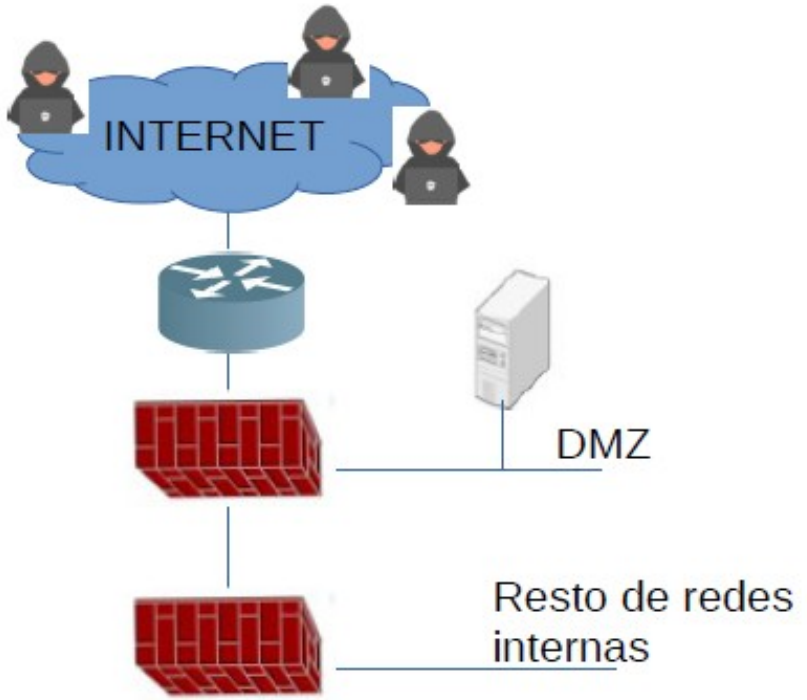
Firewalls – configuraciones: DMZ (III)

- DMZ: zona desmilitarizada(DeMilitarized Zone)
- Consiste en crear una red local, que se ubica entre Internet y la Intranet (redes internas) de la empresa.
- El firewall permitirá ciertas conexiones a equipos en la red DMZ, pero no permitirá conexiones desde este segmento hacia redes internas

Firewalls – configuraciones: DMZ (IV)



Este tipo de configuración la podemos implementar en la mayoría de nuestros routers domésticos

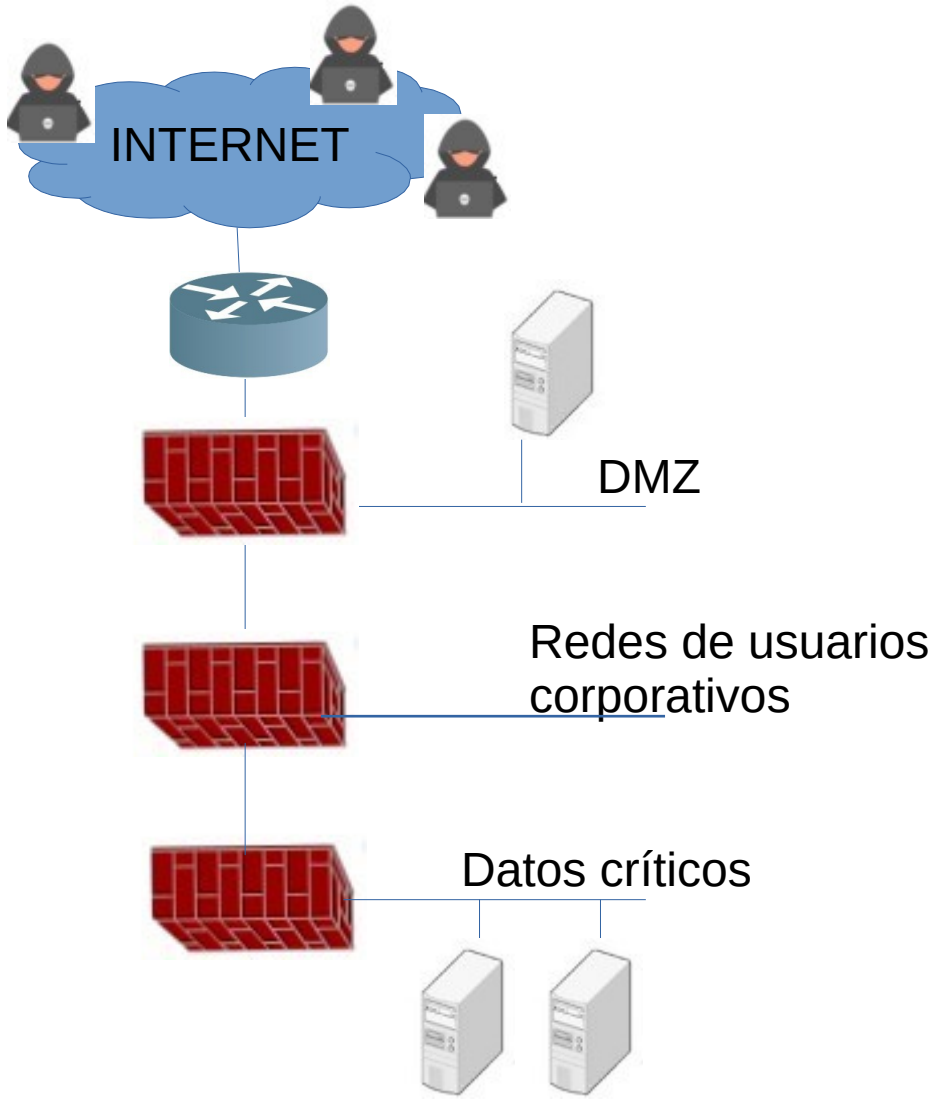


Configuración de DMZ recomendada en entornos empresariales

Firewalls – configuraciones: Datos (I)

- La configuración anterior nos protege de Internet.
- En la DMZ ubicamos los servicios, pero sin los datos. Por ejemplo, tendremos el servidor web, pero la base de datos estará en una red interna.
- De este modo, un atacante de Internet podría acceder a las páginas web, pero tiene mucho más difícil conseguir llegar a la base de datos.
- Pero, ¿qué ocurre con nuestros usuarios internos? ¿Podemos confiar?

Firewalls – configuraciones: Datos (II)



En esta configuración estamos protegiendo:

- nuestros datos y los equipos de nuestros usuarios de atacantes de Internet.
- Nuestros datos de posibles atacantes internos.

Es la configuración de mayor seguridad

De las tres arquitecturas expuestas, la que escojamos dependerá de nuestro negocio (riesgo que queremos asumir, leyes que debemos cumplir, etc.)

Firewalls – Alta disponibilidad (I)

- Los principales problemas de las arquitecturas de red con firewall son:
  - Complejidad de gestión
  - Rendimiento: debemos asegurar que no son cuello de botella en el acceso entre redes.
  - Disponibilidad: se convierten en punto único de fallo. Si se cae, dejamos indisponible el acceso a redes → soluciones de HA (alta disponibilidad)

Firewalls – Alta disponibilidad (II)

- La alta disponilidad consiste en redundar elementos de forma que si se cae uno, siempre haya al menos otro que pueda seguir realizando la función.
- Podemos encontrar alta disponibilidad a nivel de:
  - Componentes: Único equipo con componentes internos “repetidos”
  - Clúster: varios equipos que se comportan como uno solo.

Firewalls – Alta disponibilidad de componentes

- Tenemos un único equipo, con componentes críticos internos redundados, por ejemplo:
  - varias fuentes de alimentación
  - varios interfaces de red
  - más de una CPU
  - varias memorias
- En caso de fallo de alguno de ellos, el/los que quede/n deben poder asumir toda la carga.

Firewalls – Alta disponibilidad con clúster

- En este caso disponemos de 2 o más equipos, que se comportan ante el resto de la red como un único equipo.
- El resto de equipos acceden a una IP.
- Podemos encontrar:
  - Clúster activo/activo: los dos equipos están dando servicio. Las peticiones a la IP del cluster pueden ser atendidas por cualquiera de los miembros.
  - Clúster activo/pasivo: solo uno de los miembros está dando servicio. El resto están parados a la espera de que falle.

Firewalls – Otras funciones (I)

- Dada la posición estratégica de los firewalls, suelen incluir otras funciones como:
  - IDS: Sistemas de detección de intrusiones. Se trata de elementos que permiten detectar patrones de ataque y generar alarmas.
  - IPS: Protección ante intrusiones. No solo las detectan, sino que actúan de forma activa.

    Ejemplo → detectan una IP de Internet que está enviando tráfico con patrón sospechoso y la bloquean en el firewall.
  - VPN: Suelen incluir funcionalidades para establecer redes privadas virtuales.
  - NAT/PAT: traducción de direcciones y puertos.

Firewalls – NAT (I)

- NAT: Network Address Translation.
- No hay IPs públicas suficientes (en IPv4) para que cualquier equipo en el mundo tenga una IP única.
- Por ese motivo, en las redes internas de las empresas se emplean las redes privadas.
- Pero cuando un equipo con una IP privada quiere acceder a Internet, debe hacerlo con una IP pública → Internet no puede enrutar direccionamiento privado.

Firewalls – NAT (II)

- El firewall se encarga de modificar los paquetes IPs enviados a Internet, cambiando la IP origen privada por una pública.
- Cuando llegue un paquete de vuelta en respuesta, el firewall lo captura y modifica sustituyendo la IP destino por la privada, de modo que el paquete llegue al destinatario adecuado.

Firewalls – NAT: tipos

- NAT Estático: a la IP interna le asignamos siempre la misma IP pública → no resuelve el problema de agotamiento de Ips.

  Puede ser una solución válida para algún servidor concreto.
- NAT dinámico: el firewall dispone de un pool de Ips públicas. Las asigna conforme llegan las peticiones.

  Si hay más equipos en un momento dado que quieren salir a Internet que Ips públicas → se rechazan.
- PAT (Port Address Translation): con este método se puede utilizar una única IP pública para múltiples IPs internas.

Firewalls – PAT (I)

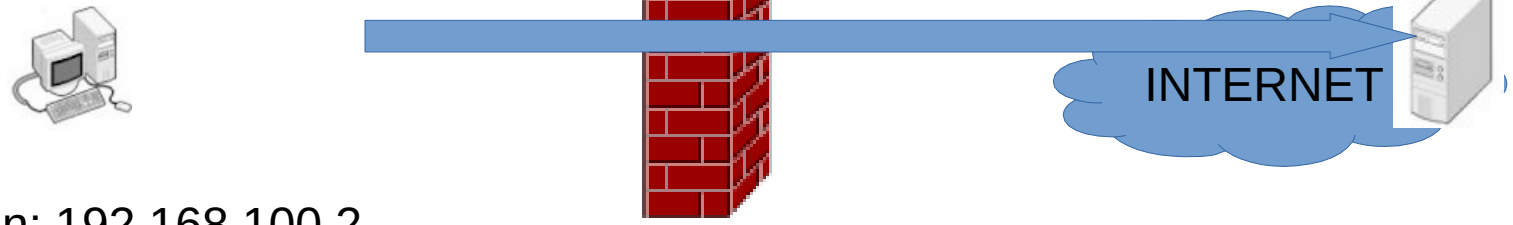
- El firewall captura los paquetes y modifica la cabecera IP, poniendo la misma IP pública.
- Adicionalmente, mantiene una tabla interna en la que registra la IP interna origen y puerto origen.
- Cuando llegue un paquete de respuesta a la IP pública, el firewall analizará el puerto destino y sustituirá la IP por la privada de acuerdo a la tabla PAT.
- Mejor lo vemos con un ejemplo.

Firewalls – PAT (I)

- Tenemos dos equipos internos, con IPs
  - 192.168.100.2
  - 192.168.100.3
- Ambos quieren comunicarse con https://www.google.es
- Nuestro proveedor de Internet nos ha asignado una sola IP: 201.28.34.4

Firewalls – PAT (II)

- El primer equipo quiere comunicarse con una web externa

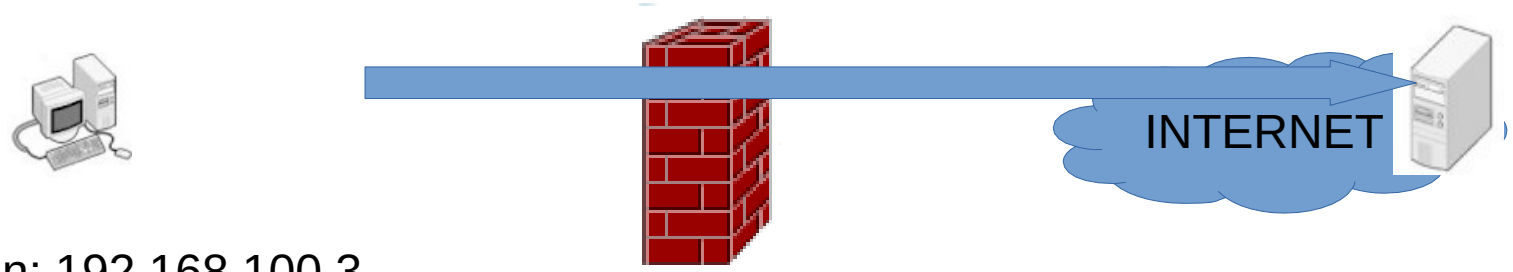


IP origen: 192.168.100.2
Puerto origen: 2001
IP destino: 142.250.200.99
Puerto destino: 443

Tabla traducciones			
IP origen	**Puerto origen**	**IP NAT**	**Puerto origen**
192.168.100.2	2001	201.28.34.4	2001

Firewalls – PAT (III)

- El segundo equipo se quiere también comunicar con el exterior

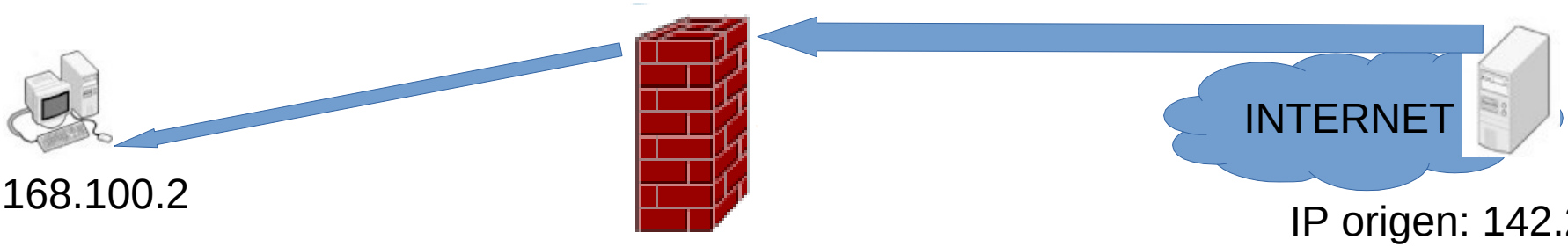


IP origen: 192.168.100.3
Puerto origen: 3001
IP destino: 142.250.200.99
Puerto destino: 443

Tabla traducciones			
IP origen	**Puerto origen**	**IP NAT**	**Puerto origen**
192.168.100.2	2001	201.28.34.4	2001
192.168.100.3	3001	201.28.34.4	3001

Firewalls – PAT (IV)

- Cuando llega un paquete de respuesta, el firewall inspecciona el puerto al que va dirigido.
- Busca en la tabla de traducciones el host interno que originó dicha comunicación, y sustituye la IP por la adecuada.



192.168.100.2

IP origen: 142.250.200.99
IP destino: 201.28.34.4
Puerto destino: 2001

192.168.100.3

Tabla traducciones			
IP origen	**Puerto origen**	**IP NAT**	**Puerto origen**
192.168.100.2	2001	201.28.34.4	2001
192.168.100.3	3001	201.28.34.4	3001

Firewalls – PAT (V)

- Si ambos equipos usaran el mismo número de puerto durante el proceso PAT se aumenta el número de puerto hasta que su valor no coincida con ningún otro usado en la tabla.
- El ejemplo que hemos visto utiliza el puerto origen para realizar la traducción en tráfico saliente.
- Existen casos en que nos interesa hacer disponible un servidor de la red interna a Internet, por ejemplo una web.
- En ese caso podemos usar PAT según el puerto destino.
- Configuraríamos nuestro firewall de modo que el tráfico dirigido a nuestra IP pública y puerto 443 (en el caso de una web por https) lo redirija a nuestra IP interna donde tenemos desplegada la web.

Firewalls – PAT (VI)

- El escenario más complejo será aquel en el que debemos traducir tanto la IP como el puerto.
- Imagina que en tu red interna hay varios servidores web, todos escuchando en el puerto 443.
- Mediante NAT y PAT puedes hacer que, según el puerto destino, el firewall las redirija a cada uno de los servidores internos.
  - Tráfico que llega de IP pública y puerto 4431 → IP1:443
  - Tráfico que llega de IP pública y puerto 4432 → IP2:443
  - Etc.