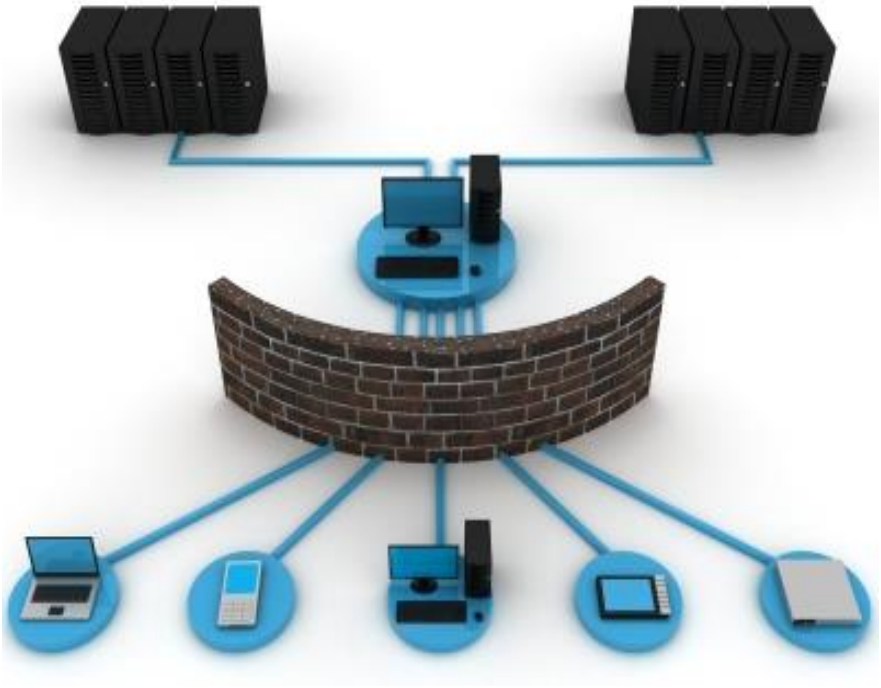
UT 9-10: Seguridad Redes- CORTAFUEGOS-PROXY

2ºSMR – Seguridad Informática

Introducción

Cuando una red corporativa se encuentra interconectada a una red pública, los peligros de ataque a sus servidores, routers y sistemas internos se multiplican.

Las medidas de **seguridad perimetral** suponen la primera línea de defensa entre las redes públicas y redes corporativas o privadas.

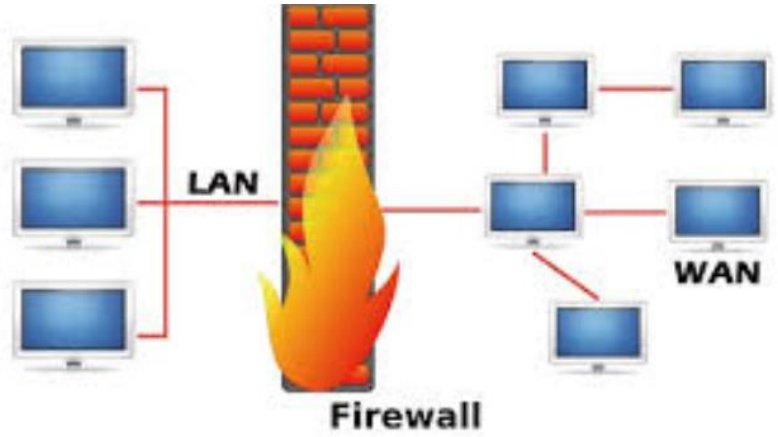


Cortafuegos

Un **cortafuegos o firewall**, es una aplicación o dispositivo diseñado para bloquear comunicaciones no autorizadas, permitiendo al mismo tiempo las que sí lo están.

La configuración para permitir y limitar el tráfico entre diferentes redes o ámbitos de una red, se realiza en base a un conjunto de normas y reglas. Mediante este mecanismo de defensa podemos mantener la seguridad de alto nivel en una red o en una máquina.

La utilización de un cortafuegos es necesaria cuando queremos proteger determinadas zonas de nuestra red o determinados hosts, de amenazas que provengan del exterior o, incluso, de amenazas que se produzcan dentro de nuestra propia red, ya sean por infecciones o ataques.



Cortafuegos Funciones

Objetivos de los cortafuegos:

- Garantizar que no se podrá acceder a los recursos internos desde el exterior sin permiso (archivos compartidos, impresoras de red, …)

- Filtrar los paquetes de entrada y salida, permitiendo o denegando el acceso según su origen o destino, tanto en lo que respecta a la IP como a los puertos.

- Utilizar herramientas de software para llevar un control sobre tráfico de la red.

Cortafuegos Funciones

Funciones de los cortafuegos:

Filtrado de paquetes de red en función de la inspección de alguno de los siguientes elementos:

- dirección MAC
- dirección IP
- puerto origen
- puerto destino

Filtrado por aplicación: permite especificar las aplicaciones concretas que se quieren impedir, así como reglas específicas para cada una de ellas.

Salida / entrada: las distintas reglas de filtrado se pueden aplicar sobre el tráfico saliente o entrante en una determinada interfaz de red.

Tipos de Cortafuegos

Una clasificación posible de unos cortafuegos es por la ubicación en la que se encuentre:

- **Firewalls basados en servidores: aplicación de firewall que se instala y ejecuta en un sistema operativo de red, que normalmente ofrece otra serie de servicios como enrutamiento, proxy, DNS, DHCP, etc.**
- **Firewalls dedicados: son equipos que tienen instalado una aplicación específica de cortafuegos y, por tanto, trabajan de forma autónoma como cortafuegos.**
- **Firewalls integrados: se integran en un dispositivo hardware para ofrecer la funcionalidad de firewall. Como ejemplos, encontramos switches o routers que integran funciones de cortafuegos.**
- **Firewalls personales: se instalan en los distintos equipos de la red de forma que los proteja individualmente de amenazas externas. Por ejemplo, en un equipo doméstico, el cortafuegos preinstalado en un sistema operativo Windows.**

Cortafuegos Arquitecturas

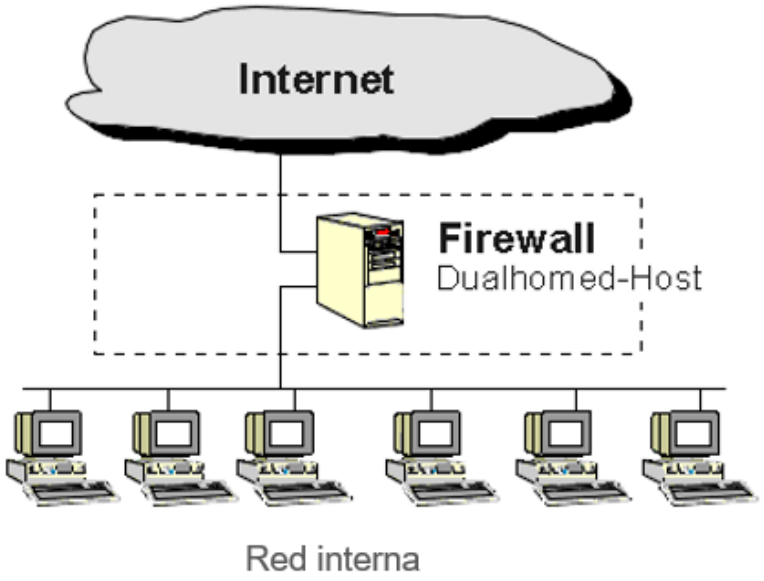
DUAL-HOMED HOST

se basa en el uso de equipos con dos o más tarjetas de red. Una de estas tarjetas se conecta a la red interna que se quiere proteger y la otra a una red externa, normalmente a internet.

Los equipos de la red interna verán al bastión a través de una de las tarjetas de red y los equipos externos a través de la otra, pero el tráfico entre ambas redes estará aislado.

Todo el tráfico debe pasar a través del firewall Instalado en el bastión, y si queremos permitir algún servicio habrá que usar un proxy en el bastión.

La desventaja de esta arquitectura es que si un atacante se hace con el equipo bastión, tendrá acceso a la red interna de la organización.



Cortafuegos Arquitecturas

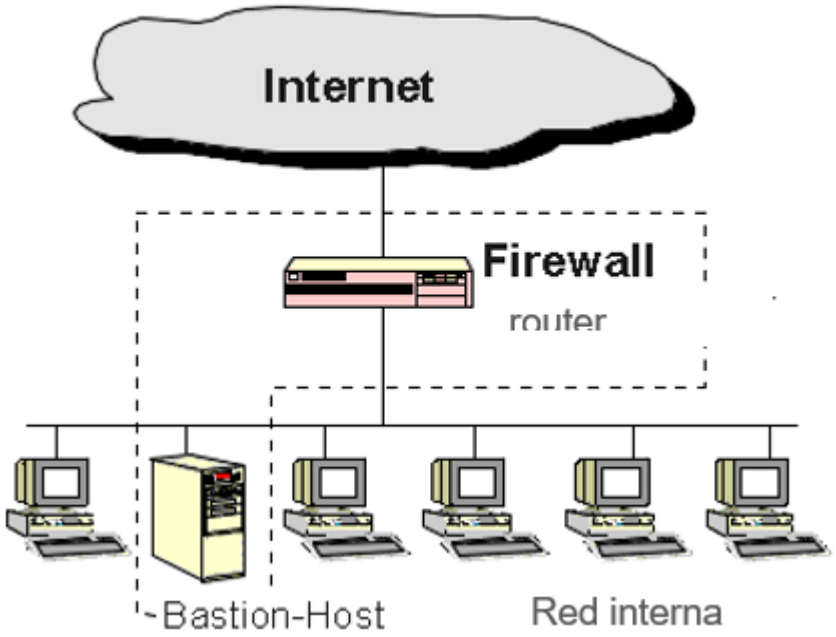
SCREENED-HOST

Arquitectura combina el uso de un router con un bastión, de modo que el filtrado de paquetes se produce en primer lugar en el router.

Cuando un equipo de la red interna quiere acceder a internet, habrá dos opciones:

- El router permitirá a las máquinas de la red interna la salida de algunos servicios, como la navegación web, filtrando los paquetes mediante las reglas de filtrado.

- El router prohíbe todo el tráfico de la red interna hacia el exterior, y si se desea acceder a algún servicio hay que hacerlo a través de la máquina bastión, igual que en la arquitectura dual-homed.



Al igual que en el caso anterior, un atacante que consiga hacerse con el control del bastión o del router, tendría acceso a la red interna.

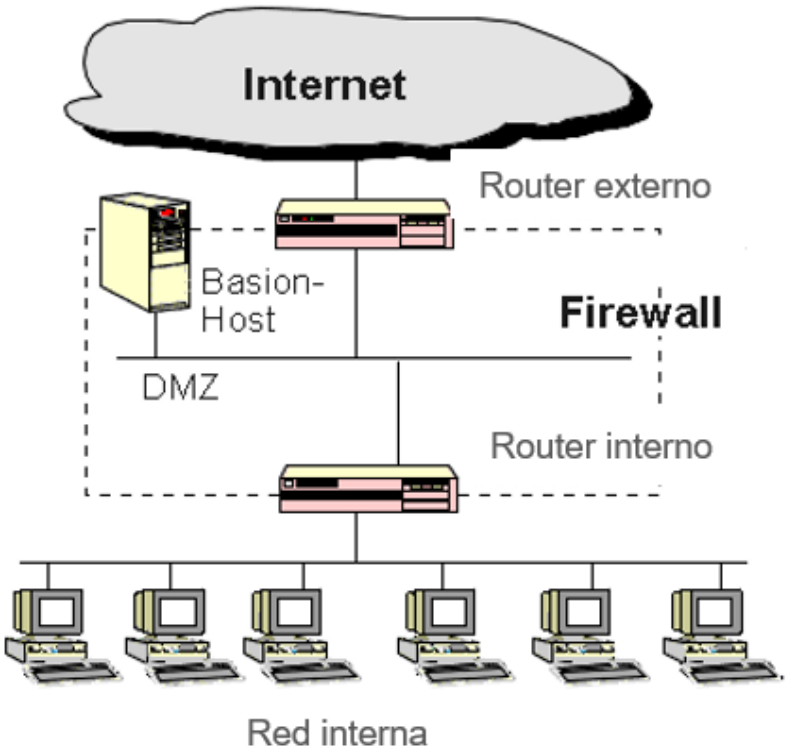
Cortafuegos Arquitecturas

SCREENED-SUBNET

El bastión se aísla en una red perimétrica, la zona DMZ (o zona desmilitarizada), que se sitúa entre la red interna y la red externa limitada por dos routers. El router externo filtra la entrada de tráfico desde la red externa y la salida hacia la misma.

El router interno se ocupa del tráfico generado y dirigido por y hacia los equipos de la red interna

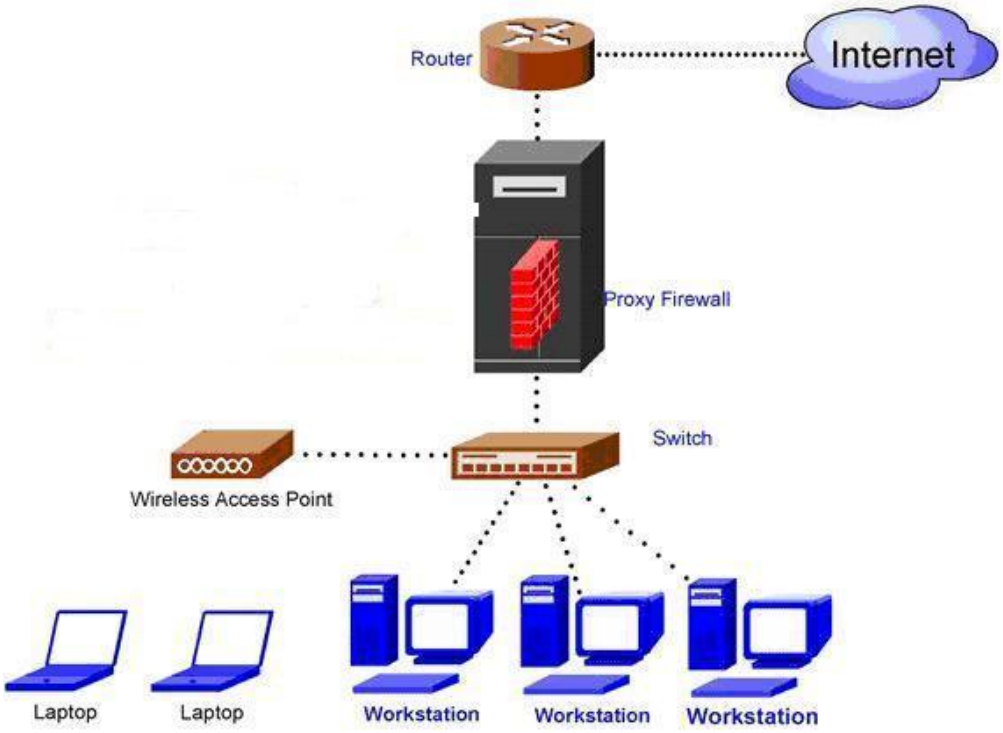
Esta arquitectura es más compleja pero también mucho más segura que las anteriores. Con ella se elimina el principal problema de las dos anteriores. Antes, cuando un atacante llegaba al bastión, tenía acceso a la red interna. Ahora, aunque consiga llegar hasta él, la red interna seguirá protegida.



PROXY

Un **servidor** proxy es una aplicación o sistema que gestiona las conexiones de red, sirviendo de intermediario entre las peticiones de servicios que requieren los clientes, y las respuestas por parte de los servidores externos.

En definitiva objetivo es la centralización del tráfico entre Internet y una red local.



PROXY

La principal **ventaja** de un servidor proxy es la mejora de velocidad de respuesta a peticiones, ya que si varios clientes van a pedir el mismo recurso, el proxy puede hacer **caché**, guardar la respuesta de una petición, y darla directamente cuando otro usuario la pida, sin tener que contactar nuevamente con el destino.

Además, la mayoría de los servidores proxy también añaden **funciones de control y autenticación de usuarios**, reglas de filtrado de los contenidos solicitados, y funciones de registro de logs.

La diferencia entre el filtrado de un firewall y el de un proxy, es que el primero lo hace según las **cabeceras de los niveles de red y transporte**, mientras que el segundo lo hace según el **nivel de aplicación**. El uso principal de un proxy es entonces controlar el acceso a Internet desde la red interna.

PROXY

Funcionamiento:

1. El navegador web (cliente) solicita una página HTML a un servidor web o solicita un archivo de un servidor FTP. Como el navegador web está configurado para acceder a Internet a través de proxy, en realidad la petición la está haciendo al servidor proxy-caché.

2. El proxy-caché recibe la petición y busca en la caché si la página solicitada está almacenada.

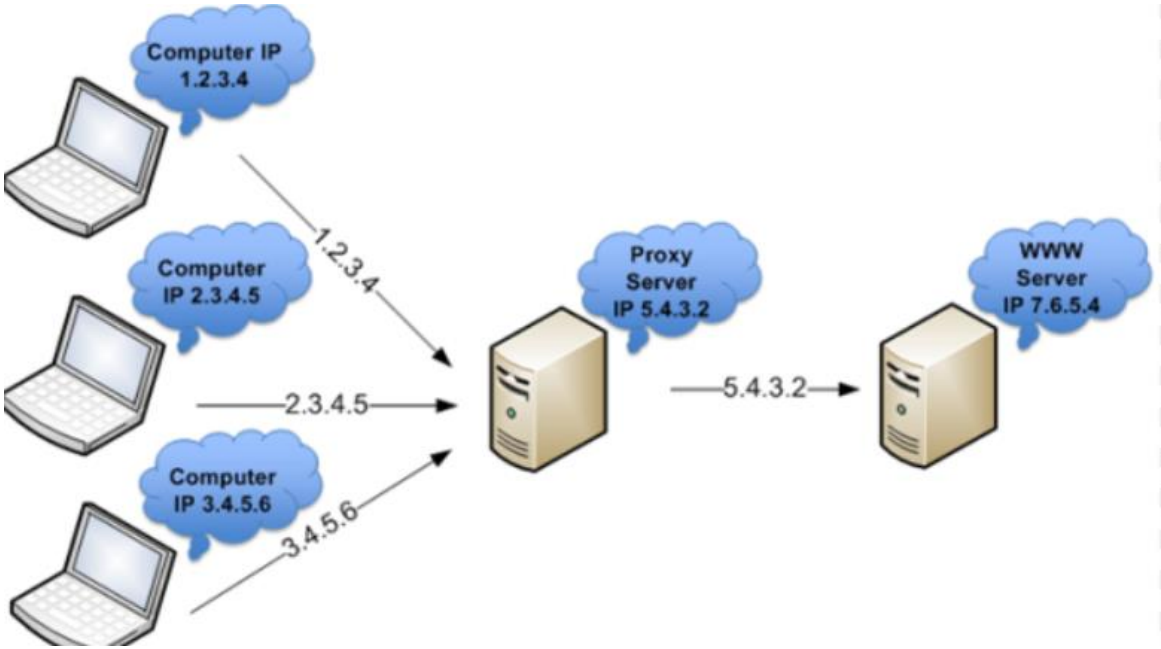
3. Si es la primera vez que se accede a esa página HTML el servidor proxy-caché no la tiene almacenada. El servidor proxy reenvía la petición al servidor web, el cual le devolverá la página solicitada. La guarda en caché y la envía al navegador web que hizo la petición

4. Si el servidor proxy-caché ya tiene almacenada la página HTML, entonces solicita al servidor web que le envíe la cabecera de la página HTML.
   Compara las cabeceras y resuelve:
   - Si la página HTML no se ha modificado, se envía la página en caché.
   - Si la página HTML se ha moficado, el proxy solicita al servidor web la nueva versión de la página

PROXY TIPOLOGÍA

Dependiendo del tipo de tráfico que circule por una red se necesita un tipo de proxy:

- **Proxy caché Web**: proxy para una aplicación específica como el acceso a la web. Mantiene copias locales de los archivos más solicitados y los sirve bajo demanda, reduciendo la velocidad y coste en la comunicación con Internet. El proxy caché almacena el contenido en la caché de los protocolos HTTP, HTTPS e incluso FTP.

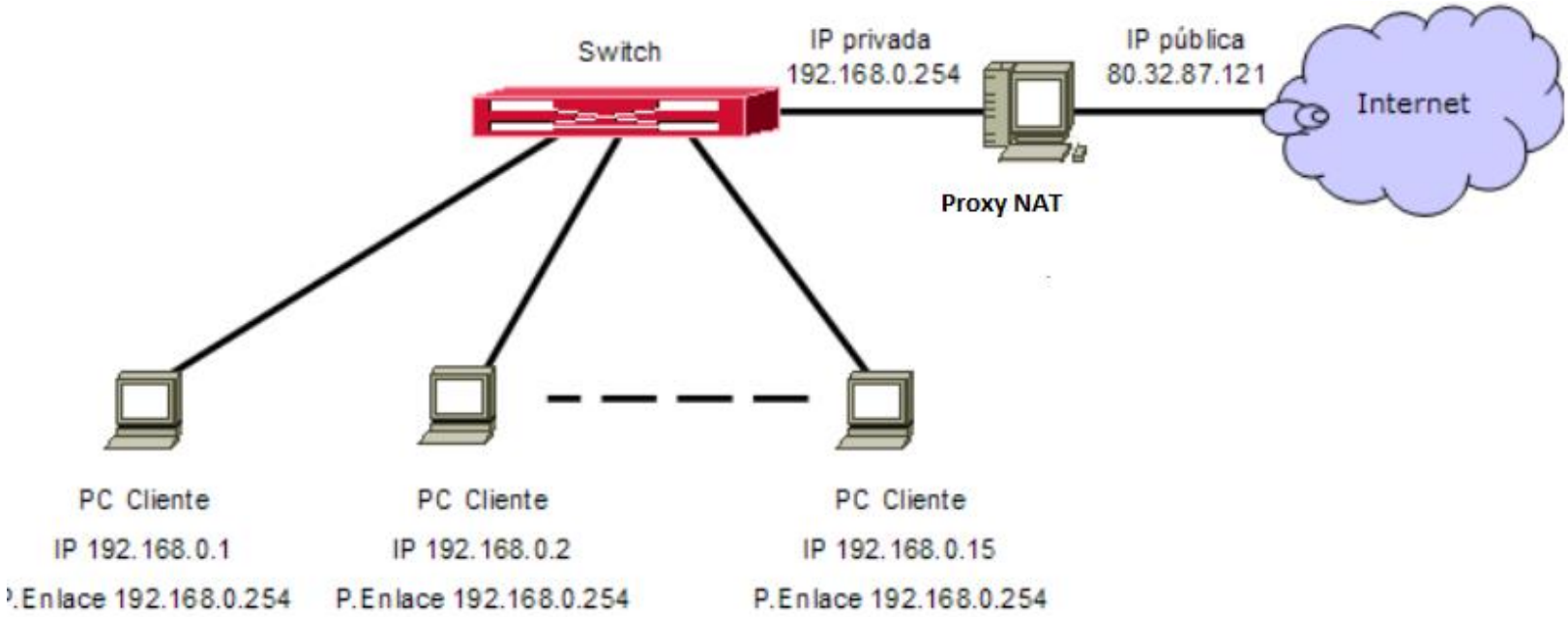


PROXY TIPOLOGÍA

Dependiendo del tipo de tráfico que circule por una red se necesita un tipo de proxy:

- **Proxy NAT**: integración de los servicios de traducción de direcciones de red y proxy.

- **Proxy transparente**: normalmente, un proxy Web o NAT no es transparente al aplicación cliente, es decir el cliente debe ser configurado manualmente para usar el proxy.



PROXY TIPOLOGÍA

Dependiendo del tipo de tráfico que circule por una red se necesita un tipo de proxy:

- **Proxy anónimo:** permiten aumentar la privacidad y el anonimato de los clientes proxy, mediante eliminación de características identificativas (dirección IP del cliente, cookies, identificadores de sesión...).

- **Proxy inverso:** es un servidor proxy instalado en una red con varios servidores web, sirviendo de intermediario a las peticiones externas, suponiendo una capa de seguridad, previa gestión y distribución de carga.