TEMA 7. SEGURIDADE PERIMETRAL

Veremos como proteger la entrada y la salida a nuestra red, para ello estudiaremos distintos elementos y configuraciones.

.

1. 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. Entre otras estudiaremos el uso de cortafuegos ofirewall destinado a bloquear las conexiones no autorizadas, y de servidores proxy que hagan de intermediario entre clientes y servidores finales, permitiendo el filtrado y monitorización de servicios.

2. Cortafuegos

Un cortafuegos o firewall, es una aplicación o dispositivo diseñado para bloquear comunicaciones no autorizadas, permitiendo al mismo tiempo las que si 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 nueva red o determinados hosts, de amenazas que provengan del exterior o, incluso, de amenazas que se provoquen dentro de nuestra propia red ya sean por infecciones o ataques.

Las características fundamentales de los cortafuegos son:

- **Filtrado de paquetes** de red en función de la inspección de direcciones de red: MAC, IP o puerto origen y destino, permitiendo con este último criterio proporcionar un filtrado según las aplicaciones asociadas a dicho puerto.
- **Filtrado por aplicación:** permite especificar las aplicaciones y reglas específicas para cada una de ellas.
- Las distintas **reglas de filtrado** se aplican sobre el tráfico de salida o de entrada en una determinada **interfaz de red**.
- **Registro o logs** de filtrado de paquetes.

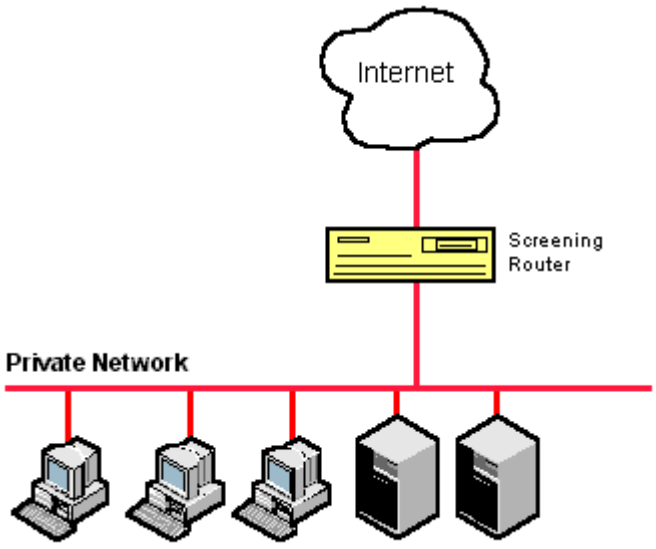
Tipos de cortafuegos

En general, para establecer las diferencias entre los distintos cortafuegos atendemos a la flexibilidad y la facilidad de configuración de los mismos, así como la capacidad de manejo de tráfico. Una clasificación posibles es por la ubicación en la que se encuentre el firewall:

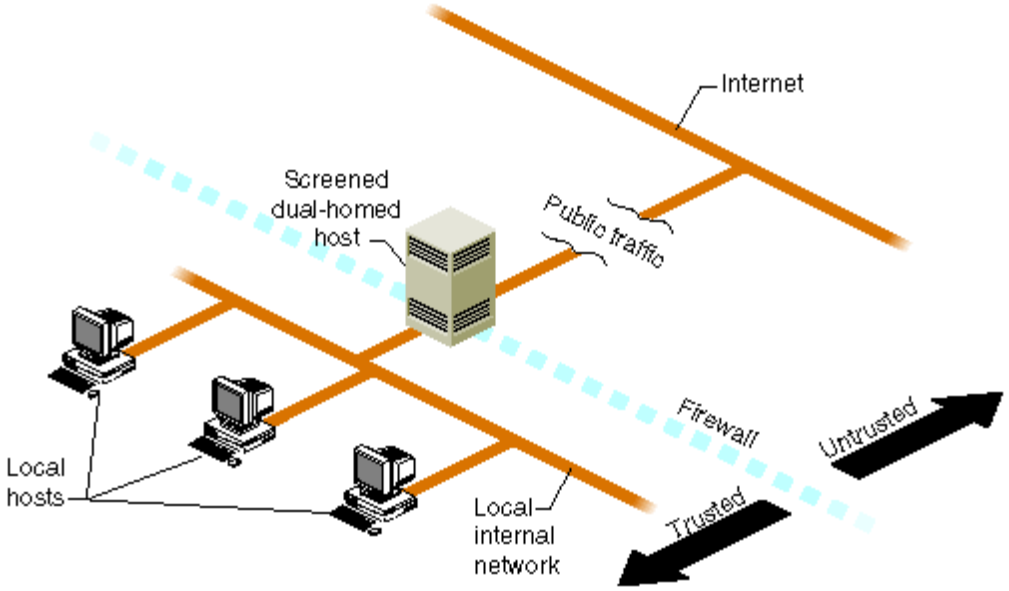
- **Firewalls basados en servidores**: consta de una aplicación de firewall que se instala y ejecuta en un sistema operativo de red (NOS), que normalmente ofrece otra serie de servicios como enrutamiento, proxy, DNS, DHCP, etc.
- **Firewalls dedicados**: son equipos que tienen instalado una aplicación 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 sistemas Windows.

Las arquitecturas de cortafuegos más implementadas son:

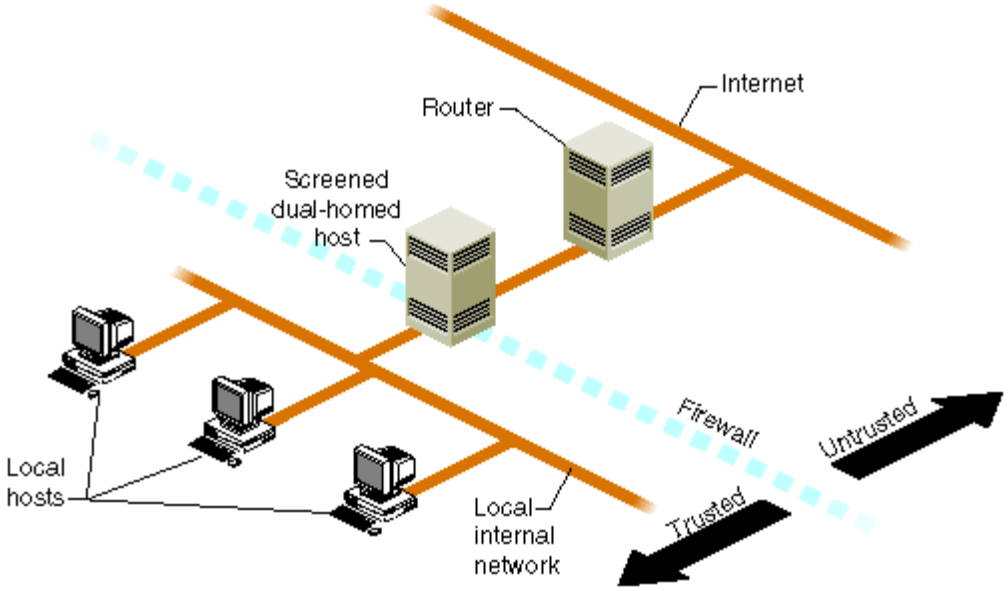
- **Screening router**: como frontera entre la red privada y la red pública se encuentra un router que realiza tareas de filtrado.



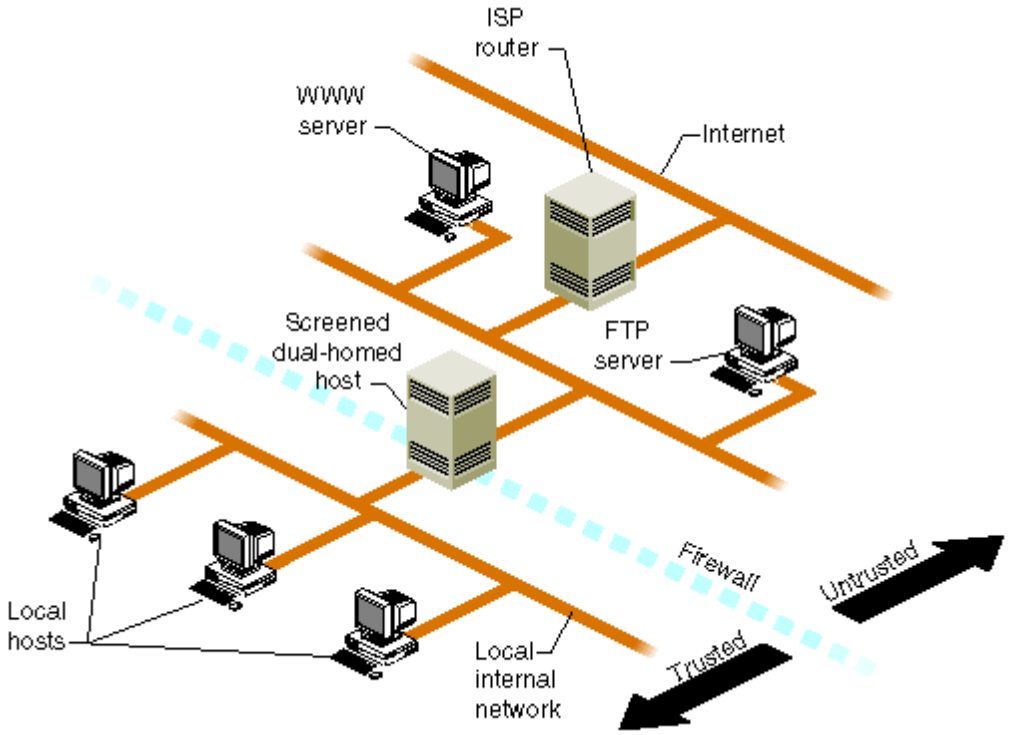
- **Dual Homed-Host**: como frontera se dispone un equipo servidor que realizará tareas de filtrado y enrutamiento mediante al menos 2 tarjetas de red, esto permitirá una mayor flexibilidad en la configuración e instalación de aplicaciones de seguridad.



- **Screened Host:** combina un router como equipo fronterizo exterior y un servidor proxy que filtrará y permitirá añadir reglas de filtrado en las aplicaciones más empleadas. Veremos el uso y configuración de servidores proxy en un apartado posterior.



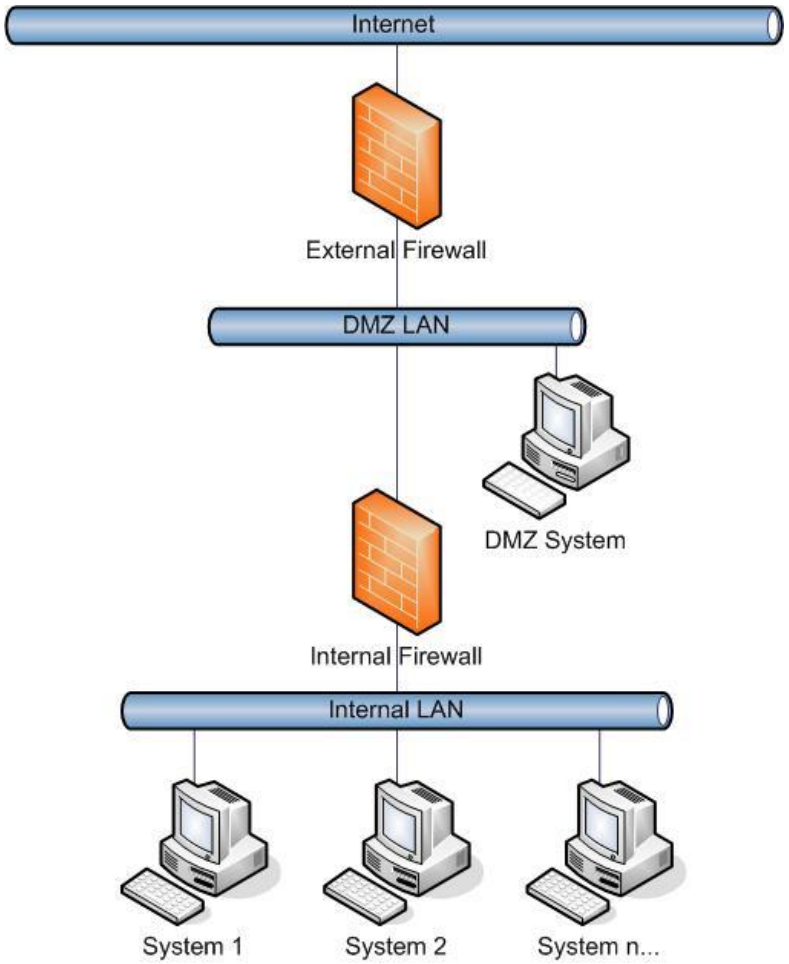
- **Screened-subnet**: mediante la creación de una subred intermedia, denominada DMZ o zona desmilitarizada, entre la red externa y la red privada interna, permitirá tener 2 niveles de seguridad, uno algo menor en el cortafuegos más externo y uno de mayor nivel de seguridad en el cortafuegos de acceso a la red interna.



DMZ

Cuando se realiza el diseño de una red es importante determinar qué equipos ofrecerán servicios de carácter público y por tanto será accesibles desde el exterior de nuestra red corporativa y qué equipos deben ser invisibles desde el exterior para mantener un cierto nivel de seguridad en las comunicaciones internas.

Surge de esta diferenciación el concepto de zona desmilitarizada o **DMZ** (demilitarized zone) o red perimetral. Se trata de una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet, donde se ubican los servidores HTTP, DNS, FTP y otros que sean de carácter público.



Habitualmente, una configuración DMZ es usar dos cortafuegos, donde la DMZ se sitúa en medio y se conecta a ambos cortafuegos, uno conectado a la red interna y el otro a la red externa. Esta configuración ayuda a prevenir configuraciones erróneas accidentales que permitan el acceso desde la red externa a la interna. Este tipo de configuración también es llamado cortafuegos de subred monitoreada (screened-subnet/treiwzZZ).

Por lo general, la política de seguridad para la DMZ es la siguiente:

- **El tráfico de la red externa a la DMZ está autorizado y a la red interna está prohibido.**
- **El tráfico de la red interna a la DMZ está autorizado y a la red externa está autorizado.**

Normalmente el DMZ host está separado de Internet a través de un router y un cortafuegos, o se encuentran integrados. Es aconsejable que en el cortafuegos se abran al exterior únicamente los puertos de los servicios que se pretende ofrecer con los servidores disponibles en la DMZ.

2. Proxy

Un servidor proxy o representante es una aplicación o sistema que gestiona las conexiones de red, sirviendo de intermediario entre las peticiones de servicios que requieren los clientes, como http, FTP, irc, telnet, ssh, etc., creando así una memoria caché de dichas peticiones y respuestas por parte de los servidores externos. La finalidad de este tipo de servidores es poder servir más

rápidamente a sus usuarios en conexiones siguientes que hayan sido solicitadas y respondidas previamente, sin tener que acceder remotamente de nuevo a los servidores externos.

La mayoría de los servidores proxy también añaden funciones de control y autenticación de usuarios, y reglas de filtrado de los contenidos solicitados, así como funciones de registro de logs.

Entre las grandes ventajas de un servidor proxy se encuentra 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 para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.

Para evitar contenidos desactualizados, los servidores proxy actuales, se conectan con el servidor remoto para comprobar que la versión que tiene en caché sigue siendo la misma que la existente en el servidor remoto.

Tipos, características y funciones principales

Dependiendo del tipo de tráfico que circulará por una red necesitaremos un proxy que cumpla con las necesidades del tráfico, ya sea para acelerar la descarga de contenidos para no sobrecargar la salida a Internet o para autenticación de usuarios. En función de las características de cada tipo de proxy podemos clasificarlos de la siguiente manera:

- **Proxy caché Web**: se trata de un proxy para una aplicación específica como el acceso a la web. Mantienen copias locales de los archivos más solicitados y los sirven bajo demanda, reduciendo la baja velocidad y coste en la comunicación con Internet. El proxy caché almacena el contenido en la caché de los protocolos HTTP, HTTPS, incluso FTP.
- **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 a la aplicación cliente: debe ser configurada para usar el proxy, manualmente. Un proxy transparente combina un servidor proxy con NAT (Network Address Translation) de manera que las conexiones al puerto 80 típicamente, son redirigidas hacía el puerto del servicio proxy.
- **Proxy anónimo:** permiten aumentar la privacidad y el anonimato de los clientes proxy, mediante una activa eliminación de características identificativas (dirección IP del cliente, cabeceras From y Referer, cookies, identificadores de sesión...).
- **Proxy inverso**: un reverse proxy 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 de las distintas peticiones externas, gestión de SSL o como caché de contenidos estáticos.
- **Proxy abierto**: acepta peticiones desde cualquier ordenador, esté o no conectado a su red. En esta configuración el proxy ejecutará cualquier petición de cualquier ordenador que pueda conectarse a él, realizándola como si fuera una petición del proxy. Por lo que permite que este tipo de proxy se use como pasarela para el envío masivo de correos de spam, muchos servidores, como los de IRC o correos electrónicos, deniegan el acceso a estos proxys a sus servicios, usando normalmente listas negras (blacklist).

Tras conocer los distintos tipos de proxy pasaremos a instalar y configurar uno.

0. Índice