Cortafuegos

Preguntas

1. ¿En qué consiste un cortafuegos o "firewall"? ¿Qué tipo de tráfico bloquea y a quien va dirigido dicho tráfico? ¿Qué tipo de tráfico no bloquea? ¿Qué no es capaz de hacer un cortafuegos?

Un cortafuegos es un elemento de seguridad de red, que permite o bloquea el tráfico de red que va de un segmento de red a otro, según los parámetros de las cabeceras de red y de transporte de los paquetes de red. En la mayoría de casos los parámetros que el cortafuegos analiza para decidir si filtra o no el paquete son la IP de origen, la IP de destino, el puerto de origen o/y el puerto de destino.

El cortafuegos tiene una lista de reglas, llamada “lista de control de acceso” o ACLs, que se intentan aplicar una a una por orden al paquete de red. Si el paquete encaja con una regla, se le aplica la acción asociada a dicha regla y se descartan las reglas que quedaban. Si el paquete no encaja con ninguna regla, se le aplica una regla más general llamada “política por defecto”.

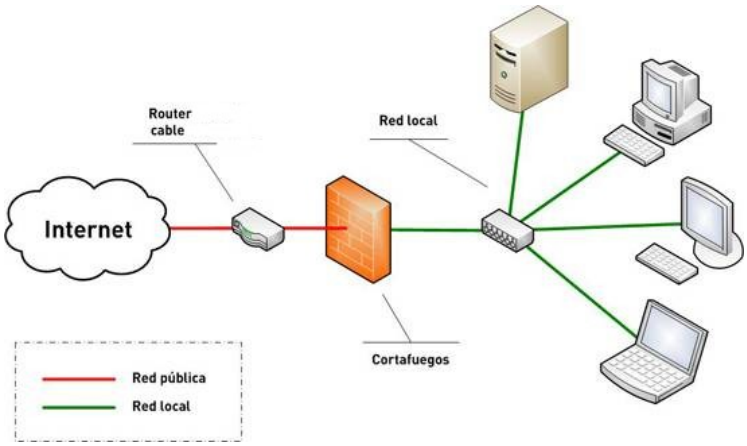
El cortafuegos puede ser un equipo específico, pero también puede estar integrado en un encaminador, por ejemplo. O incluso puede ser un equipo general como un PC con varias tarjetas de red y software específico de cortafuegos.

Debe quedar claro que un cortafuegos no filtra tráfico de red mirando el contenido de los paquetes, aunque algunos cortafuegos de ultima generación incorporan dicha característica. Son los proxy y los Sistemas de Detección de Intrusos los que exploran el contenido de los paquetes a nivel de capa de aplicación.

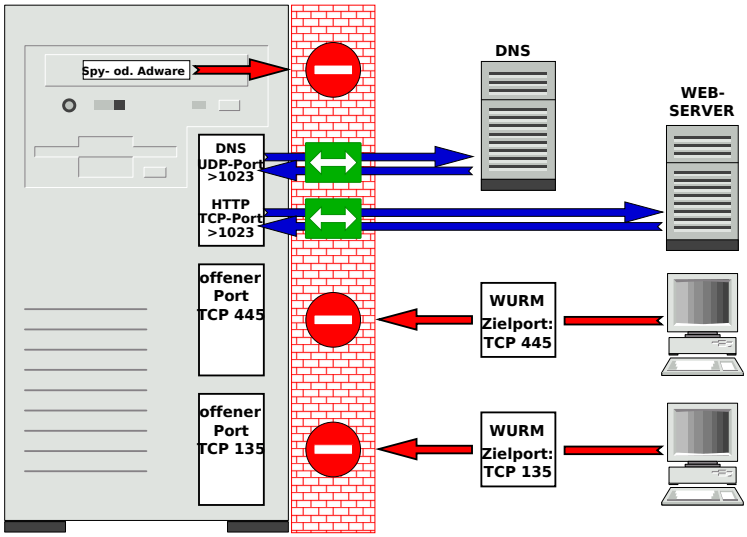
También es evidente que un cortafuegos no puede filtrar el tráfico que no pasa por él, así que una decisión importante es donde colocaremos los cortafuegos en nuestra red.

2. ¿Es lo mismo un cortafuegos de red que un cortafuegos personal? ¿Qué tipo de tráfico bloquea un cortafuegos personal y a quien va dirigido dicho tráfico?

Los cortafuegos de red aíslan redes entre sí, normalmente una red más segura y conocida que llamamos LAN (-y coloreamos en verde en los diagramas de red-) y otra red más insegura y fuera de control que llamamos WAN (-y coloreamos en rojo en los diagramas de red-).



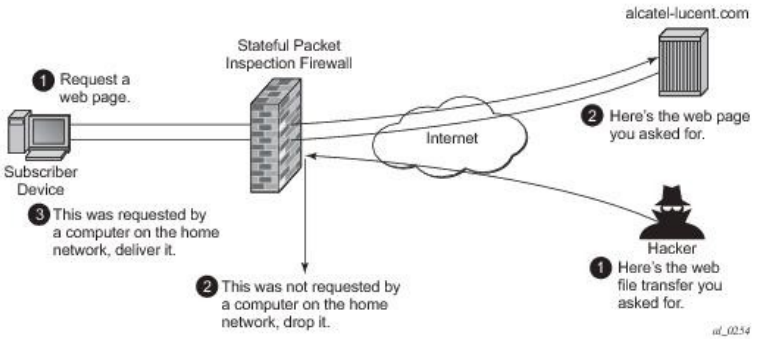
En cambio, un cortafuegos personal es un software de cortafuegos que se instala en un PC y que protege únicamente dicho ordenador. Por ejemplo, el cortafuegos personal de Windows. Debido a que se comunica con el sistema operativo, un cortafuegos personal puede llegar a filtrar paquetes teniendo en consideración la aplicación y el usuario que los lanza, así como el contenido del paquete.



3. ¿Qué es un cortafuegos sin estado o "stateless firewall"? ¿Qué diferencia hay con un cortafuegos con estado o "stateful firewall"?

Un cortafuegos sin estado (“primera generación de cortafuegos”) es un cortafuegos que no sabe en que estado se encuentra la conversación TCP de la que le llega un paquete. Solo puede filtrar utilizando IPs y puertos de origen y de destino. Si hemos dejado un puerto abierto, no sabemos si el primer paquete que llega por él es un TCP SYN de inicio de conexión u otro que no tocaba. Si un ordenador se comunica con el exterior, hemos de dejar puertos abiertos para asegurarnos que la respuesta del exterior entra.

Sin embargo, un cortafuegos con estado (“segunda generación de cortafuegos”), tiene memoria y recuerda el estado de la comunicación TCP para comprobar, no ya si las IPs y puertos son los adecuados, sino si ese paquete corresponde al estado de la conexión que toca. En un cortafuegos con estado podemos, por ejemplo, decirle que deje pasar los paquetes del exterior sólo si son respuesta a una comunicación iniciada des del interior.



4. ¿Puede un cortafuegos incorporar reglas dinámicamente des de aplicaciones? Pon un ejemplo

Sí, a medida que un cortafuegos funciona se pueden añadir nuevas reglas de filtrado.

Imagina por ejemplo un Sistemas de Prevención de Intrusos (IPS) que si detecta muchos intentos de acceso SSH infructuosos des de una misma IP, añade una regla de cortafuegos para bloquear dicha IP. O imagina un IPS que si detecta un ataque de denegación de servicio (DOS), añade una regla de cortafuegos para bloquear las IPs que lanzan el ataque.

5. ¿Qué es una DMZ ("zona desmilitarizada") y para qué sirve?

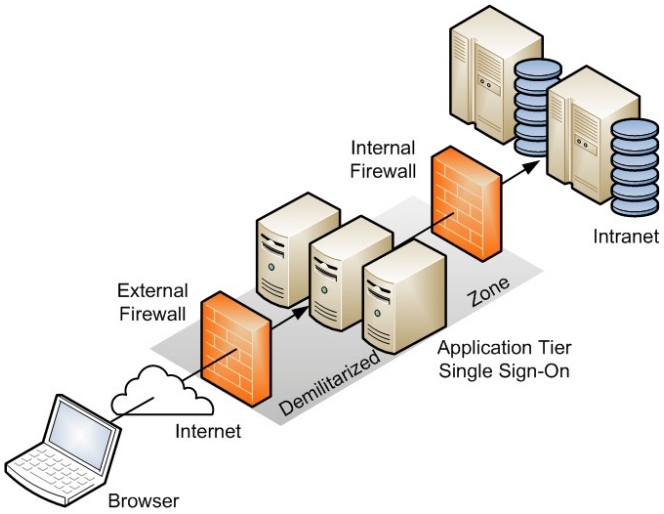
Imagina que tienes tu red protegida del exterior por un cortafuegos detrás de tu router. Sin embargo, existen algunos servicios de tu red a los que quieres dar acceso a clientes de Internet, por lo que abres puertos en el cortafuegos para dejar pasar dicho tráfico. Entonces, si un atacante del exterior consigue, mediante tráfico permitido, tomar control del servidor que está dentro de tu red, puede explorar y atacar el resto de tu red des de dicho servidor, ya que el tráfico interno de tu red no está monitorizado ni bloqueado por el cortafuegos.

Cuando hay sólo una línea de defensa, si el atacante la sobrepasa gana el control de todo. Por ejemplo, el caso de la linea Maginot en la Segunda Guerra Mundial.

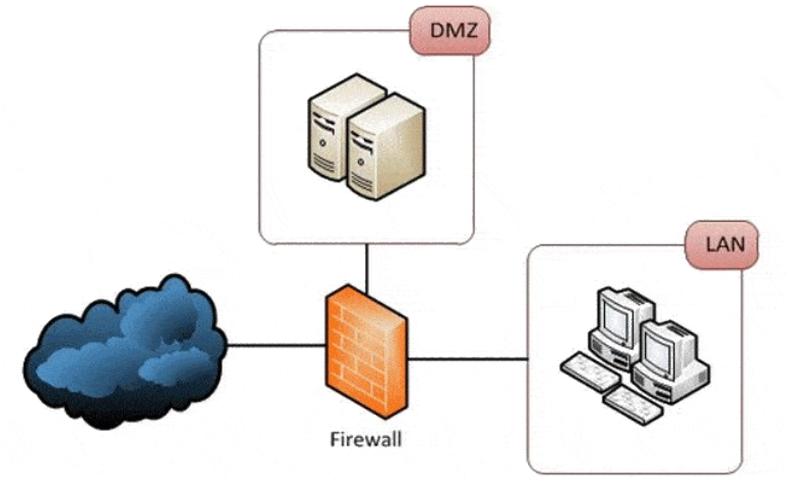
Vamos a aplicar el concepto de seguridad perimetral, en la que no hay una sola línea de defensa, sino varios perímetros defensivos. Si el atacante sobrepasa una línea de protección, detrás encuentra una segunda línea de protección resguardando ítems más valiosos. Piensa en el diseño urbanístico de las ciudades medievales: una muralla protegía toda la ciudad, pero la tenían que abrir para que durante el día entraran mercaderes, por lo que en el interior había una segunda muralla llamada ciudadela protegiendo los palacios.

Una DMZ es una zona de nuestra red (-que coloreamos en naranja en los diagramas de red-), que es parcialmente insegura porque pueden acceder des del exterior. Separamos nuestra red mediante cortafuegos en dos zonas: la DMZ a la que pueden acceder des del exterior a algunos servicios que queremos que sean públicos, y la red más interna con el resto de equipos y servidores, a la que protegemos tanto del exterior como de nuestra DMZ.

Podemos conseguir una DMZ utilizando dos cortafuegos que separan dos redes:



También podemos conseguir una DMZ utilizando un único cortafuegos que separa tres redes:



6. ¿Qué es una política restrictiva? ¿Qué es una política permisiva?

Imagina un profesor en la puerta de clase con la lista "negra" de alumnos que no pueden entrar, que deja entrar a todos los que no están en dicha lista. Pues política permisiva es un cortafuegos con reglas que rechazan paquetes y una política por defecto que deja pasar cualquier paquete que no encaje con ninguna de dichas reglas.

Imagina un vigilante en la puerta de una fiesta con la lista "blanca" de invitados que pueden entrar, que prohíbe el acceso a todos los que no están en dicha lista. Pues política restrictiva es un cortafuegos con reglas que aceptan paquetes y una política por defecto que impide pasar cualquier paquete que no encaje con ninguna de dichas reglas.

Normalmente las políticas permisivas son más fáciles de implementar, pero las políticas restrictivas son más seguras.

7. ¿Viene algún software cortafuegos con Windows Server? ¿Desde dónde se instala y desde dónde se administra? ¿Cuál es el software de cortafuegos comercial más conocido para Windows?

Con Windows viene el cortafuegos personal de Windows. Además, todos los antivirus comerciales traen software de cortafuegos personal integrado. Y por si fuera poco hay otro software de cortafuegos personal como Zone Alarm y Comodo Firewall.

Sin embargo, no conozco ningún software que convierta un Windows en un cortafuegos de red.

8. ¿Cuál es el software de cortafuegos más conocido para Linux? ¿Y para otros sistemas Unix? ¿Qué sistema Unix y distribuciones Linux son especialmente seguras para instalar PCs que hagan de cortafuegos y sistemas de detección de intrusos?

El filtro de paquetes de Linux se llama Netfilter, y en BSD se llama IPFilter.

A dicho cortafuegos se le añaden reglas mediante comandos como iptables, nftables y ufw.

También se pueden añadir reglas mediante interfaz gráfica como gufw, fwbuilder y shorewall.

Por último, existen distribuciones de Linux y BSD que convierten un PC con varias tarjetas de red en un cortafuegos de red administrado remotamente vía web. Entre ellas están Endian, pfSense, OPNsense, o IPFire.