# Firewalls

Los firewalls son la primera línea de defensa entre la red interna y las redes no confiables como Internet. Debe pensar en los firewalls en términos de lo que realmente necesita proteger, por lo que logrará el nivel adecuado de protección para su entorno.

Introducido por primera vez conceptualmente a finales de la década de 1980 en un documento técnico de Digital Equipment Corporation, "firewalls" proporcionó una función entonces nueva e importante para las redes de rápido crecimiento del día. Antes de que el hardware dedicado estuviera disponible comercialmente, las listas de control de acceso basadas en enrutador se utilizaron para proporcionar protección básica y segregación para redes. Sin embargo, demostraron ser inadecuados como emergentes malware y técnicas de hacking rápidamente desarrolladas. Consecuentemente, los firewalls evolucionaron con el tiempo para que su funcionalidad se moviera la pila OSI de la capa tres a la capa siete.

## La evolución de los firewalls

Los firewalls de primera generación eran simplemente permitir/denegar motores para el tráfico de la capa tres, trabajando mucho como un dispositivo de lista de control de acceso purposed. Originalmente, los firewalls de primera generación se utilizaron principalmente como filtros de paquetes basados en encabezados, capaces de comprender la información de origen y destino hasta la capa OSI cuatro (puertos). Sin embargo, no pudieron realizar ninguna operación "inteligente" en el tráfico que no sea "permitir o negar de esta dirección IP de origen predefinida a esta dirección IP de destino predefinida en estos puertos TCP y UDP predefinidos."

Los firewalls de segunda generación fueron capaces de realizar un seguimiento de las sesiones de red activas, poniendo su funcionalidad eficazmente en la capa cuatro. Estos se denominaron *cortafuegos con estado* o, menos comúnmente, *pasarelas de circuito*. Cuando una dirección IP (por ejemplo, un equipo de escritorio) conectado a otra dirección IP (digamos, un servidor Web) en un puerto TCP o UDP específico, el Firewall introduciría estas características de identificación en una tabla en su memoria. Esto permitió que el Firewall realizar un seguimiento de las sesiones de red, lo que podría darle la capacidad de bloquear *Man-in-the-Middle (MITM)* ataques de otras direcciones IP. En algunos firewalls sofisticados, un par de alta disponibilidad (HA) podría intercambiar tablas de sesiones de modo que si un firewall fallaba, una sesión de red podría reanudar a través del otro Firewall.

## Application Control

Desde el principio, los firewalls siempre han sido pensados para manejar el tráfico de aplicaciones. Algunas aplicaciones están autorizadas y otras no. Por ejemplo, el tráfico web saliente a los sitios web de Internet es comúnmente permitido, mientras que algunos tipos de software peer-to-Peer no lo son. En aquellas aplicaciones que se permiten, ciertos comportamientos se permiten dentro de la aplicación y otros no. Por ejemplo, el software de reuniones y colaboración basado en Web podría estar aprobado para su uso en Internet, pero las funcionalidades de uso compartido de archivos podrían estar restringidas.

Los firewalls de primera y segunda generación podrían restringir las aplicaciones sencillas que funcionaban en puertos bien conocidos. En aquel entonces, las aplicaciones se comportaban bien, comunicándose en puertos asignados que estaban bien documentados, por lo que eran fáciles de controlar. Pero los desarrolladores de aplicaciones no siempre querían estar sujetos al control, por lo que idearon una manera simple pero eficaz de obtener a través del firewall: Utilice el puerto 80. Esto se conoce como "tunelización" o "elusión". Puesto que el tráfico web utiliza el protocolo HTTP sobre el puerto TCP 80, tuvo que ser permitido pasar a través del firewall sin restricción. No había una manera práctica de realizar un seguimiento de los millones de direcciones IP en Internet, por lo que las aplicaciones podían comunicarse libremente y sus desarrolladores estaban contentos.

• **Peer-to-peer file sharing** Comunicación directa de sistema a sistema desde una estación de trabajo interna a otra en Internet que podría filtrar documentos confidenciales, o exponer a la organización a la responsabilidad de violaciones de derechos de autor de música y películas
• **Browser-based file sharing** Sitios web que proporcionan almacenamiento de archivos de Internet a través de un navegador web, que permiten a personas de confianza dentro de la red de una organización copiar archivos fuera del área de control del administrador de seguridad
• **Web mail** Servicios de correo con la capacidad de agregar archivos adjuntos a los mensajes, proporcionando un camino al robo y fuga de materiales confidenciales

• **Internet proxies and circumventors** Servicios que se ejecutan en Internet o en estaciones de trabajo locales explícitamente diseñados para eludir los controles de seguridad como el filtrado web
• **Remote access** Herramientas de administración remota, normalmente utilizadas por los administradores del sistema para admitir sistemas internos de Internet, que podrían ser abusados por atacantes de Internet

### Cuando las aplicaciones se cifran

Las aplicaciones que deseen omitir firewalls pueden cifrar su tráfico. Esto hace que el trabajo del firewall sea más difícil al renderizar la mayor parte de la comunicación ilegible. Bloquear todo el tráfico cifrado no es realmente factible, excepto en entornos altamente restringidos donde la seguridad es más importante que la funcionalidad de la aplicación, y una política de "permiso por excepción" bloquea todo el tráfico de aplicaciones cifrados, excepto en una lista blanca de aplicaciones permitidas y conocidas.

Y la capacidad de descifrado de amplio espectro no está al alcance de la mayoría de los consumidores y las empresas, a pesar de los avances de la ley de Moore pronosticados al por mayor de poder informático.

Sin embargo, el control de las comunicaciones de la aplicación todavía se puede hacer incluso si el tráfico está cifrado, por algunos de los firewalls de cuarta generación más avanzados. Las aplicaciones son más fáciles de identificar por las firmas únicas dentro de sus flujos de datos, pero también hay otras características de identificación. La mayoría tienen un "Protocolo de Handshake" que rige el inicio de una sesión, y estos suelen tener un patrón identificable. Muchos también tienen direcciones IP identificables en Internet con las que se comunican. Incluso el análisis del patrón de tráfico es posible con capacidades heurísticas. Una gran cantidad de información puede ser obtenida sólo a partir de la frecuencia, el tamaño y el tiempo de las comunicaciones.

## Características que un firewall deben tener

Se espera que los firewalls de hoy hagan mucho más que simplemente bloquear el tráfico en función de la apariencia externa del tráfico (como el puerto TCP o UDP). A medida que las aplicaciones se han vuelto cada vez más complejas y adaptables, el Firewall se ha vuelto más sofisticado en un intento de controlar esas aplicaciones. Debe esperar al menos las siguientes funcionalidades de su firewall.

### Conocimiento de la aplicación

El Firewall debe poder procesar e interpretar el tráfico por lo menos de las capas OSI del tres al siete. En la capa tres, debe ser capaz de filtrar por la dirección IP; en la capa cuatro por puerto; en la capa cinco por sesiones de red; en la capa seis por tipo de datos y, lo más importante, en la capa siete para administrar correctamente las comunicaciones entre las aplicaciones.

### Accurate Application Fingerprinting

El Firewall debe ser capaz de identificar correctamente las aplicaciones, no sólo en función de su apariencia externa, sino también por el contenido interno de sus comunicaciones de red. La identificación correcta de la aplicación es necesaria para garantizar que todas las aplicaciones están debidamente cubiertas por la configuración de la Directiva de Firewall.

### Granular Application Control

Además de permitir o negar la comunicación entre aplicaciones, el Firewall también necesita ser capaz de identificar y caracterizar las características de las aplicaciones para que puedan gestionarse adecuadamente. La transferencia de archivos, el uso compartido de escritorio, la voz y el vídeo y los juegos en la aplicación son ejemplos de características potencialmente no deseadas que el Firewall debe poder controlar.

### Administracion de Ancho de banda - Bandwidth Management (QoS)

La calidad de servicio (QoS) de las aplicaciones preferidas, que podrían incluir voz sobre IP (VoIP), por ejemplo, se puede administrar a través del firewall basándose en la disponibilidad de ancho de banda de red en tiempo real. Si un evento deportivo se transmite en directo a través de streaming de vídeo en un sitio web popular, su firewall debe ser capaz de limitar de forma proactiva o bloquear el acceso para que todas aquellas personas que quieran verla no derriten su red. El Firewall debe integrarse con otros dispositivos de red para garantizar la mayor disponibilidad posible para los servicios más críticos.

# Core Firewall Functions

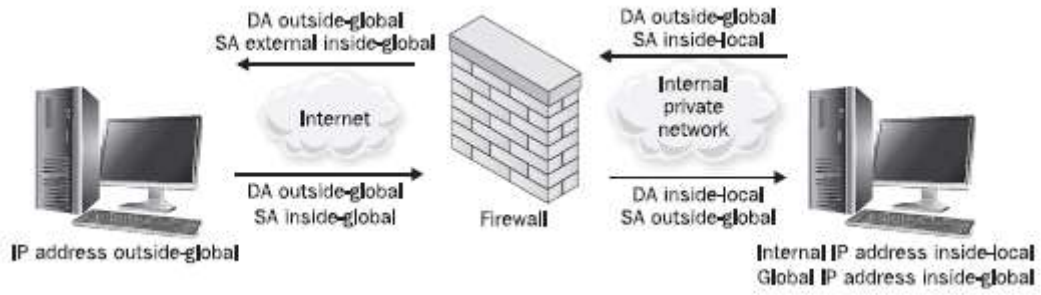
Debido a su ubicación dentro de la infraestructura de red, los firewalls están idealmente ubicados para realizar ciertas funciones además de controlar la comunicación de la aplicación. Éstos incluyen la traducción de la dirección de red (NAT), que es el proceso de convertir una dirección IP a otra, y el registro del tráfico.

# Network Address Translation (NAT)

La versión principal de TCP/IP utilizada en Internet es la versión 4 (IPv4). La versión 4 de TCP/IP se creó con un espacio de direcciones de 32 bits divididos en cuatro octetos, proporcionando matemáticamente aproximadamente 4 mil millones direcciones. Curiosamente, esto no es suficiente. Se ha desarrollado una versión más reciente de IP, denominada IPv6, para superar esta limitación de espacio de direcciones, pero aún no está en un despliegue generalizado.

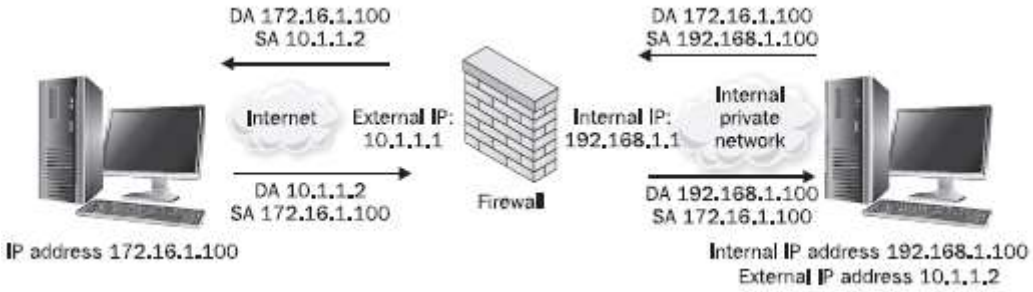
Para conservar las direcciones IPv4, RFC 1918 especifica bloques de direcciones que nunca se utilizarán en Internet. Estos rangos de red se denominan redes "privadas". Esto permite a las organizaciones utilizar estos bloques para sus propias redes corporativas sin preocuparse por conflictos con una red de Internet. Sin embargo, cuando estas redes están conectadas a Internet, deben traducir sus direcciones de red IP privadas en direcciones IP públicas (NAT) para ser enrutables. Al hacer esto, un gran número de hosts detrás de un Firewall puede turnarse o compartir algunas direcciones públicas al acceder a Internet.

| Address | Mask | Range |
|---|---|---|
| 10.0.0.0 | 255.0.0.0 | 10.0.0.0–10.255.255.255 |
| 172.16.0.0 | 255.240.0.0 | 172.16.0.0–172.31.255.255 |
| 192.168.0.0 | 255.255.0.0 | 192.168.0.0–192.168.255.255 |




## Static NAT

Una configuración NAT estática siempre da como resultado la misma traducción de direcciones. El host se define con una dirección local y una dirección global correspondiente en una relación de 1:1 y no cambian. La traducción NAT estática reescribe las direcciones IP de origen y de destino según sea necesario para cada paquete mientras viaja a través del firewall. Ninguna otra parte del paquete se ve afectada. Esto se utiliza típicamente para los servidores internos que necesitan ser accesibles de Internet confiablemente en una dirección IP que no cambie.




## Dynamic NAT

NAT dinámica se utiliza para asignar un grupo de direcciones locales internas a una o más direcciones globales. El conjunto de direcciones global suele ser menor que el número de direcciones locales internas, y la conservación de las direcciones previstas por RFC 1918 se logra solapando este espacio de direcciones. El NAT dinámico se implementa generalmente simplemente creando los NATs estáticos cuando un host interior envía

un paquete a través del firewall. El NAT entonces se mantiene en las tablas del firewall hasta que algún evento hace que se termine. Este evento es a menudo un temporizador que expira después de una cantidad predefinida de inactividad desde el host interno, eliminando así la entrada NAT. Esta dirección puede ser reutilizada por un host diferente.

Una ventaja de NAT dinámica sobre NAT estática es que proporciona un conjunto de direcciones IP en constante cambio desde la perspectiva de un atacante basado en Internet, lo que dificulta la segmentación de sistemas individuales. La mayor desventaja de NAT dinámica es el límite en el número de usuarios simultáneos en el interior que pueden acceder a recursos externos simultáneamente. El Firewall simplemente se ejecutará sin direcciones globales y no podrá asignar nuevos hasta que los temporizadores inactivos comiencen a liberar direcciones globales.

### Port Address Translation

Con la traducción de direcciones de puerto (PAT), todo el espacio de direcciones local interior se puede asignar a una única dirección global. Esto se hace modificando las direcciones de puerto de comunicación además de las direcciones IP de origen y destino. Por lo tanto, el Firewall puede utilizar una sola dirección IP para varias comunicaciones mediante el seguimiento de los puertos que están asociados con las sesiones. En el ejemplo representado en la figura 15-3, el host emisor inicia una conexión web en el puerto de origen 1045. Cuando el paquete atraviesa el firewall, además de substituir la dirección IP de origen, el Firewall traduce el puerto de origen al puerto 5500 y crea una entrada en una tabla de asignación para el uso en traducir los paquetes futuros. Cuando el Firewall recibe un paquete de nuevo para el puerto de destino 5500, sabrá cómo traducir la respuesta correctamente. Utilizando este sistema, miles de sesiones pueden ser PATed detrás de una sola dirección IP simultáneamente.

## Auditing and Logging

Los firewalls son excelentes auditores. Dado un montón de espacio en disco o capacidades de registro remoto, pueden registrar cualquier tráfico que pasa a través de ellos. Los intentos de ataque dejarán pruebas en los registros, y si los administradores están observando los sistemas diligentemente, los ataques se pueden detectar antes de que tengan éxito. Por lo tanto, es importante que la actividad del sistema se registre y monitorean. Los firewalls deben registrar los eventos del sistema que sean exitosos y infructuosos. El registro detallado y las revisiones oportunas de esos registros pueden alertar a los administradores sobre actividades sospechosas antes de que ocurra una infracción de seguridad grave. Dado que esto puede generar un gran volumen de tráfico de registro, los registros se envían mejor a un sistema de información de seguridad y administración de eventos (SIEM) que puede filtrar, analizar y realizar la detección de comportamientos heurísticos para ayudar a los administradores de red y de seguridad.

## Funcionalidades de Firewall adicionales

Los firewalls modernos pueden hacer más que administrar las comunicaciones y comportamientos de las aplicaciones; también pueden ayudar en otras áreas de calidad y rendimiento de la red. Las características varían según el fabricante y la marca, pero probablemente encontrará que puede resolver otros problemas en su entorno con el mismo firewall que utiliza para proteger el tráfico de red.

### Bloqueo de ejecución de malware de aplicaciones y sitios web

En los viejos tiempos (hace sólo unos pocos años), los virus requerían que un usuario hiciera clic en algún enlace o botón disfrazado para ejecutarlo. Si los usuarios finales eran lo suficientemente sofisticados como para reconocer los trucos de los escritores de virus, estos virus no iban a llegar muy lejos. El malware moderno puede ejecutarse y propagarse sin la intervención de los usuarios finales. A través de la ejecución automática basada en navegador de código (a través de ActiveX o Java, por ejemplo), simplemente abrir una página web puede activar un virus.

Los archivos PDF de Adobe también pueden transmitir malware, debido a su extenso marco de aplicación subyacente. Los firewalls con capacidad anti-malware avanzado deben ser capaces de detectar estos vectores "invisibles" de malware y detenerlos en sus pistas. También deben ser capaces de bloquear la comunicación "de vuelta a casa" a un servidor de comando y control (CnC) una vez que el malware se implante con éxito en un sistema de la víctima y trata de llegar de nuevo a su controlador para obtener instrucciones.

## Antivirus

Los firewalls que son lo suficientemente sofisticados para detectar malware pueden (y deberían) bloquearlo en la red. Los gusanos que intentan propagarse y extenderse automáticamente en la red, y el malware que intenta "llamar a casa", puede ser detenido por el firewall, confinando su alcance. Las soluciones de control de malware deben estar superpuestas y el Firewall puede formar un componente importante de una capacidad de bloqueo de malware basada en la red para complementar el software antivirus de su organización.

## Detección de intrusiones y prevención de intrusiones

Los sistemas de detección de intrusiones (IDSs) y los sistemas de prevención de intrusiones (IPSs) se analizan con más detalle en el capítulo 18. Los firewalls pueden proporcionar capacidades IDS e IPS en el perímetro de la red, lo que puede ser una adición o sustitución útil para los sistemas de detección y prevención de intrusiones diseñados de forma estándar, especialmente en una estrategia estratificada.

## Web Content (URL) Filtrado y almacenamiento en caché

El Firewall está posicionado óptimamente en la red para filtrar el acceso a los sitios web (entre las redes internas de una organización e Internet). Puede optar por implementar un servicio o sistema de filtrado de URL independiente, o puede obtener un firewall que tenga la capacidad incorporada. Los firewalls actuales están demostrando las capacidades de filtrado de contenido web que rivalizan con los de los sistemas construidos específicamente, por lo que es posible que pueda ahorrar dinero haciendo el filtrado en el firewall, especialmente si no cuesta más.

## E-Mail (Spam) Filtering

Al igual que con el filtrado de contenido Web, los firewalls modernos pueden restar el spam de sus mensajes de correo electrónico antes de que se entreguen a su servidor de correo. Puede registrarse para obtener un servicio externo o comprar un filtro de spam creado específicamente, pero con un firewall que incluye esta capacidad, tiene otra opción.

## Mejore el rendimiento de la red

Los firewalls deben poder ejecutarse a "velocidad de cable", lo suficientemente rápido como para evitar el tráfico de aplicaciones con cuellos de botella. Deben ser capaces de realizar todas las funciones que se han habilitado sin afectar al rendimiento. Además, los firewalls deben ser capaces de asignar el ancho de banda de red a las aplicaciones más críticas para garantizar QoS, sin sacrificar la funcionalidad de filtrado. Como las características del firewall continúan siendo más sofisticadas, el hardware subyacente necesita mantenerse al tanto. Si su red tiene una tolerancia baja para el impacto en el rendimiento, querrá considerar las plataformas de firewall que están construidas para la velocidad.

# Diseño de cortafuegos

Los firewalls pueden ser programas basados en software o, más comúnmente, dispositivos diseñados específicamente. A veces las funciones de cortafuegos son proporcionadas realmente por una colección de varios diversos dispositivos. Las características específicas de la plataforma de firewall y el diseño de la red donde reside el firewall son componentes clave de la protección de una red. Para ser efectivos, los firewalls deben colocarse en las ubicaciones correctas de la red y configurarse eficazmente. Las mejores prácticas incluyen:

• Todas las comunicaciones deben pasar a través del firewall. La efectividad del firewall se reduce considerablemente si hay disponible una ruta de enrutamiento de red alternativa; el tráfico no autorizado se puede enviar a través de una ruta de red diferente, omitiendo el control del firewall. Piense en el firewall en términos de un candado en su puerta principal. Puede ser la mejor cerradura del mundo, pero si la puerta trasera está abierta, los intrusos no tienen que romper la cerradura en la puerta principal-que pueden ir a su alrededor. Se confía en la cerradura de la puerta para evitar el acceso no autorizado a través de la puerta, y un firewall se confía semejantemente para prevenir el acceso a su red.

• El Firewall solo permite el tráfico autorizado. Si no se puede confiar en el firewall para diferenciar entre el tráfico autorizado y no autorizado, o si está configurado para permitir comunicaciones peligrosas o no necesarias, su utilidad también disminuye.

• En una situación de error o sobrecarga, un firewall siempre debe fallar en un estado "deny" o Closed, bajo el principio de que es mejor interrumpir las comunicaciones que dejar los sistemas desprotegidos.

• El Firewall debe diseñarse y configurarse para resistir ataques sobre sí mismo.
Debido a que se confía en el firewall para detener los ataques, y nada más se implementa para proteger el firewall en sí contra tales ataques, debe ser endurecido y capaz de soportar ataques directamente sobre sí mismo.

# Fortalezas y debilidades del firewall

Un Firewall es solo un componente de una arquitectura de seguridad general. Sus fortalezas y debilidades deben tenerse en cuenta al diseñar la seguridad de la red.

## Fortalezas de Firewall

Tenga en cuenta las siguientes fortalezas de Firewall al diseñar la seguridad de red:

• Los firewalls son excelentes para hacer cumplir las políticas de seguridad. Deben configurarse para restringir las comunicaciones a lo que la administración ha determinado y acordado con el negocio para ser aceptable.

• Los firewalls se utilizan para restringir el acceso a servicios específicos.
• Los firewalls son transparentes en la red, sin necesidad de software en las estaciones de trabajo del usuario final.
• Los firewalls pueden proporcionar auditorías. Dado un montón de espacio en disco o capacidades de registro remoto, pueden registrar tráfico interesante que pasa a través de ellos.
• Los firewalls pueden alertar a personas apropiadas de eventos especificados.

## Debilidades del firewall

También debe tener en cuenta las siguientes debilidades del firewall al diseñar la seguridad de red:

• Los firewalls son tan efectivos como las reglas que se configuran para aplicar. Un conjunto de reglas excesivamente permisiva reducirá la efectividad del firewall.
• Los firewalls no pueden detener los ataques de ingeniería social o un usuario autorizado intencionalmente utilizando su acceso con fines maliciosos.
• Los firewalls no pueden imponer directivas de seguridad que están ausentes o no definidas.
• Los firewalls no pueden detener los ataques si el tráfico no pasa a través de ellos.

# Ubicación del firewall

Un firewall normalmente se encuentra en el perímetro de la red, directamente entre la red y cualquier conexión externa. Sin embargo, los sistemas de Firewall adicionales pueden estar ubicados dentro del perímetro de la red para proporcionar una protección más específica a hosts concretos con requisitos de seguridad más altos.

# Configuración del firewall

Al crear una regla establecida en un firewall, tenga en cuenta las siguientes prácticas:

• Cree reglas de más a menos específicas. La mayoría de los firewalls procesan sus conjuntos de reglas de arriba a abajo y detienen el procesamiento una vez que se realiza una coincidencia. La colocación de reglas más específicas en la parte superior impide que una regla general oculte una regla específica más abajo del conjunto de reglas.

• Coloque las reglas más activas cerca de la parte superior del conjunto de reglas. Los paquetes de cribado son una operación intensiva del procesador, y como se mencionó anteriormente, un firewall dejará de procesar el paquete después de emparejarlo con una regla. Colocando sus reglas populares primero o segundo, en lugar de 30 o 31, guardará el procesador de pasar por
más de 30 reglas para cada paquete. En situaciones donde se procesan millones de paquetes y los conjuntos de reglas pueden ser miles de entradas de longitud, el ahorro de CPU podría ser considerable.

• Configure todos los firewalls para que descarte paquetes "imposibles" o "no enrutables" de Internet, como los de una interfaz externa con direcciones de origen que coincidan con la red interna, RFC 1918 direcciones IP

"privadas" y paquetes de difusión. Ninguno de estos se espera de Internet, por lo que si se ven, que representan el tráfico no deseado, como el producido por los atacantes.