FIREWALLS

INTEGRANTES:

Luque Sugrañes, Francisco Javier

Paschini, Catalina

ASIGNATURA: auditoria y seguridad informática

AÑO: 2021

DOCENTE: Mariano Aliaga

Desde tiempos antiguos, el ser humano intentó tener la mayor información posible, ya sea para ganar una guerra, invertir en un negocio, determinar políticas, entre otras para su beneficio. Para lograr esta ventaja se recurría a los métodos más ingeniosos para lograrlo, como infiltrarse dentro de una organización para acceder a sus instalaciones y así hacerse de sus secretos.

Conforme evolucionó el ser humano esta tarea fue facilitada, de manera que ya no debían infiltrarse o utilizar artículos de manera creativa y arriesgada para lograrlo. Solo bastó con utilizar la tecnología. Primero fueron los teléfonos, luego los micrófonos escondidos, hasta la actualidad, donde para poder extraerla se necesita algo tan simple como una red desprotegida. Hoy en día, en la llamada "era de la información", el acceso e importancia de esta es mayor que nunca.

Para solucionar esta situación y poder defender a las personas se crearon diversas herramientas, entre ellas, los Firewalls. En el siguiente trabajo, se expondrá la historia, los conceptos y temas referidos a los mismos que constituyen la primera línea de defensa en seguridad de red estableciendo una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet.

Historia

Los cortafuegos o este tipo de tecnología surgieron a finales del año 1980, justamente cuando el Internet era un tipo de tecnología muy nueva, en cuanto a su conectividad y su uso global. Los progenitores de los firewall o cortafuegos para la seguridad de las redes, fueron los routers usados a finales del año 1980 que conservaban separadas a las redes una de otras. La visión de Internet como un tipo de comunidad pequeña relativamente de usuarios con máquinas compatibles, que valoraban la predisposición para la colaboración y el intercambio, terminó con unas importantes series de violaciones de seguridad en el Internet, que se generó a finales de los años 80.

La primera propuesta de firewall, o filtro de paquetes, surgió en 1989 por Jeff Mogul de Digital Equipment Corp (DEC), marcando por lo tanto la primera generación.

El Bell Labs de AT & T, a través de Steve Bellovin y Bill Cheswick, desarrolló en 1991 el primer concepto de lo que se consolidaba a continuación como filtrado de paquetes stateful, o simplemente firewall stateful. Esta etapa quedó marcada como segunda generación de firewalls.

En un corto espacio de tiempo, surgió la tercera generación de firewalls, cuando se inició la comercialización del DEC SEAL, ya contando con recursos más modernos de proxies de aplicación. La combinación entre filtros de paquetes y proxy en una única solución hizo que el nombre de firewall híbrido comenzará a ser más utilizado

En 1994 Checkpoint lanzó el Firewall-1 que tuvo una gran importancia para la maduración y desarrollo del mercado de seguridad, introduciendo de forma pionera el concepto de GUI

Con la incorporación de soluciones complementarias de seguridad para los firewalls, en 2004 apareció por primera vez, a través del IDC, el término UTM (Unified Threat Management). El término no es más que una mejor denominación para la evolución ocurrida a los firewalls a lo largo de los años.

En 2006 aparecieron de forma más concreta los Web Application Firewalls (WAF), como soluciones independientes, pero también incorporadas como recurso para UTM.

Finalmente, en el año 2009, Gartner pasa a definir el concepto de firewalls de próxima generación, resolviendo básicamente el problema de desempeño presentado por UTM, y añadiendo un recurso importante que es la visibilidad y los controles basados en aplicaciones.

Concepto

Un firewall o cortafuegos es un sistema diseñado de seguridad para prevenir el acceso no autorizado hacia o desde una red privada. Se puede implementar en forma de hardware, de software o en una combinación de ambos. Poder determinar la diferencia entre estos, lleva a una mejor comprensión de los mecanismos necesarios para protegerse mejor en un ambiente privado, y en uno público.

Es importante recordar que representan una primera línea de defensa porque pueden evitar que un programa malicioso o un atacante obtengan acceso a su red y a su información antes de que se produzca cualquier posible daño ya que examinan los mensajes que ingresan o egresan de una red local y bloquean aquellos que sean necesarios, impidiendo que los usuarios no autorizados accedan a redes privadas conectadas a Internet, especialmente a intranets.

Además se debe comprender que para que el firewall pueda ser efectivo, todo el tráfico que haya entre dos redes debe pasar por él, ya que de este modo, podrá aplicar las políticas que se hayan definido.

Funciones

A continuación enlistamos las funciones específicas de los mismos para una mayor comprensión y claridad ya que generalmente difiere de las estipulaciones generales y puede llegar generar confusión.

1. **Crear** una barrera que permita o bloquee intentos para acceder a la información en su equipo.
2. **Evitar** que usuarios no autorizados accedan a los equipos y las redes de la organización que se conectan a Internet.
3. **Supervisar** la comunicación entre equipos y otros equipos en Internet.
4. **Visualizar** y **bloquear** aplicaciones que puedan generar riesgo
5. **Advertir** de intentos de conexión desde otros equipos.
6. **Advertir** de intentos de conexión mediante las aplicaciones en su equipo que se conectan a otros equipos.
7. **Detectar** aplicaciones y **actualizar** rutas para añadir futuras fuentes de información
8. **Hacer frente** a los cambios en las amenazas para la seguridad

Ante todo se debe recalcar el hecho que estos no se auto configuran y tampoco brindan una protección total frente a ataques, sino que son parte de una estrategia de seguridad. De manera que la mejor forma de asegurarnos contra softwares maliciosos, es con una combinación de estos.

También es necesario resaltar que no protege amenazas o ataques de usuarios negligentes ni protege ataques que no pasen por medio del firewall ni la copia de datos importantes si se ha accedido a ellos. Tampoco protege de ataques de ingeniería social. de modo que si bien la protección por firewall es una excelente primera línea de defensa, también es buena idea seguir estos consejos importantes para proteger sus datos y sus dispositivos:

- No haga clic en enlaces ni abra archivos adjuntos de personas que no conoce. Sin saberlo, podría estar dándoles acceso a su dispositivo.
- Sea consciente de que cada nuevo dispositivo conectado a Internet que trae a su hogar es una posible vía de ataque. Asegúrese de restablecer las contraseñas predeterminadas y mantenga esos dispositivos actualizados con las últimas versiones del fabricante.

Motivación

La motivación de los Firewalls es tratar de proteger los datos, los recursos y la reputación contra ataques de intrusos, negaciones de servicio y robos de información.

Ventajas y desventajas de utilizar un Firewall

Existe una amplia gama en el mercado de firewalls, de modo que existen distintas ventajas y desventajas dependiendo de las necesidades de cada usuario. Sin embargo también existen beneficios y debilidades a nivel generales teniendo en cuenta la implementación de los mismos independientemente de su necesidad.

Ventajas

En primer lugar, la ventaja más importante es la protección contra amenazas externas. Además el administrador de red respectivo puede tener un mayor control sobre la seguridad de la red. Él o ella pueden determinar los puertos específicos que deben recibir o enviar datos relacionados con varias tareas. Estas conllevan los siguientes beneficios:

- Controlar el tráfico
- Mayor privacidad
- Control de acceso
- Proteger la red de troyanos

Desventajas

Si bien pueden bloquear un potencial acceso de humanos, no pueden defendernos de las amenazas que existen en forma de malware como virus. Además, lo más probable es que todo el sistema informático pueda afectar incluso si el Firewall está activo y en ejecución. Por esta misma razón, se podría decir que su Firewall no es la herramienta de seguridad más completa. Entonces, lo mejor es tomar su Firewall como una 'medida de seguridad' pero no como un sistema informático sofisticado.

Para agregar, tambien se encuentran los siguientes inconvenientes a la hora de utilizar un firewall:

- costo: Se deberá tolerar una inversión inicial, aunque esta varía según el tipo del mismo
- Rendimiento: Los firewalls basados en software pueden limitar el rendimiento general de su computadora y ralentizarlo.
- Acceso restringido para usuarios: Este puede ser bastante molesto ya que si se trata de un usuario avanzado, tendrá que enfrentarse a diversas cargas para lograr tareas avanzadas
- Indefenso ante ataques malware: los cortafuegos pueden bloquear troyanos, no son efectivos en absoluto contra virus y otro malware. Estas piezas de malware pueden ingresar al sistema camufladas. Entonces, incluso si tiene un firewall, el ataque puede ocurrir.
- Complejidad: En caso de ser una organización grande, se requiere personal dedicado para realizar la instalación y mantenimiento del mismo, por lo cual se pueden asumir costos extras.

Tipos de Firewalls:

Existen diversos tipos de cortafuegos pero en primera instancia se podrían clasificar según rasgos generales en tres categorías como hardware, software o cloud también conocido como Firewall as a service (FaaS). Cabe destacar que la presencia de uno en la red no es excluyente para los otros, es decir, se puede contar con un cortafuego de hardware y uno de software. Es más, esta fórmula es recomendada ya que potencia y refuerza el esquema de seguridad.

Firewall de hardware

Los firewall de hardware vienen incluidos en algunos enrutadores y requieren poca o ninguna configuración, ya que están incorporados en su hardware. Estos firewall monitorean el tráfico de todas las computadoras y dispositivos que están conectados a la red de dicho enrutador, lo que significa que usted puede filtrar el acceso a todos ellos

solo con una pieza de equipo. Los firewalls de hardware brindan seguridad esencial para el Internet de las cosas (IoT).

Firewall de software

Los firewall de software ayudan a mantenerse protegido en lugares públicos. Se ejecutan como un programa en las computadora o dispositivo y observan de cerca el tráfico de la red para ayudar a interceptar programas maliciosos antes de que lleguen al equipo.

Firewall as a Service o Cloud firewall

Sigue el mismo principio de funcionamiento que el firewall de software, solo que vive en la nube como es Amazon, Azure, etc. La diferencia entre el firewall de software y cloud, es que con cloud, ya se tiene preconfigurado y listo para usar. Además cuenta con el beneficio de que pueden crecer a la misma magnitud que la organización y, de manera similar a los firewalls de hardware, funcionan bien con la seguridad perimetral.

A su vez, también se pueden clasificar según su estructura y funcionalidad. Entre los cuales se pueden mencionar:

- Packet-filtering firewalls o firewalls de filtrado de paquetes

Los cortafuegos de filtrado de paquetes (Packet-filtering firewalls) funcionan en el router analizando la cabecera de cada paquete y comparando cada paquete recibido con un conjunto de criterios establecidos antes de que cada uno sea enviado o suprimido.

Normalmente, las reglas en este tipo de dispositivos se basan en el protocolo de transporte (tcp, udp, icmp…), en las direcciones origen y destino del paquete y en el puerto destino (Telnet, ftp, http…). En algunos casos también se filtra el tráfico teniendo en cuenta por cual interfaz ha llegado el tráfico o por cual va a ser reenviado.

Los firewalls de filtrado de paquetes se dividen en dos categorías: con estado y sin estado. Los firewalls sin estado examinan los paquetes independientemente uno del otro y carecen de contexto, lo que los convierte en objetivos fáciles para los piratas informáticos. En contraste, los firewalls con estado recuerdan información sobre paquetes pasados previamente, como podremos ver mas adelante.

Algunas de las ventajas de este tipo de filtraje son que se puede gestionar todo de forma centralizada y que se puede filtrar de forma rápida y transparente al usuario. Sin embargo, también presenta varias desventajas: la imposibilidad de filtrar teniendo en cuenta que usuario o que servicio se está utilizando, imposibilidad de controlar el inicio y el final en una conexión TCP.

- Circuit-level gateways

Una puerta de enlace de nivel de circuito opera en la capa de transporte de los modelos de referencia de Internet o OSI y, como su nombre lo indica, implementa el filtrado a nivel de circuito en lugar del filtrado a nivel de paquete.

Este firewall comprueba la validez de las conexiones (es decir, circuitos) en la capa de transporte (generalmente conexiones TCP) contra una tabla de conexiones permitidas, antes de que se pueda abrir una sesión e intercambiar datos. Las reglas que definen una sesión válida prescriben, por ejemplo, el destino y las direcciones y puertos de origen, la hora del día, el protocolo que se utiliza, el usuario y la contraseña. Una vez que se permite una sesión, no se realizan más verificaciones, ni siquiera, por ejemplo, a nivel de paquetes individuales. Entre las desventajas de las puertas de enlace a nivel de circuito se encuentran la ausencia de filtrado de contenido y el requisito de modificaciones de software relacionadas con la función de transporte.

Si bien son extremadamente eficientes en cuanto a recursos, estos firewalls no verifican el paquete en sí. Entonces, si un paquete contenía malware, pero tenía el protocolo de enlace TCP correcto, pasaría de inmediato. Es por eso que las puertas de enlace a nivel de circuito no son suficientes para proteger su negocio por sí mismas.

- Stateful inspection firewalls

Estos cortafuegos combinan la tecnología de inspección de paquetes y la verificación de protocolo de enlace TCP para crear un nivel de protección mayor que cualquiera de las dos arquitecturas anteriores podría proporcionar por sí solo. Los cortafuegos de inspección de estado (Stateful inspection firewalls) no sólo examinan cada paquete, sino que también hacen un seguimiento de si dicho paquete forma parte o no de una sesión TCP establecida. Esto ofrece más seguridad que el filtrado de paquetes o la monitorización de circuitos por sí solos, pero supone una carga mayor para el rendimiento de la red.

La inspección de paquetes la lleva a cabo analizando los protocolos de los paquetes, con la finalidad de distinguir entre paquetes legítimos o ilegítimos. Aquellos que no se encuentren dentro de las políticas establecidas (previamente) se desechan.

Habitualmente, se consideran más seguros que los firewalls de filtrado de paquetes, ya que procesan los datos de la capa de aplicación y, por ese motivo, pueden profundizar en la transacción para comprender lo que está sucediendo. Sin embargo, estos firewalls también ejercen una mayor presión sobre los recursos informáticos. Esto puede ralentizar la transferencia de paquetes legítimos en comparación con las otras soluciones.

- Application-level gateways

Puerta de enlace de nivel de aplicación o Proxy. Este tipo de firewalls operan en la capa de aplicación del modelo OSI, filtrando el acceso según las definiciones de la aplicación. Se considera como uno de los firewalls más seguros disponibles, debido a su capacidad para inspeccionar paquetes y garantizar que se ajusten a las especificaciones de la aplicación. Debido a la cantidad de información que se procesa, los firewalls de la puerta de enlace de aplicaciones pueden ser un poco más lentos que otros firewalls, además tiende a ser un cuello de botella ya que es un punto central por donde pasa todo el tráfico de la red.

Estos filtran el tráfico de red a nivel de aplicación. A diferencia de los firewalls básicos, el proxy actúa como intermediario entre dos sistemas finales. De manera que rompen la conexión directa entre el origen y el destino y crean dos conexiones independientes: una entre el origen y el firewall, y otra entre el firewall y el destino, entonces, el cliente debe enviar una solicitud al firewall, donde luego se evalúa con respecto a un conjunto de reglas de seguridad y luego se permite o bloquea.

Es importante resaltar que los firewalls de tipo proxy permiten la utilización de servicios en los que exista un proxy: telnet http y ftp. A pesar de que solo permite filtrar estos servicios, el nivel de personalización es mucho mayor, ya que se pueden permitir determinados paquetes o comandos de estos protocolos y descartar otros paquetes o comandos (en el caso anterior es todo o nada).

- Los firewalls de traducción de direcciones de red (NAT)

Estos cortafuegos permiten que múltiples dispositivos con direcciones de red independientes se conecten a Internet utilizando una sola dirección IP, manteniendo ocultas las direcciones IP individuales.

Como resultado, los atacantes que escanean una red en busca de direcciones IP no pueden capturar detalles específicos, lo que proporciona una mayor seguridad contra los ataques. Los firewalls NAT son similares a los firewalls proxy en el sentido de que actúan como intermediarios entre un grupo de computadoras y el tráfico externo.

- Multilayer inspection firewalls

Los cortafuegos de inspección multicapa (Multilayer inspection firewalls) combinan el filtrado de paquetes con la monitorización de circuitos, a la vez que permiten conexiones directas entre los hosts locales y remotos, que son transparentes para la red. Esto se logra mediante algoritmos que reconocen qué servicio se está solicitando, en lugar de simplemente proporcionar un proxy para cada servicio protegido.

Los cortafuegos multicapa funcionan reteniendo el estado asignado a un paquete por cada componente del cortafuego a través del cual éste pasa a lo largo una serie

protocolos. Esto le da al usuario el máximo control sobre qué paquetes pueden llegar a su destino final pero también afecta al rendimiento de la red, aunque generalmente no tan drásticamente como lo hacen los proxys.

- Firewall UTM (Unified Threat Management)

Se caracteriza por combinar diferentes elementos de los dos anteriores firewalls (proxy y stateful). Lamentablemente tiene el mismo problema que el firewall proxy, puede convertirse en un cuello de botella si no se tiene la capacidad y/o rendimiento adecuado. Para un negocio pequeño es una excelente opción por las características que ofrece (filtrado, VPN, antivirus, IPS, IDS, etc.)

- Próxima generación o NGFW

La evolución de las amenazas exige soluciones cada vez más intensas, y los firewalls de próxima generación se mantienen al frente de este problema mediante la combinación de las funciones de firewalls tradicionales con sistemas de prevención contra intrusos en la red.

Un cortafuegos de próxima generación ofrece un filtrado de paquetes básico o una toma de decisiones basada en proxy dentro de las capas 3 y 4 del modelo OSI disponible dentro de los firewalls tradicionales y con estado, sin embargo, amplían su protección al tomar también decisiones en la capa de aplicación. Las características que definen a uno de los tipos de firewall más novedosos son la identificación y control de aplicaciones, autenticación basada en el usuario, protección contra malware, protección contra exploits, filtrado de contenido (incluido el filtrado de URL) y control de acceso basado en la ubicación.

Gracias a los firewalls de nueva generación la seguridad de una red se puede gestionar de forma centralizada con un solo dispositivo sin tener múltiples dispositivos donde cada uno se encarga de una cosa. Esto supone un gran ahorro económico. Además, estos firewalls ofrecen un rendimiento muy bueno, muy por encima de los otros tipos de firewalls.

- NGFW centrado en amenazas

Este tipo de firewall ofrece las mismas características del anterior, con la diferencia que detecta y corrige amenazas. Al automatizar la seguridad inteligentemente, tiene una rápida reacción al sufrir ataques además de prevenirlos, ya que detecta comportamientos extraños dentro de la red.

Arquitectura de Redes

Como hemos visto, los firewalls pueden ser configurados de diferentes formas, utilizando diferentes componentes, logrando varios niveles de seguridad a diferentes

costos de instalación y mantenimiento. Esta decisión dependerá de las necesidades y de la evaluación de costo/beneficio de llevar a cabo tal implementación.

Al hablar de arquitectura de firewall, nos referimos a aquellas representaciones físicas y lógicas en torno al posicionamiento de los activos computacionales. Por lo cual, se trata de una edificación que, a través de su diseño y planificación, sirve para implementar la estructura de la red en cuestión. Con lo cual, aprobará o denegará el tráfico de los elementos apropiados, una vez canalizado.

Según lo recientemente mencionado, proseguiremos a explicar algunas de las arquitecturas de red con un enfoque perimetral y sus variaciones:

- Cortafuegos de filtrado de paquetes o Arquitectura Screening Router

El modelo de cortafuegos más antiguo consiste en un dispositivo capaz de filtrar paquetes. Se trata de una arquitectura de firewall que solamente se encuentra basada en aprovechar la capacidad de algunos routers para efectuar un enrutamiento selectivo y así, restringir o admitir el tránsito de paquetes por medio de listas de control de acceso en función de algunas particularidades.

Por consiguiente, se encarga de tomar decisiones de procesamiento fundamentadas en direcciones de red, puertos, interfaces o protocolos. Además, se caracterizan por no guardar ninguna información del estado ni hacer ninguna investigación interna del tráfico.

Esta arquitectura es la más simple de implementar y la más utilizada en organizaciones que no precisan grandes niveles de seguridad, donde el *router* actúa como de "*pasarela"* de la subred y no hay necesidad de utilizar *proxies*, ya que los accesos desde la red interna al exterior no bloqueados son directos.

Los hosts de la red interna se comunican entre sí directamente, mientras que la comunicación entre hosts de la red privada y la red pública está restringido a aquellos paquetes que sean permitidos por el router.

Su principal inconveniente es que no disponen de ningún sistema de monitorización sofisticado. Por ende, se considera uno de los tipos de cortafuegos más inseguros, considerando que el administrador no podrá verificar si su privacidad ha sido comprometida.

- Arquitectura Screened Host

La arquitectura Screened Host posee un firewall compuesto por un router para el filtrado de paquetes y un host bastión para el filtrado de conexiones a nivel de circuito y aplicación. La primera línea de protección corresponde al router con filtrado de paquetes, el host bastión se encuentra conectado a la red interna como un host más. Es importante

resaltar que el router está exclusivamente configurado para bloquear todo el tráfico existente entre la red externa, al igual que todos los hosts de la red interna, menos un único bastión. Pues, este último, es aquel en donde se instala todo el software necesario para implementar el cortafuego efectivamente.

El router puede ser configurado de diferentes formas

- Permitir que ciertos hosts internos puedan abrir conexiones a Internet para ciertos servicios;

- Deshabilitar todas las conexiones desde los hosts internos habilitando solo al host bastión para establecer estas conexiones;

- También es posible que algunos paquetes sean dirigidos, por el router, directamente a los hosts internos.

Estos aspectos dependen de la política de seguridad elegida.

- Arquitectura Dual-Homed Host

Como podemos apreciar por el nombre de la arquitectura, se trata de un host que cuenta con dos tarjetas de red y cada una de ellas, se conecta a una red diferente. Este modelo se compone de simples máquinas Unix, denominadas anfitriones de dos bases, equipadas, como ya mencionamos, con dos tarjetas de red: una se conecta a la red interna a proteger y la otra a la red externa.

De este modo, los sistemas de la red interna se pueden comunicar con el dual-homed host, así como los sistemas del exterior también se pueden comunicar con el dual-homed host; es decir, el tráfico entre la red interna y el exterior está completamente bloqueado. En este caso el choke y el bastión coinciden en el mismo equipo.

El firewall deberá, en todos los casos, actuar como un intermediario. Es por esto que en este sistema, la función de ruteo está deshabilitada por lo que el host aísla las dos redes entre ellas al bloquear todo paquete IP que capture.

La forma de proveer servicios por parte del host bastión puede ser realizada de dos formas

- Si los usuarios de la red local poseen cuentas en el host bastión, las mismas le permiten iniciar sesiones (loguearse) para poder utilizar los servicios de Internet. Este aspecto presenta un serio riesgo de seguridad ya que la protección depende de que el usuario haya elegido bien su contraseña.

- La alternativa es que el host ejecute servicios proxy para cada servicio que se desee permitir, de esta forma el usuario se desliga de la responsabilidad de la seguridad de la red.

En esta arquitectura, este dispositivo es crítico para la seguridad de la red ya que es el único sistema que puede ser accedido (y atacado) desde Internet, por lo que debe poseer un alto nivel de protección a diferencia de un host común de la red interna. Es por esto que a estos host suele llamárseles bastión. Debe instalarse en este host la mínima cantidad necesaria de software para reducir el riesgo de que sea vulnerado.

- Arquitectura Screened Subnet

El riesgo presente en las arquitecturas anteriores de que el host bastión sea comprometido puede ser reducido configurando una red de perímetro a la cual se conecte el mismo. Esta red suele ser llamada Zona Desmilitarizada. Debido a esto la arquitectura Screened Subnet también se conoce con el nombre de red perimétrica o De-Militarized Zone (DMZ).

Para lograr esta arquitectura se introduce un router de filtrado de paquetes entre el host bastión y la red interna, por lo que el host bastión se encontrará entre los dos routers (interno y externo, uno se encuentra entre la red perimetral y la red externa y el otro entre la red perimetral y la red interna) y estará conectado a un segmento de red diferente al que están conectados los hosts de la red privada. Con esta configuración no existe un único punto vulnerable que ponga en riesgo toda la red interna.

Con esta arquitectura se agrega una nueva capa de seguridad a la arquitectura anterior que aísla la red local de Internet. Aislando al host bastión en una red de perímetro, es posible reducir el impacto de que el bastión sea vulnerado por algún ataque.

Si un atacante logra vencer la protección del host bastión, solo podrá acceder a la red perimetral ya que la red interna sigue protegida por el router interno. De esta forma el atacante sólo tendrá acceso a la red perimetral, ocultando todo el tráfico de la red local.

Esta arquitectura es la más segura de las presentadas hasta ahora ya que la red perimetral soporta aspectos de seguridad a nivel de red y de aplicación y provee un sitio seguro para conectar servidores públicos.

Funcionamiento de las Reglas de Filtrado

Lo que le da su utilidad a los firewalls como herramienta de protección es la capacidad de poder discriminar en el tráfico entrante a la red. Esto se realiza mediante las reglas de filtrado. Existen tres tipos de reglas: Permitir, Denegar y Descartar. El tráfico marcado como Permitido podrá entrar atravesar el firewall, el tráfico Denegado no podrá pasar, pero se le devolverá un error de “Unreachable”. El tráfico marcado como Descartado no podrá acceder ni se le devolverá nada. Luego, cada regla tiene además un conjunto de parámetros contra los cuales se evaluará cada paquete recibido.

Las reglas de un firewall se establecen como una cadena de reglas que evaluarán cada paquete de forma individual, es por esto que hay que tener cuidado a la hora de

armar estas cadenas. Si por ejemplo, una regla descarta todo tráfico que provenga de una dirección ip, pero una siguiente a esta permita toda conexión a un determinado puerto, los pedidos a este puerto de la dirección ip provista en la primera regla serán descartados, ya que la primera regla en la cadena que se aplique a un paquete toma prioridad. Luego existen las reglas por defecto, que se aplican a todos los paquetes que no cumplan ninguna regla de las puestas en la cadena, estas constan únicamente de la póliza que se va a tener con este tráfico (Permitir, Denegar o Descartar).

Las reglas de un firewall además son capaces de aplicarse de forma heterogénea al tráfico dependiendo de si este está intentando entrar o salir. Típicamente, un servidor admite todos los paquetes que salgan de este, ya que se asume que el server protegido es de confianza. Igualmente, se pueden poner reglas sobre el tráfico saliente para minimizar el daño que pueda causar un servidor que haya sido comprometido en un ciberataque.

El firewall utiliza cadenas estándar para manejar paquetes en función de circunstancias predefinidas. El administrador puede crear otras cadenas, que sólo se utilizarán cuando una cadena estándar haga referencia a ellas (ya sea directa o indirectamente). La tabla filter tiene tres cadenas estándar:

- INPUT: se refiere a paquetes cuyo destino es el propio firewall;
- OUTPUT: se refiere a los paquetes que emite el firewall;
- FORWARD: se refiere a los paquetes que transitan a través del firewall (que no es ni su origen ni su destino).

Productos empresariales

Actualmente, existen distintas empresas que brindan diversos productos de software, entre las cuales se encuentran Barracuda Networks, Check Point Software Technologies, Cisco, Forcepoint, Fortinet, Huawei, Juniper Networks, Palo Alto Networks, SonicWall, Sophos, and WatchGuard. Estas fueron seleccionadas a través de una evaluación de 34 criterios realizados por “The Forraster Wave”.

Estas, usualmente brindan los productos de firewalls de Nueva Generación, cloud Firewall y, además, dan la posibilidad de un paquete de seguridad las cuales brindan antivirus, antimalware, entre otros. Cabe destacar que ciertas empresas como Cisco, WatchGuard, Sophos y Juniper brindan firewalls de tipo de hardware además del software y de servicio de nube.

Ejemplo Práctico:

Configurar el firewall de Ubuntu

El firewall de Ubuntu viene en el kernel, pero por defecto está desactivado. Se puede habilitar y administrar mediante la utilidad de iptables:

```
root@fran-N56VJ:~# iptables --list
Chain INPUT (policy DROP)
target     prot opt source               destination
ufw-before-logging-input  all  --  anywhere             anywhere
ufw-before-input  all  --  anywhere             anywhere
ufw-after-input  all  --  anywhere             anywhere
ufw-after-logging-input  all  --  anywhere             anywhere
ufw-reject-input  all  --  anywhere             anywhere
ufw-track-input  all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
ufw-before-logging-forward  all  --  anywhere             anywhere
ufw-before-forward  all  --  anywhere             anywhere
ufw-after-forward  all  --  anywhere             anywhere
ufw-after-logging-forward  all  --  anywhere             anywhere
ufw-reject-forward  all  --  anywhere             anywhere
ufw-track-forward  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ufw-before-logging-output  all  --  anywhere             anywhere
ufw-before-output  all  --  anywhere             anywhere
ufw-after-output  all  --  anywhere             anywhere
```

Ahora bien, como leer el output de esa herramienta y armar las cadenas puede ser incómodo, una herramienta muy popular es ufw (UNcomplicated Firewall). QUe tiene tanto un cliente gráfico como una interfaz por linea de comandos:

```
root@fran-N56VJ:~# ufw enable
Firewall is active and enabled on system startup
root@fran-N56VJ:~#
```

Habilitando el firewall

```
root@fran-N56VJ:~# ufw disable
Firewall stopped and disabled on system startup
root@fran-N56VJ:~#
```

Deshabilitando el firewall

```
root@fran-N56VJ:~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
root@fran-N56VJ:~#
```

Viendo el status del firewall

```
root@fran-N56VJ:~# ufw status
Status: active

To                         Action      From
--                         ------      ----
53/tcp                     ALLOW       Anywhere
53/tcp (v6)                ALLOW       Anywhere (v6)

root@fran-N56VJ:~#
```

Viendo las reglas de firewall

```
root@fran-N56VJ:~# ufw deny 130/udp
Rule added
Rule added (v6)
root@fran-N56VJ:~#
```

Agregando una nueva regla de firewall

```
root@fran-N56VJ:~# ufw status
Status: active

To                         Action      From
--                         ------      ----
53/tcp                     ALLOW       Anywhere
130/udp                    DENY        Anywhere
53/tcp (v6)                ALLOW       Anywhere (v6)
130/udp (v6)               DENY        Anywhere (v6)
```

Viendo ahora la cadena

```
root@fran-N56VJ:~# ufw delete 1
Deleting:
 allow 53/tcp
Proceed with operation (y|n)? y
Rule deleted
root@fran-N56VJ:~#
```

Borrando una regla de firewall

Conclusión

Para finalizar el presente informe, podemos concluir que la seguridad en redes es algo esencial y debe ser una estrategia integral y planificada en base a los requerimientos y necesidades de los usuarios. De manera que se puede contar con herramientas como un firewall para alcanzarlo, pero este no debe ser el único elemento de dicho plan.

También podemos inferir que se pueden colocar distintos tipos de firewall para proteger cada una de las capas y establecer distintas arquitecturas con múltiples configuraciones y filtros para mantener las redes seguras.

Bibliografía

Firewall: Historia - OSTEC | Segurança digital de resultados

Qué Es Y Para Qué Sirve Un Firewall - Historia - Tipos Y Ventajas (paraquesirve.tv)

Qué es un firewall - Panda Security

¿Qué es un firewall? | McAfee

¿Qué es un firewall? - Cisco

Ventajas y desventajas del cortafuegos que todos deben saber: iStarTips

Tipos de Firewalls - Trustnet

Tipos de firewall: características y recomendaciones de uso | OBS Business School

Tipos de firewall en función de como se despliegan en la red ⚡ 2020 (tecnozero.com)

¿Cuales son los tipos de firewalls o cortafuegos que existen? - Blog de data center, cloud (hostdime.com.co)

Tipos de firewalls - firewalls hardware (firewalls-hardware.com)

Tipos de firewall: características y recomendaciones de uso | OBS Business School

Arquitecturas de Firewalls – El Blog de Especialistas Hosting

Arquitecturas de Firewall ▶ ¿Qué Son? + Diferencias ▷2021 (internetpasoapaso.com)

What is a Firewall and How Does It Work?