Recibido: Nov. 25, 2021 | Aceptado: Feb. 18, 2022

Directrices y políticas de firewall

Firewall guidelines and policies

DOI: https://doi.org/10.21803/ingecana.2.2.496

Álex Ávila[1] · Tatiana Echeverría Jiménez[2] · Christian Obando[3] & Carlos Federico Ortiz Zuleta[4]

[1] Docente de la Corporación Universitaria Americana. [2]Docente de la Corporación Universitaria Americana. [3]Ingeniero en electrónica y telecomunicaciones y especialista en seguridad informática hasta2015. E-mail: chrisobib@gmail.com. [4]Administrador de red, Universidad de Antioquia. E-mail: federico.ortiz@udea.edu.co.

Resumen

Los sistemas de información deben estar protegidos por medio de firewalls, estos están diseñados para controlar el tráfico que circula entre las redes privadas y públicas, permitiendo o denegando las peticiones realizadas por las diferentes redes con el objetivo de protegerlas de amenazas. Existen diferentes tipos de firewall que se utilizan dependiendo de las técnicas de filtrado que se deseen implementar, de acuerdo a la pila de protocolos TCP/IP ellos pueden trabajar a nivel de red, de transporte y de aplicación. Un buen diseño en las políticas del firewall, robustece la seguridad de las redes ya que con estas se puede controlar determinados tipos de tráfico de datos.

Palabras clave: Firewall, Políticas Y Directrices, Redes, Seguridad Informática.

Abstract

Information systems must be protected by firewalls, which are designed to control traffic flowing between private and public networks, allowing and denying requests made by the different networks in order to protect them from threats. There are different types of firewalls that are used depending on the filtering techniques to be implemented, according to the TCP/IP protocol stack, they can work at network, transport and application level. A good firewall policy design strengthens network security by controlling certain types of data traffic.

Keywords: *Firewall, Policies And Guidelines, Networks, Computer Security.*

Introducción

En los últimos años las TICs han evolucionado y han cobrado gran importancia a nivel mundial debido a su capacidad para estimular la creatividad, la innovación y transformar el mundo en diferentes entornos. El Ministerio de Tecnologías de la Información y la Comunicación de la República de Colombia en su Boletín trimestral de las TICs – Cifras Primer Trimestre 2013 [1] indica, entre otros, un crecimiento en la penetración de Internet de un 16% con un total de 7.531.670 suscriptores, esta tendencia a la alza se debe, entre otras, a que las TICs nos ofrecen un acceso amplio y ágil a miles de millones de contenidos pero también a recursos humanos valiosos. Internet se ha convertido en un medio fundamental para impulsar el diseño e implementación de servicios que cumplen con las necesidades de las personas y organizaciones en general, pero así mismo ha brindado la oportunidad a personas inescrupulosas de cometer delitos relacionados con la informática y la información, pues cada día hay nuevas redes susceptibles de ser atacadas y nuevos atacantes en potencia. Es por esto que una organización debe tomar conciencia e inquietarse por su seguridad, un mecanismo es la seguridad perimetral.

La seguridad perimetral debe estar diseñada para proteger todos los elementos de una red interna, incluyendo hardware, software e información, no solo de cualquier intento de acceso no autorizado desde internet sino también de ciertos ataques que pueden ser realizados dentro la red. Los firewall son dispositivos o programas que ayudan a controlar las conexiones que pueden iniciar o recibir un computador conectado a la red, este puede ser implementado de acuerdo a las necesidades de las organizaciones, creando políticas específicas de firewall para permitir, limitar y rechazar el tráfico que circula entre las diferentes redes.

Este artículo es el resultado de analizar las diferentes tecnologías de firewall, sus capacidades, ventajas y desventajas así como recomendaciones para el establecimiento de políticas de firewall y recomendaciones para seleccionar, configurar, probar, implementar y administrar soluciones de firewall.

TIPOS DE FIREWALL

Existen diferentes tipos de aplicaciones de firewall de acuerdo a las necesidades de filtrado que se desean controlar.

Filtrado de paquetes

Este tipo de firewall tiene un conjunto de reglas estáticas que permiten o bloquean el acceso de tráfico, basado en la información contenida en los encabezados de los paquetes, trabajan a nivel de red y de transporte del modelo TCP/IP, es decir se basa en direccionamiento IP origen-destino y puertos TCP o UDP; tiene una desventaja y es que no detecta el tráfico malicioso.

Firewall de aplicaciones

Trabaja en la capa de aplicaciones del modelo TCP/IP, permite detectar diferentes tipos de ataques

a múltiples niveles, es útil para detectar ataques conocidos como gusanos, spyware, troyanos y bots, esta aplicación es conocida como un sistema de detección y prevención de intrusos (IDS/IPS). La desventaja principal de esta aplicación es que afecta el rendimiento del dispositivo.

Firewall proxy

Actúa como intermediario en ciertos programas, su función es filtrar y reenviar paquetes a nivel de aplicación como TELNET, FTP y HTTP, realiza filtrado de contenidos web controlando el acceso a ciertas páginas desde una red privada, brinda opciones de control de acceso confiable para los protocolos soportados. Esta aplicación reduce el tráfico y mejora la respuesta a solicitudes, ya que permite el almacenamiento en caché de las páginas web más visitadas.

Redes privadas virtuales (vpn)

Los firewall a veces tienen que hacer más que filtrar el tráfico UDP y TCP, también cifra y descifra los flujos de datos de una red protegida y las redes externas, esto implica implementar un red privada virtual, que utiliza protocolos adicionales para cifrar el tráfico, proporcionar autenticación de usuario y proteger la integridad de la información. Es un servicio basado en certificados SSL, que se utiliza para crear túneles VPN cliente/servidor y servidor/cliente, esta flexibilidad permite que las filiales y los trabajadores remotos de una organización, puedan conectarse con seguridad a la red corporativa y realizar las tareas o solicitudes propias de su función.

Control de acceso a la red (car)

Es una aplicación del firewall que revisa los equipos que acceden a la red para comprobar que cumplan con todas las políticas de seguridad, como son actualizaciones de los antivirus, del sistema operativo y de aplicaciones.

Firewall de aplicaciones web

Es una aplicación que permite inspeccionar las peticiones que se puedan realizar sobre una web o una aplicación web, impidiendo que tráfico malicioso alcance la aplicación origen y por lo tanto salvaguardando la información más sensible. Igual que las aplicaciones anteriores se trata de un servicio que complementa a los sistemas tradicionales de seguridad perimetral (firewall), ofreciendo protección a nivel de aplicación donde un firewall tradicional no podría proteger [1].

Unified threat management- utm

Es un gestor unificado de amenazas, básicamente es un firewall que posee múltiples funciones en una misma máquina de seguridad perimetral, algunos de estos servicios son:

- Función de firewall inspección de paquetes.
- Función de VPN
- Antispam
- Antiphishing (falsificación de sitios web)
- Antispyware o Filtrado de contenidos o Antivirus de perímetro
- Detección y prevención de intrusos(IDS/IPS)

Estas funciones adicionales lo hacen un firewall más robusto, que centraliza la administración de las aplicaciones que ayudan a realizar un mejor análisis de datos a nivel de aplicaciones específicas y a la detección de ataques externos.

Actualmente existen diferentes variedades de UTM, unos son llamados open source o de código abierto y gratuito y otros que son soportados por algunos fabricantes, es decir son licenciados [2].

Firewall con ambientes virtuales

Los sistemas de virtualización incluyen la creación de redes virtualizadas como si estuviesen

en una red Ethernet estándar, el tráfico que circula dentro de las redes virtuales no se puede controlar con un firewall externo, pero algunos sistemas de virtualización ofrecen funciones de firewall que se adicionan en el sistema operativo como plugins, y cumplen la función de filtrado de paquetes dentro de las virtualizadas, dándole la seguridad perimetral que necesitan.

Firewall para equipos individuales y redes domésticas

Para dar una buena seguridad a una red, no basta con tener un firewall protegiendo de la red pública, también es necesario tener instalados firewall en las máquinas de escritorio, laptops y servidores, ya que estos ayudarían a protegerlos de ataques internos que no pueden ser filtrados ni detectados por el firewall de perímetro de la red [3].

En el mercado existen muchas aplicaciones gratuitas para esta función, pero las más recomendables son las licenciadas que vienen con los paquetes de antivirus de algunos fabricantes.

Firewall basados en host y firewall personales

Los firewall de host está disponibles como parte del sistema operativo, tales como Windows, Solaris, Linux, BSD y MAC OS X Server, su principal función es controlar el tráfico que circula en su propia red o subred y que no puede ser detectada por el firewall perimetral. Para asegurar mejor los equipos individuales se suelen instalar aplicaciones como antivirus licenciados con funcionalidad de firewall a nivel de aplicación, pero solo para la máquina local [4].

En las redes domésticas también se suele utilizar firewall para proteger las máquinas de la red externa, los más comunes son los llamados router-firewall que tiene funcionalidades anteriormente mencionadas como VPN, filtrado web, ACL y segmentación de red.

FIREWALLS Y ARQUITECTURAS DE RED

Los firewalls son utilizados para diferentes redes con diferentes requisitos de seguridad, tales como Internet y la red interna (LAN) que aloja todos los datos sensibles. Se deben ubicar firewalls donde sus redes y sistemas internos interactúan con las redes y los sistemas externos, y donde los requisitos de seguridad varían entre sus redes internas.

Es importante determinar dónde se deben colocar los firewalls y donde deben estar las redes en relación a los mismos, esto significa normalmente que los firewalls están colocados ya sea como un nodo en la red que divide varias rutas de acceso, o en línea a lo largo de una sola trayectoria.

Los proveedores de firewalls a menudo varían en su terminología para el flujo lógico de tráfico en el firewall. Un firewall toma el tráfico que no se ha comprobado, lo evalúa con la política del firewall, y luego actúa en consecuencia (por ejemplo, pasa el tráfico, lo bloquea o lo pasa con algunas modificaciones). Debido a que todo el tráfico en una red tiene una dirección, las políticas se basan en la dirección en que se mueve el tráfico, el tráfico que aún no ha sido revisado viene del “lado sin protección” del firewall y se está moviendo hacia el “lado protegido.” Algunos firewalls verifican el tráfico en ambos sentidos -por ejemplo, si se establecen para evitar que un tráfico específico de la red LAN salga a Internet. Existen varios tipos de firewall; los firewalls de red que casi siempre son dispositivos de hardware con varias interfaces de red; los firewalls basados en hosts y los firewalls personales que implican software que reside en un solo equipo y protege sólo el mismo, igualmente las aplicaciones de firewall personales que son diseñadas para proteger un equipo en una red pequeña.

Topologías de la red con firewalls

En la Figura 1 se puede ver el gráfico típico de una red de firewall actuando como router El lado sin protección del firewall se conecta a la ruta única con la etiqueta "WAN", y el lado protegido se conecta a tres caminos marcados "LAN1," "LAN2," y "LAN3." El firewall actúa como un enrutador para el tráfico entre el camino de la WAN y los caminos de la LAN. En la figura, uno de los caminos de LAN también tiene un router; algunas organizaciones prefieren utilizar múltiples capas de enrutadores debido a políticas de enrutamiento dentro de la red.

Muchos firewalls tienen una característica denominada DMZ. Las DMZs son útiles a veces para las organizaciones que tienen hosts que necesitan tener un tráfico destinado evadiendo algunas políticas del firewall, pero que requieren que el

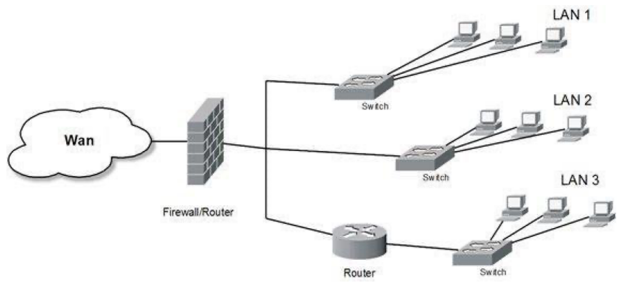

Figura 1. Firewall actuando como router.
Elaboración propia basado en [2]

tráfico procedente de los hosts de otros sistemas en la red si tenga que pasar por el firewall. Es común instalar servidores de cara al público, tales como servidores web y correo electrónico, en la zona desmilitarizada.

Un ejemplo de esto se muestra en la Figura 2, un diseño de red simple de un firewall con una DMZ. El tráfico de Internet entra en el firewall y se dirige a los sistemas en el lado protegido de este o a los sistemas ubicados en la DMZ. El tráfico entre los sistemas de la DMZ y sistemas en la red protegida pasa por el firewall, y puede tener políticas de firewall aplicadas.

En algunas ocasiones se pueden utilizar múltiples firewalls, es decir firewalls redundantes, lo que algunos vendedores ofrecen como firewalls de alta disponibilidad (high-availability firewalls), estos permiten que un firewall pueda hacerse cargo de otro en caso de que el primero falle o se desconecte para mantenimiento.

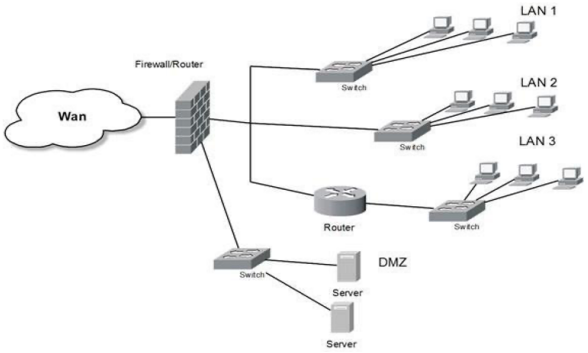

Figura 2. Firewall con DMZ.
Elaboración propia basado en [2].

Los firewalls con alta disponibilidad están desplegados en pares en el mismo lugar en la topología de red, de forma que ambos tienen las mismas conexiones externas e internas. Mientras que los firewalls de alta disponibilidad pueden aumentar la fiabilidad, también pueden presentar algunos problemas, tales como la necesidad de combinar los logs entre los pares de firewalls y puede llevar a posibles confusiones para los administradores al configurar los firewalls (por ejemplo, saber qué firewall está induciendo cambios de política en otro firewall). La Figura 3 presenta un esquema de firewall de alta disponibilidad.

Firewalls actuando como traductores de direcciones de red nat

La mayoría de los firewalls pueden realizar NAT, denominado a veces port address translation (PAT) o network address and port translation (NAPT). A pesar de la creencia popular, NAT no es parte de la funcionalidad de seguridad de un

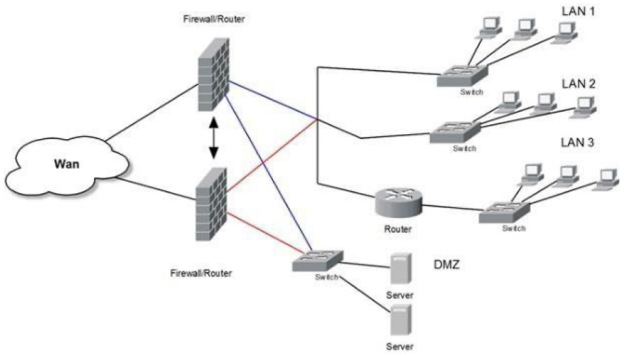

Figura 3. Firewalls de alta disponibilidad.
Elaboración propia basada en [2].

firewall. Típicamente, un NAT actúa como un router que tiene una red con direcciones privadas en el interior y una sola dirección pública en el exterior.

La forma en que un NAT realiza el mapeo varía entre implementaciones, pero casi siempre involucra lo siguiente:

> NAT cambia la dirección origen en cada paquete de salida y, dependiendo del método, también el puerto origen para que sea único. Estas traducciones de dirección se almacenan en una tabla, para recordar qué dirección y puerto le corresponde a cada dispositivo cliente y así saber dónde deben regresar los paquetes de respuesta. Si un paquete que intenta ingresar a la red interna no existe en la tabla de traducciones, es descartado. Debido a este comportamiento, se puede definir en la tabla que en un determinado puerto y dirección se pueda acceder a un determinado dispositivo, como por ejemplo un servidor web.

Arquitectura con múltiples capas de firewalls

Se pueden utilizar varios firewalls dentro de una red, es decir un administrador de red puede querer límites adicionales dentro de la red y el mecanismo para esto es implementar firewalls adicionales. Una situación típica que requiere de múltiples capas de firewalls de red es la presencia de los usuarios internos con niveles de confianza diferentes. Por ejemplo, una organización podría querer proteger sus bases de datos de contabilidad del acceso de usuarios que no forman parte del departamento de contabilidad. Esto se podría lograr mediante la instalación de un firewall en el perímetro de la red (para evitar el acceso general a la red desde Internet) y otro en el perímetro de la red interna que define el límite del departamento de contabilidad. El firewall interno bloquearía el acceso al servidor de base de datos para cualquier persona fuera de la red contable al tiempo que permite el acceso limitado a otros recursos de la red contable. La Figura 4 presenta cómo quedaría este esquema:

> Otro uso típico de los firewalls múltiples dentro de una red puede ser cuando en las organizaciones implementan puntos de acceso inalámbricos específicos dentro de sus redes para uso de los visitantes. Un firewall entre los puntos de acceso y el resto de la red interna, puede impedir que los visitantes accedan a la red local con los mismos privilegios que un empleado. La Figura 5 presenta este esquema.

Hay que tener cuidado cuando se utiliza la combinación de varios firewalls, porque se pueden cometer errores como por ejemplo omitir reglas en el firewall interior considerando que están implementadas en el firewall exterior, esto puede resultar en amenazas para la organización. Una buena práctica es duplicar las directivas de los

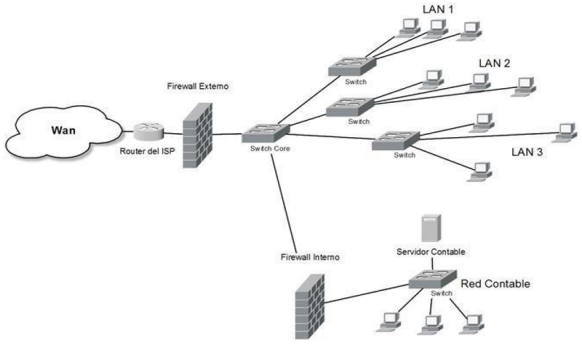

Figura 4. Arquitectura con múltiples capas de firewalls.
Elaboración propia basado en [2].

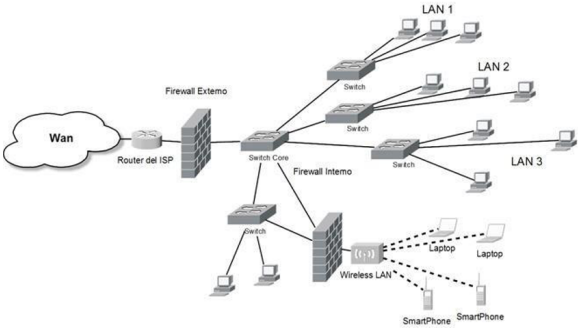

Figura 5. Firewalls múltiples en puntos de acceso inalámbricos. Elaboración propia basado en [2].

firewalls externos que también son relevantes para los firewall internos. Esto puede ser difícil si estos firewalls no son capaces de coordinar sus políticas de forma automática, lo que es probable cuando los firewalls son de diferentes fabricantes. Cuando se tienen varios firewalls puede ser más complicado para el administrador encontrar un error porque tiene que revisar las políticas de cada firewall.

POLÍTICA DE FIREWALL

Las políticas de firewall establecen cómo los firewall deben manejar el tráfico de una red basado en direcciones IP, protocolos, aplicaciones y contenido. Antes de realizar una política de firewall, se debe efectuar un tipo de análisis de riesgos basado en la evaluación de amenazas y vulnerabilidades con el fin de establecer los tipos de tráfico que necesita la organización y cómo deben protegerse [5]. Estas políticas deben considerarse en el plan de seguridad de la organización y deben ser actualizadas a medida que surjan nuevas amenazas.

La función principal de los firewall es la de bloquear todo tráfico entrante y saliente que no haya sido especificado en la política de firewall [6]. Esta práctica conocida como deny by default, reduce tanto el riesgo de ataque como el volumen de tráfico en la red.

Políticas basadas en direcciones ip y protocolos

Las políticas de firewall de una organización, solo deben permitir protocolos IP que sean necesarios, los más comunes son: ICMP, TCP, UDP, ESP y AH, a los demás protocolos se les aplica deny by default. Estos protocolos rara vez pasan entre una red externa y la red LAN de la organización, por lo que deben ser bloqueados en ambas direcciones del firewall [7].

Direcciones ip y otras características ip

Las políticas de firewall solo permiten direcciones IP de origen y destino válido. Las siguientes son recomendaciones para direcciones IP: o Se debe bloquear tráfico con direcciones de origen y destino inválidas, independientemente de la ubicación del firewall.

Se debe bloquear en el perímetro de la red el tráfico de entrada con una dirección de origen inválida o tráfico de salida con destino inválido.

- Se debe bloquear en el perímetro de la red el tráfico entrante con una dirección privada de destino o un tráfico saliente con una dirección de origen.

- Se debe bloquear el tráfico saliente con direcciones de origen inválidas.

- Se debe bloquear el tráfico entrante con dirección de destino del firewall, a menos de que el firewall esté ofreciendo servicios de conexión directa para el tráfico de entrada, por ejemplo, un proxy.

- El tráfico con información de enrutamiento permite a un sistema establecer la ruta que tomarán los paquetes desde su origen hasta su destino, también debe bloquearse o se debe bloquear el tráfico desde fuera de la red que contenga dirección de difusión que se dirija a

la red de la organización.

Los firewalls perimetrales deben bloquear tanto al tráfico que entra a la red como a los host que no deben ser accesibles desde redes externas. De la misma forma, se debe bloquear el tráfico saliente de redes y host de la organización que no deben acceder a redes externas [8].

IPv6

Aunque la longitud y el formato de las direcciones IPv6 son diferentes a las de IPV4, muchas características son similares por lo que los firewall deben funcionar igual para ambos protocolos, por ejemplo, el bloqueo de todo tráfico entrante y saliente que no haya sido especificado en las políticas firewall [9]. En todas las organizaciones ya sea que permitan o no tráfico IPv6, necesita un firewall capaz de filtrar este tráfico con las siguientes características:

- El firewall debe ser capaz de utilizar IPv6 en todas las reglas de filtrado que utilizan direcciones IPv4.

- La interfaz administrativa debe permitir al administrador clonar reglas IPv4 a IPv6 y así facilitar la administración. o El firewall debe ser capaz de bloquear protocolos IPv6 si no se requieren o si se utiliza un firewall para bloquear tráfico IPv6 entrante o saliente, éste firewall necesita reconocer y bloquear cualquier forma de túnel v6 a v4.

Las organizaciones que no utilizan IPv6 deben bloquear todo el tráfico nativo IPv6 en sus firewalls.

TCP y UDP

Los protocolos de aplicación pueden utilizar TCP, UDP o los dos dependiendo del diseño de la aplicación, por ejemplo, la búsqueda de DNS pueden realizarse en el puerto UDP 53 o TCP 53. El firewall escucha normalmente uno o más puertos UDP o TCP por lo que también se hace necesario implementar el método deny by default, aunque se utilizan políticas menos rigurosas que ésta para el tráfico saliente TCP y UDP debido a que muchas organizaciones permiten a sus usuarios acceder a muchas aplicaciones ubicadas en servidores externos [9].

ICMP

ICMP se utiliza por los protocolos de red de bajo nivel para aumentar la velocidad y fiabilidad de las redes. Aunque los ataques suelen utilizar ICMP para manipular el flujo del tráfico de la red, éste también puede ser utilizado para obtener un rendimiento razonable en internet, por lo que el bloqueo de este tráfico genera problemas de rendimiento. Otras políticas permiten el tráfico ICMP saliente pero impiden el entrante evitando el acceso al destino, por ejemplo, el comando ping es importante para realizar diagnósticos de la red, pero los ping entrantes generalmente se bloquean para evitar que los atacantes conozcan la topología de la red de la organización.

Es aconsejable bloquear el tráfico ICMP entrante y saliente en el firewall perimetral excepto cuando la organización necesite hacer uso de ellos. En resumen ICMP no debe ser bloqueado en una organización a menos que las necesidades de seguridad sean mayores que las operacionales [10].

PROTOCOLO IPSEC

La política firewall también debe definir si permite o no IPsec VPNs dentro de la red de la organización. Los protocolos ESP y AH se utilizan en IPsec VPNs, por lo que si se bloquean estos protocolos también lo harán las IPsec VPNs. Para las organizaciones que utilizan IPsec VPN deben bloquear ESP y AH excepto desde y hacia direcciones específicas de la red como las gateways IPsec que son autorizadas para ser el límite de la VPN [11].

POLÍTICAS BASADAS EN APLICACIONES

Las aplicaciones firewall o aplicaciones proxy proporcionan una capa adicional de seguridad para el tráfico de entrada mediante la validación de una parte de éste tráfico antes de llegar al servidor deseado. Estas aplicaciones también ayudan a evitar que el servidor tenga acceso directo con el exterior y a descartar tráfico malicioso antes de que llegue al servidor destino, reduciendo la carga del servidor. Las aplicaciones firewall y proxy se deben implementar cuando no se tiene un servidor capaz de protegerse de ataques [12].

Las aplicaciones firewall pueden presentar problemas si éstos no son lo suficientemente rápidos para manejar el tráfico destinado al servidor, pero si el servidor no posee recursos suficientes para soportar un ataque, estas aplicaciones pueden ser utilizadas como escudos.

Las aplicaciones proxy de salida permiten detectar sistemas que realizan conexiones inapropiadas o peligrosas dentro de la red, por ejemplo, cuando un proxy HTTP filtra contenido puede alertar al usuario que el sitio web visitado envió contenido filtrado. El mayor beneficio de un proxy HTTP no tiene que ver con seguridad sino con la caché de las páginas web para aumentar la velocidad y disminuir el ancho de banda utilizado [7].

Políticas basadas en la identidad de usuario

La implementación de VPNs permite aplicar en el firewall políticas basadas en la identidad del usuario. IPsec VPN o SSL VPN tienen varias formas para autenticar usuarios como por ejemplo con certificados digitales controlados por cada usuario. Las aplicaciones firewall y proxies pueden permitir o no el acceso a los usuarios en función de la autenticación que hagan los usuarios dentro de éstas aplicaciones. El firewall que permite estas políticas debe ser capaz de registrar tanto la IP del usuario como su identidad [11].

Políticas basadas en la actividad de la red

Estas políticas permiten al administrador del firewall bloquear las conexiones establecidas después de un determinado periodo de inactividad. Las políticas basadas en el tiempo son eficaces para mitigar los ataques causados por inicios de sesión olvidadas por el usuario original [10]. Sin embargo, éstas también pueden ser incómodas para los usuarios que inician conexiones pero no las utilizan con frecuencia.

Planificación e implementación de firewalls

La adopción de un esquema por etapas para la planeación e implementación de firewalls minimiza la probabilidad de ocurrencia de problemas y permite identificar fallas desde el principio. La Figura 6 presenta las etapas, las cuales se detallan a continuación.

Planeación

Esta primera fase del proceso consiste en identificar todos los requisitos que debe tener en cuenta una organización, para determinar el tipo de firewall que implementará para apoyar el cumplimiento de las políticas de seguridad de la organización. Debe partir de una evaluación

Figura 6 – Etapas para la planeación e implementación de firewalls.
Elaboración propia basado en [2]

inicial de riesgos del sistema en todo su conjunto, que considere mínimamente las amenazas y vulnerabilidades, la probabilidad e impacto de ocurrencia y los controles. En esta etapa se deben considerar los siguientes principios básicos:

- Utilizar los dispositivos para lo que están diseñados, un firewall sirve para controlar el flujo entre redes no para proveer servicios web.

- Crear defensa en profundidad, esto es múltiples capas de seguridad, lo cual permite una mejor gestión ya que si una capa se ve comprometida otra puede contener el ataque.

- Analizar las amenazas internas, centrar la atención solo en amenazas externas puede dejar puertas abiertas a los atacantes desde el interior.

- Documentar las capacidades de firewall, estas son las características que afectan positiva o negativamente la planificación y la estrategia de implementación.

Cada red y organización presenta requisitos y condiciones diferentes por lo que requieren soluciones únicas, por lo tanto es importante considerar a la hora de implementar firewalls la expresión "las reglas están hechas para romperse". Al adquirir una solución de firewall las organizaciones deben considerar, entre otras, las capacidades de seguridad, de gestión, de rendimiento, de integración, los medios físicos, las personas y las necesidades futuras.

Configuración

Esta fase incluye todos los aspectos de la configuración de la plataforma del firewall, incluyendo la instalación de hardware y software, configuración de políticas, configuración de logs y alertas, y la integración del firewall en la arquitectura de red.

- Configuración e instalación de hardware y software: los firewall se deben fortalecer para minimizar el riesgo de vulnerabilidades y proteger el sistema contra accesos no autorizados. Algunos elementos a tener en cuenta son: instalación de los últimos parches y actualizaciones y consolas de administración remota, configuración de cuentas de administración, inhabilitación de servicios de gestión como SNMP y sincronización de relojes. Adicionalmente los requisitos medioambientales recomendados para el producto como temperatura, humedad, espacio, energía, etc., y el espacio debe ser físicamente seguro para evitar que personas no autorizadas accedan.

- Configuración de políticas: el conjunto de reglas describe cómo funcionará el firewall e implementa la política de firewall de la organización por lo tanto debe ser lo más específico posible. Los detalles de la creación de conjunto de reglas varían según el tipo de firewall y productos específicos, sin embargo se debe tener claro el tipo de tráfico requerido por las aplicaciones de la organización, incluyendo los protocolos.

- Configuración de logs y alertas: Los logs son un paso crítico en la prevención y recuperación de fallas, así como para asegurar que se han establecido las configuraciones de seguridad adecuadas en el firewall. Un log adecuado puede proporcionar información vital para responder a los incidentes de seguridad. También se deben configurar las alertas en tiempo real para notificar cuando se produzcan eventos importantes en el firewall. Las notificaciones pueden incluir modificación o desactivación de las reglas de firewall, reinicios del sistema, espacio en discos y otros eventos operacionales.

Pruebas

Antes de la implementación de nuevos firewalls es necesario realizarles pruebas para asegurarse de que funcionan correctamente. Estas deben realizarse en redes aisladas de producción y

deben tratar de replicar las de producción lo más exactamente posible, incluyendo la topología y el tráfico de red que viajaría a través del firewall. Para las pruebas deben tenerse en cuenta aspectos como la conectividad, los conjunto de reglas, la compatibilidad con aplicaciones, administración, logs, el rendimiento, la seguridad de la aplicación, interoperabilidad de componentes, sincronización de políticas y algunas características adicionales como VPNs y capacidades antimalware.

Implementación

- Luego de finalizar las pruebas y resolver todos los problemas, la siguiente fase es la implementación, la cual se debe realizar en conformidad con las políticas de la organización. Previo a esto se debe informar a los usuarios o propietarios de sistemas sobre la nueva implementación para que ellos puedan evaluar el impacto en sus sistemas; todos los cambios necesarios deben ser coordinados como parte de la implementación del firewall. La política de seguridad global de la organización debe incluir la política de seguridad expresada en la configuración del firewall y todos los cambios deben integrarse con los procesos de gestión de la configuración de la organización.

- Para el despliegue de varios firewalls, incluyendo firewalls personales o en múltiples dependencias, se debe considerar un enfoque gradual o por etapas y la realización de un programa piloto, especialmente para identificar y resolver los problemas de las políticas en conflicto. Esto proporcionará a los administradores la oportunidad de evaluar el impacto de la solución de firewall y resolver los problemas antes de la implementación en toda la empresa.

- La conexión de un firewall implica no solo incluirlo en la topología de red sino integrarlo con otros elementos de la red que van a interactuar con él. Esto es, integrarse en la estructura de enrutamiento de la red, implicando en algunos casos sustituir routers, cambiar tablas de enrutamiento de otros routers de la red de la organización para gestionar la incorporación del nuevo dispositivo, aún para los que utilizan enrutamiento dinámico, cambios de configuración de los switches, entre otros.

Gestión

Esta última fase es la de mayor duración, pues la gestión incluye el mantenimiento de la arquitectura, las políticas, el software, y los otros componentes de la solución. En esta etapa: (1) Se deben actualizar las políticas con las nuevas amenazas y los cambios de requisitos que ocurran. (2) Se debe monitorear el rendimiento de los componentes del firewall para asegurar que se identifican y se tratan con tiempo los posibles problemas de los recursos. (3) Por otra parte, los logs y las alertas también deben ser controlados continuamente para identificar amenazas –exitosas y no exitosas- que se realizan en el sistema. (4) Se deben ejecutar pruebas periódicas para comprobar que las reglas del firewall están funcionando como se espera.

Además, (5) las políticas y los conjuntos de reglas del firewall se deben respaldar con regularidad en los múltiples formatos que se requieran. (6) Como los cambios en los conjuntos de reglas del firewall o en las políticas mismas impactan en la seguridad se debe integrar con el proceso formal de gestión de la configuración. (7) Se debe mantener un log asociado con el firewall que incluya todas las decisiones frente a las políticas y los cambios.

(8) Siempre que sea posible, los conjuntos de reglas se deben documentar con comentarios sobre cada regla específica. (9) Se deben utilizar

las restricciones sobre quién puede realizar cambios en el conjunto de reglas, y sobre las direcciones desde las que los administradores pueden hacer tales modificaciones.

Con el tiempo los conjuntos de reglas pueden hacerse cada vez más complejos debido al ingreso de nuevas reglas, esto se puede originar por el ingreso de nuevos usuarios, hosts o simplemente nuevos requisitos de negocio. El mantenimiento servirá tanto para identificar reglas obsoletas como para identificar nuevas necesidades de las políticas que se deben agregar al firewall.

Las mejores prácticas de NIST 800-41 indican que la política firewall se debe revisar a intervalos regulares para que esos hallazgos no ocurran en las auditorías de seguridad, o, peor aún, sólo en casos de emergencia. Cada revisión debe incluir una evaluación detallada de todos los cambios desde la última revisión, quien lo realizó y las circunstancias sobre las que lo hizo. Personas diferentes al equipo que revisan periódicamente las políticas deben realizar una revisión con el objetivo de obtener una visión externa del cumplimiento de los objetivos de seguridad. Debe hacerse uso de las herramientas de diagnóstico que traen algunos firewall con el objetivo de buscar cosas como reglas redundantes o reglas que faltan y que son ampliamente recomendables.

Las pruebas de penetración, que permiten evaluar la seguridad global del perímetro de la red son un mecanismo recomendado, estas pruebas se pueden utilizar para comprobar que un conjunto de reglas del firewall está funcionando según lo previsto Deben ser usadas como complemento a las auditorías.

CONCLUSIONES

La seguridad perimetral en las redes de datos de cualquier organización es de vital importancia, ya que con ella se minimizan los riesgos que vulneran los sistemas de información y la información misma. Los firewall cumplen este papel puesto que se encargan de controlar el tráfico de datos entre la redes privadas e internet y lo puede realizar en las capas de red, transporte y aplicación del modelo TCP/IP, dependiendo del tipo que se desee implementar, sin embargo se sabe que estos dispositivos por si solos no son la solución a la implementación de seguridad en una red, se requieren delimitar claramente las políticas para que realmente cumpla con su objetivo.

El firewall puede trabajar en cualquier topología de red que se desee proteger, con unas buenas políticas de firewall que controlen el tráfico y un buen control por direccionamiento IP y que estén alineadas con las políticas de seguridad de la información de la organización. En general, debe encajar en el diseño de una red actual, sin embargo, una organización puede cambiar su arquitectura de la red al mismo tiempo que se implementa un firewall como parte de un programa de actualización de seguridad en general

Diferentes arquitecturas de red comunes conducen a opciones muy diferentes de dónde ubicar un firewall, por lo que una organización debe evaluar qué arquitectura le funciona mejor para sus objetivos de seguridad. En algunos entornos, ubicar un firewall detrás de otro puede conducir al objetivo de seguridad deseado, pero en general estas múltiples capas de firewalls pueden ser problemáticas [11].

Si un firewall perimetral tiene una DMZ, tenga en cuenta cuales de los servicios orientados hacia el exterior deben ejecutarse desde la zona desmilitarizada y cuales deben permanecer en el interior de la red.

Para robustecer el firewall nos podemos

apoyar en sistemas de prevención y detección de intrusos (IDS/IPS) que trabajan en la capa de aplicación, estos ayudan a detectar el software malicioso que pueden vulnerar las aplicaciones de las organizaciones.

Para la implementación de un firewall es aconsejable realizar una planificación acorde a las necesidades de la red, realizar la configuración de las políticas del firewall, hacer pruebas que identifiquen posibles fallas y por último, gestionar el mantenimiento de la aplicación para mantenerlo en buen funcionamiento.

REFERENCIAS

[1] NEXICA. Aplicaciones más seguras y rentables. [En línea]. Disponible en: http://www.nexica.com/es/firewallaplicaciones

[2] FORTINET. Protecting your network from viruses. [En línea]. Disponible en: http://docs.fortinet.com/cb/html/index.html#page/FOS_Cookbook/UTM/cb_utm_av_basic_db.html

[3] SOPHOS UTM Home edition. [En línea]. Disponible en: http://www.sophos.com/es-es/products/freetools/ sophos-utm-home-edition.aspx

[4] Á. Gomez Vieites. Enciclopedia de la seguridad informática. Cap 4 Los aspectos técnicos para implantar las medidas de seguridad en las redes. RA-MA. 2011.

[5] NSS labs. Next Generation Firewall (NGFW). V5.3. Disponible en: https://www.fortinet.com/lat/products/next-generation-firewall

[6] R. Bustamante. Seguridad en Redes. Universidad Autónoma de Hidalgo. Disponible en: http://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/do cumentos/Seguridad%20en%20redes.pdf

[7] K. Scarfone, P. Hoffman. Guidelines on firewall and policy. V1. National Institute of Standard and TechnologyNIST. 2009.

[8] R. Ziegler. Firewalls Linux Guía Avanzada. Prentice Hall. Disponible en: http://hack.dk/~dvc/doc/Prentice.Hall.-.Firewalls.Linux.(libro-book-espa%C3%B1ol).%5Bwww.elbuscaelinks.com%5D.pdf

[9] R. Hunt. Internet/Intranet firewall security - policy, architecture and transaction services. 1998.

[10] PALO ALTO NETWORKS. Protección contra botnets con el firewall de nueva generación. The network security company. Disponible en: http://www.exevi.com/doc/PAN_WP_BotNet_ES.pdf

[11]ELSEVIER. Formal security policy implementations in network firewalls. 2012. Computers & Security. Disponible en: http://www.deepdyve.com/lp/elsevier/formalsecurity-policy-implementations-in-network-firewalls-A6AwrNm6ne