National Institute of
Standards and Technology
U.S. Department of Commerce

Publicación especial 800-41
Revisión 1

Directrices sobre cortafuegos y Política de cortafuegos

Recomendaciones del Instituto Nacional de Estándares y Tecnología

Karen Bufanda
Pablo Hoffman

Publicación especial del NIST 800-41
Revisión 1

Directrices sobre cortafuegos y cortafuegos Política

Recomendaciones del Consejo Nacional
Instituto de Estándares y Tecnología

Karen Bufanda
Pablo Hoffman

LA SEGURIDAD INFORMÁTICA

División de Seguridad Informática
Laboratorio de Tecnología de la Información
Instituto Nacional de Estándares y Tecnología
Gaithersburg, MD 20899-8930

Septiembre 2009

Departamento de Comercio de EE. UU.

Gary Locke, Secretario

Instituto Nacional de Estándares y Tecnología

Patrick D. Gallagher, subdirector

Informes sobre tecnología de sistemas informáticos

El Laboratorio de Tecnología de la Información (ITL) del Instituto Nacional de Estándares y Tecnología (NIST) promueve la economía y el bienestar público de los EE. UU. brindando liderazgo técnico para la infraestructura de estándares y mediciones del país. ITL desarrolla pruebas, métodos de prueba, datos de referencia, implementaciones de prueba de concepto y análisis técnicos para avanzar en el desarrollo y el uso productivo de la tecnología de la información. Las responsabilidades de ITL incluyen el desarrollo de estándares y directrices técnicos, físicos, administrativos y de gestión para la seguridad y privacidad rentables de información confidencial no clasificada en los sistemas informáticos federales. Esta publicación especial de la serie 800 informa sobre los esfuerzos de investigación, orientación y divulgación de ITL en seguridad informática y sus actividades de colaboración con la industria, el gobierno y las organizaciones académicas.

Publicación especial del Instituto Nacional de Estándares y Tecnología 800-41 Revisión 1 Natl. Inst.
Pararse. Tecnología. Especificaciones. Publ. 800-41 rev1, 48 páginas (septiembre de 2009)

Expresiones de gratitud

Los autores, Karen Scarone del Instituto Nacional de Estándares y Tecnología (NIST) y Paul Hoffman del Virtual Private Network Consortium, desean agradecer a sus colegas que revisaron los borradores de este documento y contribuyeron a su contenido técnico. Los autores desean agradecer a Tim Grance, Murugiah Souppaya, Sheila Frankel y Gale Richter del NIST, y a Matthew Goche, David Klug, Logan Lodge, John Pearce, Noel Richards, Anne Roudabush y Steven Sharma de Booz Allen Hamilton, por su Asistencia entusiasta y perspicaz durante todo el desarrollo del documento. Un agradecimiento especial a Brahim Asfahani de Booz Allen Hamilton por sus contribuciones a los primeros borradores del documento. Los autores también agradecen a todos los revisores que brindaron comentarios durante el período de comentarios públicos, en particular a Joel Snyder (Opus One), Ron Colvin (Administración Nacional de Aeronáutica y del Espacio [NASA]), Dean Farrington (Wells Fargo), Raffael Marty (Splunk), y David Newman (Prueba de red).

Los autores también desean expresar su agradecimiento a las personas y organizaciones que contribuyeron a la versión original de la publicación, incluidos John Wack del NIST y Ken Cutler y Jamie Pole del MIS Training Institute, autores de la versión original, y otros contribuyentes y revisores—particularmente Peter Batista y Wayne Bavry (Tesoro de Estados Unidos); Harriet Feldman (Ingeniería Informática Integrada, Inc.); Rex Sanders (Servicio Geológico de Estados Unidos); y Timothy Grance, D. Richard Kuhn, Peter Mell, Gale Richter y Murugiah Souppaya (NIST).

Tabla de contenido

Lista de apendices

Lista de Figuras

Lista de tablas

Resumen ejecutivo

Los firewalls son dispositivos o programas que controlan el flujo de tráfico de red entre redes o hosts que emplean diferentes posturas de seguridad. Hubo un tiempo en que la mayoría de los firewalls se implementaban en los perímetros de la red. Esto proporcionó cierta medida de protección para los hosts internos, pero no pudo reconocer todas las instancias y formas de ataque, y los ataques enviados de un host interno a otro a menudo no pasan a través de los firewalls de la red.
Debido a estos y otros factores, los diseñadores de redes ahora suelen incluir funcionalidad de firewall en lugares distintos al perímetro de la red para proporcionar una capa adicional de seguridad, así como para proteger los dispositivos móviles que se colocan directamente en redes externas.

Las amenazas han pasado gradualmente de ser más frecuentes en las capas inferiores del tráfico de la red a la capa de aplicación, lo que ha reducido la eficacia general de los firewalls para detener las amenazas transmitidas a través de las comunicaciones de la red. Sin embargo, todavía se necesitan firewalls para detener las amenazas importantes que continúan funcionando en las capas inferiores del tráfico de la red. Los cortafuegos también pueden proporcionar cierta protección en la capa de aplicación, complementando las capacidades de otras tecnologías de seguridad de red.

Existen varios tipos de firewalls, cada uno con diferentes capacidades para analizar el tráfico de red y permitir o bloquear instancias específicas comparando las características del tráfico con las políticas existentes. Comprender las capacidades de cada tipo de firewall, diseñar políticas de firewall y adquirir tecnologías de firewall que aborden eficazmente las necesidades de una organización son fundamentales para lograr la protección de los flujos de tráfico de la red. Este documento proporciona una descripción general de las tecnologías de firewall y analiza en detalle sus capacidades de seguridad y sus ventajas y desventajas relativas. También proporciona ejemplos de dónde se pueden colocar los firewalls dentro de las redes y las implicaciones de implementar firewalls en ubicaciones particulares. El documento también hace recomendaciones para establecer políticas de firewall y para seleccionar, configurar, probar, implementar y administrar soluciones de firewall.

Este documento no cubre las tecnologías denominadas "firewalls", sino que examina principalmente sólo la actividad de la capa de aplicación, no las capas inferiores de tráfico de red. Las tecnologías que se centran en la actividad de un tipo particular de aplicación, como los cortafuegos de correo electrónico que bloquean mensajes de correo electrónico con contenido sospechoso, no se tratan en detalle en este documento.

Para mejorar la eficacia y seguridad de sus firewalls, las organizaciones deben implementar las siguientes recomendaciones:

Cree una política de firewall que especifique cómo los firewalls deben manejar el tráfico de red entrante y saliente.

Una política de firewall define cómo los firewalls de una organización deben manejar el tráfico de red entrante y saliente para direcciones IP específicas y rangos de direcciones, protocolos, aplicaciones y tipos de contenido según las políticas de seguridad de la información de la organización. Las organizaciones deben realizar análisis de riesgos para desarrollar una lista de los tipos de tráfico que necesita la organización y cómo deben protegerse, incluido qué tipos de tráfico pueden atravesar un firewall y en qué circunstancias. Los ejemplos de requisitos de política incluyen permitir que solo pasen los protocolos de Protocolo de Internet (IP) necesarios, utilizar direcciones IP de origen y destino apropiadas, acceder a puertos particulares de Protocolo de control de transmisión (TCP) y Protocolo de datagramas de usuario (UDP), y ciertos requisitos de control de Internet. Tipos y códigos de protocolo de mensajes (ICMP) que se utilizarán.
En general, todo el tráfico entrante y saliente que no esté expresamente permitido por la política de firewall debe bloquearse porque la organización no lo necesita. Esta práctica reduce el riesgo de ataque y también puede disminuir el volumen de tráfico transportado en las redes de la organización.

Identifique todos los requisitos que se deben considerar al determinar qué firewall implementar.

Hay muchas consideraciones que las organizaciones deben incluir en sus procesos de planificación y selección de firewalls. Las organizaciones deben determinar qué áreas de red deben protegerse y qué tipos de tecnologías de firewall serán más efectivas para los tipos de tráfico que requieren protección. También existen varias consideraciones importantes sobre el rendimiento, así como preocupaciones con respecto a la integración del firewall en las infraestructuras de red y seguridad existentes. Además, el diseño de la solución de firewall implica requisitos relacionados con el entorno físico y el personal, así como la consideración de posibles necesidades futuras, como planes para adoptar nuevas tecnologías IPv6 o redes privadas virtuales (VPN).

Cree conjuntos de reglas que implementen la política de firewall de la organización y al mismo tiempo respalden el rendimiento del firewall.

Los conjuntos de reglas del firewall deben ser lo más específicos posible con respecto al tráfico de red que controlan. Crear un conjunto de reglas implica determinar qué tipos de tráfico se requieren, incluidos los protocolos que el firewall puede necesitar para fines de administración. Los detalles de la creación de conjuntos de reglas varían ampliamente según el tipo de firewall y productos específicos, pero se puede mejorar el rendimiento de muchos firewalls optimizando los conjuntos de reglas de firewall. Por ejemplo, algunos cortafuegos comparan el tráfico con las reglas de forma secuencial hasta encontrar una coincidencia; Para estos firewalls, las reglas que tienen la mayor probabilidad de coincidir con los patrones de tráfico deben colocarse en la parte superior de la lista siempre que sea posible.

Administre arquitecturas de firewall, políticas, software y otros componentes durante la vida útil de las soluciones de firewall.

Hay muchos aspectos de la gestión del firewall. Por ejemplo, elegir el tipo o tipos de cortafuegos que se implementarán y sus posiciones dentro de la red puede afectar significativamente las políticas de seguridad que los cortafuegos pueden aplicar. Es posible que sea necesario actualizar las reglas de políticas a medida que cambian los requisitos de la organización, como cuando se implementan nuevas aplicaciones o hosts dentro de la red. También es necesario monitorear el rendimiento de los componentes del firewall para permitir identificar y abordar posibles problemas de recursos antes de que los componentes se vean abrumados. Los registros y alertas también deben monitorearse continuamente para identificar amenazas, tanto exitosas como fallidas. Los conjuntos de reglas y políticas de firewall deben gestionarse mediante un proceso formal de control de gestión de cambios debido a su potencial para afectar la seguridad y las operaciones comerciales, con revisiones o pruebas de conjuntos de reglas realizadas periódicamente para garantizar el cumplimiento continuo de las políticas de la organización. El software de firewall debe recibir parches a medida que los proveedores proporcionan actualizaciones para abordar las vulnerabilidades.

1. Introducción

1.1 Autoridad

El Instituto Nacional de Estándares y Tecnología (NIST) desarrolló este documento en cumplimiento de sus responsabilidades legales bajo la Ley Federal de Gestión de Seguridad de la Información (FISMA) de 2002, Ley Pública 107-347.

El NIST es responsable de desarrollar estándares y directrices, incluidos los requisitos mínimos, para proporcionar una seguridad de la información adecuada para todas las operaciones y activos de la agencia; pero dichas normas y directrices no se aplicarán a los sistemas de seguridad nacionales. Esta directriz es consistente con los requisitos de la Circular A-130 de la Oficina de Gestión y Presupuesto (OMB), Sección 8b(3), “Protección de los sistemas de información de las agencias”, tal como se analiza en A-130, Apéndice IV: Análisis de secciones clave. Se proporciona información complementaria en A-130, Apéndice III.

Esta guía ha sido preparada para uso de agencias federales. Puede ser utilizado por organizaciones no gubernamentales de forma voluntaria y no está sujeto a derechos de autor, aunque se desea atribución.

Nada en este documento debe considerarse en contradicción con las normas y directrices que el Secretario de Comercio ha hecho obligatorias y vinculantes para las agencias federales en virtud de la autoridad legal, ni estas directrices deben interpretarse como una alteración o sustitución de las autoridades existentes del Secretario de Comercio, Director de la OMB, o cualquier otro funcionario federal.

1.2 Propósito y Alcance

Este documento busca ayudar a las organizaciones a comprender las capacidades de las tecnologías y políticas de firewall. Proporciona orientación práctica sobre el desarrollo de políticas de firewall y la selección, configuración, prueba, implementación y administración de firewalls.

1.3 Audiencia

Este documento se ha creado principalmente para personal técnico de tecnología de la información (TI), como ingenieros y administradores de redes, seguridad y sistemas que son responsables del diseño, selección, implementación y administración del firewall. Otro personal de TI con responsabilidades de seguridad de redes y sistemas también puede encontrar útil este documento. El contenido asume algunos conocimientos básicos de redes y seguridad de redes.

1.4 Estructura del documento

El resto de este documento está organizado en cuatro secciones principales:

La Sección 2 proporciona una descripción general de una serie de tecnologías de firewall de red, incluido el filtrado de paquetes, la inspección de estado y la puerta de enlace de proxy de aplicaciones, y también proporciona información sobre firewalls personales y basados en host.

La sección 3 analiza la ubicación de firewalls dentro de las arquitecturas de red.

La sección 4 analiza las políticas de firewall y hace recomendaciones sobre los tipos de tráfico que deben especificarse como prohibidos.

La Sección 5 proporciona una descripción general de la planificación e implementación del firewall. Enumera los factores a considerar al seleccionar soluciones de firewall y proporciona recomendaciones para la configuración, prueba, implementación y administración del firewall.

El documento también contiene apéndices con material de apoyo:

Los apéndices A y B contienen un glosario y una lista de acrónimos y abreviaturas, respectivamente.

El Apéndice C enumera recursos impresos y en línea que pueden ser útiles para comprender mejor los firewalls.

2. Descripción general de las tecnologías de firewall

Los firewalls son dispositivos o programas que controlan el flujo de tráfico de red entre redes o hosts que emplean diferentes posturas de seguridad. Si bien los cortafuegos a menudo se analizan en el contexto de la conectividad a Internet, también pueden tener aplicabilidad en otros entornos de red. Por ejemplo, muchas redes empresariales emplean firewalls para restringir la conectividad hacia y desde las redes internas utilizadas para dar servicio a funciones más sensibles, como contabilidad o personal. Al emplear firewalls para controlar la conectividad a estas áreas, una organización puede evitar el acceso no autorizado a sus sistemas y recursos.
La inclusión de un firewall adecuado proporciona una capa adicional de seguridad. Las organizaciones a menudo necesitan utilizar firewalls para cumplir con los requisitos de seguridad de los mandatos (por ejemplo, FISMA); algunos mandatos, como el Estándar de seguridad de datos de la industria de tarjetas de pago (PCI),1 requieren específicamente firewalls.

Hay varios tipos de tecnologías de firewall disponibles. Una forma de comparar sus capacidades es observar las capas del Protocolo de control de transmisión/Protocolo de Internet (TCP/IP) que cada uno puede examinar. Las comunicaciones TCP/IP se componen de cuatro capas que trabajan juntas para transferir datos entre hosts. Cuando un usuario desea transferir datos a través de redes, los datos se pasan desde la capa más alta a través de capas intermedias hasta la capa más baja, y cada capa agrega más información. La capa más baja envía los datos acumulados a través de la red física, y luego los datos pasan hacia arriba a través de las capas hasta su destino. En pocas palabras, los datos producidos por una capa son encapsulados en un contenedor más grande por la capa debajo de ella. Las cuatro capas TCP/IP, de mayor a menor, se muestran en la Figura 2-1.

Capa de aplicación. Esta capa envía y recibe datos para aplicaciones particulares, como el Sistema de nombres de dominio (DNS), el Protocolo de transferencia de hipertexto (HTTP) y el Protocolo simple de transferencia de correo (SMTP). La propia capa de aplicación tiene capas de protocolos dentro de ella. Por ejemplo, SMTP encapsula la sintaxis del mensaje Solicitud de comentarios (RFC) 2822, que encapsula las extensiones multipropósito de correo de Internet (MIME), que pueden encapsular otros formatos como el lenguaje de marcado de hipertexto (HTML).
Capa de transporte. Esta capa proporciona servicios orientados a la conexión o sin conexión para transportar servicios de la capa de aplicación entre redes y, opcionalmente, puede garantizar la confiabilidad de las comunicaciones. El Protocolo de control de transmisión (TCP) y el Protocolo de datagramas de usuario (UDP) son protocolos de capa de transporte comúnmente utilizados.2
Capa IP (también conocida como capa de red). Esta capa enruta paquetes a través de redes. El Protocolo de Internet versión 4 (IPv4) es el protocolo de capa de red fundamental para TCP/IP. Otros protocolos comúnmente utilizados en la capa de red son el Protocolo de Internet versión 6 (IPv6), ICMP y el Protocolo de administración de grupos de Internet (IGMP).
Capa de hardware (también conocida como capa de enlace de datos). Esta capa maneja las comunicaciones en los componentes físicos de la red. El protocolo de capa de enlace de datos más conocido es Ethernet.

Figura 2-1. Capas TCP/IP

Las direcciones en la capa de enlace de datos, que se asignan a interfaces de red, se conocen como direcciones de control de acceso a medios (MAC); un ejemplo de esto es una dirección Ethernet que pertenece a una tarjeta Ethernet.
Las políticas de firewall rara vez se ocupan de la capa de enlace de datos. Las direcciones en la capa de red se denominan direcciones IP. La capa de transporte identifica aplicaciones de red y sesiones de comunicación específicas en lugar de direcciones de red; un host puede tener cualquier número de sesiones de capa de transporte con otros hosts en la misma red. La capa de transporte también puede incluir la noción de puertos :
un número de puerto de destino generalmente identifica un servicio que escucha en el host de destino, y un puerto de origen generalmente identifica el número de puerto en el host de origen al que el host de destino debe responder. Los protocolos de transporte como TCP y UDP tienen puertos, mientras que otros protocolos de transporte no. La combinación de

1 El Estándar de seguridad de datos PCI puede aplicarse a algunas agencias federales. Se define en https://www.pcisecuritystandards.org/.
2 Las diferencias entre TCP y UDP se explican en varios de los recursos de impresión enumerados en el Apéndice C.

La dirección IP de origen y el puerto con la dirección IP y el puerto de destino ayudan a definir la sesión. La capa más alta representa las aplicaciones del usuario final: los firewalls pueden inspeccionar el tráfico de las aplicaciones y utilizarlo como base para decisiones políticas.

Los firewalls básicos operan en una o varias capas (generalmente las capas inferiores), mientras que los firewalls más avanzados examinan todas las capas que se muestran en la Figura 2-1. Aquellos que examinan más capas pueden realizar exámenes más granulares y completos. Los cortafuegos que comprenden la capa de aplicación pueden potencialmente acomodar aplicaciones y protocolos avanzados y proporcionar servicios orientados al usuario. Por ejemplo, un firewall que solo maneja capas inferiores generalmente no puede identificar usuarios específicos, pero un firewall con capacidades de capa de aplicación puede imponer la autenticación de usuarios y registrar eventos para usuarios específicos.

2.1 Tecnologías de cortafuegos

Esta sección de la publicación proporciona una descripción general de las tecnologías de firewall e información básica sobre las capacidades de varios tipos de uso común. El cortafuegos a menudo se combina con otras tecnologías: sobre todo el enrutamiento, y muchas tecnologías a menudo asociadas con firewalls son, con mayor precisión, parte de estas otras tecnologías. Por ejemplo, a veces se piensa que la traducción de direcciones de red (NAT) es una tecnología de firewall, pero en realidad es una tecnología de enrutamiento. Muchos firewalls también incluyen funciones de filtrado de contenido para hacer cumplir las políticas de la organización que no están directamente relacionadas con la seguridad. Algunos firewalls incluyen tecnologías de sistemas de prevención de intrusiones (IPS), que pueden reaccionar a los ataques que detectan para evitar daños a los sistemas protegidos por el firewall.

Los cortafuegos suelen colocarse en el perímetro de una red. Se puede decir que dicho firewall tiene un externo e interfaz interna , siendo la interfaz externa la que está fuera de la red. A veces se hace referencia a estas dos interfaces como desprotegidas y protegidas, respectivamente. Sin embargo, decir que algo está o no protegido suele ser inapropiado porque las políticas de un firewall pueden funcionar en ambas direcciones; por ejemplo, podría haber una política para evitar que se envíe código ejecutable desde dentro del perímetro a sitios fuera del perímetro.

2.1.1 Filtrado de paquetes

La característica más básica de un firewall es el filtro de paquetes. Los firewalls más antiguos que eran solo filtros de paquetes eran esencialmente dispositivos de enrutamiento que proporcionaban funcionalidad de control de acceso para direcciones de host y sesiones de comunicación. Estos dispositivos, también conocidos como firewalls de inspección sin estado, no realizan un seguimiento del estado de cada flujo de tráfico que pasa a través del firewall; esto significa, por ejemplo, que no pueden asociar entre sí varias solicitudes dentro de una sola sesión. El filtrado de paquetes es el núcleo de la mayoría de los firewalls modernos, pero hoy en día se venden pocos firewalls que solo realizan filtrado de paquetes sin estado. A diferencia de los filtros más avanzados, los filtros de paquetes no se preocupan por el contenido de los paquetes. Su funcionalidad de control de acceso se rige por un conjunto de directivas denominadas conjunto de reglas. Las capacidades de filtrado de paquetes están integradas en la mayoría de los sistemas operativos y dispositivos capaces de enrutamiento; El ejemplo más común de un dispositivo de filtrado de paquetes puro es un enrutador de red que emplea listas de control de acceso.

En su forma más básica, los firewalls con filtros de paquetes operan en la capa de red. Esto proporciona control de acceso a la red basado en varios datos contenidos en un paquete, que incluyen:

- La dirección IP de origen del paquete: la dirección del host desde el que se originó el paquete (como 192.168.1.1)

- La dirección de destino del paquete: la dirección del host al que intenta llegar el paquete (por ejemplo, 192.168.2.1).

La red o el protocolo de transporte que se utiliza para comunicarse entre los hosts de origen y de destino, como TCP, UDP o ICMP.

Posiblemente algunas características de las sesiones de comunicaciones de la capa de transporte, como los puertos de origen y destino de la sesión (por ejemplo, TCP 80 para el puerto de destino que pertenece a un servidor web, TCP 1320 para el puerto de origen que pertenece a una computadora personal que accede al servidor)

La interfaz que atraviesa el paquete y su dirección (entrante o saliente).

El filtrado del tráfico entrante se conoce como filtrado de entrada. El tráfico saliente también se puede filtrar, proceso denominado filtrado de salida. Aquí, las organizaciones pueden implementar restricciones en su tráfico interno, como bloquear el uso de servidores de protocolo de transferencia de archivos (FTP) externos o evitar que se lancen ataques de denegación de servicio (DoS) desde dentro de la organización contra entidades externas. Las organizaciones solo deben permitir el tráfico saliente que utilice las direcciones IP de origen que utiliza la organización, un proceso que ayuda a bloquear el tráfico con direcciones falsificadas para que no se filtre a otras redes. Las direcciones falsificadas pueden deberse a eventos maliciosos, como infecciones de malware o hosts comprometidos que se utilizan para lanzar ataques, o a configuraciones erróneas inadvertidas.

Los filtros de paquetes sin estado generalmente son vulnerables a ataques y exploits que aprovechan problemas dentro de la especificación TCP/IP y la pila de protocolos. Por ejemplo, muchos filtros de paquetes no pueden detectar cuando la información de dirección de la capa de red de un paquete ha sido falsificada o alterada de otro modo, o utilizan opciones permitidas por los estándares pero que generalmente se utilizan con fines maliciosos, como el enrutamiento de origen IP. Los intrusos generalmente emplean ataques de suplantación de identidad, como el uso de direcciones incorrectas en los encabezados de los paquetes, para eludir los controles de seguridad implementados en una plataforma de firewall. Los cortafuegos que operan en capas superiores pueden frustrar algunos ataques de suplantación de identidad verificando que se haya establecido una sesión o autenticando a los usuarios antes de permitir el paso del tráfico. Debido a esto, la mayoría de los firewalls que utilizan filtros de paquetes también mantienen cierta información de estado de los paquetes que atraviesan el firewall.

Algunos filtros de paquetes pueden filtrar específicamente paquetes fragmentados. La fragmentación de paquetes está permitida por las especificaciones TCP/IP y se recomienda en situaciones donde sea necesaria. Sin embargo, la fragmentación de paquetes se ha utilizado para hacer que algunos ataques sean más difíciles de detectar (colocándolos dentro de paquetes fragmentados), y también se ha utilizado una fragmentación inusual como forma de ataque. Por ejemplo, algunos ataques basados en redes han utilizado paquetes que no deberían existir en las comunicaciones normales, como enviar algunos fragmentos de un paquete pero no el primero, o enviar fragmentos de paquetes que se superponen entre sí. Para evitar el uso de paquetes fragmentados en ataques, se han configurado algunos firewalls para bloquear paquetes fragmentados.

Hoy en día, los paquetes fragmentados en Internet a menudo ocurren no debido a ataques, sino a tecnologías de redes privadas virtuales (VPN) que encapsulan paquetes dentro de otros paquetes. Si encapsular un paquete causaría que el nuevo paquete exceda el tamaño máximo permitido para el medio en el que se transmitirá, el paquete debe fragmentarse. Los paquetes fragmentados bloqueados por firewalls son una causa común de problemas de interoperabilidad de VPN.

Algunos firewalls pueden volver a ensamblar fragmentos antes de pasarlos a la red interna, aunque esto requiere recursos de firewall adicionales, particularmente memoria. Los cortafuegos que tienen esta función de reensamblaje deben implementarla con cuidado; de lo contrario, alguien puede montar fácilmente un ataque de denegación de servicio. Elegir si bloquear, reensamblar o pasar paquetes fragmentados es una compensación entre la interoperabilidad general de la red y la seguridad total del sistema. Teniendo en cuenta esto, no se recomienda el bloqueo automático de todos los paquetes fragmentados debido a los usos legítimos y necesarios de la fragmentación en Internet.

2.1.2 Inspección de estado

La inspección de estado mejora las funciones de los filtros de paquetes al rastrear el estado de las conexiones y bloquear los paquetes que se desvían del estado esperado. Esto se logra incorporando una mayor conciencia de la capa de transporte. Al igual que con el filtrado de paquetes, la inspección con estado intercepta paquetes en la capa de red y los inspecciona para ver si están permitidos por una regla de firewall existente, pero a diferencia del filtrado de paquetes, la inspección con estado realiza un seguimiento de cada conexión en una tabla de estado. Si bien los detalles de las entradas de la tabla de estado varían según el producto de firewall, normalmente incluyen la dirección IP de origen, la dirección IP de destino, los números de puerto y la información del estado de la conexión.

Existen tres estados principales para el tráfico TCP: establecimiento, uso y terminación de la conexión (que se refiere tanto a un punto final que solicita que se cierre una conexión como a una conexión con un largo período de inactividad). La inspección de estado en un firewall examina ciertos valores en el TCP encabezados para monitorear el estado de cada conexión. El firewall compara cada nuevo paquete con la tabla de estado del firewall para determinar si el estado del paquete contradice su estado esperado. Por ejemplo, un atacante podría generar un paquete con un encabezado que indique que es parte de una conexión establecida, con la esperanza de que atraviese un firewall. Si el firewall utiliza una inspección de estado, primero verificará que el paquete sea parte de una conexión establecida que figura en la tabla de estado.

En el caso más simple, un firewall permitirá el paso de cualquier paquete que parezca ser parte de una conexión abierta (o incluso una conexión que aún no esté completamente establecida). Sin embargo, muchos firewalls conocen mejor las máquinas de estado de protocolos como TCP y UDP, y bloquearán los paquetes que no se adhieran estrictamente a la máquina de estado apropiada. Por ejemplo, es común que los firewalls verifiquen atributos como los números de secuencia TCP y rechacen paquetes que están fuera de secuencia. Cuando un firewall proporciona servicios NAT, suele incluir información NAT en su tabla de estado.

La tabla 2-1 proporciona un ejemplo de una tabla de estados. Si un dispositivo en la red interna (que se muestra aquí como 192.168.1.100) intenta conectarse a un dispositivo fuera del firewall (192.0.2.71), primero se verifica el intento de conexión para ver si está permitido por el conjunto de reglas del firewall. Si está permitido, se agrega una entrada a la tabla de estado que indica que se está iniciando una nueva sesión, como se muestra en la primera entrada bajo "Estado de la conexión" en la Tabla 2-1. Si 192.0.2.71 y 192.168.1.100 completan el protocolo de enlace TCP de tres vías, el estado de la conexión cambiará a "establecido" y todo el tráfico posterior que coincida con la entrada podrá pasar a través del firewall.

Tabla 2-1. Ejemplo de tabla de estado

Dirección de origen	Puerto de origen	Destino DIRECCIÓN	Destino Puerto	Estado de conexión
192.168.1.100	1030	192.0.2.71	80	Iniciado
192.168.1.102	1031	10.12.18.74	80	Establecido
192.168.1.101	1033	10.66.32.122	25	Establecido
192.168.1.106	1035	10.231.32.12	79	Establecido

Debido a que algunos protocolos, en particular UDP, no tienen conexión y no tienen un proceso formal para inicializar, establecer y terminar una conexión, su estado no puede establecerse en la capa de transporte como ocurre con TCP. Para estos protocolos, la mayoría de los firewalls con inspección de estado solo pueden rastrear las direcciones IP y los puertos de origen y destino. Los paquetes UDP aún deben coincidir con una entrada en la tabla de estado basada en la dirección IP de origen y destino y la información del puerto para que se les permita pasar; una respuesta DNS de una fuente externa solo se permitiría pasar si el firewall hubiera visto previamente una consulta DNS correspondiente. de una fuente interna.
Dado que el firewall no puede determinar cuándo

Una vez finalizada la sesión, la entrada se elimina de la tabla de estado después de alcanzar un valor de tiempo de espera preconfigurado. Los firewalls a nivel de aplicación que pueden reconocer DNS a través de UDP finalizarán una sesión después de recibir una respuesta de DNS y pueden actuar de manera similar con el Protocolo de tiempo de red (NTP).

2.1.3 Cortafuegos de aplicaciones

Una tendencia más reciente en la inspección de estado es la adición de una capacidad de análisis de protocolo con estado , a la que algunos proveedores se refieren como inspección profunda de paquetes. El análisis de protocolos con estado mejora la inspección con estado estándar al agregar tecnología básica de detección de intrusiones: un motor de inspección que analiza protocolos en la capa de aplicación para comparar perfiles desarrollados por proveedores de actividad de protocolo benigna con eventos observados para identificar desviaciones. Esto permite que un firewall permita o niegue el acceso según cómo se ejecuta una aplicación en la red. Por ejemplo, un firewall de aplicaciones puede determinar si un mensaje de correo electrónico contiene un tipo de archivo adjunto que la organización no permite (como un archivo ejecutable) o si se utiliza mensajería instantánea (IM) a través del puerto 80 (normalmente utilizado para HTTP). . Otra característica es que puede bloquear conexiones sobre las cuales se están realizando acciones específicas (por ejemplo, se podría impedir que los usuarios utilicen el comando "put" de FTP, que permite a los usuarios escribir archivos en el servidor FTP). Esta característica también se puede utilizar para permitir o denegar páginas web que contienen tipos particulares de contenido activo, como Java o ActiveX, o que tienen certificados SSL firmados por una autoridad certificadora (CA) particular, como una CA comprometida o revocada.

Los firewalls de aplicaciones pueden permitir la identificación de secuencias inesperadas de comandos, como emitir el mismo comando repetidamente o emitir un comando que no fue precedido por otro comando del que depende. Estos comandos sospechosos a menudo se originan en ataques de desbordamiento de búfer, ataques DoS, malware y otras formas de ataque llevados a cabo dentro de protocolos de aplicación como HTTP.
Otra característica común es la validación de entradas para comandos individuales, como las longitudes mínima y máxima de los argumentos. Por ejemplo, un argumento de nombre de usuario con una longitud de 1000 caracteres es sospechoso, más aún si contiene datos binarios. Los firewalls de aplicaciones están disponibles para muchos protocolos comunes, incluidos HTTP, bases de datos (como SQL), correo electrónico (SMTP, protocolo de oficina postal [POP] y protocolo de acceso a mensajes de Internet [IMAP])3, voz sobre IP (VoIP) y marcado extensible. Idioma (XML).4

Otra característica que se encuentra en algunos firewalls de aplicaciones implica hacer cumplir las máquinas de estado de las aplicaciones, que son esencialmente controles del cumplimiento del tráfico con el estándar del protocolo en cuestión.
Esta verificación de cumplimiento, a veces denominada “cumplimiento RFC” porque la mayoría de los protocolos se definen en RFC emitidos por el Grupo de Trabajo de Ingeniería de Internet (IETF), puede ser una bendición a medias. Muchos productos implementan protocolos de manera que coinciden casi, pero no completamente, con la especificación, por lo que generalmente es necesario permitir que dichas implementaciones se comuniquen a través del firewall. La verificación de cumplimiento solo es útil cuando detecta y bloquea comunicaciones que pueden ser perjudiciales para los sistemas protegidos.

Los firewalls con capacidades de inspección y análisis de protocolos de estado no son sistemas completos de detección y prevención de intrusiones (IDPS), que generalmente ofrecen capacidades de detección y prevención de ataques mucho más amplias. Por ejemplo, los IDPS también utilizan análisis basados en firmas y/o anomalías para detectar problemas adicionales dentro del tráfico de la red.5

---

3 Para obtener información adicional sobre la seguridad del correo electrónico, consulte la publicación especial (SP) 800-45 versión 2 del NIST, Directrices sobre seguridad del correo electrónico (http://csrc.nist.gov/publications/PubsSPs.html).

4 Para obtener información adicional sobre XML y firewalls XML, consulte NIST SP 800-95, Guía para servicios web seguros. (http://csrc.nist.gov/publications/PubsSPs.html).

5 Para obtener información adicional sobre IDPS, consulte NIST SP 800-94, Guía de sistemas de prevención y detección de intrusiones (IDPS) (http://csrc.nist.gov/publications/PubsSPs.html).

2.1.4 Puertas de enlace de proxy de aplicaciones

Una puerta de enlace de proxy de aplicación es una característica de los firewalls avanzados que combina el control de acceso de la capa inferior con la funcionalidad de la capa superior. Estos firewalls contienen un agente proxy que actúa como intermediario entre dos hosts que desean comunicarse entre sí y nunca permite una conexión directa entre ellos.
Cada intento de conexión exitoso en realidad resulta en la creación de dos conexiones separadas: una entre el cliente y el servidor proxy, y otra entre el servidor proxy y el destino verdadero.
El proxy debe ser transparente para los dos hosts: desde sus perspectivas existe una conexión directa. Debido a que los hosts externos solo se comunican con el agente proxy, las direcciones IP internas no son visibles para el mundo exterior. El agente proxy interactúa directamente con el conjunto de reglas del firewall para determinar si se debe permitir que una instancia determinada de tráfico de red transite el firewall.

Además del conjunto de reglas, algunos agentes proxy tienen la capacidad de requerir autenticación de cada usuario individual de la red. Esta autenticación puede adoptar muchas formas, incluida la identificación de usuario y la contraseña, el token de hardware o software, la dirección de origen y los datos biométricos.

Al igual que los firewalls de aplicaciones, la puerta de enlace proxy opera en la capa de aplicación y puede inspeccionar el contenido real del tráfico. Estas puertas de enlace también realizan el protocolo de enlace TCP con el sistema de origen y pueden proteger contra explotaciones en cada paso de una comunicación. Además, las puertas de enlace pueden tomar decisiones para permitir o denegar el tráfico basándose en la información contenida en los encabezados o cargas útiles del protocolo de la aplicación.
Una vez que la puerta de enlace determina que se deben permitir los datos, se reenvía al host de destino.

Las puertas de enlace de proxy de aplicaciones son bastante diferentes a los firewalls de aplicaciones. En primer lugar, una puerta de enlace de proxy de aplicación puede ofrecer un mayor nivel de seguridad para algunas aplicaciones porque evita las conexiones directas entre dos hosts e inspecciona el contenido del tráfico para identificar violaciones de políticas. Otra ventaja potencial es que algunas puertas de enlace de proxy de aplicaciones tienen la capacidad de descifrar paquetes (por ejemplo, cargas útiles protegidas por SSL), examinarlos y volver a cifrarlos antes de enviarlos al host de destino. Los datos que la puerta de enlace no puede descifrar se pasan directamente a la aplicación. Al elegir el tipo de firewall a implementar, es importante decidir si el firewall realmente necesita actuar como un proxy de aplicación para que pueda coincidir con las políticas específicas que necesita la organización.

Los cortafuegos con puertas de enlace de proxy de aplicaciones también pueden tener varias desventajas en comparación con el filtrado de paquetes y la inspección de estado. En primer lugar, debido al “conocimiento total de los paquetes” de las puertas de enlace de proxy de aplicaciones, el firewall dedica mucho más tiempo a leer e interpretar cada paquete. Debido a esto, algunas de estas puertas de enlace no son adecuadas para aplicaciones de gran ancho de banda o en tiempo real, pero hay disponibles puertas de enlace de proxy de aplicaciones clasificadas para un gran ancho de banda. Para reducir la carga en el firewall, se puede utilizar un servidor proxy dedicado (que se analiza en la Sección 2.1.5) para proteger servicios menos urgentes, como el correo electrónico y la mayor parte del tráfico web. Otra desventaja es que las puertas de enlace de proxy de aplicaciones tienden a estar limitadas en términos de soporte para nuevas aplicaciones y protocolos de red: se requiere un agente proxy individual y específico de la aplicación para cada tipo de tráfico de red que necesita atravesar un firewall. Muchos proveedores de firewalls de puerta de enlace de proxy de aplicaciones proporcionan agentes proxy genéricos para admitir aplicaciones o protocolos de red no definidos.
Esos agentes genéricos tienden a anular muchas de las fortalezas de la arquitectura de puerta de enlace de proxy de aplicación porque simplemente permiten que el tráfico pase a través del firewall.

2.1.5 Servidores proxy dedicados

Los servidores proxy dedicados se diferencian de las puertas de enlace de proxy de aplicaciones en que, si bien los servidores proxy dedicados retienen el control del tráfico, generalmente tienen capacidades de firewall mucho más limitadas. Se describen en esta sección debido a su estrecha relación con los firewalls de puerta de enlace de proxy de aplicaciones. Muchos servidores proxy dedicados son específicos de la aplicación y algunos realmente realizan análisis y validación de protocolos de aplicación comunes, como HTTP. Debido a que estos servidores tienen capacidades de firewall limitadas,

Por ejemplo, simplemente bloquear el tráfico en función de su origen o destino, normalmente se implementan detrás de plataformas de firewall tradicionales. Normalmente, un firewall principal podría aceptar tráfico entrante, determinar a qué aplicación se dirige y transferir el tráfico al servidor proxy apropiado (por ejemplo, proxy de correo electrónico). Este servidor realizaría operaciones de filtrado o registro del tráfico y luego lo reenviaría a los sistemas internos. Un servidor proxy también podría aceptar tráfico saliente directamente desde sistemas internos, filtrar o registrar el tráfico y pasarlo al firewall para su entrega saliente. Un ejemplo de esto es un proxy HTTP implementado detrás del firewall; los usuarios necesitarían conectarse a este proxy en el camino para conectarse a servidores web externos.
Los servidores proxy dedicados generalmente se utilizan para disminuir la carga de trabajo del firewall y realizar filtrado y registro especializados que pueden ser difíciles de realizar en el propio firewall.

En los últimos años, el uso de servidores proxy entrantes ha disminuido drásticamente. Esto se debe a que un servidor proxy entrante debe imitar las capacidades del servidor real que está protegiendo, lo que resulta casi imposible cuando se protege un servidor con muchas funciones. El uso de un servidor proxy con menos capacidades que el servidor que está protegiendo inutiliza las capacidades no coincidentes. Además, las características esenciales que deberían tener los servidores proxy entrantes (registro, control de acceso, etc.) suelen estar integradas en los servidores reales.
La mayoría de los servidores proxy que se utilizan actualmente son servidores proxy salientes , siendo los más comunes los servidores proxy HTTP.

La Figura 2-2 muestra un diagrama de muestra de una red que emplea un servidor proxy HTTP dedicado que se ha colocado detrás de otro sistema de firewall. El proxy HTTP manejaría conexiones salientes a servidores web externos y posiblemente filtraría contenido activo. Las solicitudes de los usuarios primero van al proxy, y luego el proxy envía la solicitud (posiblemente modificada) al servidor web externo. La respuesta de ese servidor web regresa al proxy, que la transmite al usuario.
Muchas organizaciones habilitan el almacenamiento en caché de páginas web utilizadas con frecuencia en el proxy para reducir el tráfico de red y mejorar los tiempos de respuesta.

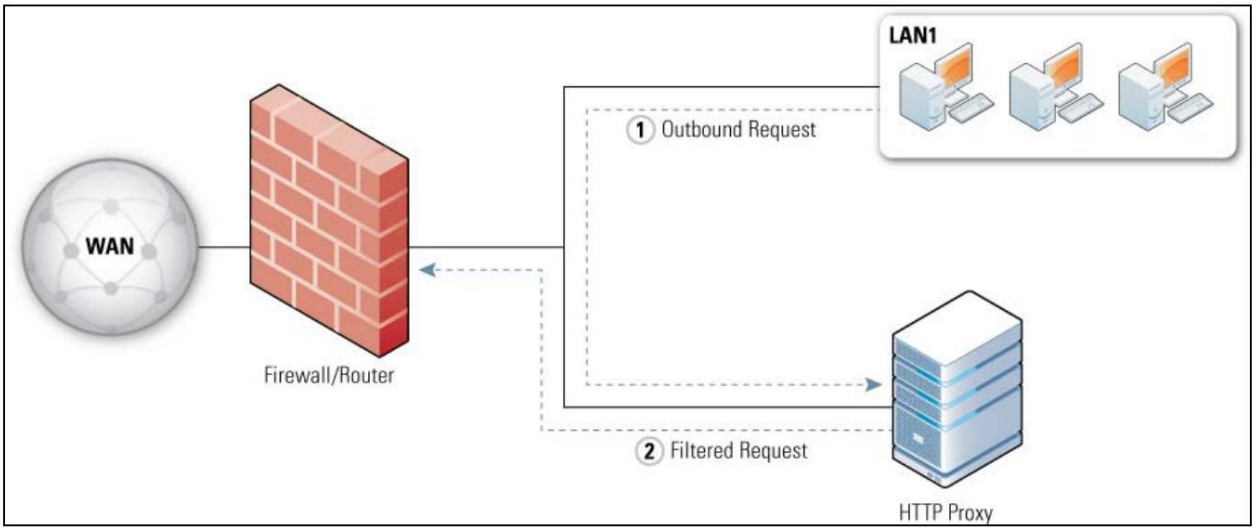

Figura 2-2. Configuración del proxy de aplicación

2.1.6 Redes privadas virtuales

A veces se requiere que los dispositivos de firewall en el borde de una red hagan más que bloquear el tráfico no deseado. Un requisito común para estos firewalls es cifrar y descifrar flujos de tráfico de red específicos entre la red protegida y las redes externas. Esto casi siempre involucra redes privadas virtuales (VPN), que utilizan protocolos adicionales para cifrar el tráfico y proporcionar autenticación de usuario y verificación de integridad. Las VPN se utilizan con mayor frecuencia para proporcionar comunicaciones de red seguras a través de redes que no son de confianza. Por ejemplo, la tecnología VPN se usa ampliamente para ampliar la red protegida de un sitio múltiple.

organización a través de Internet y, a veces, para proporcionar acceso seguro a usuarios remotos a las redes internas de la organización a través de Internet. Dos opciones comunes para VPN seguras son IPsec6 y Secure Sockets Layer (SSL)/Transport Layer Security (TLS).7

Las dos arquitecturas VPN más comunes son puerta de enlace a puerta de enlace y host a puerta de enlace.8 Las arquitecturas de puerta de enlace a puerta de enlace conectan múltiples sitios fijos a través de líneas públicas mediante el uso de puertas de enlace VPN: por ejemplo, para conectar sucursales con la sede de una organización. Una puerta de enlace VPN suele ser parte de otro dispositivo de red, como un firewall o un enrutador. Cuando se establece una conexión VPN entre las dos puertas de enlace, los usuarios en las sucursales no son conscientes de la conexión y no requieren ninguna configuración especial en sus computadoras. El segundo tipo de arquitectura, de host a puerta de enlace, proporciona una conexión segura a la red para usuarios individuales, generalmente llamados usuarios remotos, que se encuentran fuera de la organización (en casa, en un hotel, etc.). Aquí, un cliente en la máquina del usuario negocia la conexión segura con la puerta de enlace VPN de la organización.9 Para las VPN de puerta de enlace a puerta de enlace y de host a puerta de enlace, la funcionalidad de VPN suele ser parte del propio firewall. Colocarlo detrás del firewall requeriría que el tráfico VPN pasara a través del firewall mientras está cifrado, lo que evitaría que el firewall inspeccione el tráfico.

Todas las VPN de acceso remoto (host a puerta de enlace) permiten al administrador del firewall decidir qué usuarios tienen acceso a qué recursos de la red. Este control de acceso normalmente está disponible por usuario y por grupo; es decir, la política de VPN puede especificar qué usuarios y grupos están autorizados a acceder a qué recursos, en caso de que una organización necesite ese nivel de granularidad. Las VPN generalmente dependen de protocolos de autenticación como el Servicio de autenticación remota telefónica de usuario (RADIUS).10 RADIUS utiliza varios tipos diferentes de credenciales de autenticación, siendo los ejemplos más comunes nombre de usuario y contraseña, firmas digitales y tokens de hardware. Otro protocolo de autenticación que suelen utilizar las VPN es el Protocolo ligero de acceso a directorios (LDAP); Es particularmente útil para tomar decisiones de acceso para usuarios y grupos individuales.

Para ejecutar la funcionalidad VPN en un firewall se requieren recursos adicionales que dependen de la cantidad de tráfico que fluye a través de la VPN y el tipo de cifrado que se utiliza. Para algunos entornos, el tráfico adicional asociado con las VPN puede requerir recursos y planificación de capacidad adicionales. También es necesaria una planificación para determinar el tipo de VPN (de puerta de enlace a puerta de enlace y/o de host a puerta de enlace) que debe incluirse en el firewall. Muchos firewalls incluyen aceleración de hardware para el cifrado a fin de minimizar el impacto de los servicios VPN.

2.1.7 Control de acceso a la red

Otro requisito común para los firewalls en el borde de una red es realizar comprobaciones de clientes para conexiones entrantes de usuarios remotos y permitir o no el acceso en función de esas comprobaciones. Esta verificación, comúnmente llamada control de acceso a la red (NAC) o protección de acceso a la red (NAP), permite el acceso según las credenciales del usuario y los resultados de realizar "verificaciones de estado" en la computadora del usuario. Los controles de estado generalmente consisten en verificar que uno o más de los siguientes cumplan con la política de la organización:

---

6 Para obtener información adicional sobre IPsec, consulte NIST SP 800-77, Guía de VPN IPsec (http://csrc.nist.gov/publications/PubsSPs.html).

7 Para obtener información adicional sobre SSL y TLS, consulte NIST SP 800-52, Directrices para la selección y uso de implementaciones de seguridad de la capa de transporte (TLS) y NIST SP 800-113, Guía de VPN SSL (http://csrc.nist.gov /publicaciones/PubsSPs.html).

8 Para obtener información adicional sobre arquitecturas VPN, consulte NIST SP 800-77, Guía de VPN IPsec y NIST SP 800-113, Guía de VPN SSL (http://csrc.nist.gov/publications/PubsSPs.html).

9 Las arquitecturas de host a puerta de enlace generalmente requieren cierta participación del usuario, como iniciar la conexión VPN o proporcionar credenciales a la VPN para autenticación.

10 RADIUS se define en RFC 2865 (http://www.rfc-editor.org/rfc/rfc2865.txt).

Últimas actualizaciones de software antimalware y firewall personal

Ajustes de configuración para antimalware y software de firewall personal

Tiempo transcurrido desde el análisis de malware anterior

Nivel de parche del sistema operativo y aplicaciones seleccionadas

Configuración de seguridad del sistema operativo y aplicaciones seleccionadas.

Estas comprobaciones de estado requieren software en el sistema del usuario que esté controlado por el firewall. Si el usuario tiene credenciales aceptables pero el dispositivo no pasa la verificación de estado, el usuario y el dispositivo solo pueden obtener acceso limitado a la red interna con fines de reparación.

2.1.8 Gestión unificada de amenazas (UTM)

Muchos firewalls combinan múltiples funciones en un solo sistema, con la idea de que es más fácil establecer y mantener políticas en un solo sistema que en muchos sistemas implementados en la misma ubicación de una red. Un sistema típico de gestión unificada de amenazas (UTM) tiene un firewall, detección y erradicación de malware, detección y bloqueo de sondas de red sospechosas, etc. Existen ventajas y desventajas al fusionar múltiples funciones que no están completamente relacionadas en un solo sistema. Por ejemplo, implementar un UTM reduce la complejidad al hacer que un solo sistema sea responsable de múltiples objetivos de seguridad, pero también requiere que el UTM tenga todas las características deseadas para cumplir con cada uno de los objetivos. Otra desventaja es el rendimiento: un único sistema que maneja múltiples tareas debe tener suficientes recursos, como velocidad de CPU y memoria, para manejar cada tarea que se le asigne. Algunas organizaciones encontrarán que el equilibrio favorece un UTM, mientras que otras utilizarán varios firewalls en la misma ubicación de su red.

2.1.9 Cortafuegos de aplicaciones web

El protocolo HTTP utilizado en los servidores web ha sido explotado por atacantes de muchas maneras, como para colocar software malicioso en la computadora de alguien que navega por la web o para engañar a una persona para que revele información privada que de otro modo no tendría. Muchos de estos exploits pueden ser detectados por firewalls de aplicaciones especializados llamados firewalls de aplicaciones web que residen frente al servidor web.

Los firewalls de aplicaciones web son una tecnología relativamente nueva, en comparación con otras tecnologías de firewall, y el tipo de amenazas que mitigan todavía cambian con frecuencia. Debido a que se colocan delante de los servidores web para evitar ataques al servidor, a menudo se los considera muy diferentes a los firewalls tradicionales.

2.1.10 Firewalls para Infraestructuras Virtuales

Muchas soluciones de virtualización permiten que se ejecute más de un sistema operativo en una sola computadora simultáneamente, cada uno de los cuales aparece como si fuera una computadora real. Esto se ha vuelto popular recientemente porque permite a las organizaciones hacer un uso más eficiente del hardware informático. La mayoría de estos tipos de sistemas de virtualización incluyen redes virtualizadas, que permiten que múltiples sistemas operativos se comuniquen como si estuvieran en una Ethernet estándar, aunque no exista hardware de red real.

La actividad de red que pasa directamente entre sistemas operativos virtualizados dentro de un host no puede ser monitoreada por un firewall externo. Sin embargo, algunos sistemas de virtualización ofrecen firewalls integrados o permiten agregar firewalls de software de terceros como complementos. El uso de firewalls para monitorear redes virtualizadas es un área relativamente nueva de la tecnología de firewalls y es probable que cambie significativamente a medida que el uso de la virtualización siga aumentando.

2.2 Firewalls para hosts individuales y redes domésticas

Aunque los firewalls en el perímetro de una red brindan cierta medida de protección para los hosts internos, en muchos casos se requiere protección de red adicional. Los firewalls de red no pueden reconocer todas las instancias y formas de ataque, lo que permite que algunos ataques penetren y alcancen los hosts internos, y es posible que los ataques enviados de un host interno a otro ni siquiera pasen a través de un firewall de red. Debido a estos y otros factores, los diseñadores de redes suelen incluir la funcionalidad de firewall en lugares distintos al perímetro de la red para proporcionar una capa adicional de seguridad. Esta sección describe firewalls diseñados específicamente para su implementación en hosts individuales y redes domésticas.

2.2.1 Cortafuegos basados en host y cortafuegos personales

Los firewalls basados en host para servidores y los firewalls personales para computadoras personales (PC) de escritorio y portátiles brindan una capa adicional de seguridad contra ataques basados en la red. Estos firewalls están basados en software y residen en los hosts que protegen; cada uno monitorea y controla el tráfico de red entrante y saliente para un único host. Pueden proporcionar una protección más granular que los firewalls de red para satisfacer las necesidades de hosts específicos.

Los firewalls basados en host están disponibles como parte de sistemas operativos de servidores como Linux, Windows, Solaris, BSD y Mac OS X Server, y también se pueden instalar como complementos de terceros. La configuración de un firewall basado en host para permitir solo el tráfico necesario al servidor brinda protección contra actividades maliciosas de todos los hosts, incluidos aquellos en la misma subred o en otras subredes internas no separadas por un firewall de red. Limitar el tráfico saliente de un servidor también puede ser útil para evitar que cierto malware que infecta un host se propague a otros hosts.11 Los cortafuegos basados en host generalmente realizan registros y, a menudo, pueden configurarse para realizar controles de acceso basados en direcciones y aplicaciones. Muchos firewalls basados en host también pueden actuar como sistemas de prevención de intrusiones (IPS) que, después de detectar un ataque en curso, toman medidas para frustrar al atacante y evitar daños al host objetivo.

Un firewall personal es un software que se ejecuta en una computadora de escritorio o portátil con un sistema operativo centrado en el usuario, como Microsoft Windows Vista o Macintosh OS X. Un firewall personal es similar a un firewall basado en host, pero debido a que la computadora que se protege está destinada a para los usuarios finales, la interfaz suele ser diferente (y presumiblemente más fácil de entender para el usuario típico). Un firewall personal proporciona una capa adicional de seguridad para las PC ubicadas dentro y fuera del perímetro de firewall (por ejemplo, usuarios de computadoras portátiles móviles), porque puede restringir las comunicaciones entrantes y, a menudo, también puede limitar las comunicaciones salientes. Esto no sólo permite que los firewalls personales protejan las PC de ataques entrantes, sino que también limita la propagación de malware desde las PC infectadas y el uso de software no autorizado, como utilidades para compartir archivos entre pares. Los cortafuegos personales suelen incluir programas antimalware, software de detección de intrusos y otras utilidades de seguridad.12

Algunos firewalls personales permiten la creación de diferentes perfiles según la ubicación, como un perfil para usar dentro de la red de la organización y un perfil diferente para usar en una ubicación remota. Esto es particularmente importante cuando una computadora se usa en una red externa que no es de confianza, porque tener un perfil de firewall separado para usar en dichas redes puede restringir la actividad de la red más estrictamente y brindar una protección más sólida que tener un perfil único para todas las redes.

---

11 Si un atacante compromete un host y obtiene privilegios de nivel de administrador, puede desactivar o eludir el firewall basado en el host.

12 Para obtener información adicional sobre firewalls personales, consulte NIST SP 800-114, Guía del usuario para proteger dispositivos externos para teletrabajo y acceso remoto (http://csrc.nist.gov/publications/PubsSPs.html).

Además del filtrado de estado tradicional, muchos firewalls personales se pueden configurar para permitir comunicaciones basadas en listas de aplicaciones autorizadas (como navegadores web que se comunican con servidores web y clientes de correo electrónico que envían y reciben mensajes de correo electrónico) y para denegar comunicaciones que involucren a otras aplicaciones. Estos se conocen como firewalls basados en aplicaciones. El control de acceso se basa en las aplicaciones o servicios lanzados, y no en los puertos o servicios.

La gestión de firewalls personales debe centralizarse, en la medida de lo posible, para ayudar a crear, distribuir y hacer cumplir políticas de manera eficiente para todos los usuarios y grupos. Hacer esto garantizará que la política de seguridad de la organización esté vigente siempre que un usuario acceda a los recursos informáticos de la organización. Pero independientemente de si un firewall personal es administrado por administradores centrales o usuarios individuales, cualquier mensaje de advertencia que genere el firewall debe mostrarse al usuario de la PC para ayudarlo a rectificar los problemas que encuentre.

2.2.2 Dispositivos de firewall personales

Además de utilizar cortafuegos personales en sus PC, algunos teletrabajadores también utilizan un dispositivo pequeño y económico llamado dispositivo cortafuegos o enrutador cortafuegos para proteger las computadoras de sus redes domésticas. Un dispositivo de firewall personal realiza funciones similares a un firewall personal, incluidas algunas de las funciones más avanzadas enumeradas anteriormente en esta sección, como VPN. Incluso si cada computadora en una red doméstica utiliza un firewall personal, un dispositivo de firewall sigue siendo una valiosa capa adicional de seguridad. En caso de que un firewall personal en una computadora funcione mal, esté deshabilitado o mal configurado, el dispositivo de firewall aún puede proteger la computadora de comunicaciones de red no autorizadas desde computadoras externas. Los dispositivos de firewall personales son esencialmente como firewalls de pequeñas empresas que se implementan fuera de la organización, por lo que la capacidad de realizar gestión y administración central es tan importante para los dispositivos de firewall personales como lo es para los firewalls empresariales.13

Algunos dispositivos de firewall personales pueden configurarse parcialmente mediante Universal Plug and Play (UPnP), que permite que las aplicaciones en las PC detrás del firewall le soliciten automáticamente que abra ciertos puertos para que las aplicaciones puedan tener comunicaciones bidireccionales con un sistema externo. La mayoría de los firewalls personales que admiten la reconfiguración dinámica a través de UPnP tienen esta función desactivada de forma predeterminada porque es un riesgo de seguridad significativo permitir que aplicaciones no confiables alteren la política de seguridad de un firewall.

2.3 Limitaciones de la inspección del firewall

Los cortafuegos sólo pueden funcionar eficazmente en el tráfico que pueden inspeccionar. Independientemente de la tecnología de firewall elegida, un firewall que no pueda comprender el tráfico que fluye a través de él no lo manejará adecuadamente; por ejemplo, permitirá el tráfico que debería bloquearse. Muchos protocolos de red utilizan criptografía para ocultar el contenido del tráfico. La sección 2.1.6 cubrió IPsec y TLS; otros protocolos de cifrado incluyen Secure Shell (SSH) y Secure Real-time Transport Protocol (SRTP). Los cortafuegos tampoco pueden leer datos de aplicaciones cifrados, como correo electrónico cifrado mediante los protocolos S/MIME u OpenPGP, o archivos cifrados manualmente. Otra limitación que enfrentan algunos firewalls es comprender el tráfico tunelizado, incluso si no está cifrado. Por ejemplo, el tráfico IPv6 se puede canalizar en IPv4 de muchas maneras diferentes. Es posible que el contenido aún esté sin cifrar, pero si el firewall no comprende el mecanismo de túnel particular utilizado, el tráfico no se puede interpretar.

En todos estos casos, las reglas del firewall determinarán qué hacer con el tráfico que no comprende (o, en el caso del tráfico cifrado, no puede comprender). Una organización debe tener políticas sobre cómo manejar el tráfico en tales casos, como permitir o bloquear el tráfico cifrado que no está autorizado a cifrarse.

---

[13] Información adicional sobre dispositivos de firewall personales está disponible en NIST SP 800-114.

2.4 Resumen de recomendaciones

Los siguientes elementos resumen las principales recomendaciones de esta sección:

- El uso de NAT debe considerarse una forma de enrutamiento, no un tipo de firewall.
- Las organizaciones solo deben permitir el tráfico saliente que utilice las direcciones IP de origen que utiliza la organización.
- La verificación de cumplimiento solo es útil en un firewall cuando puede bloquear comunicaciones que pueden ser dañinas para los sistemas protegidos.
- Al elegir el tipo de firewall a implementar, es importante decidir si el firewall debe actuar como un proxy de aplicación.
- La gestión de firewalls personales debe centralizarse para ayudar a crear, distribuir y hacer cumplir políticas de manera eficiente para todos los usuarios y grupos.

3. Cortafuegos y arquitecturas de red

Los firewalls se utilizan para separar redes con diferentes requisitos de seguridad, como Internet y una red interna que alberga servidores con datos confidenciales. Las organizaciones deben utilizar firewalls siempre que sus redes y sistemas internos interactúen con redes y sistemas externos, y donde los requisitos de seguridad varíen entre sus redes internas. Esta sección tiene como objetivo ayudar a las organizaciones a determinar dónde se deben colocar los firewalls y dónde se deben ubicar otras redes y sistemas en relación con los firewalls.

Dado que una de las funciones principales de un cortafuegos es evitar que el tráfico no deseado entre en una red (y, en algunos casos, salga de ella), los cortafuegos deben colocarse en el borde de los límites lógicos de la red.14 Esto normalmente significa que los cortafuegos se colocan en ya sea como un nodo donde la red se divide en múltiples rutas o en línea a lo largo de una única ruta. En las redes enrutadas, el firewall generalmente reside solo en la red en la ubicación inmediatamente antes de que el tráfico ingrese al enrutador (el punto de ingreso) y, a veces, es co-residente con el enrutador. Es raro colocar el firewall para un nodo de rutas múltiples después del enrutador porque el dispositivo de firewall necesitaría vigilar cada una de las múltiples rutas de salida que normalmente existen en tales situaciones. La gran mayoría de los dispositivos de firewall de hardware contienen capacidades de enrutador y, en las redes conmutadas, un firewall suele ser parte del propio conmutador para permitirle proteger tantos segmentos conmutados como sea posible.

Los proveedores de firewalls a menudo varían en su terminología para el flujo lógico del tráfico del firewall. Un firewall toma el tráfico que no ha sido verificado, lo compara con la política del firewall y luego actúa en consecuencia (por ejemplo, pasa el tráfico, lo bloquea, lo pasa con alguna modificación). Debido a que todo el tráfico en una red tiene una dirección, las políticas se basan en la dirección en la que se mueve el tráfico. A los efectos de este documento, el tráfico que aún no se ha verificado proviene del "lado desprotegido" del firewall y se dirige hacia el "lado protegido". Algunos firewalls verifican el tráfico en ambas direcciones, por ejemplo, si están configurados para evitar que un tráfico específico de la red de área local (LAN) de una organización escape a Internet.15 En estos casos, el lado protegido del firewall es el que mira hacia la red exterior.

La Sección 2 enumera muchos tipos diferentes de tecnologías de firewall. Los cortafuegos de red son casi siempre dispositivos de hardware con múltiples interfaces de red; los firewalls personales y basados en host implican software que reside en una sola computadora y protege solo esa computadora; y los dispositivos de firewall personales están diseñados para proteger una sola PC o una red de oficina pequeña/oficina en casa. Esta sección se centra en los firewalls de red porque los otros tipos generalmente no están relacionados con problemas de topología de red.

3.1 Diseños de red con firewalls

La Figura 3-1 muestra un diseño de red típico con un dispositivo firewall de hardware que actúa como enrutador. El lado desprotegido del firewall se conecta a una única ruta denominada "WAN" y el lado protegido se conecta a tres rutas denominadas "LAN1", "LAN2" y "LAN3". El firewall actúa como enrutador para el tráfico entre la ruta de la red de área amplia (WAN) y las rutas LAN. En la figura, una de las rutas LAN también tiene un enrutador; Algunas organizaciones prefieren utilizar múltiples capas de enrutadores debido a políticas de enrutamiento heredadas dentro de la red.

---

14 Además de los límites de red tradicionales, esto también incluye límites relacionados con el uso de máquinas virtuales. Por ejemplo, puede ser necesario restringir la actividad de la red entre dos máquinas virtuales con políticas de seguridad diferentes.

15 Algunos firewalls están configurados para permitir el tráfico en una sola dirección; por ejemplo, un firewall configurado como protección para permitir flujos de tráfico limitados desde un sistema de mayor impacto a un sistema de menor impacto, pero ningún tráfico iniciado por el sistema de menor impacto. para llegar al sistema de mayor impacto.

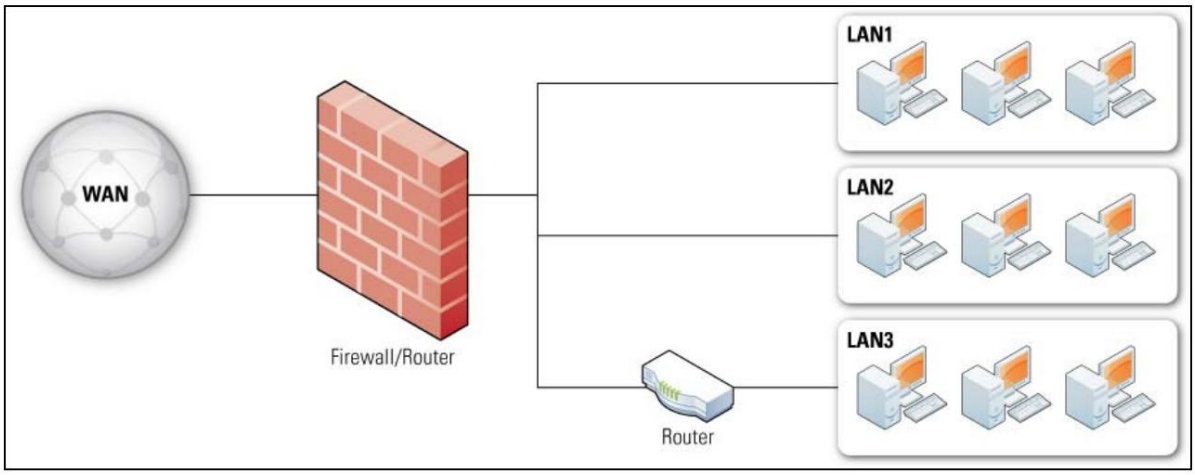

Figura 3-1. Red enrutada simple con dispositivo firewall

Muchos dispositivos de firewall de hardware tienen una característica llamada DMZ, un acrónimo relacionado con las zonas desmilitarizadas que a veces se establecen entre países en guerra. Si bien no existe una definición técnica única para las DMZ de firewall, generalmente son interfaces en un firewall de enrutamiento que son similares a las interfaces que se encuentran en el lado protegido del firewall. La principal diferencia es que el tráfico que se mueve entre la DMZ y otras interfaces en el lado protegido del firewall aún pasa a través del firewall y se le pueden aplicar políticas de protección de firewall. Las DMZ a veces son útiles para organizaciones que tienen hosts que necesitan que todo el tráfico destinado al host evite algunas de las políticas del firewall (por ejemplo, porque los hosts DMZ están suficientemente reforzados), pero el tráfico que viene de los hosts a otros sistemas en la organización La red necesita pasar a través del firewall. Es común colocar servidores públicos, como servidores web y de correo electrónico, en la DMZ. Un ejemplo de esto se muestra en la Figura 3-2, un diseño de red simple de un firewall con una DMZ. El tráfico de Internet ingresa al firewall y se enruta a sistemas en el lado protegido del firewall o a sistemas en la DMZ. El tráfico entre los sistemas en la DMZ y los sistemas en la red protegida pasa a través del firewall y se le pueden aplicar políticas de firewall.

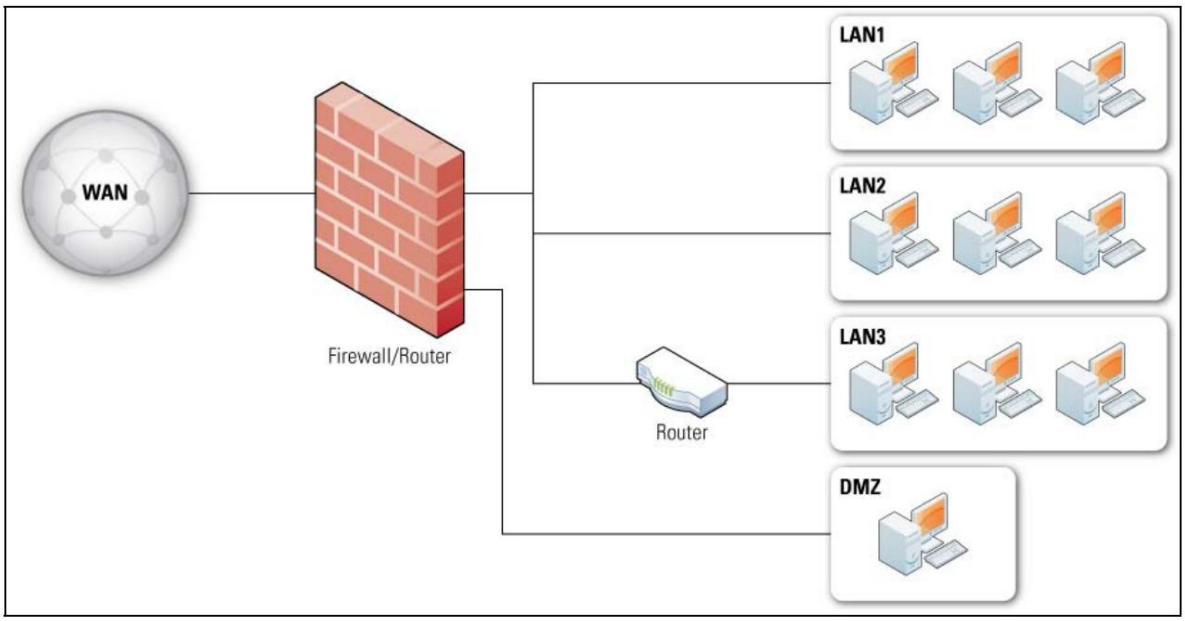

Figura 3-2. Cortafuegos con DMZ

La mayoría de las arquitecturas de red son jerárquicas, lo que significa que una única ruta desde una red externa se divide en múltiples rutas en la red interna y, en general, es más eficiente colocar un firewall en el nodo donde se dividen las rutas. Esto tiene la ventaja de colocar el firewall donde no hay dudas sobre qué hay "afuera" y qué hay "adentro". Sin embargo, puede haber motivos para tener firewalls adicionales en el interior de la red, como por ejemplo para proteger un conjunto de computadoras de otro. Si la arquitectura de una red no es jerárquica, se deben utilizar las mismas políticas de firewall en todos los ingresos a la red. En muchas organizaciones, se supone que solo debe haber un ingreso a la red, pero otros ingresos se configuran ad hoc, a menudo de maneras que no están permitidas por la política general. En estas situaciones, si no se coloca un firewall configurado correctamente en cada punto de entrada, el tráfico malicioso que normalmente sería bloqueado por el ingreso principal puede ingresar a la red por otros medios.

Los diagramas de las Figuras 3-1 y 3-2 muestran cada uno un único firewall; sin embargo, muchas implementaciones utilizan varios firewalls. Algunos proveedores venden firewalls de alta disponibilidad (HA) , que permiten que un firewall reemplace a otro si el primero falla o se desconecta para mantenimiento. Los firewalls HA se implementan en pares en el mismo lugar de la topología de la red para que ambos tengan las mismas conexiones externas e internas. Si bien los firewalls HA pueden aumentar la confiabilidad, también pueden introducir algunos problemas, como la necesidad de combinar registros entre los firewalls emparejados y una posible confusión por parte de los administradores al configurar los firewalls (por ejemplo, saber qué firewall está enviando sus cambios de política al otro firewall).). La funcionalidad HA se puede proporcionar a través de una variedad de técnicas específicas del proveedor.

3.2 Firewalls que actúan como traductores de direcciones de red

La mayoría de los firewalls pueden realizar NAT, que a veces se denomina traducción de direcciones de puertos (PAT) o traducción de direcciones de red y puertos (NAPT). A pesar de la idea errónea popular, NAT no forma parte de la funcionalidad de seguridad de un firewall. El beneficio de seguridad de NAT (evitar que un host fuera del firewall inicie contacto con un host detrás de NAT) puede lograrse fácilmente mediante un firewall con estado con menos interrupción de los protocolos que no funcionan tan bien detrás de NAT. Sin embargo, activar la función NAT de un firewall suele ser más fácil que configurar correctamente la política del firewall para que tenga las mismas protecciones, por lo que mucha gente piensa que las NAT son principalmente una característica de seguridad.

Normalmente, una NAT actúa como un enrutador que tiene una red con direcciones privadas en el interior y una única dirección pública en el exterior. La forma en que una NAT realiza este mapeo de muchos a uno varía entre implementaciones, pero casi siempre implica lo siguiente:

- Los hosts en la red interna que inician conexiones a la red externa hacen que NAT asigne el puerto de origen de la conexión a un puerto de origen diferente controlado por NAT. La NAT utiliza este número de puerto de origen para asignar conexiones desde el exterior al host interno.
- Los hosts en el exterior de la red no pueden iniciar contacto con los hosts en la red interna. En algunos firewalls, la NAT se puede configurar para asignar un puerto de destino particular en la NAT a un host particular en el interior de la NAT; por ejemplo, todas las solicitudes HTTP que van a NAT podrían dirigirse a un único host en el lado protegido del firewall. Esta característica a veces se denomina poros.

Aunque las NAT no son en sí mismas características de seguridad de un firewall, interactúan con la política de seguridad del firewall. Por ejemplo, cualquier política que requiera que todos los servidores HTTP accesibles desde el exterior estén en la DMZ debe impedir que la NAT localice el puerto TCP 80. Otro ejemplo de dónde interactúan las NAT con la política de seguridad es la capacidad de identificar la fuente de tráfico en el firewall de un firewall. registros. Si se utiliza una NAT, debe informar la dirección privada en los registros en lugar de la dirección pública traducida; de lo contrario, los registros identificarán incorrectamente muchos hosts mediante una única dirección pública.

3.3 Arquitectura con múltiples capas de firewalls

No existe ninguna limitación sobre dónde se puede colocar un firewall en una red. Si bien los cortafuegos deben estar en el borde de un límite lógico de la red, creando un "interior" y un "exterior" a cada lado del cortafuegos, es posible que un administrador de red desee tener límites adicionales dentro de la red e implementar cortafuegos adicionales para establecer dichos límites. El uso de múltiples capas de firewalls es bastante común para brindar una defensa en profundidad. Un ejemplo de esto se mencionó en la Sección 2.2.1, donde un firewall basado en host crea un límite justo antes del host en el que está instalado y agrega otro conjunto de políticas de firewall a la arquitectura de la red. El uso de múltiples capas de firewalls de red es otra técnica común.

Una situación típica que requiere múltiples capas de firewalls de red es la presencia de usuarios internos con distintos niveles de confianza. Por ejemplo, una organización podría querer proteger sus bases de datos contables para que no accedan usuarios que no formen parte del departamento de contabilidad. Esto podría lograrse colocando un firewall en el borde de la red (para evitar el acceso general a la red desde Internet) y otro en el borde de la red interna que define los límites del departamento de contabilidad. El firewall interno bloquearía el acceso al servidor de la base de datos por parte de cualquier persona fuera de la red contable y al mismo tiempo permitiría un acceso limitado a otros recursos en la red contable. Otro uso típico de los cortafuegos dentro de una red con un cortafuegos en el borde implica a los visitantes que necesitan acceso a Internet. Muchas organizaciones implementan puntos de acceso inalámbrico 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.

Colocar un firewall dentro de una red que ya tiene uno en el borde requiere una buena planificación y coordinación de políticas para evitar fallos de seguridad involuntarios. Al diseñar políticas para un firewall interno, el administrador podría hacer suposiciones que resulten en elecciones de políticas deficientes; por ejemplo, si el administrador del firewall interno supone que el firewall externo ya está impidiendo que ciertos tipos de tráfico lleguen al firewall interno, y el firewall externo ya está impidiendo que ciertos tipos de tráfico lleguen al firewall interno. Si el administrador modifica posteriormente la política existente, los hosts detrás del firewall interno quedarán expuestos a amenazas adicionales. Un mejor enfoque es duplicar las políticas de firewall externos que también sean relevantes para los firewalls internos en cada firewall interno. Esto puede resultar difícil si estos firewalls no pueden coordinar sus políticas automáticamente, lo que es particularmente probable cuando los firewalls son de diferentes fabricantes.

Otro problema común con el uso de múltiples capas de firewalls de red es la mayor dificultad que presenta para rastrear los problemas del firewall. Si un firewall se interpone entre un usuario y un servidor, y el usuario no puede conectarse al servidor, es fácil verificar los registros de ese firewall para ver si se permite la conexión. Pero si hay varios firewalls involucrados, el problema se vuelve más difícil porque un administrador debe ubicar todos los firewalls en la cadena y verificar sus registros para encontrar dónde se origina el problema. La presencia de múltiples capas de puertas de enlace de proxy de aplicaciones es particularmente desalentadora, porque cada puerta de enlace puede cambiar un mensaje, lo que dificulta aún más la depuración.

3.4 Resumen de recomendaciones

Los siguientes elementos resumen las principales recomendaciones de esta sección:

- En general, un firewall debería encajar en el diseño de una red actual. Sin embargo, una organización puede cambiar su arquitectura de red al mismo tiempo que implementa un firewall como parte de una actualización de seguridad general.
- Las diferentes arquitecturas de red comunes conducen a opciones muy diferentes sobre dónde colocar un firewall, por lo que una organización debe evaluar qué arquitectura funciona mejor para sus objetivos de seguridad.

Si un firewall perimetral tiene una DMZ, considere qué servicios externos deben ejecutarse desde la DMZ y cuáles deben permanecer en la red interna.

No confíe en las NAT para obtener los beneficios de los firewalls.

En algunos entornos, colocar un firewall detrás de otro puede conducir a un objetivo de seguridad deseado, pero en general, estas múltiples capas de firewalls pueden resultar problemáticas.

4. Política de cortafuegos

Una política de firewall dicta cómo los firewalls deben manejar el tráfico de red para direcciones IP específicas y rangos de direcciones, protocolos, aplicaciones y tipos de contenido (por ejemplo, contenido activo) según las políticas de seguridad de la información de la organización. Antes de crear una política de firewall, se debe realizar algún tipo de análisis de riesgos para desarrollar una lista de los tipos de tráfico que necesita la organización y categorizar cómo deben protegerse, incluido qué tipos de tráfico pueden atravesar un firewall y en qué circunstancias.16 Este análisis de riesgos debe basarse en una evaluación de las amenazas; vulnerabilidades; contramedidas implementadas para mitigar las vulnerabilidades; y el impacto si los sistemas o los datos se ven comprometidos.
La política de firewall debe documentarse en el plan de seguridad del sistema y mantenerse y actualizarse con frecuencia a medida que surgen clases de nuevos ataques o vulnerabilidades, o a medida que cambian las necesidades de la organización con respecto a las aplicaciones de red. La política también debe incluir orientación específica sobre cómo abordar los cambios en el conjunto de reglas.

Generalmente, los firewalls deben bloquear todo el tráfico entrante y saliente que no haya sido permitido expresamente por la política del firewall (tráfico que la organización no necesita). Esta práctica, conocida como denegación por defecto, disminuye el riesgo de ataque y también puede reducir el volumen de tráfico transportado por las redes de la organización. Debido a la naturaleza dinámica de los hosts, redes, protocolos y aplicaciones, denegar de forma predeterminada es un enfoque más seguro que permitir todo el tráfico que no esté explícitamente prohibido.

Esta sección proporciona detalles sobre qué tipos de tráfico deben bloquearse. La sección 4.1 analiza las políticas para el filtrado de paquetes y la inspección de estado basada en direcciones IP y otras características de IP. La Sección 4.2 cubre las políticas relacionadas con el tráfico específico de la aplicación. La Sección 4.3 cubre el acceso basado en la identidad del usuario y la Sección 4.4 describe las políticas activadas por la actividad de la red.

4.1 Políticas basadas en direcciones IP y protocolos

Las políticas de firewall solo deben permitir el paso de los protocolos IP necesarios. Ejemplos de protocolos IP comúnmente utilizados, con sus números de protocolo IP,17 son ICMP (1), TCP (6) y UDP (17). Otros protocolos IP, como los componentes IPsec que encapsulan la carga útil de seguridad (ESP) (50) y el encabezado de autenticación (AH) (51) y los protocolos de enrutamiento, también pueden necesitar pasar a través de firewalls. Estos protocolos necesarios deben restringirse siempre que sea posible a los hosts y redes específicos dentro de la organización que necesiten utilizarlos. Al permitir sólo los protocolos necesarios, todos los protocolos IP innecesarios se deniegan de forma predeterminada.

Algunos protocolos IP rara vez se transmiten entre una red externa y la LAN de una organización y, por lo tanto, pueden simplemente bloquearse en ambas direcciones en el firewall. Por ejemplo, IGMP es un protocolo utilizado para controlar redes de multidifusión, pero la multidifusión rara vez se utiliza y, cuando se utiliza, a menudo no se utiliza en Internet. Por lo tanto, es factible bloquear todo el tráfico IGMP en ambas direcciones si no se utiliza la multidifusión.

4.1.1 Direcciones IP y otras características IP

Las políticas de firewall solo deben permitir el uso de direcciones IP de origen y destino adecuadas. Las recomendaciones específicas para direcciones IP incluyen:

- El tráfico con direcciones de origen o destino no válidas siempre debe bloquearse, independientemente de la ubicación del firewall. Ejemplos de direcciones IPv4 no válidas relativamente comunes son 127.0.0.0 a

16 El proceso para realizar una evaluación de riesgos y crear este tipo de lista no se detalla aquí. Para obtener información adicional, consulte NIST SP 800-30, Guía de gestión de riesgos para sistemas de tecnología de la información y SP 800-18 Revisión 1, Guía para el desarrollo de planes de seguridad para sistemas de información federales, en http://csrc.nist.gov/publications/ PubsSPs.html.

17 Las asignaciones de números de protocolo IP se definen en http://www.iana.org/assignments/protocol-numbers.

127.255.255.255 (también conocidas como direcciones de host local) y 0.0.0.0 (interpretadas por algunos sistemas operativos como un host local o una dirección de transmisión). Estos no tienen ningún uso legítimo en una red. Además, se debe bloquear el tráfico que utiliza direcciones de enlace local (169.254.0.0 a 169.254.255.255).

El tráfico con una dirección de origen no válida para el tráfico entrante o una dirección de destino para el tráfico saliente (una dirección “externa” no válida) debe bloquearse en el perímetro de la red. Este tráfico suele ser causado por malware, suplantación de identidad, ataques de denegación de servicio o equipos mal configurados. El tipo más común de direcciones externas no válidas es una dirección IPv4 dentro de los rangos de RFC 1918, Asignación de direcciones para Internet privadas, que están reservadas para redes privadas. Estos rangos son 10.0.0.0 a 10.255.255.255 (10.0.0.0/8 en notación de enrutamiento entre dominios sin clases [CIDR]), 172.16.0.0 a 172.31.255.255 (172.16.0.0/12) y 192.168.0.0 a 192.168. 255.255 (192.168.0.0/16).

El tráfico con una dirección de destino privada para el tráfico entrante o una dirección de origen para el tráfico saliente (una dirección "interna") debe bloquearse en el perímetro de la red. Los dispositivos perimetrales pueden realizar servicios de traducción de direcciones para permitir que los hosts internos con direcciones privadas se comuniquen a través del perímetro, pero las direcciones privadas no deben pasar a través del perímetro de la red.

Se debe bloquear el tráfico saliente con direcciones de origen no válidas (esto a menudo se denomina filtrado de salida). Los sistemas que han sido comprometidos por atacantes pueden usarse para atacar otros sistemas en Internet; El uso de direcciones de origen no válidas hace que este tipo de ataques sea más difícil de detener. Bloquear este tipo de tráfico en el firewall de una organización ayuda a reducir la efectividad de estos ataques.

El tráfico entrante con una dirección de destino del propio firewall debe bloquearse a menos que el firewall ofrezca servicios para el tráfico entrante que requieran conexiones directas (por ejemplo, si el firewall actúa como un proxy de aplicación).

Las organizaciones también deben bloquear los siguientes tipos de tráfico en el perímetro:

Tráfico que contiene información de enrutamiento de origen IP, que permite a un sistema especificar las rutas que emplearán los paquetes mientras viajan desde el origen al destino. Potencialmente, esto podría permitir que un atacante construya un paquete que eluda los controles de seguridad de la red. El enrutamiento de origen IP rara vez se utiliza en las redes modernas y las aplicaciones válidas son aún menos comunes en Internet.

Tráfico desde fuera de la red que contiene direcciones de difusión que se dirige al interior de la red. Cualquier sistema que responda a la transmisión dirigida enviará su respuesta al sistema especificado por la fuente, en lugar de al sistema fuente mismo. Estos paquetes se pueden utilizar para crear enormes "tormentas" de tráfico de red para ataques de denegación de servicio. Las direcciones de transmisión habituales, así como las direcciones utilizadas para IP de multidifusión, pueden o no ser apropiadas para bloquear en el firewall de una organización. Las redes de multidifusión y difusión rara vez se utilizan en entornos de redes normales, pero cuando se utilizan tanto dentro como fuera de la organización, se debe permitir a través de firewalls.

Los firewalls en el perímetro de la red deben bloquear todo el tráfico entrante a las redes y hosts a los que no debería poder accederse desde redes externas. Estos firewalls también deben bloquear todo el tráfico saliente de las redes y hosts de la organización a los que no se les debe permitir acceder a redes externas. Decidir qué direcciones deben bloquearse suele ser uno de los aspectos que más tiempo consumen en el desarrollo de políticas IP de firewall. También es uno de los más propensos a errores, porque la dirección IP asociada con una entidad no deseada a menudo cambia con el tiempo.

4.1.2 IPv6

IPv6 es una nueva versión de IP que se está implementando cada vez más. Aunque el formato interno y la longitud de la dirección de IPv6 difieren de los de IPv4, muchas otras características siguen siendo las mismas, y algunas de ellas son relevantes para los firewalls. Para las características que son iguales entre IPv4 e IPv6, los firewalls deberían funcionar igual. Por ejemplo, el bloqueo de todo el tráfico entrante y saliente que no haya sido permitido expresamente por la política de firewall debe realizarse independientemente de si el tráfico tiene o no una dirección IPv4 o IPv6.

Al momento de escribir este artículo, algunos firewalls no pueden manejar el tráfico IPv6 en absoluto; otros pueden manejarlo pero tienen capacidades limitadas para filtrar el tráfico IPv6; y otros pueden filtrar el tráfico IPv6 aproximadamente en la misma medida que el tráfico IPv4. Toda organización, permita o no que el tráfico IPv6 entre en su red interna, necesita un firewall que sea capaz de filtrar este tráfico. Estos firewalls deben tener las siguientes capacidades:

- El firewall debería poder utilizar direcciones IPv6 en todas las reglas de filtrado que utilicen direcciones IPv4.
- La interfaz administrativa debería permitir a los administradores clonar reglas IPv4 en direcciones IPv6 para facilitar la administración.
- El firewall debe poder filtrar ICMPv6, como se especifica en RFC 4890, Recomendaciones para filtrar mensajes ICMPv6 en firewalls.
- El firewall debería poder bloquear protocolos relacionados con IPv6, como túneles 6 a 4 y 4 a 6, Teredo y el protocolo de direccionamiento automático de túneles dentro del sitio (ISATAP), si no son necesarios.
- Muchos sitios tunelizan paquetes IPv6 en paquetes IPv4. Esto es particularmente común para los sitios que experimentan con IPv6, porque actualmente es más fácil obtener tránsito IPv6 de un intermediario de túneles a través de un túnel v6 a v4 que obtener tránsito IPv6 nativo de un proveedor de servicios de Internet (ISP). Existen varias formas de hacerlo y los estándares para la construcción de túneles aún están evolucionando. Si el firewall puede inspeccionar el contenido de los paquetes IPv4, necesita saber cómo inspeccionar el tráfico en busca de cualquier método de túnel utilizado por la organización. Un corolario de esto es que si una organización utiliza un firewall para prohibir que IPv6 entre o salga de su red, ese firewall debe reconocer y bloquear todas las formas de túnel v6 a v4.

Tenga en cuenta que la lista anterior es breve y no todas las reglas son específicas de seguridad. Debido a que la implementación de IPv6 aún se encuentra en sus primeras etapas, aún no existe un acuerdo generalizado en la comunidad de operaciones de IPv6 sobre lo que debe hacer un firewall IPv6 que sea diferente de los firewalls IPv4.

Para los firewalls que permiten el uso de IPv6, el tráfico con direcciones IPv6 de origen o destino no válidas siempre debe bloquearse; esto es similar a bloquear el tráfico con direcciones IPv4 no válidas. Dado que se ha invertido mucho más esfuerzo en crear listas de direcciones IPv4 no válidas que en direcciones IPv6, encontrar listas de direcciones IPv6 no válidas puede resultar difícil. Además, IPv6 permite a los administradores de red asignar direcciones en sus rangos asignados de diferentes maneras. Esto significa que en un rango de direcciones particular asignado a una organización, puede haber literalmente billones de direcciones IPv6 no válidas y solo unas pocas que sean válidas. Por necesidad, enumerar qué direcciones IPv6 no son válidas tendrá que ser menos detallado que enumerar direcciones IPv4 no válidas, y las reglas de firewall que utilizan estas listas serán menos efectivas que sus contrapartes IPv4.

Las organizaciones que aún no utilizan IPv6 deben bloquear todo el tráfico IPv6 nativo y tunelizado en sus firewalls. Tenga en cuenta que dicho bloqueo limita las pruebas y la evaluación de IPv6 y de las tecnologías de túnel IPv6 para futuras implementaciones. Para permitir dicho uso, el administrador del firewall puede desbloquear selectivamente IPv6 o las tecnologías de túnel específicas de interés para que las utilicen los evaluadores autorizados.

4.1.3 TCP y UDP

Los protocolos de aplicación pueden utilizar TCP, UDP o ambos, según el diseño del protocolo. Un servidor de aplicaciones normalmente escucha en uno o más puertos TCP o UDP fijos. Algunas aplicaciones utilizan un solo puerto, pero muchas aplicaciones utilizan varios puertos. Por ejemplo, aunque SMTP usa el puerto TCP 25 para enviar correo, usa el puerto TCP 587 para enviar correo. De manera similar, FTP usa al menos dos puertos, uno de los cuales puede ser impredecible, y aunque la mayoría de los servidores web usan solo el puerto TCP 80, es común tener sitios web que también usan puertos adicionales como el puerto TCP 8080. Algunas aplicaciones usan ambos puertos TCP. y UDP; por ejemplo, las búsquedas de DNS pueden realizarse en el puerto UDP 53 o en el puerto TCP 53. Los clientes de aplicaciones suelen utilizar cualquiera de una amplia gama de puertos.

Al igual que con otros aspectos de los conjuntos de reglas del firewall, se deben utilizar políticas de denegación predeterminadas para el tráfico TCP y UDP entrante. Generalmente se utilizan políticas menos estrictas para el tráfico TCP y UDP saliente porque la mayoría de las organizaciones permiten a sus usuarios acceder a una amplia gama de aplicaciones externas ubicadas en millones de hosts externos.

Además de permitir y bloquear el tráfico UDP y TCP, muchos firewalls también pueden informar o bloquear el tráfico UDP y TCP mal formado dirigido hacia el firewall o a hosts protegidos por el firewall. Este tráfico se utiliza con frecuencia para buscar hosts y también puede utilizarse en ciertos tipos de ataques. El firewall puede ayudar a bloquear dicha actividad, o al menos informar cuando se produce dicha actividad.

4.1.4 ICMP

Los atacantes pueden utilizar varios tipos y códigos de ICMP para realizar reconocimientos o manipular el flujo de tráfico de la red.18 Sin embargo, el ICMP es necesario para muchas cosas útiles, como obtener un rendimiento razonable en Internet. Algunas políticas de firewall bloquean todo el tráfico ICMP, pero esto a menudo genera problemas de diagnóstico y rendimiento. Otras políticas comunes permiten todo el tráfico ICMP saliente, pero limitan el ICMP entrante a aquellos tipos y códigos necesarios para el descubrimiento de la unidad de transmisión máxima de ruta (PMTU) (código ICMP 3) y la accesibilidad al destino.

Para evitar actividades maliciosas, los firewalls en el perímetro de la red deben denegar todo el tráfico ICMP entrante y saliente, excepto aquellos tipos y códigos específicamente permitidos por la organización. Para ICMP en IPv4, los mensajes ICMP tipo 3 no deben filtrarse porque se utilizan para diagnósticos de red importantes. El comando ping (código ICMP 8) es un diagnóstico de red importante, pero los pings entrantes a menudo son bloqueados por políticas de firewall para evitar que los atacantes aprendan más sobre la topología interna de la red de la organización. Para ICMP en IPv6, se deben permitir muchos tipos de mensajes en circunstancias específicas para habilitar varias funciones de IPv6. Consulte RFC 4890, Recomendaciones para filtrar mensajes ICMPv6 en firewalls, para obtener información detallada sobre cómo seleccionar qué tipos de ICMPv6 permitir o no para un tipo de firewall en particular.

ICMP se utiliza a menudo en protocolos de red de bajo nivel para aumentar la velocidad y la confiabilidad de la red. Por lo tanto, ICMP dentro de la red de una organización generalmente no debe ser bloqueado por firewalls que no estén en el perímetro de la red, a menos que las necesidades de seguridad superen las necesidades operativas de la red. De manera similar, si una organización tiene más de una red, no se debe bloquear el ICMP que proviene o va a otras redes dentro de la organización.

[18] El tipo ICMP y los números de código se definen en http://www.iana.org/assignments/icmp-parameters.

4.1.5 Protocolos IPsec

Una organización necesita tener una política para permitir o no VPN IPsec que comiencen o terminen dentro del perímetro de su red. Los protocolos ESP y AH se utilizan para las VPN IPsec y un firewall que bloquee estos protocolos no permitirá el paso de las VPN IPsec. Si bien bloquear ESP puede obstaculizar el uso del cifrado para proteger datos confidenciales, también puede obligar a los usuarios que normalmente cifrarían sus datos con ESP a permitir que sean inspeccionados, por ejemplo, mediante un firewall de inspección de estado o una puerta de enlace de proxy de aplicación.

Las organizaciones que permiten VPN IPsec deben bloquear ESP y AH, excepto hacia y desde direcciones específicas en la red interna; esas direcciones pertenecen a puertas de enlace IPsec a las que se les permite ser puntos finales de VPN.[19] Para hacer cumplir esta política será necesario que las personas dentro de la organización obtengan la aprobación de la política adecuada para abrir el acceso ESP y/o AH a sus enrutadores IPsec. Esto también reducirá la cantidad de tráfico cifrado proveniente del interior de la red que no puede ser examinado por los controles de seguridad de la red.

4.2 Políticas basadas en aplicaciones

La mayoría de los primeros trabajos de firewall implicaban simplemente bloquear el tráfico sospechoso o no deseado en el límite de la red. Los firewalls de aplicaciones entrantes o los servidores proxy de aplicaciones adoptan un enfoque diferente: permiten que el tráfico destinado a un servidor en particular ingrese a la red, pero capturan ese tráfico en un servidor que lo procesa como un firewall basado en puertos. El enfoque basado en aplicaciones proporciona una capa adicional de seguridad para el tráfico entrante al validar parte del tráfico antes de que llegue al servidor deseado. La teoría es que la capa de seguridad adicional del firewall o proxy de la aplicación entrante puede proteger el servidor mejor de lo que el servidor puede protegerse a sí mismo, y también puede eliminar el tráfico malicioso antes de que llegue al servidor para ayudar a reducir la carga del servidor. En algunos casos, un firewall de aplicación o un proxy pueden eliminar el tráfico que el servidor quizás no pueda eliminar por sí solo porque tiene mayores capacidades de filtrado. Un firewall o proxy de aplicación también impide que el servidor tenga acceso directo a la red exterior.

Si es posible, se deben utilizar servidores proxy y firewalls de aplicaciones entrantes frente a cualquier servidor que no tenga suficientes funciones de seguridad para protegerlo de ataques específicos de aplicaciones. Las principales consideraciones a la hora de decidir si utilizar o no un firewall o proxy de aplicación entrante son:

- ¿Está disponible un firewall de aplicaciones adecuado? O, si corresponde, ¿hay disponible un proxy de aplicación adecuado?
- ¿El servidor ya está suficientemente protegido por los cortafuegos existentes?
- ¿Puede el servidor principal eliminar contenido malicioso con tanta eficacia como el firewall o el proxy de la aplicación?
- ¿La latencia causada por un proxy de aplicación es aceptable para la aplicación?
- ¿Qué tan fácil es actualizar las reglas de filtrado en el servidor principal y el firewall o proxy de la aplicación para manejar las amenazas recientemente desarrolladas?

Los servidores proxy de aplicaciones pueden presentar problemas si no son muy capaces. A menos que un proxy de aplicación sea significativamente más robusto que el servidor y fácil de mantener actualizado, generalmente es mejor quedarse solo con el servidor de aplicaciones. Los firewalls de aplicaciones también pueden presentar problemas si no son lo suficientemente rápidos para manejar el tráfico destinado al servidor. Sin embargo, también es importante considerar los recursos del servidor: si el servidor no tiene recursos suficientes para resistir ataques, el firewall o proxy de la aplicación podría usarse como escudo.

---

[19] Siempre que exista una política para permitir el tráfico ESP y/o AH a través de un firewall, es muy probable que el firewall también necesite una política para permitir el tráfico de Intercambio de claves de Internet (IKE). IKE se ejecuta en el puerto UDP 500 y también puede usar el puerto UDP 4500 para sistemas IPsec que admiten cruce NAT.

Cuando un firewall o proxy de aplicación entrante está detrás de un firewall perimetral o en la DMZ del firewall, el firewall perimetral debe bloquearse según las direcciones IP, como se describió anteriormente en esta sección, para reducir la carga en el firewall o proxy de la aplicación. Hacer esto coloca una mayor parte de la política específica de direcciones en un solo lugar (el firewall principal) y reduce la cantidad de tráfico visto por el firewall o proxy de la aplicación, liberando más poder para filtrar contenido. Por supuesto, si el firewall perimetral es también el firewall de la aplicación y no se utiliza un proxy de aplicación interno, no se necesitan tales reglas.

Los servidores proxy de aplicaciones salientes son útiles para detectar sistemas que realizan conexiones inapropiadas o peligrosas desde el interior de la red protegida. Con diferencia, el tipo más común de proxy saliente es HTTP. Los servidores proxy HTTP salientes permiten a una organización filtrar contenido peligroso antes de que llegue a la PC solicitante. También ayudan a una organización a comprender y registrar mejor el tráfico web de sus usuarios y a detectar la actividad que se canaliza a través de HTTP. Cuando un proxy HTTP filtra contenido, puede alertar al usuario web de que el sitio visitado envió el contenido filtrado. El beneficio no relacionado con la seguridad más destacado de los servidores proxy HTTP es el almacenamiento en caché de páginas web para aumentar la velocidad y reducir el uso del ancho de banda. La mayoría de las organizaciones deberían emplear servidores proxy HTTP.

4.3 Políticas basadas en la identidad del usuario

El filtrado de paquetes tradicional no ve las identidades de los usuarios que se comunican en el tráfico que atraviesa el firewall, por lo que las tecnologías de firewall sin capacidades más avanzadas no pueden tener políticas que permitan o nieguen el acceso en función de esas identidades. Sin embargo, muchas otras tecnologías de firewall pueden ver estas identidades y, por lo tanto, implementar políticas basadas en la autenticación del usuario. Una de las formas más comunes de hacer cumplir la política de identidad del usuario en un firewall es mediante el uso de una VPN. Tanto las VPN IPsec como las VPN SSL tienen muchas formas de autenticar a los usuarios, como con secretos que se proporcionan usuario por usuario, con autenticación multifactor (por ejemplo, tokens criptográficos basados en el tiempo protegidos con PIN) o con autenticación digital. certificados controlados por cada usuario. NAC también se ha convertido en un método popular para que los firewalls permitan o nieguen a los usuarios el acceso a determinados recursos de la red. Además, los servidores de seguridad y los servidores proxy de aplicaciones pueden permitir o denegar el acceso a los usuarios basándose en la autenticación del usuario dentro de las propias aplicaciones.

Los firewalls que aplican políticas basadas en la identidad del usuario deberían poder reflejar estas políticas en sus registros. Es decir, probablemente no sea útil registrar únicamente la dirección IP desde la que se conectó un usuario en particular si al usuario se le permitió ingresar mediante una política específica del usuario; También es importante registrar la identidad del usuario.

4.4 Políticas basadas en la actividad de la red

Muchos firewalls permiten al administrador bloquear las conexiones establecidas después de un cierto período de inactividad. Por ejemplo, si un usuario fuera de un firewall inició sesión en un servidor de archivos pero no realizó ninguna solicitud durante los últimos 15 minutos, la política podría ser bloquear cualquier tráfico adicional en esa conexión. Las políticas basadas en el tiempo son útiles para frustrar ataques causados por un usuario que ha iniciado sesión y se aleja de una computadora y otra persona se sienta y utiliza las conexiones establecidas (y, por lo tanto, las credenciales del usuario que ha iniciado sesión). Sin embargo, estas políticas también pueden resultar molestas para los usuarios que establecen conexiones pero no las utilizan con frecuencia. Por ejemplo, un usuario puede conectarse a un servidor de archivos para leer un archivo y luego dedicar mucho tiempo a editarlo. Si el usuario no guarda el archivo en el servidor de archivos antes del tiempo de espera exigido por el firewall, el tiempo de espera podría provocar que se pierdan los cambios en el archivo.

Algunas organizaciones tienen mandatos sobre cuándo los firewalls deben bloquear las conexiones que se consideran inactivas, cuándo las aplicaciones deben desconectar las sesiones si no hay actividad, etc. Un firewall utilizado por dicha organización debería poder establecer políticas que coincidan con los mandatos y al mismo tiempo ser específicas. suficientes para cumplir con el objetivo de seguridad de los mandatos.

Un tipo diferente de política de firewall basada en la actividad de la red es aquella que limita o redirige el tráfico si la tasa de tráfico que coincide con la regla de política es demasiado alta. Por ejemplo, un firewall podría redirigir las conexiones realizadas a una dirección interna particular a una ruta más lenta si la velocidad de las conexiones supera un cierto umbral.
Otra política podría ser descartar los paquetes ICMP entrantes si la velocidad es demasiado alta. Elaborar dichas políticas es bastante difícil porque la limitación y el redireccionamiento pueden provocar que se pierda el tráfico deseado o que se produzcan fallos transitorios difíciles de diagnosticar.

4.5 Resumen de recomendaciones

Los siguientes elementos resumen las principales recomendaciones de esta sección:

- La política de firewall de una organización debe basarse en un análisis de riesgos integral.
- Las políticas de firewall deben basarse en bloquear todo el tráfico entrante y saliente, con excepciones para el tráfico deseado.
- Las políticas deben tener en cuenta el origen y el destino del tráfico además del contenido.
- Muchos tipos de tráfico IPv4, como el de direcciones privadas o no válidas, deben bloquearse de forma predeterminada.
- Las organizaciones deben tener políticas para manejar el tráfico IPv6 entrante y saliente.
- Una organización debe determinar qué aplicaciones pueden enviar tráfico hacia o desde su red y establecer políticas de firewall para bloquear el tráfico de otras aplicaciones.

5. Planificación e implementación del cortafuegos

Esta sección se centra en la planificación e implementación de firewalls en la empresa. Al igual que con cualquier implementación de nueva tecnología, la planificación e implementación del firewall deben abordarse en un enfoque por fases.
Se puede lograr una implementación exitosa del firewall siguiendo un proceso claro de planificación e implementación paso a paso.
El uso de un enfoque gradual para la implementación puede minimizar los problemas imprevistos e identificar posibles dificultades desde el principio. Esta sección explora en profundidad cada una de las fases de planificación e implementación del firewall, incluyendo:

1. Planificar. La primera fase del proceso implica identificar todos los requisitos que una organización debe considerar al determinar qué firewall implementar para hacer cumplir la política de seguridad de la organización.

2. Configurar. La segunda fase involucra todas las facetas de la configuración de la plataforma de firewall. Esto incluye la instalación de hardware y software, así como la configuración de reglas para el sistema.

3. Prueba. La siguiente fase implica implementar y probar un prototipo de la solución diseñada en un laboratorio o entorno de prueba. Los objetivos principales de las pruebas son evaluar la funcionalidad, el rendimiento, la escalabilidad y la seguridad de la solución, e identificar cualquier problema (como la interoperabilidad) con los componentes.

4. Implementar. Una vez que se completan las pruebas y se resuelven todos los problemas, la siguiente fase se centra en la implementación. del firewall en la empresa.

5. Gestionar. Una vez implementado el firewall, se administra durante todo su ciclo de vida para incluir mantenimiento de componentes y soporte para problemas operativos. Este proceso de ciclo de vida se repite cuando es necesario incorporar mejoras o cambios significativos a la solución.

5.1 Planificar

La fase de planificación para elegir e implementar un firewall debe comenzar sólo después de que una organización haya determinado que es necesario un firewall para hacer cumplir la política de seguridad de la organización. Esto suele ocurrir después de una evaluación de riesgos del sistema en general. Una evaluación de riesgos incluye (1) la identificación de amenazas y vulnerabilidades en el sistema de información; (2) el impacto potencial o la magnitud del daño que una pérdida de confidencialidad, integridad o disponibilidad tendría en los activos u operaciones de la organización (incluida la misión, función, imagen o reputación) en caso de una amenaza de explotación de las vulnerabilidades identificadas; y (3) la identificación y análisis de controles de seguridad para el sistema de información20.

Los principios básicos que las organizaciones deben seguir al planificar la implementación de firewalls incluyen:

Utilice los dispositivos tal y como fueron diseñados. Los cortafuegos no deben construirse con equipos que no estén destinados al uso de cortafuegos. Por ejemplo, los enrutadores están diseñados para manejar el enrutamiento, no un filtrado altamente complejo, que puede causar una carga excesiva en el procesador del enrutador. Además, no se debe esperar que los firewalls proporcionen servicios que no sean de seguridad, como actuar como servidor web o servidor de correo electrónico.

Crea una defensa en profundidad. La defensa en profundidad implica la creación de múltiples capas de seguridad. Esto permite gestionar mejor el riesgo, porque si una capa de defensa se ve comprometida, otra capa está ahí para contener el ataque. En el caso de los firewalls, la defensa en profundidad se puede lograr mediante el uso de múltiples firewalls en toda una organización, incluso en el perímetro, frente a departamentos internos sensibles y en computadoras individuales. Para que la defensa en profundidad sea realmente efectiva, los cortafuegos deben

[20] Para obtener información adicional sobre evaluaciones de riesgos, consulte NIST SP 800-30, Guía de gestión de riesgos para sistemas de tecnología de la información (http://csrc.nist.gov/publications/PubsSPs.html).

Sea parte de un programa de seguridad general que también incluya productos como antimalware y software de detección de intrusiones.

Preste atención a las amenazas internas. Centrar la atención únicamente en las amenazas externas deja la red abierta a ataques desde dentro. Es posible que estas amenazas no provengan directamente de personas internas, pero pueden involucrar hosts internos infectados por malware o comprometidos de otra manera por atacantes externos. Los sistemas internos importantes deben colocarse detrás de cortafuegos internos.

Documente las capacidades del firewall. Cada modelo de firewall tiene diferentes capacidades y limitaciones. En ocasiones, estos afectarán la planificación de la política de seguridad y la estrategia de implementación del firewall de la organización. Cualquier característica que afecte positiva o negativamente esta planificación debe escribirse en el documento de planificación general.

Tenga en cuenta que la expresión “todas las reglas deben romperse” se aplica cuando se construyen cortafuegos. Si bien los implementadores de firewalls deben tener en cuenta las reglas anteriores durante la planificación, cada red y organización tiene requisitos e idiosincrasias únicos que podrían requerir soluciones únicas.

Las organizaciones deben considerar lo siguiente al comprar e implementar una solución de firewall:

Capacidades de seguridad

– ¿ Qué áreas de la organización necesitan protegerse (el perímetro, departamentos internos, oficina remota, hosts individuales, servicios específicos, clientes móviles, etc.)?

– ¿ Qué tipos de tecnologías de firewall abordarán mejor los tipos de tráfico que deben ser protegido (filtrado de paquetes, inspección de estado, firewall de aplicaciones, puerta de enlace de proxy de aplicaciones, etc.)?

– ¿ Qué funciones de seguridad adicionales (como capacidades de detección de intrusiones, VPN y filtrado de contenido) debe admitir el firewall?

Gestión

– ¿Qué protocolos admite el firewall para la administración remota, como HTTP sobre SSL, ¿SSH y acceso a través de un cable serie?

– ¿Alguno de los protocolos de gestión remota del firewall es aceptable para su uso, de acuerdo con las las políticas de la organización?

– ¿ Se puede restringir la administración remota a ciertas interfaces de firewall y direcciones IP de origen, como las de una red interna particular?

– ¿El firewall admite la administración centralizada de múltiples dispositivos (no necesariamente solo cortafuegos) del mismo proveedor?

– Si la gestión centralizada está disponible, ¿la realiza una aplicación específica del proveedor o puede ser controlado por otras aplicaciones?

Rendimiento (generalmente solo para firewalls de red)

– ¿ Qué cantidad de rendimiento, conexiones simultáneas máximas, conexiones por segundo y requisitos de latencia se deben cumplir para evitar que el firewall sea un cuello de botella para el acceso a la red, tanto para las necesidades de tráfico actuales como futuras?

– ¿ Se requieren funcionalmente el equilibrio de carga y la conmutación por error para garantizar una alta disponibilidad?

– ¿ Se debe considerar la preferencia por un firewall basado en hardware versus un firewall basado en software?

Integración

– ¿El firewall requerirá hardware específico para integrarse adecuadamente dentro de la infraestructura de red de la organización (capacidades de energía específicas, tipo específico de tarjeta de interfaz de red [NIC], dispositivo de respaldo específico, etc.)?

– ¿Es necesario que el firewall sea compatible con otros dispositivos de la red que brinden seguridad? u otros servicios?

– ¿El registro del firewall interopera con los sistemas de gestión de registros existentes?

– ¿ La instalación de un firewall requerirá cambios en otras áreas de la red?

Entorno físico (generalmente una consideración para los firewalls de red, aunque también puede aplicarse a los componentes centralizados de las implementaciones de firewalls basados en host)

– ¿ Dónde estará ubicado físicamente el firewall para garantizar la seguridad física y la protección contra desastres?

– ¿ Existe suficiente espacio en estantes o bastidores en la ubicación física donde se colocará el firewall?

– ¿ Se necesitarán energía adicional, energía de respaldo, aire acondicionado y/o conexiones de red en la ubicación física?

Personal

– ¿ Quién será responsable de gestionar el firewall?

– ¿ Los administradores del sistema necesitarán capacitación antes de implementar el firewall?

Necesidades futuras

– ¿El firewall satisfará las necesidades futuras de la organización (planes de pasar a IPv6, requisitos de ancho de banda anticipados, cumplimiento de las regulaciones que se espera implementar, etc.)?

Otros elementos a considerar al comprar e implementar firewalls personales y basados en host incluyen:

¿Las estaciones de trabajo o los servidores cumplen con los requisitos mínimos del sistema del firewall que se está evaluando?

¿Será el firewall compatible con otro software de seguridad en la estación de trabajo o servidor (por ejemplo, software antimalware)?

¿Se puede administrar el firewall de manera centralizada y permitir que las políticas que hacen cumplir la política de seguridad de la organización se envíen a los clientes?

¿Puede el firewall informar violaciones de políticas a un servidor central?

¿Se puede bloquear el firewall para evitar que nadie, excepto los administradores, modifique su configuración?

¿El firewall entrará en conflicto con los firewalls personales o basados en host integrados en los sistemas operativos de los hosts? Si es así, ¿con qué facilidad se pueden resolver estos conflictos?

5.2 Configurar

La fase de configuración involucra todas las facetas de la configuración de la plataforma del firewall. Esto incluye instalar hardware y software, configurar políticas, configurar registros y alertas e integrar el firewall en la arquitectura de la red.

5.2.1 Instalación de hardware y software

Una vez que se haya elegido y adquirido el firewall, se deben instalar el hardware, el sistema operativo y el software de firewall subyacente para un firewall basado en software. A continuación, tanto para los firewalls basados en software como en hardware, se deben instalar parches y actualizaciones de proveedores en el sistema. Durante esta etapa, el firewall también debe reforzarse para disminuir el riesgo de vulnerabilidades y proteger el sistema contra accesos no autorizados. En este momento también se debe instalar cualquier software de consola necesario para el acceso remoto.

Durante la instalación y configuración, sólo el administrador que realiza ese trabajo debería poder administrar el firewall. Todos los demás servicios de administración del firewall, como SNMP, deben estar deshabilitados y estos servicios deben dejarse deshabilitados permanentemente a menos que sea necesario. Si el firewall admite tener una cuenta de administrador separada para cada persona que realiza tareas de administración del firewall, configure dichas cuentas.

Los firewalls de red deben colocarse en una habitación que cumpla con los requisitos ambientales recomendados por el producto en cuanto a temperatura, humedad, espacio, energía, etc. Esta sala también debe estar asegurada físicamente para evitar que personal no autorizado acceda al firewall.

Comparar los registros de múltiples sistemas al analizar problemas es muy importante, por lo que los relojes internos de cada firewall deben ser consistentes con los de todos los demás sistemas utilizados por la organización. La mejor manera de hacerlo es sincronizar todos los sistemas con una fuente horaria autorizada.

5.2.2 Configuración de políticas

Una vez que el hardware y el software se hayan instalado y protegido, los administradores pueden crear las políticas del firewall. Algunos firewalls implementan políticas a través de reglas explícitas; algunos firewalls requieren configurar ajustes de firewall que luego crean reglas internas; algunos cortafuegos crean políticas y reglas automáticamente; y otros más utilizan una combinación de estos tres tipos de configuración. El resultado final es un conjunto de reglas llamado conjunto de reglas que describe cómo actúa el firewall. Algunos proveedores tienen restricciones o sugerencias sobre el orden de las reglas en un conjunto de reglas. Si bien es común pensar que las reglas de un firewall afectan el tráfico que aparece en las interfaces internas o externas, la mayoría de los firewalls también permiten configurar políticas que no están basadas en el tráfico, como quién puede ver o cambiar las reglas, o dónde se encuentran los servidores DNS externos y Se pueden encontrar servidores de sincronización horaria.

Estos conjuntos de reglas deben implementar la política de firewall de la organización según lo documentado en el plan de seguridad del sistema y deben ser lo más específicos posible con respecto al tráfico de red que controlan. Para crear un conjunto de reglas, primero se debe determinar qué tipos de tráfico (protocolos, direcciones de origen y destino, etc.) requieren las aplicaciones aprobadas para la organización. Esto debe incluir los protocolos que el propio firewall pueda necesitar (DNS, Protocolo simple de administración de red [SNMP], NTP, registro, etc.)

Los detalles de la creación de un conjunto de reglas varían según el tipo de firewall y productos específicos. Por ejemplo, muchos cortafuegos comparan el tráfico con las reglas de forma secuencial hasta encontrar una coincidencia. Para estos firewalls, las reglas con mayor probabilidad de coincidir con los patrones de tráfico deben colocarse lo más arriba posible en la lista para mejorar el rendimiento del firewall. Otros firewalls tienen formas más complejas de procesar conjuntos de reglas, como verificar primero las reglas de "denegar" y luego verificar las reglas de "permitir".

La mayoría de los firewalls permiten que cada regla de un conjunto de reglas tenga un comentario. Completar dicho comentario es importante para que otros determinen por qué se creó una regla. Los comentarios también son muy útiles para las personas que auditan conjuntos de reglas. Aunque las reglas para comentar pueden parecer triviales, pueden resultar muy valiosas más adelante y requieren poco esfuerzo. Los cambios de reglas y los comentarios asociados deben copiarse en el registro de administración de configuración apropiado.

Como mínimo, se deben definir las siguientes reglas:

El filtrado de puertos debe habilitarse en el borde exterior de la red y probablemente también en lugares dentro de la red.

El filtrado de contenidos debe realizarse lo más cerca posible del receptor de contenidos.

Existen muchas formas de definir reglas y cada organización tendrá sus propias necesidades y conjuntos específicos de personal que deberían participar en la configuración del conjunto de reglas.

Si varios firewalls necesitan tener las mismas reglas o un subconjunto común de reglas, esas reglas deben sincronizarse entre los firewalls. Por lo general, esto se hace de manera específica del proveedor. Tenga en cuenta que es probable que algunos de los firewalls tengan políticas algo diferentes, dependiendo de su ubicación en la red de la organización. Por ejemplo, una organización podría querer que solo uno de sus firewalls actúe como puerta de enlace VPN, aunque todos los firewalls podrían tener las mismas reglas de filtrado para el tráfico que no sea VPN.

Por lo tanto, es importante sincronizar únicamente las reglas que son comunes entre los firewalls.

5.2.3 Configuración de registros y alertas

El siguiente paso en el proceso de configuración es configurar el registro y las alertas. El registro es un paso fundamental para prevenir y recuperarse de fallas, así como para garantizar que se establezcan las configuraciones de seguridad adecuadas en el firewall. El registro adecuado también puede proporcionar información vital para responder a incidentes de seguridad.
Siempre que sea posible, el firewall debe configurarse para almacenar registros localmente y enviarlos a una infraestructura de administración de registros centralizada. Las limitaciones de recursos, las capacidades de registro del firewall y otras situaciones pueden afectar la capacidad de almacenar registros tanto de forma local como central.

La decisión de qué registrar y durante cuánto tiempo conservarlos debe realizarse caso por caso. Por ejemplo, algunos administradores de red desean registrar todas las conexiones entrantes aceptadas para poder asegurarse de que no aceptan tráfico no deseado. Otros administradores no querrían registrar las conexiones entrantes aceptadas porque son muy numerosas o porque el registro consumiría demasiados recursos. De manera similar, algunos administradores no querrían registrar todo el tráfico entrante denegado por el firewall porque el número de exploraciones y sondeos realizados por partes potencialmente maliciosas es muy alto y no se puede tomar ninguna medida en respuesta a ellos; sin embargo, otros administradores querrían saber acerca de los análisis y sondeos en caso de que puedan detectar un patrón que les alerte sobre un posible ataque que luego pueda prevenirse.

Si el firewall admite cuentas de administrador con diferentes capacidades, cree una o más cuentas de usuario administrativo con acceso de lectura a los registros, si es posible. Utilice estas credenciales cuando realice tareas de solo lectura, como auditorías e inspecciones periódicas de los registros.

Además de configurar el registro, también se deben configurar alertas en tiempo real para notificar a los administradores cuando ocurren eventos importantes en el firewall. Las notificaciones pueden incluir lo siguiente:

Cualquier modificación o desactivación de las reglas del firewall.

Reinicios del sistema, escasez de discos y otros eventos operativos

Cambios de estado del sistema secundario, si corresponde.

5.3 Prueba

Los nuevos firewalls deben probarse y evaluarse antes de su implementación para garantizar que funcionen correctamente. Las pruebas deben completarse en una red de prueba sin conectividad a la red de producción. Esta red de prueba debe intentar replicar la red de producción lo más fielmente posible, incluida la topología de la red y el tráfico de la red que atravesaría el firewall. Los aspectos de la solución a evaluar incluyen los siguientes:

Conectividad. Los usuarios pueden establecer y mantener conexiones a través del firewall.

Conjunto de reglas: se permite el tráfico específicamente permitido por la política de seguridad. Se bloquea todo el tráfico que no esté permitido por la política de seguridad. La verificación del conjunto de reglas debe incluir revisarlo manualmente y probar si las reglas funcionan como se espera.

Compatibilidad de aplicaciones. Las soluciones de firewall personales o basadas en host no interrumpen ni interfieren con el uso de las aplicaciones de software existentes. Esto incluye comunicaciones de red entre componentes de la aplicación. Las soluciones de firewall de red no interfieren con aplicaciones que tienen componentes que interactúan a través del firewall (por ejemplo, software de cliente y servidor).

Gestión. Los administradores pueden configurar y gestionar la solución de forma eficaz y segura.

Inicio sesión. El registro y la gestión de datos funcionan de acuerdo con las políticas y estrategias de la organización.

Actuación. Las soluciones proporcionan un rendimiento adecuado durante el uso normal y pico. En muchos casos, la mejor manera de probar el rendimiento bajo la carga de una implementación prototipo es utilizar generadores de tráfico simulados en una red de prueba en vivo para imitar las características reales del tráfico esperado lo más fielmente posible. Simular las cargas causadas por ataques DoS también puede resultar útil para evaluar el rendimiento del firewall. Las pruebas deben incorporar una variedad de aplicaciones que atravesarán el firewall, especialmente aquellas que tienen más probabilidades de verse afectadas por problemas de latencia o rendimiento de la red.

Seguridad de la Implementación. La propia implementación del firewall puede contener vulnerabilidades y debilidades que los atacantes podrían aprovechar. Es posible que las organizaciones con altas necesidades de seguridad deseen realizar evaluaciones de vulnerabilidad de los componentes del firewall.

Interoperabilidad de componentes. Los componentes de la solución de firewall deben funcionar juntos correctamente. Esto es de gran preocupación cuando se utilizan una variedad de componentes de diferentes proveedores.

Sincronización de políticas. Si hay varios firewalls que ejecutan políticas sincronizadas o grupos de reglas, pruebe que la sincronización funcione en varios escenarios (por ejemplo, si uno o más nodos están fuera de línea).

Características adicionales. Las funciones adicionales que utilizará el firewall, como VPN y capacidades antimalware, deben probarse para garantizar que funcionan correctamente.

5.4 Implementar

Una vez que se completan las pruebas y se resuelven todos los problemas, la siguiente fase del modelo de planificación e implementación del firewall es la implementación, que debe realizarse de acuerdo con las políticas de la organización. Antes de implementar el firewall, los administradores deben notificar a los usuarios o propietarios de sistemas potencialmente afectados sobre la implementación planificada e indicarles a quién deben notificar si encuentran algún problema. Cualquier

Los cambios requeridos en otros equipos también deben coordinarse como parte de la implementación del firewall. La política de seguridad expresada por la configuración del firewall debe agregarse a la política de seguridad general de la organización, y los cambios continuos en su configuración deben integrarse con los procesos de gestión de la configuración de la organización. Si se están implementando varios firewalls, incluidos firewalls personales o en varias sucursales, se debe considerar un enfoque gradual o por fases; Un programa piloto también sería útil, especialmente para identificar y resolver problemas de políticas contradictorias.
Esto brindará a los administradores la oportunidad de evaluar el impacto de la solución de firewall y resolver problemas antes de la implementación en toda la empresa.

Conectar un firewall a la red de la organización requiere algo más que simplemente insertar el firewall en el flujo de tráfico desde el exterior de la red hacia el interior: también implica integrar el firewall con otros elementos de la red que interactuarán con el firewall. Dado que los cortafuegos suelen actuar como enrutadores, el cortafuegos debe integrarse en la estructura de enrutamiento de la red. Esto a menudo significa reemplazar un enrutador que está en el mismo lugar en la topología de la red donde se coloca el firewall, pero también puede significar cambiar las tablas de enrutamiento de otros enrutadores en la red de la organización para manejar la adición de este nuevo enrutador. Si los elementos de la red utilizan enrutamiento dinámico, probablemente será necesario modificar su configuración para conocer el enrutamiento del firewall. Además, es posible que sea necesario reconfigurar el conmutador de red en el exterior de la red que se está protegiendo para manejar el direccionamiento del firewall. Si el firewall es un conjunto de sistemas con conmutación por error entre los sistemas, es posible que sea necesario configurar el conmutador de red para manejar la conmutación por error.

5.5 Administrar

Esta última fase del modelo de planificación e implementación del firewall es la más duradera, porque administrar la solución implica mantener la arquitectura, las políticas, el software y otros componentes del firewall elegidos para implementar. Un ejemplo de una acción de mantenimiento típica es probar y aplicar parches a los dispositivos de firewall.21 Es posible que sea necesario actualizar las reglas de políticas a medida que se identifican nuevas amenazas y cambian los requisitos, como cuando se implementan nuevas aplicaciones o hosts dentro de la red, y también se deben actualizar. Se revisan periódicamente para garantizar que cumplan con la política de seguridad. También es importante monitorear el rendimiento de los componentes del firewall para garantizar que se identifiquen y aborden los posibles problemas de recursos antes de que los componentes se vean abrumados. Los registros y alertas también deben monitorearse continuamente para identificar las amenazas (exitosas y no exitosas) que se realizan al sistema. Otra tarea importante es realizar pruebas periódicas para verificar que las reglas del firewall funcionan según lo esperado. Además, se deben realizar copias de seguridad periódicas de las políticas y conjuntos de reglas del firewall. Algunos firewalls pueden almacenar esta información en múltiples formatos, como un formato binario que se utiliza para configurar el firewall y un formato legible por humanos que pueden leer los auditores. Si hay varios formatos disponibles, se deben mantener copias de seguridad en todos ellos.

Los cambios en los conjuntos de reglas o políticas del firewall afectan la seguridad y deben gestionarse como parte de un proceso formal de gestión de la configuración. Muchos firewalls cuentan con auditoría de cambios como parte de sus interfaces administrativas, pero esto no necesariamente rastrea los cambios de políticas. Como mínimo, se debe mantener un registro de todas las decisiones políticas y cambios en el conjunto de reglas, y este registro debe estar asociado de alguna manera con el firewall. Por ejemplo, el registro se puede adjuntar físicamente al dispositivo o el archivo de registro se puede mantener en la misma parte del sistema de gestión de inventario de la organización que el firewall. Además, algunos firewalls permiten mantener comentarios para cada regla; Siempre que sea práctico, los conjuntos de reglas deben documentarse con comentarios sobre cada regla. La mayoría de los cortafuegos permiten restricciones sobre quién puede realizar cambios en el conjunto de reglas; algunos incluso permiten restricciones sobre las direcciones desde las cuales los administradores pueden realizar dichos cambios. Estas restricciones deben utilizarse cuando sea posible.

---

21 Para obtener información adicional sobre la administración de parches, consulte NIST SP 800-40 Versión 2, Creación de un programa de administración de parches y vulnerabilidades (http://csrc.nist.gov/publications/PubsSPs.html).

Tenga en cuenta que los conjuntos de reglas del firewall pueden volverse cada vez más complicados con la edad. Por ejemplo, un nuevo conjunto de reglas de firewall podría contener entradas para dar cabida únicamente al tráfico de usuarios salientes y al tráfico de correo electrónico entrante (además de permitir las conexiones entrantes de retorno requeridas por TCP/IP), pero probablemente contendrá muchas más reglas cuando el sistema de firewall alcance la final de su primer año de producción. Si bien los nuevos requisitos comerciales o de usuarios suelen impulsar estos cambios, también pueden reflejar otras influencias dentro de una organización. Es importante revisar la política del firewall con frecuencia. Una revisión de este tipo puede descubrir reglas que ya no son necesarias, así como nuevos requisitos de políticas que deben agregarse al firewall.

Es mejor revisar la política de firewall a intervalos regulares para que dichas revisiones no ocurran sólo durante las auditorías de políticas o de seguridad (o, peor aún, sólo durante emergencias). Cada revisión debe incluir un examen detallado de todos los cambios desde la última revisión periódica, en particular quién realizó los cambios y bajo qué circunstancias. También es útil realizar ocasionalmente auditorías generales del conjunto de reglas por parte de personas que no forman parte del equipo normal de revisión de políticas para obtener una visión externa de cómo la política coincide con los objetivos de la organización. Algunos firewalls tienen herramientas que pueden realizar revisiones automáticas de políticas, buscando reglas redundantes o faltantes que sean ampliamente recomendadas. Si dichas herramientas están disponibles para el firewall de una organización, deberían usarse periódicamente, probablemente como parte de la revisión periódica de las políticas.

Es posible que las organizaciones quieran considerar la realización de pruebas de penetración para evaluar la seguridad general de su entorno de red. Esta prueba se puede utilizar para verificar que un conjunto de reglas de firewall funciona según lo previsto generando tráfico de red y monitoreando cómo lo maneja el firewall en comparación con su respuesta esperada. Las pruebas de penetración deben emplearse además de, y no en lugar de, un programa de auditoría convencional.22

22 Para obtener más información sobre pruebas de penetración, consulte NIST SP 800-115, Guía técnica para pruebas y evaluaciones de seguridad de la información (http://csrc.nist.gov/publications/PubsSPs.html).

Apéndice A—Glosario

Los términos seleccionados utilizados en la publicación se definen a continuación.

Firewall de aplicaciones: un firewall que utiliza análisis de protocolo con estado para analizar el tráfico de red para una o más aplicaciones.

Puerta de enlace de proxy de aplicación: una capacidad de firewall que combina control de acceso de capa inferior con funcionalidad de capa superior e incluye un agente proxy que actúa como intermediario entre dos hosts que desean comunicarse entre sí.

Servidor proxy dedicado: una forma de servidor proxy que tiene capacidades de firewall mucho más limitadas que una puerta de enlace de proxy de aplicación.

Zona desmilitarizada (DMZ): una interfaz en un firewall de enrutamiento que es similar a las interfaces que se encuentran en el lado protegido del firewall. El tráfico que se mueve entre la DMZ y otras interfaces en el lado protegido del firewall aún pasa a través del firewall y se le pueden aplicar políticas de protección de firewall.

Denegar de forma predeterminada: para bloquear todo el tráfico entrante y saliente que no haya sido permitido expresamente por la política de firewall.

Filtrado de salida: filtrado del tráfico de red saliente.

Firewall: dispositivo o programa que controla el flujo de tráfico de red entre redes o hosts que emplean diferentes posturas de seguridad.

Firewall basado en host: un firewall basado en software instalado en un servidor para monitorear y controlar el tráfico de red entrante y saliente.

Filtrado de ingreso: filtrado del tráfico de red entrante.

Control de acceso a la red (NAC): una función proporcionada por algunos firewalls que permite el acceso según las credenciales de un usuario y los resultados de las comprobaciones de estado realizadas en el dispositivo cliente de teletrabajo.

Traducción de direcciones de red (NAT): una tecnología de enrutamiento utilizada por muchos firewalls para ocultar las direcciones internas del sistema de una red externa mediante el uso de un esquema de direccionamiento.

Filtro de paquetes: un dispositivo de enrutamiento que proporciona funcionalidad de control de acceso para direcciones de host y sesiones de comunicación.

Firewall personal: un firewall basado en software instalado en una computadora de escritorio o portátil para monitorear y controlar el tráfico de red entrante y saliente.

Dispositivo de firewall personal: dispositivo que realiza funciones similares a un firewall personal para un grupo de computadoras en una red doméstica.

Conjunto de reglas: conjunto de directivas que rigen la funcionalidad de control de acceso de un firewall. El firewall utiliza estas directivas para determinar cómo se deben enrutar los paquetes entre sus interfaces.

Inspección de estado: filtrado de paquetes que también rastrea el estado de las conexiones y bloquea los paquetes que se desvían del estado esperado.

Análisis de protocolo con estado: una capacidad de firewall que mejora la inspección de estado estándar al agregar tecnología básica de detección de intrusiones. Esta tecnología consiste en un motor de inspección que analiza protocolos en la capa de aplicación para comparar perfiles desarrollados por proveedores de actividad de protocolo benigna con eventos observados para identificar desviaciones, lo que permite que un firewall permita o niegue el acceso según cómo se ejecuta una aplicación en una red.

Inspección sin estado: consulte "Filtrado de paquetes".

Apéndice B—Siglas y abreviaturas

A continuación se definen las siglas y abreviaturas seleccionadas utilizadas en la publicación.

Ah	Encabezado de autenticación
ALG	Puertas de enlace de la capa de aplicación
California	Autoridad certificada
CIDR	itinerario entre recesos
UPC	Unidad Central de procesamiento
DMZ	Zona desmilitarizada
DNS	sistema de nombres de dominio
DoS	Negación de servicio
ESP	Encapsulación de carga útil de seguridad
FISMA	Ley Federal de Gestión de Seguridad de la Información
ftp	Protocolo de transferencia de archivos
JA	Alta disponibilidad
HTML	Lenguaje de marcado de hipertexto
HTTP	Protocolo de Transferencia de Hipertexto
ICMP	Protocolo de mensajes de control de Internet
desplazados internos	Sistema de detección y prevención de intrusiones
IETF	Grupo de Trabajo de Ingeniería de Internet
IGMP	Protocolo de gestión de grupos de Internet
IKE	Intercambio de claves por Internet
SOY	Mensajería instantánea
IMAP	Protocolo de acceso a mensajes de Internet
IP	protocolo de Internet
IPS	Sistema de Prevención de Intrusión
IPSec	Seguridad del protocolo de Internet
IPv4	Protocolo de Internet versión 4
IPv6	Protocolo de Internet versión 6
ISATAP	Protocolo de direccionamiento automático de túneles dentro del sitio
ISP	Proveedor de servicios de Internet
ÉL	Tecnologías de la información
DIT	Laboratorio de Tecnología de la Información
LAN	Red de área local
LDAP	Protocolo ligero de acceso a directorios
MAC	El control de acceso a medios
MÍMICA	Extensiones de correo de Internet multipropósito
NAC	Control de acceso a la red
SIESTA	Protección de acceso a la red
TNA	Traducción de direcciones de red y puertos
NAT	Traducción de Direcciones de Red

tarjeta de red	Tarjeta de interfaz de red
NIST	Instituto Nacional de Estándares y Tecnología
NTP	Protocolo de tiempo de red
OMB	Oficina de Gerencia y Presupuesto
PALMADITA	Traducción de direcciones de puertos
ordenador personal	Computadora personal
PCI	Industria de tarjetas de pago
PMTU	Unidad de transmisión máxima de ruta
ESTALLIDO	Protocolo de la Oficina postal
RADIO	Servicio de usuario telefónico de autenticación remota
RFC	Solicitud de comentarios
SMTP	Protocolo simple de transferencia de correo
SNMP	Protocolo Simple de Manejo de Red
SP	Publicación especial
SQL	lenguaje de consulta estructurado
SSL	Capa de sockets seguros
tcp	Protocolo de Control de Transmisión
TCP/IP	Protocolo de Control de Transmisión / Protocolo de Internet
TLS	Transport Layer Security
UDP	Protocolo de datagramas de usuario
UPnP	Conexión y reproducción universales
URL	Localizador Uniforme de Recursos
UTM	Gestión Unificada de Amenazas
VoIP	Voz sobre Protocolo de Internet
vpn	Red privada virtual
VPNC	Consorcio de redes privadas virtuales
PÁLIDO	Red de área amplia
XML	Lenguaje de marcado extensible

Apéndice C—Recursos

Las listas siguientes proporcionan ejemplos de recursos que pueden resultar útiles.

Documentos y sitios de recursos del NIST

Nombre del recurso	Localizador uniforme de recursos (URL)
Programa de lista de verificación nacional del NIST	http://checklists.nist.gov/
NIST SP 800-18 Revisión 1, Guía para desarrollar la seguridad Planes para sistemas de información federales	http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf http://
NIST SP 800-30, Guía de gestión de riesgos para obtener información Sistemas Tecnológicos	csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf http://
NIST SP 800-40 Versión 2, Creación de un parche y Programa de gestión de vulnerabilidades	csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
NIST SP 800-44 Versión 2, Directrices para proteger al público Servidores web	http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf
NIST SP 800-45 Versión 2, Directrices sobre correo electrónico Seguridad	http://csrc.nist.gov/publications/nistpubs/800-45-versión2/SP800-45v2.pdf
NIST SP 800-46 Revisión 1, Guía para el teletrabajo empresarial y la seguridad del acceso remoto	http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf http://
NIST SP 800-52, Directrices para la selección y uso de Implementaciones de seguridad de la capa de transporte (TLS)	csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf http://
NIST SP 800-61 Revisión 1, Incidente de seguridad informática Guía de manejo	csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf
NIST SP 800-70 Revisión 1 (borrador), Lista de verificación nacional Programa para productos de TI: directrices para usuarios y desarrolladores de listas de verificación	http://csrc.nist.gov/publications/PubsSPs.html
NIST SP 800-77, Guía de VPN IPsec	http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf http://
NIST SP 800-81 Revisión 1 (borrador), Nombre de dominio seguro Guía de implementación del sistema (DNS)	csrc.nist.gov/publications/PubsSPs.html
NIST SP 800-86, Guía para integrar técnicas forenses en la respuesta a incidentes	http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
NIST SP 800-92, Guía para el registro de seguridad informática Gestión	http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf
NIST SP 800-94, Guía para la detección de intrusiones y Sistemas de Prevención (PDI)	http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf http://
NIST SP 800-95, Guía para servicios web seguros	csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf http://
NIST SP 800-97, Establecimiento de redes de seguridad inalámbricas sólidas: una guía para IEEE 802.11i	csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf http://
NIST SP 800-113, Guía de VPN SSL	csrc.nist.gov/publications/nistpubs/800-113/SP800-113.pdf
NIST SP 800-114, Guía del usuario para proteger dispositivos externos Dispositivos para Teletrabajo y Acceso Remoto	http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf
NIST SP 800-115, Guía técnica para la seguridad de la información Pruebas y evaluación	http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

Otros sitios y documentos de recursos técnicos

Nombre del recurso	Localizador uniforme de recursos (URL)
Lograr una defensa en profundidad con firewalls internos	http://www.sans.org/reading_room/whitepapers/firewalls/7 97.php?portal=a4d358dbd051422110d917753a0ebb7c
Mejores prácticas para administrar registros de firewall	http://www.zdnet.com.au/insight/print.htm?TYPE=story&A T=120265680-139023731t-110000100c
Defensa en profundidad: bases para una seguridad y Empresas de TI resilientes	http://www.cert.org/archive/pdf/Defense_in_Depth092106. pdf
Evolución del firewall: inspección profunda de paquetes ¿En	http://www.securityfocus.com/infocus/1716 http://
qué se diferencian las puertas de enlace a nivel de circuito y las puertas de enlace a nivel de aplicación?	searchsecurity.techtarget.com/expert/Knowledgebas eAnswer/0,289625,sid14_gci1197999,00.html http://nvd.nist.gov/
Base de datos nacional de vulnerabilidad	http://www.securityfocus.com/
Los peligros de la inspección profunda de paquetes	infocus/1817 http://www.securityfocus.com/infocus/1737
Dispositivos de firewall puente transparentes	http:/ /searchwebservices.techtarget.com/tip/1,289483,sid2
El asesor de servicios web: cortafuegos XML	6_gci855052,00.html