



RESUMEN TÉCNICO

Seguridad de Redes: Una guía para imple- mentar Firewalls

Seguridad de Redes

Una guía para implementar Firewalls

La pérdida de datos insustituibles es una amenaza real para cualquier empresa que conecta su red con el mundo exterior. Por otra parte, el acceso remoto y la conexión a Internet permiten mejorar la comunicación a un nivel sin precedente. Además de proveer una extensa fuente de información, el acceso a Internet abre las puertas a un gran universo de comunicación con los clientes y proveedores. No obstante, estas mismas oportunidades exponen sus redes locales (LAN) a sufrir ataques de "hackers", así como al uso inadecuado por parte de sus propios empleados.

Para comprender el nivel de seguridad que su red requiere, es necesario considerar varios factores. En primer lugar, debe determinar cuál es el valor de sus datos. La respuesta lógica es: "probablemente más de lo que usted se imagina". Cuando evalúe el valor de sus datos, tome en cuenta los riesgos, tales como la responsabilidad legal, la pérdida de su ventaja competitiva o el impacto de la pérdida en la productividad de su empresa como consecuencia de haber comprometido su red. La mayoría de analistas lo expresan claramente: "si su empresa está conectada a Internet, usted necesita un firewall".

Los beneficios de conectarse a Internet son evidentes. Este documento describe los riesgos que su empresa enfrenta cuando se conecta a Internet, el tipo de ataques que pueden ocurrir y ofrece un resumen general de la tecnología de firewall que puede proteger su red contra los "hackers". Más específicamente, discutimos la implementación de un firewall y los factores que debe tener en cuenta para seleccionar el firewall adecuado para sus necesidades.

¿Por qué implementar un Firewall? ¿Realmente existe algún riesgo?

Cualquier persona puede convertirse en un "hacker". No se necesita ser un genio en informática para causar estragos en su red. Existe un amplio rango de herramientas y utilitarios que pueden descargarse fácilmente a través de

Internet, para convertir a cualquier persona en un "hacker" competente.

Hay expertos que dicen: "si su empresa está conectada a Internet, usted necesita un firewall". La decisión es así de fácil. No obstante, usted probablemente tendrá que considerar varios factores. Comience con las inquietudes básicas que usted tendría sobre cualquier otro sistema de seguridad.

¿Tengo alguna información que valga la pena proteger?

Tome en cuenta:

- La información confidencial sobre sus clientes, proveedores y empleados que podrían exponerlo a un proceso legal si permitiera que alguien más la accediera
- La propiedad intelectual que le proporciona una ventaja competitiva en el mercado
- Los registros esenciales de su negocio que tendrían que ser recuperados y recreados

No siempre es bueno suponer que nadie más está interesado en sus datos. Algunos "hackers" operan sin tener algún beneficio en mente. Simplemente roban sus datos o corrompen su sistema por el hecho de poder hacerlo.

¿Mi información esencial está adecuadamente protegida?

La realidad es que si usted posee propiedad electrónica de gran valor, existe una gran posibilidad de que no esté tan bien protegida como cree. Usted puede contribuir mucho para proteger su sistema:

- Realizando respaldos de su información al final de la jornada de trabajo
- Protegiendo las carpetas no compartidas con claves de acceso o políticas estrictas de acceso
- Utilizando su router o navegador de acceso remoto para filtrar el tráfico entrante proveniente de todos los sitios, excepto de fuentes confiables

Desafortunadamente, los "hackers" cuentan con herramientas de software sofisticadas. Con suficiente tiempo y determinación, un "hacker" habilidoso puede sobrepasar las medidas de seguridad de su empresa.

ÍNDICE

¿Por qué implementar un Firewall?	
¿Realmente existe algún riesgo?	1
¿Qué es un Firewall?	2
Tipos de ataque	2
Tecnologías de Firewall	3
Características y funciones adicionales de un Firewall	4
Selección del Firewall	5
Diseñando un Firewall para su red	6
Conclusión	6

3DES Estándar de encriptación de datos (168 bits)

DMZ Zona desmilitarizada

DoS Negación de servicio

FTP Protocolo de transferencia de archivos

HTTP Protocolo de transferencia de hipertexto

ICSA Asociación Internacional de Seguridad de Computadoras

LAN Red local

NAT Conversión de direcciones de red

POP3 POP 3 versión 3

SMTP Protocolo de transferencia de e-mail

TCP/IP Protocolo de control de transmisión / Protocolo de Internet

VPN Red privada virtual

WAN Red de área amplia

Si logra hacerlo, también puede ejecutar programas y cambiar o acceder a sus claves de acceso. Es por esta razón que si su empresa posee datos valiosos y su red está expuesta a sistemas externos, es muy probable que usted necesite un firewall.

¿Qué es un Firewall?

Un firewall es un sistema que permite ejercer políticas de control de acceso entre dos redes, tales como su red LAN privada e Internet, una red pública y vulnerable. El firewall define los servicios que pueden accederse desde el exterior y viceversa. Los medios a través de los cuales se logra esta función varían notoriamente, pero en principio, un firewall puede considerarse como: un mecanismo para bloquear el tráfico y otro para permitirlo. Un firewall constituye más que una puerta cerrada con llave al frente de su red. Es su servicio de seguridad particular.

Los firewalls son también importantes porque le proporcionan un único "punto de restricción", donde se pueden aplicar políticas de seguridad y auditoría. Un firewall proporciona al administrador de la red, entre otros datos, información acerca del tipo y cantidad de tráfico que ha fluído a través del mismo y cuántas veces se ha intentado violar la seguridad. De manera similar a un sistema de circuito cerrado de TV, su firewall no sólo bloquea el acceso, sino también monitorea a aquellos que están merodeando y le ayuda a identificar los usuarios que han intentado violar su seguridad.

Objetivo básico de un Firewall

En pocas palabras, un firewall lleva a cabo tres funciones para proteger su red:

- Bloquea los datos entrantes que pueden contener el ataque de un "hacker"
- Oculta la información acerca de la red, haciendo que todo parezca como si el tráfico de salida se originara del firewall y no de la red. Esto también se conoce como NAT (Network Address Translation)
- Filtra el tráfico de salida, con el fin de restringir el uso de Internet y el acceso a localidades remotas

Niveles de filtración

Un firewall puede filtrar tanto el tráfico que sale como el que entra. Debido a que el tráfico que entra constituye

una amenaza mucho mayor para la red, éste es inspeccionado mucho más estrictamente que el tráfico que sale.

Al momento de evaluar productos de hardware y software de firewall, probablemente escuchará acerca de tres tipos de filtración:

- La filtración que bloquea cualquier dato de entrada que no haya sido específicamente solicitado por un usuario de la red
- La filtración basada en la dirección del remitente
- La filtración basada en el contenido de la comunicación

Imagínese que los niveles de filtración son un proceso de eliminación. El firewall inicialmente determina si la transmisión entrante ha sido solicitada por un usuario de la red y, de no ser así, la rechaza. Luego, cualquier dato que haya sido permitido se inspecciona cuidadosamente. El firewall verifica la dirección de la computadora del remitente, con el fin de certificar que proviene de un sitio confiable. Finalmente, se encarga de verificar el contenido de la transmisión.

Tipos de ataque

Antes de definir exactamente qué tipo de firewall necesita, debe entender la naturaleza de los tipos de amenazas de seguridad que existen. Internet es una extensa comunidad, y como tal, existen sujetos buenos y malos. Los sujetos malos abarcan desde individuos incompetentes que provocan daños sin intención, hasta "hackers" habilidosos y maliciosos que planean ataques deliberados a las empresas, utilizando Internet como su arma preferida.

Por lo general, existen tres tipos de ataques que pueden potencialmente impactar en forma negativa a su negocio:

- *Hurto de información:* Robo de información confidencial, tales como registros de clientes y empleados, o hurto de propiedad intelectual de su empresa
- *Sabotaje de información:* Cambios a la información, en un intento de dañar la reputación de una persona o empresa. Como por ejemplo, elaborando cambios a los registros educativos y médicos de los empleados o publicando contenido malintencionado en su sitio Web.

- *Negación de servicio (DoS, Denial of Service)*: Bloqueo de los servidores o red de su empresa, de forma que los usuarios legítimos no puedan acceder a la información o, para impedir la operación normal de su empresa.

Intentos para lograr acceso

Un “hacker” puede intentar obtener acceso a su red por diversión o ambición. Un intento de lograr acceso, por lo general, comienza con la recolección de información acerca de la red. Luego, esta información se utiliza para realizar un ataque con un propósito específico, ya sea para apoderarse o destruir datos.

Un “hacker” puede usar un scanner de puertos, un software que permite ver la estructura de la red. Esto les permite averiguar cómo está estructurada la red y qué software se está ejecutando en la misma.

Una vez que el “hacker” tiene una idea de la estructura de la red, puede aprovecharse de todas las debilidades conocidas del software y utilizar las herramientas de “hacking” para ocasionar estragos en su ambiente de TI. Es posible, inclusive, ingresar a los archivos de los administradores y dejar en blanco los discos, aunque una buena clave de acceso por lo general puede dificultar esta tarea.

Afortunadamente, un buen firewall es inmune a un escaneo de puertos y, a medida que se desarrollan nuevos scanners de puertos para evadir esta inmunidad, los fabricantes de firewall producen actualizaciones para preservarla.

Ataques de negación de servicio (DoS, Denial of Service)

Los ataques DoS son puramente maliciosos. No producen ningún beneficio para el “hacker”, más que el “placer” de que las redes, o parte de ellas, queden inaccesibles para sus usuarios. Un ataque DoS sobrecarga el sistema de manera que lo deja inhabilitado, negando así la posibilidad de utilizar los servicios de la red. Los “hackers” envían grandes paquetes de datos o programas que requieren que el sistema responda continuamente a comandos falsos.

Para llevar a cabo un ataque DoS, un “hacker” tiene que conocer la dirección IP del sistema que va a atacar, pero un buen firewall no revela su propia dirección IP

o las direcciones IP de la red. El “hacker” puede pensar que se ha comunicado con la red, cuando en realidad sólo se ha contactado con el firewall y, desde ese punto, no es posible bloquear la red. Así mismo, cuando un “hacker” lanza un ataque, algunos firewalls pueden identificar los datos como tal, rechazar los datos, alertar al administrador del sistema y realizar un seguimiento del origen de los datos, para capturar al individuo que los envió.

Tecnologías de Firewall

Hay firewalls de todo tipo, tamaño y precio. Para seleccionar el firewall correcto, usted debe tomar en cuenta los requerimientos de su negocio y el tamaño de su red. Esta sección aborda los diferentes tipos y tecnologías de firewall y los formatos disponibles en el mercado.

Lo esencial es que, independientemente del tipo de firewall o funcionalidad que escoja, usted debe asegurarse de que se trata de una solución segura y de que ha sido certificada por una organización confiable, como por ejemplo, la Asociación Internacional de Seguridad de Computadoras (ICSA). ICSA clasifica los firewalls en tres categorías: firewalls de filtración de paquetes, servidores proxy a nivel de aplicación y firewalls de inspección de paquetes (SPI, Stateful Packet Inspection).

Firewall de filtración de paquetes

Cada computadora de una red tiene una dirección comúnmente llamada dirección IP. Un firewall de filtración de paquetes verifica la dirección de donde proviene el tráfico entrante y rechaza cualquier tráfico que no coincida con la lista de las direcciones confiables. El firewall de filtración de paquetes utiliza reglas para negar el acceso, según la información contenida en el paquete, como por ejemplo: el número del puerto TCP/IP, la dirección IP de la fuente/origen o el tipo de datos. Las restricciones pueden ser tan estrictas o tan flexibles como usted requiera.

Un router común de una red puede filtrar el tráfico por dirección, pero los “hackers” tienen un pequeño truco llamado “spoofing” de IP, con el cual los datos parecen provenir de una fuente confiable o incluso de una dirección de su propia red. Desafortunadamente, el firewall de filtración de paquetes es propenso al “spoofing” de IP y son muy difíciles de configurar. Cualquier error en su configuración, puede dejarlo vulnerable a los ataques.

Servidor Proxy a nivel de aplicación

Un servidor proxy a nivel de aplicación examina la aplicación usada por cada paquete IP, con el fin de verificar su autenticidad. El tráfico de cada aplicación, tales como HTTP para la Web, FTP para la transferencia de archivos y SMTP/POP3 para e-mail, por lo general, requieren de la instalación y configuración de un proxy de aplicaciones diferente. Con frecuencia, los servidores requieren que los administradores reconfiguren su red y aplicaciones (por ejemplo los navegadores de Web) para soportar el proxy, lo cual puede resultar en un proceso muy trabajoso.

Firewall de SPI

Constituye la última generación en la tecnología de firewall. Los expertos en Internet consideran que SPI es la tecnología más avanzada y segura, gracias a que examina todos los componentes de un paquete IP para decidir si acepta o rechaza la comunicación.

El firewall mantiene un registro de todas las solicitudes de información que se originan de su red. Luego, inspecciona toda comunicación entrante para verificar si realmente fue solicitada y rechaza cualquiera que no lo haya sido. Los datos solicitados aprobados proceden al siguiente nivel de inspección y el software determina el estado de cada paquete de datos.

Características y funciones adicionales de un Firewall

Además de las capacidades de seguridad estándares, se ha integrado una gran cantidad de características y funciones adicionales a los productos de firewall. Entre estas figuran: soporte para servidores públicos de Web y correo electrónico, por lo general llamada zona desmilitarizada (DMZ), filtración de contenido, soporte de encriptación de VPN y de antivirus.

Firewalls con zona desmilitarizada (DMZ)

Un firewall que provee protección DMZ es una solución efectiva para empresas que ofrecen a sus clientes la posibilidad de conectarse a su red a partir de cualquier medio externo, ya sea a

través de Internet o cualquier otra ruta, como por ejemplo, una compañía de "hosting" de Web o que vende sus productos o servicios por Internet.

La decisión de optar por un firewall con DMZ debe basarse en la cantidad de usuarios externos que acceden a la red y la frecuencia con la que lo hacen.

Un firewall con DMZ crea un área de información protegida ("desmilitarizada") en la red. Los usuarios externos pueden ingresar al área protegida, pero no pueden acceder al resto de la red. Esto permite a los usuarios externos acceder a la información que usted quiere que vean, pero previene que obtengan información no autorizada.

Filtración de contenido

Un filtro de sitios Web o filtro de contenido extiende las capacidades del firewall para bloquear el acceso a ciertos sitios Web. Usted puede usar esta función adicional para asegurarse de que sus empleados no accedan contenido inapropiado, como por ejemplo, material pornográfico o racista. Esta funcionalidad le permite definir categorías de material inadecuado y obtener un servicio que lista miles de sitios Web que incluyen dicho tipo de material. Como siguiente paso, puede escoger si quiere bloquear totalmente el acceso a estos sitios o permitir su uso, pero manteniendo un registro del mismo. Tal servicio debe actualizar automática y regularmente la lista de sitios Web que no pueden ser accedidos.

Redes Privadas Virtuales (VPN)

Una VPN es una red privada de datos que utiliza la infraestructura de la red pública, es decir, Internet. El propósito de una red VPN es ofrecer a las empresas las mismas capacidades de las líneas telefónicas privadas, pero a un costo mucho menor. Una red VPN permite compartir recursos públicos en forma segura, mediante el uso de técnicas de encriptación, garantizando así que solamente los usuarios autorizados puedan ver o entrar en la red privada de la empresa.

Hoy en día, las redes VPN son consideradas por las empresas como un medio rentable de conectar en forma segura sus sucursales, trabajadores remotos, socios y clientes principales a sus redes LAN privadas. Una creciente cantidad de firewalls ahora

cuenta con capacidades de encriptación VPN, ya sea integradas o como característica opcional. Este recurso ofrece a las empresas una alternativa sencilla y rentable, en comparación con las líneas dedicadas tradicionales o el acceso remoto a través de módem.

Al momento de implementar una VPN, usted necesita asegurarse de que todos los dispositivos soporten el mismo nivel de encriptación y que proporcione suficiente seguridad. A la fecha, el nivel más avanzado de encriptación públicamente disponible es el estándar 3DES de 168 bits que, según los expertos de seguridad, es inquebrantable. Uno de los factores que deben tenerse en cuenta, es que entre más avanzado sea el nivel de encriptación, mayor capacidad de procesamiento requerirá el firewall. Un pequeño número de proveedores ofrece ahora la aceleración de VPN por hardware, con el fin de optimizar el rendimiento del tráfico VPN.

Protección a través de antivirus

Todos debemos preocuparnos seriamente por las amenazas de los virus, uno de los esquemas más nocivos de "hacking" de computadoras. Los usuarios pueden dañar rápidamente toda una red si, inadvertidamente, bajan material desconocido o diseminan virus peligrosos en las redes. Empresas de todo tipo y tamaño han perdido enormes cantidades de dinero, debido al impacto negativo en la productividad y los costos de reparación de la red causados por un virus

Los firewalls no están diseñados para remover o limpiar virus. No obstante, pueden ayudar a detectarlos, lo cual es un factor esencial de cualquier plan de protección contra virus.

Es importante observar que el firewall sólo puede proteger la red a partir del dispositivo de WAN al cual está conectado. Un servidor de acceso remoto o una PC con un módem puede servir como puerta de acceso a la red, el cual puede burlar las medidas de seguridad del firewall. Lo mismo puede ocurrir cuando un empleado introduce un diskette infectado con un virus en su PC. El lugar más apropiado para instalar el software antivirus es en la PC de cada usuario. No obstante, un firewall puede contribuir a la detección de virus, exigiendo que cada usuario que ingrese a Internet o baje correo

electrónico, utilice, como mínimo, la última versión del software antivirus.

Selección del Firewall

Las funciones de un firewall pueden implementarse ya sea como software o como una adición a su router o gateway. Alternativamente, la demanda de los dispositivos dedicados de firewall está creciendo, principalmente debido a su facilidad de uso, mejor rendimiento y bajo costo.

Firewalls basados en routers / firmware

Algunos routers proveen capacidades limitadas de firewall. Estas pueden incrementarse con software u opciones de firmware adicional. No obstante, es importante que tenga cuidado de no sobrecargar su router con servicios adicionales de firewall. Además, es posible que algunas funciones de firewall, como VPN, DMZ, filtración de contenido o protección a través de antivirus, no estén disponibles o sean muy costosas de implementar.

Firewalls basados en software

Por lo general, los firewalls basados en software son aplicaciones sofisticadas y complejas que se ejecutan en servidores dedicados UNIX o NT. Estos productos se tornan aún más costosos cuando usted suma los costos de software, sistema operativo, hardware de servidor y mantenimiento continuo requerido para soportar su implementación.

Resulta esencial también que el administrador del sistema monitoree constantemente e instale las actualizaciones más recientes de seguridad y del sistema operativo, tan pronto como se encuentren disponibles. Sin estas actualizaciones que cubren los nuevos peligros de seguridad, el software de firewall puede volverse totalmente inservible.

Dispositivos de firewall dedicados

La mayoría de los dispositivos de firewall son sistemas de hardware dedicados. Estos dispositivos son menos susceptibles a las fallas de seguridad inherentes de los sistemas operativos Windows NT o UNIX, gracias a que integran sistemas operativos desarrollados específicamente para utilizarse como firewall. Estos firewalls de alto rendimiento han sido diseñados para satisfacer los altos requerimientos de

rendimiento o del procesador, exigidos por los firewalls SPI.

Debido a que no es necesario fortalecer el sistema operativo, por lo general, los dispositivos de firewall son más fáciles de instalar y configurar que los productos de firewall de software. Estos ofrecen potencialmente un nivel de instalación "Plug-and-Play", requieren mínimo mantenimiento y una solución completa. También constituyen una solución rentable en comparación con otras implementaciones de firewall.

Diseñando un Firewall para su red

Una vez que esté familiarizado con los diferentes tipos de firewall disponibles en el mercado, el siguiente paso es definir sus propias políticas de firewall. Por ejemplo, ¿el firewall rechazará explícitamente todos los servicios, excepto aquellos que son críticos para conectarse a Internet? o ¿su objetivo será proveer un esquema de acceso comprobado, de forma que no asuma riesgo alguno? Estas decisiones tienen que ver más con las políticas que con la ingeniería del firewall.

La siguiente decisión es optar por el nivel de monitoreo, redundancia y control que usted necesita. Esto requiere un análisis de las necesidades, inclusive la evaluación de riesgos, para luego determinar los requisitos, por lo general conflictivos, y finalmente decidir qué solución se implementará.

En lo que respecta a firewalls, usted debe dar mayor énfasis a la seguridad que a la conectividad. Como estándar, debe considerar el bloqueo general de todos los servicios, excepto aquellos que realmente necesita, analizándolos caso por caso. Su tarea será mucho más sencilla si decide bloquear todo, excepto un conjunto específico de servicios.

Conclusión

Las fallas de seguridad son reales y muy peligrosas. Hoy en día, todas las empresas están conscientes de la facilidad con que pueden ser víctimas de ataques aleatorios o deliberados y del daño que pueden causar. Una buena noticia para su empresa es que 3Com Corporation también está consciente de estas amenazas y, como resultado, está desarrollando soluciones de seguridad más sólidas y eficientes. Tanto empresas como oficinas remotas pueden beneficiarse de las soluciones de firewall de 3Com, las cuales son menos costosas y complicadas que las soluciones de firewall tradicionales.

Aunque los firewalls son apenas uno de los componentes de un sistema de seguridad, constituyen un componente esencial y las empresas deben invertir el tiempo para evaluar el sistema que mejor se ajuste a sus necesidades, para luego implementarlo a la brevedad posible. Las deficiencias de seguridad son un peligro constante y no existe mejor oportunidad para proteger la valiosa información de su empresa, que implementar un firewall hoy mismo.



Oficinas Corporativas de 3Com Corporation, 5400 Bayfront Plaza, P.O. Box 58145 Santa Clara, CA 95052-8145, EE.UU.

Para mayor información acerca de las soluciones 3Com, visite: www.3com.com

La información contenida aquí representa el punto de vista de 3Com al momento de la publicación de este documento. Dado que 3Com debe adaptarse a las condiciones cambiantes del mercado, este documento no debe interpretarse como un compromiso de parte de 3Com y 3Com no puede garantizar la exactitud de cualquier información presentada después de la fecha de publicación. Este documento es exclusivamente de carácter informativo. 3Com no ofrece garantías, explícitas o implícitas, en este documento.

Copyright © 2001 3Com Corporation. Todos los derechos reservados. 3Com y el logotipo de 3Com son marcas registradas de 3Com Corporation. Todos los demás nombres de empresas y productos pueden ser marcas registradas de sus respectivos propietarios. Producido en los EE.UU. 503090-001S 01/01