

Firewalls y Seguridad en Internet

1. Firewalls y seguridad en Internet

Introducción.

La seguridad es el principal tema a tratar cuando una organización desea conectar su red privada a Internet. Sin tomar en cuenta el tipo de negocios, se ha incrementado el número de usuarios de redes privadas por la demanda de acceso a los servicios de Internet. Adicionalmente los usuarios corporativos buscan las ventajas que ofrecen las páginas web y los servidores FTP de acceso público.

Los administradores de red tienen que incrementar la seguridad de sus sistemas, debido a que se expone la privacidad de sus datos así como la infraestructura de su red.

Para proveer el nivel de protección requerida, la organización necesita seguir una política de seguridad que evite el acceso no-autorizado a los recursos de la red privada, y protegerse contra la exportación no autorizada de información.

Aún si una organización no está conectada al Internet, debería establecerse una política de seguridad interna para administrar el acceso de usuarios a porciones de red y proteger la información secreta.

1.1. Firewalls

Un Firewall de sistema o grupo de sistemas impone una política de seguridad entre la organización de red privada y el Internet.

El firewall determina a cuáles de los servicios de red se puede acceder desde fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización.

Para que un firewall sea efectivo, todo tráfico de información a través de Internet deberá pasar a través del mismo, donde podrá ser inspeccionada la información. El firewall podrá autorizar o no el paso, y él mismo deberá ser inmune a la penetración. Desafortunadamente, este sistema no ofrece protección una vez que el agresor lo traspasa o permanece entorno a este.

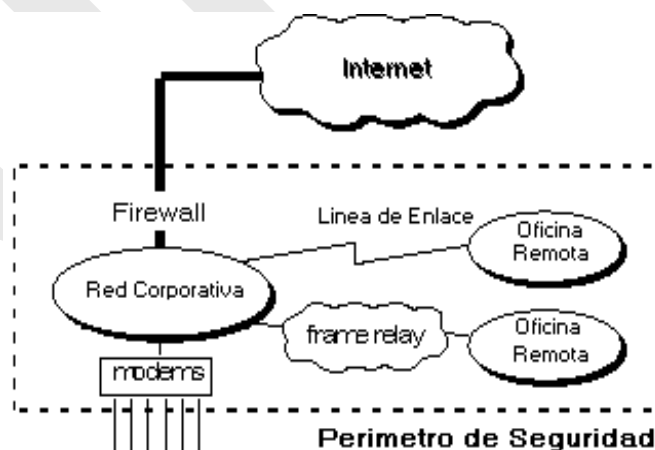


Ilustración 1-1

La Política De Seguridad Crea Un Perímetro De Defensa.

Un firewall de Internet no es justamente un ruteador, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñado para proteger las fuentes de información.

Esta política de seguridad podrá incluir publicación de guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dial-in y dial-out, reglas de encriptación de datos y discos, normas de protección de virus, y entrenamiento.

Todos los puntos potenciales de ataque en la red deberán protegerse con el mismo nivel de seguridad. Un firewall de Internet sin una política de seguridad clara es como poner una puerta de acero en una tienda.

1.1.1.1. Beneficios de un firewall en Internet

Los firewalls en Internet administran los accesos posibles de Internet a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se expone al ataque de otros servidores en e Internet. Esto significa que la seguridad en la red privada depende de la “dureza” con que cada uno de los servidores cuenta.

El firewall permite al administrador de la red definir un “choke point” (embudo), manteniendo al margen los usuarios no-autorizados de fuera de la red, prohibiendo la entrada o salida de tráfico que pueda vulnerar los servicios de la red, y proporcionar protección contra varios tipos de ataques posibles.

Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, puesto que una vez que se consolida la seguridad en el sistema firewall, se verifica su eficacia respecto de seguridad distribuida en cada uno de los servidores de la red privada.

El firewall ofrece un punto de monitoreo de la seguridad, donde se genera una alarma en caso de actividad sospechosa, o suceda algún problema en el transito de los datos. Es importante que el administrador audite y lleve una bitácora del trafico significativo a través del firewall. También es importante que el administrador de la red examine regularmente los registros de base. Es ineficaz un firewall, si el administrador de red desconoce que el sistema ha sido exitosamente atacado!.

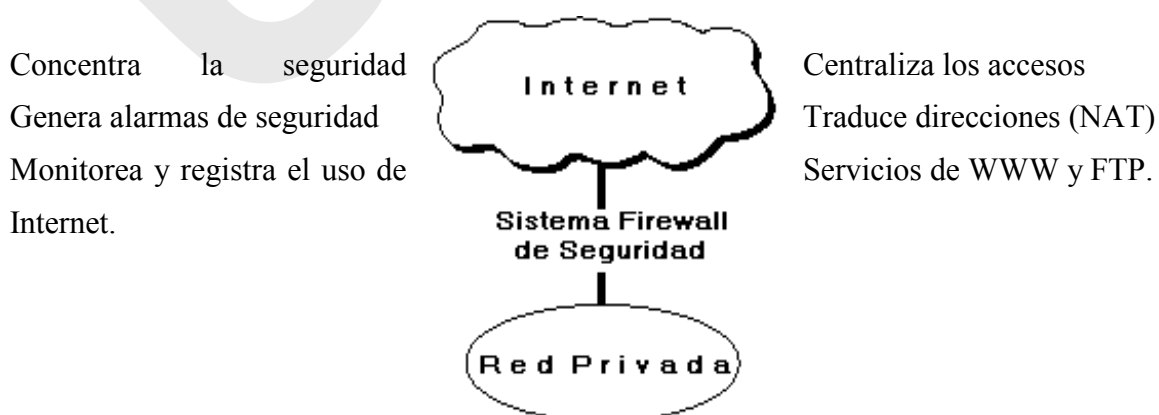


Ilustración 1-2

Beneficios De Un Firewall De Internet.

Con el paso de los años, Internet ha experimentado una crisis en el sistema de asignación de direcciones, y el direccionamiento IP es insuficiente respecto de los requerimientos, debido a esto ya no es posible registrar suficientes direcciones IP para responder a la población de usuarios que demanda servicios..

Un firewall es un lugar lógico para desplegar un Traductor de Direcciones de Red (NAT)¹ esto puede ayudar aliviando el espacio de direccionamiento, acortando y eliminando lo innecesario y permitiendo reenumerar cuando la organización cambie del Proveedor de Servicios de Internet (ISPs)².

Un firewall de Internet es el punto perfecto para auditar o registrar el uso de Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda,

Un firewall de Internet ofrece un punto de reunión para la organización. Si una de sus metas es proporcionar y entregar servicios, información a consumidores, el firewall de Internet es ideal para desplegar servidores WWW y FTP.

Finalmente, el firewall puede presentar los problemas que genera un punto de falla simple. Enfatizando si este punto de falla se presenta en la conexión al Internet, aun así la red interna de la organización puede seguir operando - únicamente el acceso a Internet esta perdido - .

La preocupación principal del administrador de red, son los múltiples accesos a Internet. Estos puntos de acceso son los puntos potenciales de ataque a la red interna que tendrán que ser monitoreados regularmente!

1.1.2. Limitaciones de un firewall

Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.

Por ejemplo, si existe una conexión dialup sin restricciones es posible ingresar a la red protegida, a través de un usuario que realice una conexión SLIP o PPP a Internet.

Este tipo de conexiones disminuyen la seguridad provista por el firewall, creando una puerta de ataque. Los usuarios deben estar concientes de que este tipo de conexiones no son permitidas como parte de integral de la arquitectura de la seguridad en la organización.

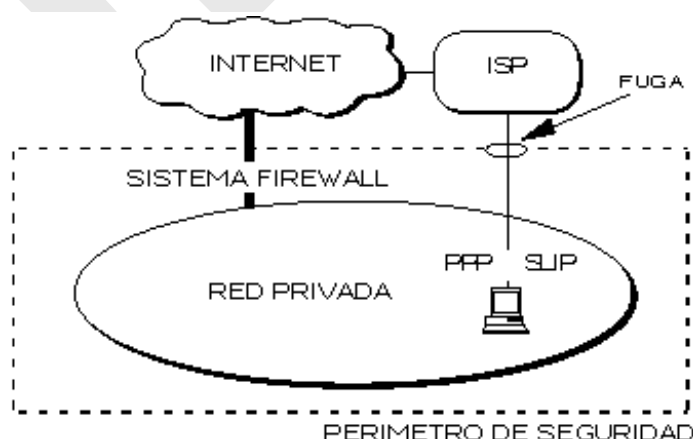


Ilustración 1-3 Conexión Circunvecina Al Firewall De Internet.

¹ Network Address Translator.

² Internet Service Providers.

El firewall no puede protegerse de las amenazas a que esta sometido por sabotaje o usuarios inconscientes. El firewall no puede prohibir que espías corporativos copien datos importantes en disquetes o tarjetas PCMCIA y las retiren de la empresa.

El firewall no puede proteger contra los ataques de la “Ingeniería Social”, por ejemplo si un Hacker que pretende ser un supervisor o un nuevo empleado despistado, persuade al menos sofisticado de los usuarios a que le permita usar su contraseña al servidor corporativo o que le permita el acceso “temporal” a la red.

Para controlar estas situaciones, los empleados deberían ser advertidos acerca de los tipos posibles de ataque social, y cambiar sus contraseñas periódicamente.

El firewall tampoco puede proteger ni protegerse contra los ataques posibles a la red interna debido a archivos y software infectado por virus.

El firewall de Internet no puede contar con un sistema preciso de SCAN³ para cada tipo de virus que se puedan presentar en los archivos que pasan a través de el.

La solución consiste en hacer que la organización sea consciente de la necesidad de instalar software antivirus en cada terminal, para protegerse de los virus que llegan por medio de disquetes o cualquier otra fuente.

Finalmente, el firewall de Internet no puede protegerse contra los ataques posibles derivados de la transferencia de datos, estos ocurren cuando aparentemente datos inocuos son enviados o copiados a un servidor interno y son ejecutados despachando un ataque.

Por ejemplo, una transferencia de datos podría causar que un servidor modificara los archivos relacionados con la seguridad, haciendo mas fácil el acceso de un intruso al sistema.

Los servidores Proxy son un excelente medio de prohibir las conexiones directas de agentes externos y reducen las amenazas posibles por los ataques con transferencia de datos.

1.2. Herramientas del intruso

Es difícil describir el ataque “típico” de un hacker debido a que los intrusos poseen diferentes niveles de técnicos y experiencia y son motivados por diversos factores. Algunos hackers son incentivados por el desafío, otros intentan provocar inconvenientes, y otros substraen datos delicados para algún beneficio propio.

1.2.1. Recolección de información

El primer paso es saber en que forma se recolecta la información. La meta del intruso es obtener una base de datos que contenga la organización de la red y la información acerca de los servidores residentes.

Esta es una lista de herramientas que un hacker puede usar para obtener esta información:

- El protocolo SNMP, puede utilizarse para examinar la tabla de ruteo en un dispositivo inseguro, esto sirve para aprender los detalles mas íntimos acerca de la topología de red en una organización.
- El programa TraceRoute puede revelar el numero de redes intermedias y los ruteadores en torno al servidor específico.
- El protocolo Whois, es un servicio de información que provee datos acerca de todos los dominios DNS y el administrador del sistema responsable para cada dominio.

³ System Control Antivirus Network.

- Puede accederse a servidores DNS para obtener una lista de las direcciones IP y sus correspondientes Nombres (Programa Nslookup).
- El protocolo Finger puede revelar información detallada acerca de los usuarios (nombres de Login, números telefónicos, tiempo y última sesión, etc.) de un servidor específico.
- El programa Ping puede ser empleado para localizar un servidor particular y determinar si se encuentra operativo. Esta simple herramienta puede ser usada como un programa de escaneo pequeño que por medio de llamadas a la dirección de un servidor haga posible construir una lista de los servidores residentes en la red.

1.2.2. Sondeo del sistema para debilitar la seguridad

Después que obtiene la información de red perteneciente a una organización, el hacker trata de explorar cada uno de los servidores mediante herramientas automáticas, para debilitar la seguridad, .

- Una vez obtenida una lista pequeña de la vulnerabilidad de servicios en la red, un intruso puede escribir un pequeño programa que intente conectarse a un puerto especificando el tipo de servicio que está asignado al servidor en cuestión. La corrida del programa presenta una lista de los servidores que soportan servicio de Internet y están expuestos al ataque.
- Están disponibles varias herramientas del dominio público, tal es el caso como el Rastreador de Seguridad en Internet (ISS)⁴ o la Herramienta para Análisis de Seguridad para Auditar Redes (SATAN)⁵, el cual puede rastrear una subred o un dominio y ver las posibles fugas de seguridad. Estos programas determinan la debilidad de cada uno de los sistemas con respecto a varios puntos de vulnerabilidad habituales en un sistema.
- El intruso usa la información recolectada por este tipo de rastreadores para intentar el acceso no-autorizado al sistema de la organización.

Un administrador de redes debería usar estas herramientas en su red privada para descubrir los puntos potencialmente débiles y determinar que servidores necesitan ser remendados y actualizados en el software.

1.2.3. Acceso a sistemas protegidosⁱ

El intruso utiliza los resultados obtenidos a través de las pruebas para poder intentar acceder a los servicios específicos de un sistema.

Después de tener el acceso al sistema protegido, el hacker tiene disponibles las siguientes opciones:

- Puede atentar destruyendo posteriormente toda evidencia del asalto y crear nuevas fugas en el sistema o partes subalternas para seguir teniendo acceso sin que el ataque original sea descubierto.
- Pueden instalar paquetes de sondeo que incluyan códigos binarios conocidos como “caballos de Troya” enmascarando su actividad. Los paquetes de sondeo colectan las cuentas y contraseñas para los servicios de Telnet y FTP permitiendo al hacker expandir su ataque a otras máquinas.

⁴ Internet Security Scanner .

⁵ Security Analysis Tool for Auditing Networks.

- Pueden encontrar otros servidores que realmente comprometan al sistema. Esto permite al hacker usando un servidor sencillo explotar la vulnerabilidad de todos aquellos que se encuentren en la red corporativa.
- Si el hacker puede obtener acceso privilegiado en un sistema compartido, podrá leer el correo, buscar en archivos, etc

1.3. Bases para el diseño decisivo del firewall

Cuando se diseña un firewall de Internet, se deben tener en cuenta:

- * Posturas sobre la política del Firewall.
- * La política interna propia de la organización para la seguridad total.
- * El costo financiero del Proyecto “Firewall”.
- * Los componentes o secciones del Firewall.

1.3.1. Políticas del firewall.

Las posturas del sistema firewall describen la filosofía fundamental de la seguridad en la organización. Estas son dos posturas diametralmente opuestas que la política de un firewall de Internet puede tomar:

- “Todo lo que no está específicamente permitido, esta prohibido”
- “Todo lo que no está específicamente prohibido esta permitido”

la primera postura asume que un firewall puede obstruir todo el trafico y cada uno de los servicios o aplicaciones, las que serán posteriormente implementadas caso por caso.

La desventaja es que el punto de vista de “seguridad” es mas importante que - facilitar el uso - de los servicios.

La segunda postura asume que el firewall puede permitir todo el trafico y que cada servicio potencialmente peligroso necesitara ser aislado posteriormente, caso por caso.

Esta propuesta crea ambientes mas flexibles al disponer mas servicios para los usuarios de la comunidad. La desventaja de esta postura se basa en la importancia de “facilitar el uso” que la propia - seguridad - del sistema.

También, el administrador de la red puede incrementar la seguridad del sistema conforme crece la red.

Política interna de seguridad

Un firewall de Internet no se aplica en forma aislada - es parte de la política de seguridad total en una organización -

La política de seguridad define todos los aspectos referentes al perímetro de defensa.

Para que sea exitosa, la organización debe conocer que es lo que se esta protegiendo.

La política de seguridad se basara en el análisis de la seguridad, la asesoría en caso de riesgo, y la situación del negocio.

Si no se posee información detallada de la política a seguir, aun con un firewall cuidadosamente desarrollado y armado, se estará exponiendo la red privada a un posible atentado.

1.3.2. Costo del firewall

¿Cuanto puede ofrecer una organización por su seguridad?, un simple paquete de filtrado firewall puede tener un costo mínimo si la organización necesita un ruteador conectado a Internet, si dicho paquete está incluido como estándar del equipo. Un sistema comercial de firewall incrementa la seguridad pero su costo puede ser de \$1,000 hasta \$50,000 dólares, dependiendo de la complejidad y el número de sistemas protegidos.

Si la organización posee personal capacitado, puede usarse un software firewall de dominio público, pero este ahorro de recursos repercute en términos del tiempo de desarrollo y despliegue del sistema firewall. Por otra parte, requiere soporte continuo para la administración, mantenimiento general, actualización de software, reparación de seguridad, e incidentes de manejo.

1.3.3. Componentes del sistema firewall

Después de las decisiones previas, la organización puede determinar específicamente los componentes del sistema. Un firewall típico se compone de uno, o una combinación, de los siguientes componentes.

- Ruteador Filtra-paquetes.
- Gateway a Nivel-aplicación.
- Gateway a Nivel-circuito.

1.4. *Edificando obstáculos: ruteador filtra-paquetes*

Este ruteador toma las decisiones de rehusar/permitir el paso de cada uno de los paquetes que son recibidos. El ruteador examina cada datagrama para determinar si ha sido aprobado por sus reglas.

Las reglas de filtrado se basan en revisar la información que poseen los paquetes en su encabezado,

Esta información consiste en la dirección IP fuente, la dirección IP destino, el protocolo de encapsulado (TCP, UDP, ICMP, o IP tunnel), el puerto fuente TCP/UDP, el puerto destino TCP/UDP, el tipo de mensaje ICMP, la interfaz de entrada del paquete, y la interfaz de salida del paquete. Si las reglas permiten el paso del paquete, este se desplazará de acuerdo a la información de la tabla de ruteo, si las reglas niegan el paso, el paquete es descartado. Si estos no corresponden a las reglas, un parámetro configurable, determina descartar o desplazar el paquete.

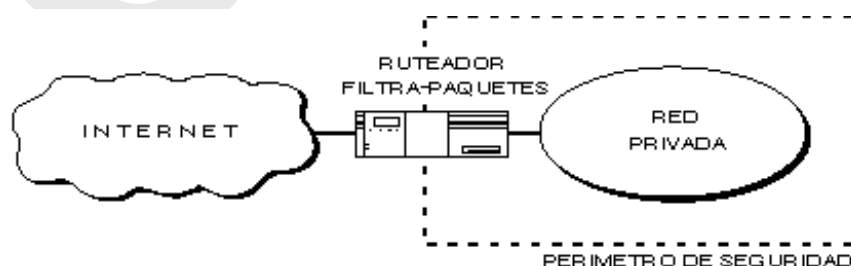


Ilustración 1-4 Ruteador Filtra-Paquetes.

1.4.1. Servicio dependiente del filtrado

Las reglas acerca del filtrado de paquetes a través de un ruteador para rehusar/permitir el tráfico son específicas, puesto que muchos servicios usan puertos TCP/UDP conocidos.

Por ejemplo, un servidor Telnet esta a la espera para conexiones remotas en el puerto 23 TCP y un servidor SMTP espera las conexiones de entrada en el puerto 25 TCP. Para bloquear todas las entradas de conexión Telnet, el ruteador simplemente descarta todos los paquetes que contengan el valor del puerto destino TCP igual a 23. Para restringir las conexiones Telnet a un limitado numero de servidores internos, el ruteador podrá rehusar el paso a todos aquellos paquetes que contengan el puerto destino TCP igual a 23 y que no contengan la dirección destino IP de uno de los servidores permitidos.

Algunas características típicas de filtrado que un administrador de redes podría solicitar en un ruteador filtra-paquetes para perfeccionar su funcionamiento serian:

- Permitir la entrada de sesiones Telnet únicamente a una lista específica de servidores internos.
- Permitir la entrada de sesiones FTP únicamente a los servidores internos especificados.
- Permitir todas las salidas para sesiones Telnet.
- Permitir todas las salidas para sesiones FTP.
- Rehusar todo el tráfico UDP.

1.4.2. Servicio independiente del filtrado

Este tipo de ataques ciertamente son difíciles de identificar usando la información básica de los encabezados debido a que son independientes del tipo de servicio. Los ruteadores pueden ser configurados para protegerse de este tipo de ataques, pero las reglas de filtrados son mas difíciles de especificar por cuanto se requiere información adicional que pueda ser estudiada y examinada por la tabla de ruteo. Se deben inspeccionar las opciones específicas de IP, revisando fragmentos especiales de edición, etc. Algunos ejemplos de este tipo de ataques incluyen:

Agresiones Originadas Por El Direcccionamiento IP.

En este tipo de ataque, el intruso transmite paquetes desde afuera pretendiendo pasar como servidor interno

Los paquetes poseen una dirección fuente IP falsa de un servidor interno del sistema

El agresor espera que usando este impostor se pueda penetrar al sistema para emplearlo como dirección fuente, autenticando los paquetes transmitidos y haciendo que los del servidor auténtico sean descartados. Los ataques por pseudo-fuentes pueden ser frustrados si descartamos la dirección fuente de cada paquete con una dirección fuente “interno” siempre que el paquete arrive por una de las interfaces del ruteador “externo”.

Agresiones Originadas en el Ruteador.

En un ataque de ruteo, la estación de origen especifica la ruta que un paquete deberá tomar cuando cruce a través de Internet. Este tipo de ataques son diseñados para cuantificar las debilidades de seguridad y encauzan al paquete por un inesperado camino a su destino. Los ataques originados en el ruteador pueden ser frustrados simplemente descartando todos los paquetes que contengan fuentes de ruteo opcionales.

Agresiones Por Fragmentación.

Por este tipo de ataques, se utilizan las características de fragmentación para crear fragmentos extremadamente pequeños obligando a la información del encabezado TCP a separarse en paquetes. Estos pequeños fragmentos son diseñados para evitar las reglas definidas por el filtrado de un ruteador examinando los primeros fragmentos y el resto pasa sin ser visto.

Una agresión de este tipo puede ser frustrada si se descartan todos los paquetes donde el tipo de protocolo es TCP y la fragmentación de compensación IP es igual a 1.

1.4.3. Beneficios del ruteador filtra-paquetes

La mayoría de sistemas firewall son desplegados usando únicamente ruteadores filtra-paquetes.

En otros casos se planifican los filtros y se configura el ruteador.

El costo de implementar el filtrado de paquetes no es alto; ya que los componentes básicos de los ruteadores incluyen paquetes de software para tal fin.

El acceso a Internet es generalmente provisto a través de interfaces WAN, optimizando la operación del ruteador moderando el tráfico y definiendo menos filtros. Finalmente, el ruteador de filtrado es por lo general transparente a los usuarios finales y a las aplicaciones por lo que no se requiere entrenamiento especializado o software específico que deba ser instalado en cada servidor.

1.4.4. Limitaciones del ruteador filtra-paquetes

Definir el filtrado de paquetes puede ser una tarea compleja porque el administrador de redes necesita hacer un detallado estudio de varios servicios de Internet, como los formatos del encabezado de los paquetes, y los valores específicos que se espera encontrar en cada campo.

Si las necesidades de filtrado son muy complejas, se necesitara soporte adicional con lo cual el conjunto de reglas puede hacer mas difícil la administración y comprensión del sistema.

Después de configurar las reglas de filtrado, será mas difícil la verificación posterior y modificación cuando sea necesario, aumentando el riesgo potencial de una verificación incompleta.

Cualquier paquete que pasa directamente a través de un ruteador puede ser potencialmente usado como parte inicial de un ataque dirigido de datos.

Este tipo de ataques ocurren cuando datos aparentemente inocuos se desplazan por el ruteador a un servidor interno. Si los datos contienen instrucciones ocultas, pueden causar que el servidor modifique su control de acceso y seguridad facilitando el acceso al sistema por parte del intruso.

Los ruteadores se optimizan para extraer la dirección destino IP de cada paquete, haciendo relativamente simple la consulta a la tabla de ruteo, y el desplazamiento de paquetes hacia la interfaz apropiada de la transmisión.

El filtrado de paquetes IP no es capaz de proveer el suficiente control sobre el tráfico.

Un ruteador Filtra-Paquetes puede permitir o negar un servicio en particular, pero no es capaz de comprender el contexto/dato del servicio.

Por ejemplo, un administrador de red necesita filtrar el tráfico de una capa de aplicación - limitando el acceso a un subconjunto de comandos disponibles por FTP o Telnet, bloquear la

importación de Mail o Newsgroups concerniente a tópicos específicos. Este tipo de control es muy perfeccionado a las capas altas por los servicios de un servidor Proxy y en Gateways a Nivel-aplicación.

1.5. *Edificando obstáculos: gateways a nivel-aplicación*

Los gateways a nivel-aplicación permiten al administrador de red la implementación de una política de seguridad mas estricta que la permitida por un ruteador filtra-paquetes.

En el gateway se instala un código de propósito-especial (un servicio Proxy) para cada aplicación deseada

Si el administrador de red no instala el código Proxy para la aplicación particular, el servicio no es soportado y no podrá desplazarse a través del firewall.

El código Proxy puede ser configurado para soportar únicamente las características específicas de una aplicación que el administrador de red considere aceptable, mientras se deniegan todas las otras.

Un aumento de seguridad de este tipo incrementa los costos en función del tipo de gateway seleccionado, los servicios de aplicaciones del Proxy, el tiempo y los conocimientos requeridos para configurar el gateway, y un decrecimiento en el nivel de los servicios que podrán obtener nuestros usuarios, dando como resultado un sistema carente de amigabilidad hacia los usuarios.

Como en todos los casos el administrador de redes debe de balancear las necesidades en seguridad, con la demanda de “fácil de usar” de la comunidad de usuarios.

Es importante notar que los usuarios tienen acceso a los servicios a través de un servidor Proxy, pero no podrán acceder al Gateway a nivel-aplicación. Si se permite a los usuarios accionar en el sistema de firewall, la seguridad se verá amenazada puesto que un intruso podría ejecutar actividades que comprometen la efectividad del sistema.

Por ejemplo, el intruso podría obtener el acceso de root, instalar un troyano, para recoger contraseñas, y modificar la configuración de los archivos de seguridad en el firewall.

1.5.1. Servidor de defensa

Un ruteador filtra-paquetes permite la circulación directa de los paquetes dentro y fuera del sistema, en cambio el Gateway a nivel-aplicación permite que la información circule entre los sistemas.

El principal problema, cuando se permite que los paquetes se intercambien dentro y fuera del sistema, se debe al servidor residente en los sistemas de protección de la red, el cual deberá asegurarse contra cualquier amenaza representada por los servicios permitidos.

Un Gateway a nivel-aplicación por lo regular es descrito como un “servidor de defensa” porque es un sistema diseñado específicamente blindado y protegido contra cualquier ataque. Hay varias características de diseño que son usadas para hacer mas seguro un servidor de defensa:

- ⇒ La plataforma de Hardware del servidor de defensa ejecuta una versión “segura” de su sistema operativo. Por ejemplo, si el servidor de defensa es una plataforma UNIX, se ejecutara una versión segura del sistema operativo UNIX que es diseñado específicamente para proteger los sistemas operativos vulnerables y garantizar la integridad del firewall.

- ⇒ Únicamente los servicios que el administrador de redes considere esenciales son instalados en el servidor de defensa. La lógica de operación es que si el servicio no está instalado, no puede ser atacado. Generalmente, en este servidor se instala un conjunto limitado de aplicaciones Proxy tales como Telnet, DNS, FTP, SMTP, y autenticación de usuarios.
- ⇒ El servidor de defensa podrá requerir una autenticación adicional para que el usuario acceda a los servicios Proxy. Por ejemplo, el servidor de defensa es ideal para colocar un sistema fuerte de supervisión de autorización (tal como la tecnología “una-sola vez” de contraseña donde una tarjeta inteligente genera un código de acceso único por medios criptográficos). Adicionalmente, cada servicio Proxy podrá requerir de autorización propia después que el usuario tenga acceso a su sesión.
- ⇒ Cada servicio Proxy es configurado para soportar únicamente un subconjunto de aplicaciones estándar dentro de un conjunto de comandos. Si un comando estándar no es soportado por la aplicación Proxy, no está disponible para el usuario.
- ⇒ Cada Proxy está configurado para permitir acceso únicamente a los servidores especificados en el sistema. Esto significa que existe un conjunto de características/comandos que podrán ser aplicados para un subconjunto de sistemas en la red protegida.
- ⇒ Cada Proxy mantiene la información detallada y auditada de todos los registros del tráfico, cada conexión, y la duración de cada conexión. El registro de audición es una herramienta esencial para descubrir y finalizar el ataque de un intruso.
- ⇒ Cada servicio Proxy es un programa pequeño y sencillo específicamente diseñado para la seguridad de redes. Este permite que el código fuente de la aplicación pueda revisarse y analizar posibles intrusos y fugas de seguridad. Por ejemplo, una típica aplicación - UNIX mail⁶ - puede tener alrededor de 20,000 líneas de código cuando un correo Proxy puede contener menos de mil.
- ⇒ Cada servicio Proxy es independiente de todas las demás aplicaciones Proxy en el servidor de defensa. Si se suscitara un problema con la operación de cualquier Proxy, o si se descubriera una vulnerabilidad, este puede desinstalarse sin afectar la operación de las demás aplicaciones. Aun, si la población de usuarios requiere el soporte de un nuevo servicio, el administrador de redes puede fácilmente instalar el servicio Proxy requerido en el servidor de defensa.
- ⇒ Un Proxy generalmente funciona sin acceso al disco, lo único que hace es leer su archivo de configuración inicial. Desde que la aplicación Proxy no ejecuta su acceso al disco para soporte, un intruso podrá encontrar más dificultades para instalar caballos de Troya perjudiciales y otro tipo de archivos peligrosos en el servidor de defensa.
- ⇒ Cada Proxy corre como un usuario no-privilegiado en un directorio privado y seguro del servidor de defensa.

1.5.1.1.Ejemplo: telnet proxy

La figura ilustra la operación de un Telnet Proxy en un servidor de defensa. Para este ejemplo, un cliente externo ejecuta una sesión Telnet hacia un servidor integrado dentro del sistema de seguridad por el Gateway a nivel-aplicación.

⁶ Correo Electrónico por UNIX.

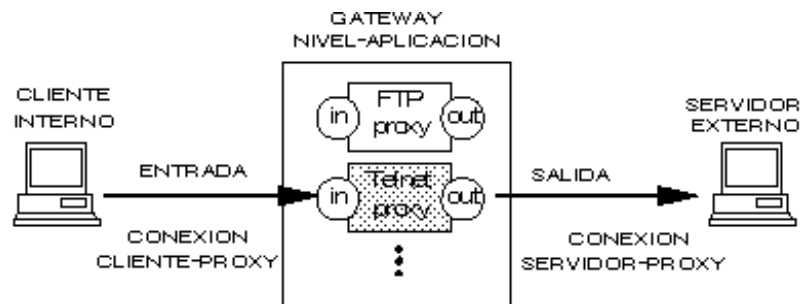


Ilustración 1-5 Telnet Proxy.

El Telnet Proxy nunca permite al usuario remoto que se registre o tenga acceso directo al servidor interno. El cliente externo ejecuta un telnet al servidor de defensa donde es autorizado por la tecnología “una-sola vez” de contraseña. Después de ser autenticado, el cliente obtiene acceso a la interfaz de usuario del Telnet Proxy. Este únicamente permite un subconjunto de comandos Telnet y además determina cual de los servidores están disponibles para el acceso vía Telnet.

```

Outside-Client > telnet servidor_defensa
Username: Larry Emd
Challenge Number "237936"
Challenge Response: 723456
Trying 200.43.67.17 ...

HostOS UNIX (servidor_defensa)

bh-telnet-proxy> help
Valid commands are:
connect hostname
help/?
Quit/exit
bh-telnet-proxy> connect servidor_interno

HostOS UNIX (servidor_interno)

login: Larry Emd
Password: #####
Last login: Wendnesday June 15 11:17:15
Welcome

Servidor_Interno >_

```

Ilustración 1-6 Sesión Vía Terminal De Telnet Proxy.

Los usuarios externos especifican el servidor de destino y el Telnet Proxy una vez hecha la conexión, desplaza los comandos internos hacia el cliente externo. El cliente externo cree que el Telnet Proxy es el servidor interno real, mientras el servidor interno cree que el Telnet proxy es un cliente externo.

La ilustración 1-6 presenta la salida en pantalla de la terminal de un cliente externo establecida como una “conexión” al servidor interno. Nótese que el cliente no se está registrando al servidor de defensa - el usuario comienza su sesión autenticándose por el servidor de defensa e intercambia respuestas, una vez que se le ha permitido sesionar se comunica con el Telnet

Proxy -. Después de pasar el intercambio de respuestas, el servidor Proxy ofrece un conjunto de comandos y destinos que están disponibles para los clientes externos.

La autenticación puede basarse en “algo conocido por los usuarios” (como una contraseña) o “algo que tengan” que posean físicamente (como una tarjeta electrónica). Ambas técnicas están sujetas a plagio, pero usando una combinación de ambos métodos se incrementa la probabilidad del uso correcto de la autenticación. En el ejemplo de Telnet, el Proxy transmite un requerimiento de registro y el usuario, con la ayuda de su tarjeta electrónica, obtendrá una respuesta de validación a través de un número. Típicamente, se le entrega al usuario su tarjeta desactivada para que el introduzca un PIN y se le regresa la tarjeta, la que se usa posteriormente como llave “secreta” de encriptación, con un reloj interno propio.

1.5.2. Beneficios del gateway a nivel-aplicación

Son muchos los beneficios obtenidos a partir de un gateway a nivel-aplicación. Proporcionan a la administración de red un completo control de cada servicio, a partir de aplicaciones proxy limitadas por un conjunto de comandos y la determinación del servidor interno donde se puede acceder a los servicios.

Aun cuando, el administrador de la red tenga el completo control acerca de que servicios son permitidos, cuando se carece de un servicio proxy para uno en particular significa que el servicio esta completamente bloqueado.

Los gateways a nivel-aplicación soportan autenticaciones forzando al usuario a proveer información detallada de registro. Finalmente, las reglas de filtrado para un gateway de este tipo son mucho mas fáciles de configurar y probar que en un ruteador filtra-paquetes.

1.5.3. Limitaciones del gateway a nivel-aplicación

Una de las mayores limitaciones de un gateway a nivel-aplicación es que requiere modificar la conducta del usuario, o bien instalación de software especializado en cada sistema que acceda a los servicios Proxy. Por ejemplo, el acceso de Telnet vía gateway a nivel-aplicación demanda modificar la conducta del usuario puesto que se requieren dos pasos para hacer una conexión.

Sin embargo, se podrá instalar software especializado en un sistema terminado, para hacer las aplicaciones del gateway transparentes, permitiendo a los usuarios especificar el servidor de destino, en lugar del propio, en un comando de telnet.

1.6. Edificando obstáculos: gateway a nivel-circuito

Un Gateway a nivel-circuito es en si una función perfeccionada de un Gateway a nivel-aplicación. A nivel-circuito simplemente se trasmiten las conexiones TCP sin cumplir ningún proceso adicional en filtrado de paquetes.

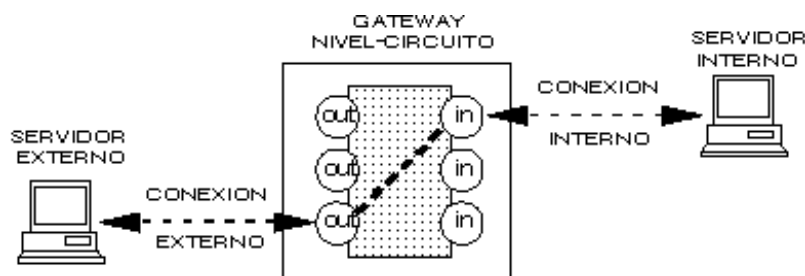


Ilustración 1-7 Gateway Nivel-Circuito.

La Ilustración 1-7 muestra la operación de una conexión típica Telnet a través de un Gateway a nivel-circuito. Tal como se mencionó, este gateway simplemente transmite la conexión a través del firewall sin examinarlo adicionalmente, filtrarlo, o dirigiendo el protocolo de Telnet. El gateway a nivel-circuito actúa como un cable copiando los bytes entre la conexión interna y la conexión externa.

La conexión del sistema externo actúa como si esta fuera originada por el sistema de firewall, encubriendo la información sobre la red interna.

El Gateway a nivel-circuito se usa frecuentemente para las conexiones de salida.

Una ventaja importante es que el servidor de defensa puede ser configurado como un Gateway “híbrido” soportando nivel-aplicación o servicios Proxy para conexiones de venida y funciones de nivel-circuito para conexiones de ida.

Esto hace que el sistema de firewall sea fácil de usar para los usuarios internos quienes tienen acceso directo a los servicios de Internet, mientras se proveen las funciones de firewall necesarias para proteger a la organización de los ataques externos.

*Apunte basado en el documento del Ing. Daniel R. Elorreaga Madrigal de la Universidad Nacional Autónoma de México.
Cisco Systems, Inc. y Novell, Inc.*
