www.coral-systems.com

Firewalls y Seguridad en Internet

1. Firewalls y seguridad en Internet

Introducción.

La seguridad ha sido el principal concerniente a tratar cuando una organización desea conectar su red privada al Internet. Sin tomar en cuenta el tipo de negocios, se ha incrementado el numero de usuarios de redes privadas por la demanda del acceso a los servicios de Internet tal es el caso del World Wide Web (WWW), Internet Mail (e-mail), Telnet, y File Transfer Protocol (FTP). Adicionalmente los corporativos buscan las ventajas que ofrecen las paginas en el WWW y los servidores FTP de acceso publico en el Internet.

Los administradores de red tienen que incrementar todo lo concerniente a la seguridad de sus sistemas, debido a que se expone la organización privada de sus datos así como la infraestructura de sus red a los Expertos de Internet (*Internet Crakers*). Para superar estos temores y proveer el nivel de protección requerida, la organización necesita seguir una política de seguridad para prevenir el acceso no-autorizado de usuarios a los recursos propios de la red privada, y protegerse contra la exportación privada de información. Todavía, aun si una organización no esta conectada al Internet, esta debería establecer una política de seguridad interna para administrar el acceso de usuarios a porciones de red y proteger sensitivamente la información secreta.

1.1. Firewalls

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo trafico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del trafico, y el mismo podrá ser inmune a la penetración. desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.

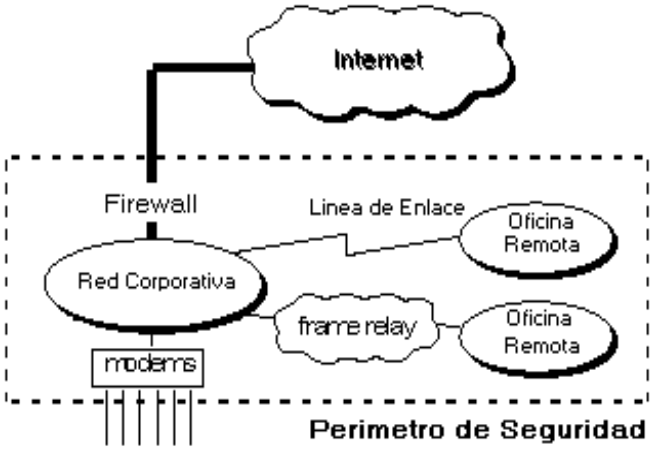


Ilustración 1-1 La Política De Seguridad Crea Un Perímetro De Defensa.

esto es importante, ya que debemos de notar que 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 diseñada para proteger las fuentes de información. Esta política de seguridad podrá incluir publicaciones con las 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 enciptacion de datos y discos, normas de protección de virus, y entrenamiento. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad. Un firewall de Internet sin una política de seguridad comprensiva 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 del Internet a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se exponen al ataque de otros servidores en el Internet. Esto significa que la seguridad en la red privada depende de la “Dureza” con que cada uno de los servidores cuenta y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.

El firewall permite al administrador de la red definir un “choke point” (envudo), manteniendo al margen los usuarios no-autorizados (tal, como., hackers, crakers, vándalos, y espías) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles. Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran nuestra red privada.

El firewall ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa , este generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el transito de los datos. Esto se podrá notar al acceder la organización al Internet, la pregunta general es “si” pero “cuando” ocurrirá el ataque. Esto es extremadamente importante para que el administrador audite y lleve una bitácora del trafico significativo a través del firewall. También, si el administrador de la red toma el tiempo para responder una alarma y examina regularmente los registros de base. Esto es innecesario para el firewall, desde que el administrador de red desconoce si ha sido exitosamente atacado!.

Concentra la seguridad

Genera alarmas de direcciones (NAT)

Monitorea y registra el WWW y FTP.

Internet.

Centraliza los accesos

seguridad Traduce

uso de Servicios de

Ilustración 1-2 Beneficios De Un Firewall De Internet.

Con el paso de algunos años, el Internet ha experimentado una crisis en las direcciones, logrando que el direccionamiento IP sea menos generoso en los recursos que proporciona. Por este medio se organizan las compañías conectadas al Internet, debido a esto hoy no es posible obtener suficientes registros de direcciones IP para responder a la población de usuarios en demanda de los 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 necesario para re-enumerar 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 del Internet. Esto permite al administrador de red justificar el gasto que implica la coneccion al Internet, localizando con precisión los cuellos de botella

[1] Network Address Translator.
[2] Internet Service Providers.

potenciales del ancho de banda, y promueve el método de cargo a los departamentos dentro del modelo de finanzas de la organización.

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 al Internet esta perdido - .

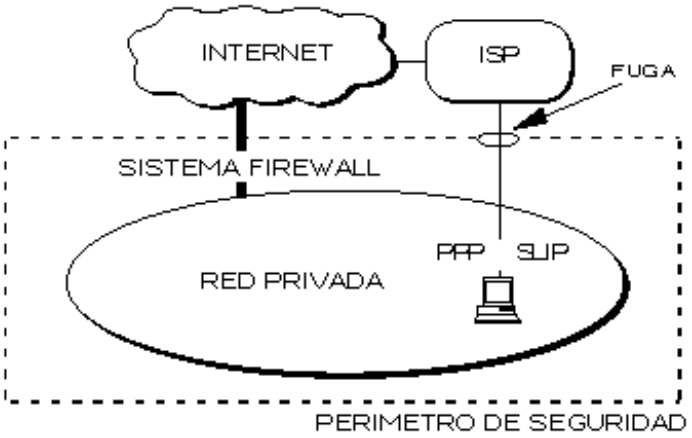
La preocupación principal del administrador de red, son los múltiples accesos al Internet, que se pueden registrar con un monitor y un firewall en cada punto de acceso que posee la organización hacia el Internet. Estos dos puntos de acceso significa dos puntos potenciales de ataque a la red interna que 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 coneccion dial-out sin restricciones que permita entrar a nuestra red protegida, el usuario puede hacer una coneccion SLIP o PPP al Internet. Los usuarios con sentido común suelen "irritarse" cuando se requiere una autenticación adicional requerida por un Firewall Proxy server (FPS)[3] lo cual se puede ser provocado por un sistema de seguridad circunvecino que esta incluido en una conexión directa SLIP o PPP del ISP.

Este tipo de conexiones derivan la seguridad provista por firewall construido cuidadosamente, creando una puerta de ataque. Los usuarios pueden estar consientes de que este tipo de conexiones no son permitidas como parte de integral de la arquitectura de la seguridad en la organización.



[3] Servidor Apoderado del Firewall.

Ilustración 1-3 Conexión Circunvecina Al Firewall De Internet.

El firewall no puede protegerse de las amenazas a que esta sometido por traidores o usuarios inconscientes. El firewall no puede prohibir que los traidores o espías corporativos copien datos sensitivos en disquettes o tarjetas PCMCIA y substraigan estas del edificio.

El firewall no puede proteger contra los ataques de la "Ingeniería Social", por ejemplo 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 del corporativo o que le permita el acceso "temporal" a la red.

Para controlar estas situaciones, los empleados deberían ser educados acerca de los varios tipos de ataque social que pueden suceder, y a cambiar sus contraseñas si es necesario periódicamente.

El firewall no puede protegerse contra los ataques posibles a la red interna por virus informativos a través de archivos y software. Obtenidos del Internet por sistemas operativos al momento de comprimir o descomprimir archivos binarios, el firewall de Internet no puede contar con un sistema preciso de SCAN[4] para cada tipo de virus que se puedan presentar en los archivos que pasan a través de el.

La solución real esta en que la organización debe ser consciente en instalar software anti-viral en cada despacho para protegerse de los virus que llegan por medio de disquettes o cualquier otra fuente.

Finalmente, el firewall de Internet no puede protegerse contra los ataques posibles en la transferencia de datos, estos ocurren cuando aparéntente 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 a la seguridad haciendo mas fácil el acceso de un intruso al sistema.

Como nosotros podemos ver, el desempeño de los servidores Proxy en un servidor de defensa es un excelente medio de prohibición a las conexiones directas por agentes externos y reduce las amenazas posibles por los ataques con transferencia de datos.

1.2. Herramientas del hacker

Es difícil describir el ataque "típico" de un hacker debido a que los intrusos poseen diferentes niveles de técnicos por su experiencia y son además son motivados por diversos factores. Algunos hackers son intrigosos por el desafío,

[4] System Control Antivirus Network.

otros mas gozan de hacer la vida difícil a los demás, y otros tantos substraen datos delicados para algún beneficio propio.

1.2.1. Recolección de información

Generalmente, el primer paso es saber en que forma se recolecta la información y además que tipo de información es. La meta es construir una base de datos que contenga la organización de la red y colectar la información acerca de los servidores residentes.

Esta es una lista de herramientas que un hacker puede usar para colectar 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 del objetivo de la topología de red perteneciente a una organización.
- El programa TraceRoute puede revelar el numero de redes intermedias y los ruteadores en torno al servidor especifico.
- El protocolo Whois que es un servicio de información que provee datos acerca de todos los dominios DNS y el administrador del sistema responsable para cada dominio. No obstante que esta información es anticuada.
- Servidores DNS pueden accesarce 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 ultima sesión, etc.) de un servidor en especifico.
- El programa Ping puede ser empleado para localizar un servidor particular y determinar si se puede alcanzar. 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 que actualmente son residentes en la red.

1.2.2. Sondeo del sistema para debilitar la seguridad

Después que se obtienen la información de red perteneciente a dicha organización, el hacker trata de probar cada uno de los servidores para debilitar la seguridad.

Estos son algunos usos de las herramientas que un hacker puede utilizar automáticamente para explorar individualmente los servidores residentes en una red:

- Una vez obtenida una lista no obstantemente pequeña de la vulnerabilidad de servicios en la red, un hacker bien instruido puede escribir un pequeño programa que intente conectarse a un puerto especificando el tipo de servicio que esta 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 publico, tal es el caso como el Rastreador de Seguridad en Internet (ISS)[5] o la Herramienta para Análisis de Seguridad para Auditar Redes (SATAN)[6] , 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 comunes en un sistema. El intruso usa la información collectada por este tipo de rastreadores para intentar el acceso no-autorizado al sistema de la organización puesta en la mira.

Un administrador de redes hábil puede usar estas herramientas en su red privada para descubrir los puntos potenciales donde esta debilitada su seguridad y así determina que servidores necesitan ser remendados y actualizados en el sofware.

[5] Internet Security Scanner .
[6] Security Analysis Tool for Auditing Networks.

1.2.3. Acceso a sistemas protegidos[i]

El intruso utiliza los resultados obtenidos a través de las pruebas para poder intentar accesar 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 toda evidencia del asalto y además podrá crear nuevas fugas en el sistema o en partes subalternas con el compromiso de seguir teniendo acceso sin que el ataque original sea descubierto.
- Pueden instalar paquetes de sondeo que incluyan códigos binarios conocidos como “caballos de Troya” protegiendo su actividad de forma transparente. Los paquetes de sondeo colectan las cuentas y contraseñas para los servicios de Telnet y FTP permitiendo al hacker expandir su ataque a otras maquinas.
- Pueden encontrar otros servidores que realmente comprometan al sistema. Esto permite al hacker explotar vulnerablemente desde un servidor sencillo todos aquellos que se encuentren a través de la red corporativa.
- Si el hacker puede obtener acceso privilegiado en un sistema compartido, podrá leer el correo, buscar en archivos

1.3. Bases para el diseño decisivo del firewall

Cuando se diseña un firewall de Internet, se tiene que tomar algunas decisiones que pueden ser asignadas por el administrador de red:

* 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 la construcción de 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:

– “No todo lo específicamente permitido esta prohibido”
– “Ni todo lo específicamente prohibido esta permitido”

la primera postura asume que un firewall puede obstruir todo el trafico y cada uno de los servicios o aplicaciones deseadas necesariamente para ser implementadas básicamente caso por caso.

Esta propuesta es recomendada únicamente a un limitado numero de servicios soportados cuidadosamente seleccionados en un servidor. La desventaja es que el punto de vista de "seguridad" es mas importante que - facilitar el uso - de los servicios y estas limitantes numeran las opciones disponibles para los usuarios de la comunidad. Esta propuesta se basa en una filosofía conservadora donde se desconocen las causas acerca de los que tienen la habilidad para conocerlas.

La segunda postura asume que el firewall puede desplazar todo el trafico y que cada servicio potencialmente peligroso necesitara ser aislado básicamente 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 además, el administrador de la red esta en su lugar de incrementar la seguridad en el sistema conforme crece la red. Desigual a la primer propuesta, esta postura esta basada en la generalidad de conocer las causas acerca de los que no tienen la habilidad para conocerlas

1.3.2. Política interna de la seguridad

Tan discutidamente escuchada, un firewall de Internet no esta solo - es parte de la política de seguridad total en una organización -, la cual define todos los aspectos en competentes al perímetro de defensa. Para que esta sea exitosa, la organización debe de conocer que es lo se esta protegiendo. La política de seguridad se basara en una conducción cuidadosa analizando la seguridad, la asesoría en caso riesgo, y la situación del negocio. Si no se posee con la información detallada de la política a seguir, aun que sea un firewall cuidadosamente desarrollado y armado, estará exponiendo la red privada a un posible atentado.

1.3.3. Costo del firewall

¿Cuanto puede ofrecer una organización por su seguridad?, un simple paquete de filtrado firewall puede tener un costo mínimo ya que la organización necesita un ruteador conectado al Internet, y dicho paquete ya esta incluido como estándar del equipo. Un sistema comercial de firewall provee un incremento mas a la seguridad pero su costo puede ser de $32,000 hasta $240,000 pesos dependiendo de la complejidad y el numero de sistemas protegidos. Si la organización posee al experto en casa, un firewall casero puede ser construido con software de dominio publico pero este ahorro de recursos repercuten en términos del tiempo de desarrollo y el despliegue del sistema firewall. Finalmente requiere de soporte continuo para la administración, mantenimiento general, actualización de software, reparación de seguridad, e incidentes de manejo.

1.3.4. Componentes del sistema firewall

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

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

por lo que resta del capitulo, se discutirá cada una de las opciones para la edificación de obstáculos y se describirá como se puede trabajar junto con ellos para construir un efectivo sistema firewall de Internet.

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 este corresponde a uno de sus paquetes filtrados y que a su vez haya sido aprobado por sus reglas. Las reglas de filtrado se basan en revisar la información que poseen los paquetes en su encabezado, lo que hace posible su desplazamiento en un proceso de IP. 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 interface de entrada del paquete, y la interface de salida del paquete. Si se encuentra la correspondencia y las reglas permiten el paso del paquete, este será desplazado de acuerdo a la información a la tabla de ruteo, si se encuentra la correspondencia y las reglas niegan el paso, el paquete es descartado. Si estos no corresponden a las reglas, un parámetro configurable por incumplimiento determina descartar o desplazar el paquete.

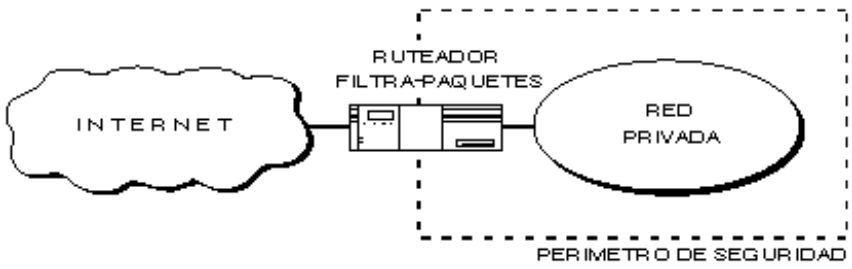


Ilustración 1-4 Ruteador Filtra-Paquetes.

1.4.1. Servicio dependiente del filtrado

Las reglas acerca del filtrado de paquetes a través de un ruteador para rehusar/permitir el trafico esta basado en un servicio en especifico, desde entonces muchos servicios vierten su información en numerosos 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 perfecionar su funcionamiento serian:

- Permitir la entrada de sesiones Telnet únicamente a una lista especifica 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 trafico 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 estos son independientes al tipo de servicio. Los ruteadores pueden ser configurados para protegerse de este tipo de ataques pero son mas difíciles de especificar desde entonces las reglas para el filtrado requieren de información adicional que pueda ser estudiada y examinada por la tabla de ruteo, inspeccionando las opciones especificas IP, revisando fragmentos especiales de edición, etc. Algunos ejemplos de este tipo de ataques incluye:

Agresiones Originadas Por El Direccionamiento IP.

Para este tipo de ataque, el intruso trasmite 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 seguramente como dirección fuente donde los paquetes que trasmita sean autentificados y los del otro servidor sean descartados dentro del sistema. Los ataques por seudo-fuentes pueden ser frustrados si descartamos la dirección fuente de cada paquete con una dirección fuente "interno" si el paquete arriva en 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 de tomar cuando cruce a través del Internet. Este tipo de ataques son diseñados para cuantificar las derivaciones 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, los intrusos utilizan las características de fragmentación para crear fragmentos extremadamente pequeños y obligan a la información del encabezado TCP a separarce 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. Aunque si bien únicamente es explotado por sencillos decodificadores , una agresión pequeñisima 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. Otros que tienen tiempo planean los filtros y

configuran el ruteador, sea este pequeño o no , el costoso para implementar la filtración de paquetes no es cara; desde que los componentes básicos de los ruteadores incluyen revisiones estándar de software para dicho efecto. Desde entonces el acceso a Internet es generalmente provisto a través de interfaces WAN, optimando la operación del ruteador moderando el trafico 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 de entrenamiento especializado o software especifico que tenga que ser instalado en cada uno de los servidores.

1.4.4. Limitaciones del ruteador filtra-paquetes

Definir el filtrado de paquetes puede ser una tarea compleja porque el administrador de redes necesita tener un detallado estudio de varios servicios de Internet, como los formatos del encabezado de los paquetes, y los valores específicos esperados a encontrase en cada campo. Si las necesidades de filtrado son muy complejas, se necesitara soporte adicional con lo cual el conjunto de reglas de filtrado puede empezar a complicar y alargar el sistema haciendo mas difícil su administración y comprensión. Finalmente, estas serán menos fáciles de verificar para las correcciones de las reglas de filtrado después de ser configuradas en el ruteador. Potencialmente se puede dejar una localidad abierta sin probar su vulnerabilidad.

Cualquier paquete que pasa directamente a través de un ruteador puede ser posiblemente usado como parte inicial un ataque dirigido de datos. Haciendo memoria este tipo de ataques ocurren cuando los datos aparentementes inocuos se desplazan por el ruteador a un servidor interno. Los datos contienen instrucciones ocultas que pueden causar que el servidor modifique su control de acceso y seguridad relacionando sus archivos facilitando al intruso el acceso al sistema.

Generalmente, los paquetes entorno al ruteador disminuyen conforme el numero de filtros utilizados se incrementa. Los ruteadores son optimizados para extraer la dirección destino IP de cada paquete, haciendo relativamente simple la consulta a la tabla de ruteo, y el desplazamiento de paquetes para la interface apropiada de la transmisión. Si esta autorizado el filtro, no únicamente podrá el ruteador tomar la decisión de desplazar cada paquete, pero también sucede aun aplicando todas las reglas de filtrado. Esto puede consumir ciclos de CPU e impactar el perfecto funcionamiento del sistema.

El filtrado de paquetes IP no puede ser capaz de proveer el suficiente control sobre el trafico. 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 trafico 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 nivel-aplicación permiten al administrador de red la implementación de una política de seguridad estricta que la que permite un ruteador filtra-paquetes. Mucho mejor que depender de una herramienta genérica de filtra-paquetes para administrar la circulación de los servicios de Internet a través del firewall, se instala en el gateway un código de proposito-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 podrán desplazarse a través del firewall.

Aun cuando, el código Proxy puede ser configurado para soportar únicamente las características especificas de una aplicación que el administrador de red considere aceptable mientras niega todas las otras.

Un aumento de seguridad de este tipo incrementa nuestros costos en términos 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 transparencia en el manejo de los usuarios en un ambiente “amigable”. Como en todos los casos el administrador de redes debe de balancear las necesidades propias en seguridad de la organización con la demanda de “fácil de usar” demandado por la comunidad de usuarios.

Es importante notar que los usuarios tienen acceso por un servidor Proxy, pero ellos jamas podrán seccionar en el Gateway a nivel-aplicación. Si se permite a los usuarios seccionar en el sistema de firewall, la seguridad es amenazada desde el momento en que un intruso puede potencialmente ejecutar muchas actividades que comprometen la efectividad del sistema.

Por ejemplo, el intruso podría obtener el acceso de root, instalar un caballo de troya para colectar las contraseñas, y modificar la configuración de los archivos de seguridad en el filrewall.

1.5.1. Servidor de defensa

Un ruteador filtra-paquetes permite la circulación directa de los paquetes dentro y fuera del sistema, diferente a esto el Gateway a nivel-aplicación deja que la información circule entre los sistemas pero no permite el intercambio directo de paquetes. El principal riesgo de permitir que los paquetes se intercambien dentro y fuera del sistema se debe a que el servidor residente en los sistemas de protección de la red podrá ser asegurado 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.

⇒ Unicamente los servicios que el administrador de redes considera esenciales son instalados en el servidor de defensa. La lógica de operación es que si el servicio no esta instalado, este puede ser atacado. Generalmente, un conjunto limitado de aplicaciones Proxy tales como Telnet, DNS, FTP, SMTP, y autenticación de usuarios son instalados en este servidor.

⇒ El servidor de defensa podrá requerir de una autenticación adicional para que el usuario accese 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 generaba 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 Proxy es configurado para soportar únicamente un subconjunto de aplicaciones estándar de un conjunto de comandos. Si un comando estándar no es soportado por la aplicación Proxy, es porque simplemente no esta disponible para el usuario.

⇒ Cada Proxy esta configurado para dejar acceder 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 trafico, cada conexión , y la duración de cada conexión. El

registro de audición es un herramienta esencial para descubrir y finalizar el ataque de un intruso.

⇒ Cada Proxy es un programa pequeño y sencillo específicamente diseñado para la seguridad de redes. Este permite que el código fuente de la aplicación pueda revisar y analizar posibles intrusos y fugas de seguridad. Por ejemplo, una típica aplicación - UNIX mail[7] - puede tener alrededor de 20,000 líneas de código cuando un correo Proxy puede contener menos de mil.

⇒ Cada Proxy es independiente de todas las demás aplicaciones Proxy en el servidor de defensa. Si se sucitara un problema con la operación de cualquier Proxy, o si se descubriera un sistema vulnerable, 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 mas 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-previlegiado en un directorio privado y seguro del servidor de defensa.

[7] Correo Electrónico por UNIX.

1.5.1.1.Ejemplo: telnet proxy

La 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.

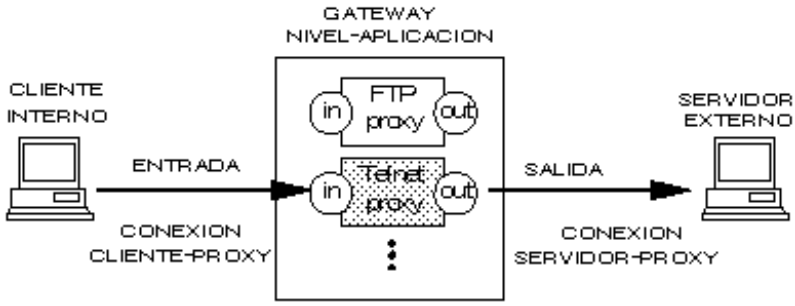


Ilustración 1-5 Telnet Proxy.

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 autentificado, el cliente obtiene acceso a la interface de usuario del Telnet Proxy. Este únicamente permite un subconjunto de comandos Telnet y además determina cual de los servidores son 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, los comandos internos son desplazados 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.

El Ilustración 1-7 presenta la salida en pantalla de la terminal de un cliente externo como la "conexión" a el servidor interno una vez establecida. Nótese que el cliente no se esta registrando al servidor de defensa - el usuario comienza su sesión autentificándose por el servidor de defensa e intercambia respuestas, una vez que se le ha permitido seccionar se comunica con el Telnet Proxy -. Después de pasar el intercambio de respuestas, el servidor Proxy limita 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) cualquiera de las dos. 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 por un numero. Típicamente, se le entrega al usuario su tarjeta desactivada para que el introduzca un PIN[8] y se le regresa la tarjeta, basada en parte como llave "secreta" de encriptacion y con un reloj interno propio, una vez que se establece la sesión se obtiene un valor de respuesta encriptado.

1.5.2. Beneficios del gateway a nivel-aplicación

Son muchos los beneficios desplegados en un gateway a nivel-aplicación. Ellos dan a la administración de red un completo control de cada servicio desde aplicaciones proxy limitadas por un conjunto de comandos y la determinación del servidor interno donde se puede accesar a los servicios. Aun cuando, el administrador de la red tenga el completo control acerca de que servicios que son permitidos desde la carencia de un servicio proxy para uno en particular significa que el servicio esta completamente bloqueado. Los gateways a nivel-aplicación tienen la habilidad de soportar autenticaciones forzando al usuario para 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

Probablemente una de las grandes limitaciones de un gateway a nivel-aplicación es que requiere de modificar la conducta del usuario o requiere de la instalación de software especializado en cada sistema que accese a los servicios Proxy. Por ejemplo, el acceso de Telnet vía gateway a nivel-

[8] Post Identidy Number

aplicación demanda modificar la conducta del usuario desde el momento en que se requiere de dos pasos para hacer una conexión mejor que un paso. Como siempre, el software especializado podrá ser instalado en un sistema terminado para hacer las aplicaciones del gateway transparentes al permitir a los usuarios especificar el servidor de destino, mejor que el propio, en un comando de telnet.

1.6. Edificando obstáculos: gateway a nivel-circuito

Un Gateway a nivel-circuito es en si una función que puede ser perfeccionada en un Gateway a nivel-aplicación. A nivel-circuito simplemente trasmite las conexiones TCP sin cumplir cualquier proceso adicional en filtrado de paquetes.

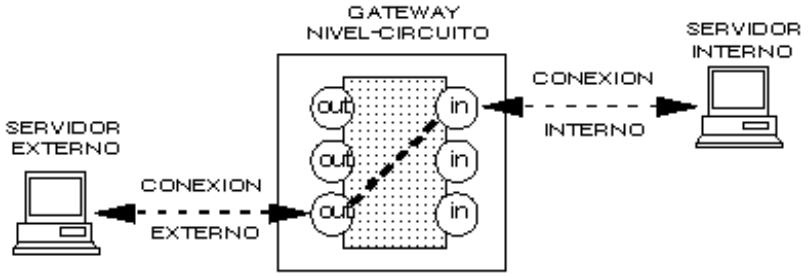


Ilustración 1-8Gateway Nivel-Circuito.

La Ilustración 1-9 muestra la operación de una conexión típica Telnet a través de un Gateway a nivel-circuito. Tal como se menciono anteriormente, este gateway simplemente trasmite la conexión a través del firewall sin examinarlo adicionalmente, filtrarlo, o dirigiendo el protocolo de Telnet. El gateway a nivel-circuito acciona como una cable copiando los bytes antes y después entre la conexión interna y la conexión externa. De cualquier modo, la conexión del sistema externo actúa como si fuera originada por el sistema de firewall tratando de beneficiar el encubrir la información sobre la protección de la red.

El Gateway a nivel-circuito se usa frecuentemente para las conexiones de salida donde el administrador de sistemas somete a los usuarios internos. La ventaja preponderante 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 desean tener acceso directo a los servicios de Internet mientras se proveen las funciones del firewall necesarias para proteger la organización de los ataques externos.

Autor: Daniel Ramón Elorreaga Madrigal
Ing. Electronico
Universidad Nacional Autonoma de Mexico
e-mail: dan_dds@yahoo.com

[i] ©1994 Cisco System, Inc. , © 1983 Novell, Inc.