SEGURIDAD EN REDES Y SISTEMAS INFORMÁTICOS

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

Ana González (Kao)

UNIDAD 8. Seguridad en redes

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

Ana González (Kao)

ÍNDICE UNIDAD 8

UNIDAD 8. SEGURIDAD EN REDES.

1. Conceptos de red.
2. Red Privada Virtual.
3. Redes inalámbricas.
4. Cortafuegos.
5. Sistemas de detección de intrusiones.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

1. Conceptos de red

Para poder entender los factores de riesgo dentro de una red primero debemos de conocer qué son y cómo funcionan las redes. En la primera parte de este tema nos vamos a centrar en describirlas y comprenderlas. Más adelante, entraremos en conceptos de seguridad en redes a partir de textos de diferentes autores.

Objetivos de las redes

Las redes en general, consisten en "compartir recursos". Los objetivos a la hora del diseño de una nueva red son:

1. Disponibilidad: hacer que todos los programas, datos y equipos estén disponibles para cualquier usuario de la red que así lo solicite, sin importar la localización física del recurso y del usuario.
2. Alta Fiabilidad: Contar con fuentes alternativas de suministro, si existen múltiples CPUs y una deja de funcionar, las otras pueden hacer su trabajo.
3. Ahorro económico: Se debe tener en cuenta la relación costo/rendimiento, a la hora de comprar equipamiento intentando adecuarse lo máximo posible a las necesidades de la empresa.

Estructuras

Definir el concepto de redes implica diferenciar entre el concepto de redes físicas y redes de comunicación. Una Red la constituyen dos o más computadoras que comparten determinados recursos.

Podemos decir que existe una red cuando están involucrados un componente humano que comunica, un componente tecnológico (computadoras, telecomunicaciones) y un componente administrativo (institución que mantiene los servicios). Así, a una Red más que varias computadoras conectadas, la forman personas que solicitan, proporcionan e intercambian experiencias e informaciones a través de sistemas de comunicación.

Modelos de interconexión

La forma de acceder a los datos nos permite diferenciar dos modos claros de conexión:

1. Redes Point–To–Point (Punto a punto) donde un host se conecta directamente a otro.

2. Modelo cliente/servidor donde el cliente (un usuario de PC) solicita un servicio (por ejemplo imprimir) que un Servidor (un procesador conectado a la LAN) le proporciona.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

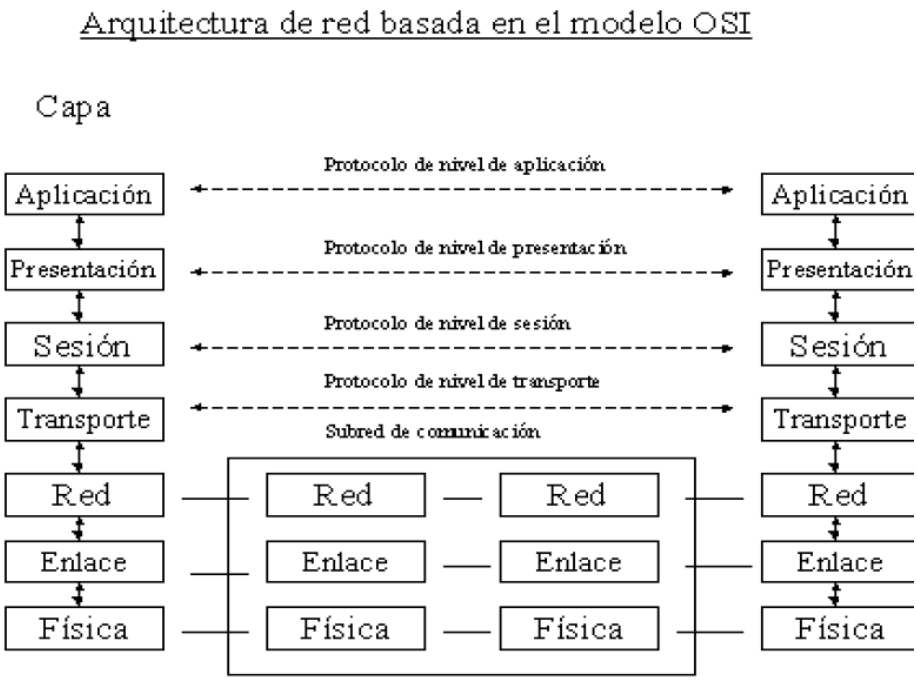
Protocolo

Un protocolo es un acuerdo de reglas semánticas y sintácticas, (lenguaje de reglas y símbolos), que rigen la comunicación entre dos equipos o dos servicios. Esto quiere decir que se ponen de acuerdo para hablar de una forma determinada, si lo trasladamos a la vida diaria, nosotros no hablamos igual, no utilizamos el mismo lenguaje, con nuestra suegra que con nuestra pareja, ni con nuestra pareja que con nuestros compañeros de trabajo, ya que con todos ellos utilizamos protocolos distintos de comunicación.

En el nivel físico, esto se realiza a través de tarjetas de red, y una conexión entre las mismas. Lógicamente se debe establecer una comunicación "del mismo lenguaje" entre distintos sistemas operativos y tarjetas de red independientemente del fabricante de las mismas. A este lenguaje se le llama protocolo.

Modelo OSI

A principios de los 80 los fabricantes informáticos más importantes se reunieron para unificar diferencias y permitir así la comunicación y compatibilidad entre sus distintos dispositivos, ya que en aquel entonces no eran compatibles. De esta reunión nació el **modelo OSI** (Modelo abierto de internetwork), de Iso (International Organization for Standardization, organización internacional de estandarización), creando el siguiente modelo basado en 7 capas:



Esto aportó una serie de **beneficios** que se mantienen hoy día:

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

Menos complejidad: Divide los conceptos en partes más pequeñas lo que permite la especialización	Interfaces Estándares: Las definiciones de interfaz estándar entre cada capa permiten la competencia abierta entre los fabricantes lo cual favorece el producto final	Mejora del aprendizaje: Al hacer menos abstractos los términos de la comunicación es más fácil poder explicarlos
Mejor desarrollo: Los profesionales pueden dedicarse a desarrollar de forma especializada para cada una de las capas sin tener que prestar atención o tener conocimientos sobre el resto	Interoperatibilidad multifabricante: Ordenadores de distintos fabricantes y dispositivos de red de diversos fabricantes pueden coexistir en la misma red funcionando perfectamente	Ingeniería modular: Un fabricante puede escribir software que funcione en las primeras capas y otro que funcione en las siguientes

Cada una de las capas tiene un propósito en la trasmisión de los datos. Vamos a verlas detenidamente.

1. Capa de aplicación:

- Es la capa final más cercana al usuario y la única que no proporciona servicios a ninguna otra capa.
- Ofrece a las aplicaciones (de usuario o no), la posibilidad de acceder a las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos.
- Proporciona la interfaz entre las aplicaciones que usamos para comunicarnos y la red subyacente en la cual se trasmiten los mensajes
- Los protocolos de la capa de aplicación se utilizan para intercambiar datos entre los programas que se ejecutan en el host de origen y de destino.

En esta capa aparecen diferentes protocolos y servicios, más adelante hablaremos con más detalle de los protocolos y servicios en general:

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

Protocolos de la capa de aplicación:

FTP (File Transfer Protocol - Protocolo de transferencia de archivos) para transferencia de archivos.
DNS (Domain Name Service - Servicio de nombres de dominio).
DHCP (Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de anfitrión).
HTTP (HyperText Transfer Protocol) para acceso a páginas web.
POP (Post Office Protocol) para correo electrónico.
SMTP (Simple Mail Transport Protocol).
SSH (Secure SHell)
TELNET para acceder a equipos remotos.
TFTP (Trival File Transfer Protocol).
LDAP (Lightweight Directory Access Protocol).

Servicios de la capa de aplicación:
Aplicaciones de Red
www (World Wide Web).
Enlace a capas inferiores
Esta capa contiene las aplicaciones visibles para el usuario.

Algunas consideraciones son: seguridad y cifrado, DNS (Domain Name Service). Una de las aplicaciones más usadas hoy en día en Internet es el WWW (World Wide Web).

2. Capa de presentación:

Se encarga de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres (ASCII, Unicode, EBCDIC), números (little-endian tipo Intel, big-endian tipo Motorola), sonido o imágenes, los datos lleguen de manera reconocible.

Esta capa es la primera en trabajar más el contenido de la comunicación que cómo se establece la misma. En ella se tratan aspectos tales como la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas.

La Capa 6, o capa de presentación, cumple tres funciones principales. Estas funciones son las siguientes:

- Formato de datos Ej: Ascii, Unicode, EBCDIC
- Cifrado de datos Ej: clave de cifrado el lugar origen y de descifrado en lugar de destino
- Compresión de datos Ej: Gif, MPG, JPG, MP3...

3. Capa de sesión:

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

Define cómo iniciar, controlar y terminar las conversaciones (sesiones) entre las aplicaciones.

4. Capa de trasporte:

Es la encargada de la comunicación confiable entre el host, control de flujo y de la corrección de errores. Los datos son divididos en segmentos, identificados con un encabezado y con un número de puerto que identifica la aplicación de origen.

Sus principales *funciones* son:

- Seguimiento de la comunicación individual entre las aplicaciones de host de origen y destino
- Segmentación de los datos y gestión de cada porción
- Re-ensamblaje de los segmentos en flujos de aplicación.
- Identificación de los segmentos

Protocolos:

- Tcp Trasfer Control Protocol o protocolo de control de trasferencia. Es un protocolo orientado a la conexión de entrega confiable y control de flujo. Tiene 20bytes de carga en el encabezado que engloban:
    - Puerto de origen y destino
    - Secuenciamiento para la entrega en el mismo orden.
    - Reconocimiento de segmentos recibidos
    - Control del flujo y administración de la saturación.

- -UDP User Datagram Protocol (UDP) es un protocolo del nivel de transporte basado en el intercambio de datagramas. Es un protocolo sin conexión con datagramas de 8bytes de máximo esfuerzo

5. Capa de Red

La capa de red provee servicios para intercambiar secciones de datos individuales a través de la red entre dispositivos finales identificados

Tiene tres *características* principales:

- Direccionamiento lógico: define como cada dispositivo puede tener una dirección que el proceso de enrutamiento puede usar.
- Enrutamiento (envío) Definen cómo los dispositivos, normalmente routers, envían los paquetes a su destino final.
- Determinación de la ruta. Se refiere al trabajo realizado por los protocolos de enrutamiento, según el cual se aprenden todas las rutas pero sólo se elige la mejor para su uso.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

Sus *protocolos* son:

-Protocolo de internet IPv4
-Protocolo de internet IPv6
-IPX Intercambio novell de paquetes de internetwork
-Apple talk
-CLNS/Decnet Servicio de red sin conexión

6. Capa de enlace de datos

Permite a las capas superiores acceder a los medios usando técnicas como tramas. Controla cómo se ubican los datos en los medios y cómo se reciben usando técnicas de control de acceso a los medios y de detección de errores.

Los protocolos de la capa de enlace de datos regulan como se da formato a una trama para utilizarla en diferentes medios.

Tiene dos subcapas:

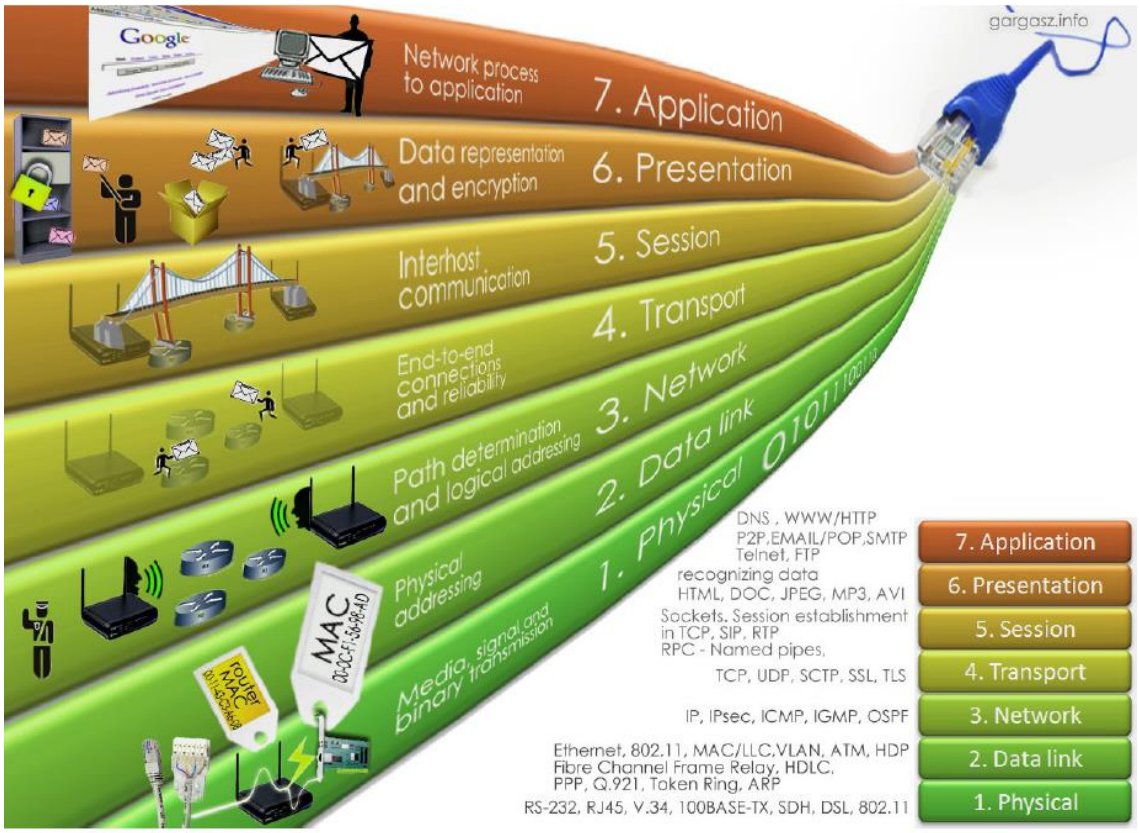
- LLC Control de enlace lógico: Entrama el paquete de la capa de red e identifica el protocolo de la capa de red.
- MAC Control de acceso al medio: Direcciona la trama y marca su comienzo y su fin.

Sus protocolos son: Ethernet, 802.2, 802.3, HDLC, Frame-Relay...etc

7. Capa física

Se encarga de los medios, conectores, especificaciones eléctricas, lumínicas y de la codificación. Los bits son trasformados en pulsos eléctricos, en luz o en radio frecuencia para ser enviados según sea el medio en que se propaguen.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes



Un envío de datos típico bajo el modelo de referencia OSI comienza con una aplicación en un nodo cualquiera de la red. Esta Aplicación genera los datos que quiere enviar a su contraparte en otro nodo.

1. La Capa de **Aplicación** toma los datos y los encapsula añadiendo un encabezado que puede contener información de control o estar vacío. Envía el paquete resultante a la Capa de Presentación.
2. La Capa de **Presentación** recibe el paquete y no intenta decodificarlo o separar sus componentes, sino que lo toma como datos y le añade un encabezado con información de control de esta capa.
3. Las Capa de **Sesión** y de **Transporte** reciben el paquete, que también son sólo datos para ellas y le añaden un encabezado de control. El resultado es enviado a la capa inferior.
4. La Capa de **Red** se encarga de enrutar el paquete a su destino.
5. Las Capas de Red, **Enlace de datos** y **Física** toman, respectivamente, el paquete que les envía la capa superior y añaden a éste un encabezado definido por el protocolo que corresponde a cada capa y pasan el resultado a la capa inferior.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

6. La Capa **Física**, por último, traducirá el último paquete a las señales apropiadas para que viajen por el medio físico hasta el nodo destino.
7. En el nodo destino comienza el camino inverso; es decir que cada capa quita su encabezado de control y envía el paquete a la capa superior hasta llegar a la de Aplicación en el nodo destino.

Como puede apreciarse, todas las capas, excepto la de Aplicación, procesan los paquetes realizando operaciones que sirven para verificar que el paquete de datos real esté íntegro, o para que éste llegue a su destino sin que los datos sufran alguna alteración.

2. Red privada virtual

Introducción a redes virtuales privadas

Los métodos tradicionales de acceso remoto y creación de WAN privadas resultan ser bastante costosos. Puesto que las redes públicas resultan ser mucho más económicas que las privadas, se buscaron maneras de poder establecer una red privada dentro de una red pública.

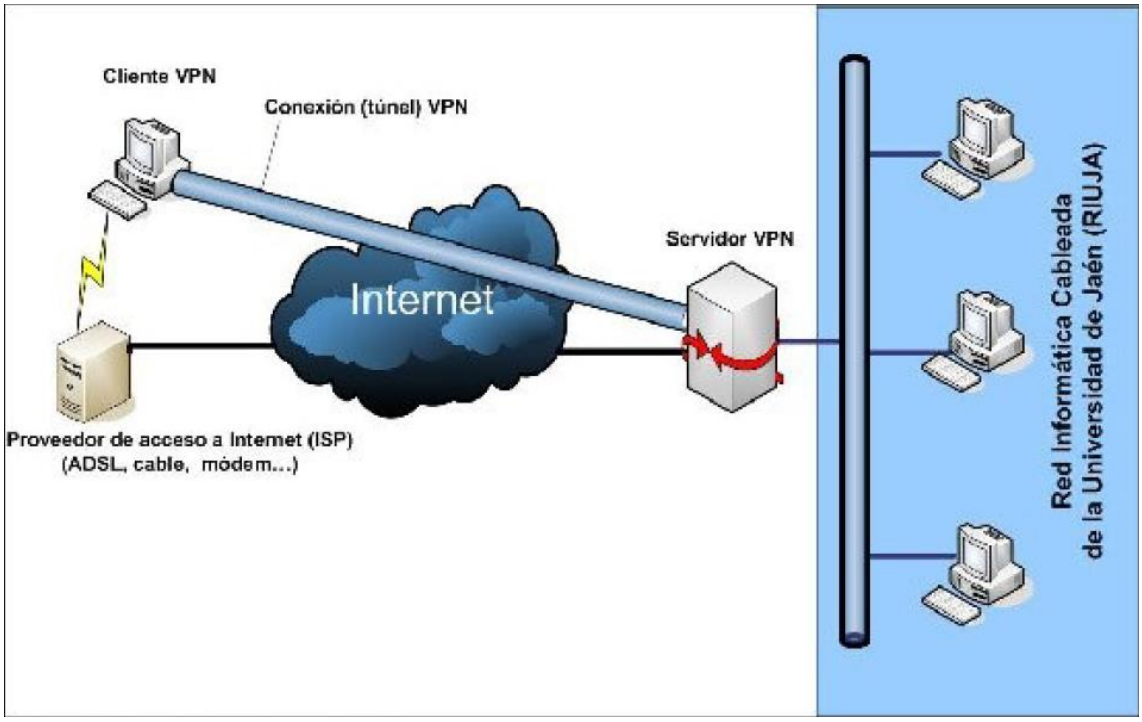
El resultado fue el surgimiento de las Redes Privadas Virtuales (VPN) las cuales han ofrecido ventajas muy amplias a las corporaciones siendo la principal de ellas la reducción de costos de instalación y mantenimiento de forma muy significativa.

Se puede definir a una VPN de la siguiente manera:
Una Red Privada Virtual (VPN, Virtual Private Network) es una red privada que utiliza la infraestructura de una red pública para poder transmitir información.

Una VPN combina dos conceptos: redes virtuales y redes privadas. En una red virtual, los enlaces de la red son lógicos y no físicos. La topología de esta red es independiente de la topología física de la infraestructura utilizada para soportarla.

Un usuario de una red virtual no será capaz de detectar la red física, el sólo podrá ver la red virtual. Desde la perspectiva del usuario, la VPN es una conexión punto a punto entre el equipo (el cliente VPN) y el servidor de la organización (el servidor VPN). La infraestructura exacta de la red pública es irrelevante dado que lógicamente parece como si los datos se enviaran a través de un vínculo privado dedicado.

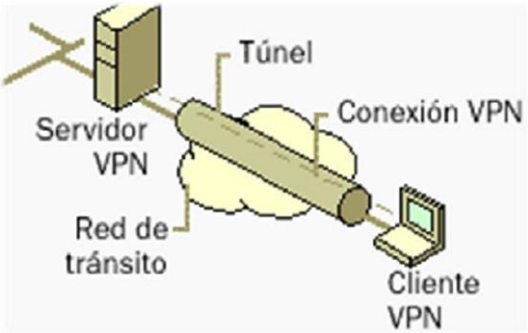
El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes



Las redes privadas son definidas como redes que pertenecen a una misma entidad administrativa. Un ejemplo típico de esta clase de red es una intranet corporativa, o la intranet de una universidad, la cual puede ser utilizada sólo por los usuarios autorizados. De los conceptos de red privada y red virtual es como nace el concepto de red privada virtual.

Debido al hecho de ser una red privada que utiliza una red pública, la cuestión de la seguridad en una VPN es muy importante, ya que la información que circula en una red pública puede ser vista por cualquiera si no se toman las debidas precauciones. Y en una red pública como Internet existen muchas personas con diferentes intenciones.

Es por eso que una VPN debe de poseer excelentes mecanismos de autenticación y de encriptación de la información para que ésta viaje segura a través de una red pública.



Los componentes básicos de una VPN son:

- Servidor VPN
- Túnel
- Conexión VPN
- Red pública de tránsito
- Cliente VPN

Para emular un vínculo punto a punto en una VPN, los datos se encapsulan o empaquetan con un encabezado que proporciona la información de enrutamiento que permite a los datos recorrer la red pública hasta alcanzar su destino.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

Para emular un vínculo privado, los datos se cifran para asegurar la confidencialidad. Los paquetes interceptados en la red compartida o pública no se pueden descifrar si no se dispone de las claves de cifrado. La parte de la conexión en la cual los datos privados son encapsulados es conocida como túnel. La parte de la conexión en la que se encapsulan y cifran los datos privados se denomina conexión VPN.

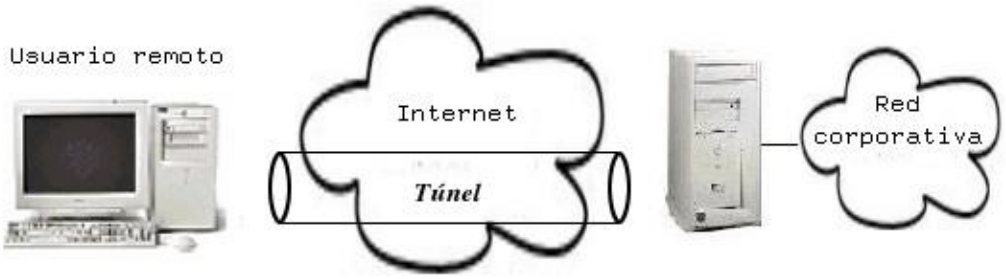
Arquitectura de una VPN

Existen básicamente dos tipos de arquitectura para una VPN. Estos son:
- VPN de acceso remoto
- VPN de sitio a sitio

La VPN de sitio a sitio también puede ser llamada VPN LAN a LAN o VPN POP a POP. Las VPN de sitio a sitio se dividen a su vez en VPN extranet y VPN intranet. Las VPN de acceso remoto se dividen en VPN Dial-up y VPN directas.

VPN de acceso remoto

Esta VPN proporciona acceso remoto a una intranet o extranet corporativa. Una VPN de acceso remoto permite a los usuarios acceder a los recursos de la compañía siempre que lo requieran. Con el cliente VPN instalado en un dispositivo, el usuario es capaz de conectarse a la red corporativa, no importa donde se encuentre.



El cliente de acceso remoto inicia una conexión VPN a través de Internet con el servidor VPN de la compañía. Una vez que se ha establecido el enlace, el usuario puede acceder a los recursos de la intranet privada de la empresa.

De acuerdo a la tecnología utilizada para establecer la conexión, las VPN de acceso remoto se puede dividir en VPN dial-up y VPN directas.

VPN dial-up. En esta VPN, el usuario realiza una llamada local al ISP utilizando un módem. El uso de este tipo de VPN se da más entre los usuarios móviles, ya que no en todos los lugares a donde se viaja se pueden tener disponibles conexiones de alta velocidad.
VPN directa. En esta VPN, se utilizan las tecnologías de conexión a Internet de alta velocidad.
Este tipo de VPN se puede encontrar principalmente entre los teletrabajadores. Actualmente se pueden obtener conexiones a Internet desde el hogar utilizando estas tecnologías.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

VPN de sitio a sitio

Las VPN de sitio a sitio son utilizadas para conectar sitios geográficamente separados de una corporación. En las redes tradicionales, las distintas oficinas de una corporación son conectadas utilizando tecnologías como T1, E1, ATM o Frame Relay.

Con una VPN, es posible conectar las LAN corporativas utilizando Internet. El envío de información se realiza a través de una conexión VPN. De esta forma, se puede crear una WAN utilizando una VPN. Una empresa puede hacer que sus redes se conecten utilizando un ISP local y establezcan una conexión de sitio a sitio a través de Internet.

Funcionamiento de las VPNs

Los costos de la comunicación se reducen enormemente porque el cliente sólo paga por el acceso a Internet. Las oficinas remotas se conectan a través de túneles creados sobre Internet. Con el uso de la infraestructura de Internet, una empresa puede desechar la difícil tarea de tener que estar administrando los dispositivos como los que se utilizan en las WAN tradicionales.

En base a los problemas comerciales que resuelven, las VPN de sitio a sitio pueden subdividirse a su vez en VPN intranet y VPN extranet.

VPN intranet. Las VPN intranet se utilizan para la comunicación interna de una compañía. Enlazan una oficina central con todas sus sucursales. Se disfrutan de las mismas normas que en cualquier red privada.

Un enrutador realiza una conexión VPN de sitio a sitio que conecta dos partes de una red privada. El servidor VPN proporciona una conexión enrutada a la red a la que está conectado el servidor VPN.

VPN extranet. Estas VPN enlazan clientes, proveedores, socios o comunidades de interés con una intranet corporativa. Se puede implementar una VPN extranet mediante acuerdo entre miembros de distintas organizaciones. Las empresas disfrutan de las mismas normas que las de una red privada. Sin embargo, las amenazas a la seguridad en una extranet son mayores que en una intranet, por lo que una VPN extranet debe ser cuidadosamente

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

diseñada con muchas políticas de control de acceso y acuerdos de seguridad entre los miembros de la extranet.

Tipos de VPN

Existen diferentes formas de que una organización puede implementar una VPN. Cada fabricante o proveedor ofrece diferentes tipos de soluciones VPN. Cada corporación tendrá que decidir la que más le convenga. Los tipos diferentes de VPN son:

- VPN de firewall
- VPN de router y de concentrador
- VPN de sistema operativo
- VPN de aplicación
- VPN de proveedor de servicios

VPN de firewall

Un firewall (llamado también cortafuegos o servidor de seguridad) es un sistema de seguridad que implanta normas de control de acceso entre dos o más redes.

Se trata de un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no. Un firewall puede ser un dispositivo software o hardware, vamos a hablar detenidamente sobre firewalls más adelante.

Es muy común que se utilice un firewall para proporcionar servicios VPN.

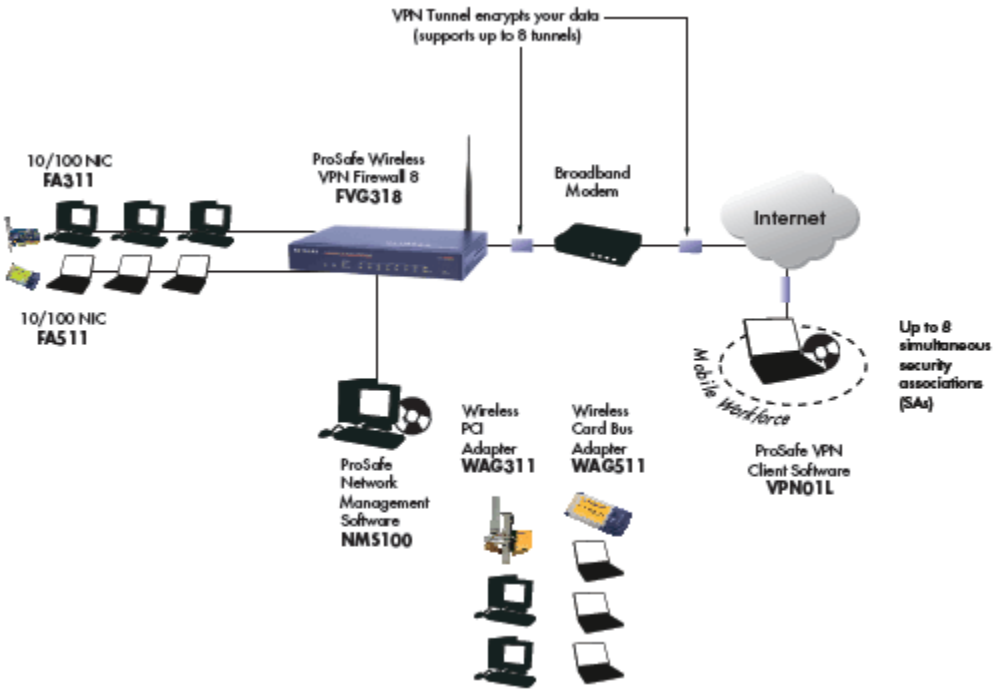
Empresas como Cisco Systems, Nortel Networks y 3Com ofrecen en muchos de sus dispositivos firewall soporte para VPN. Una VPN basada en firewall tiene la ventaja de que simplifica la arquitectura de la red al establecer un único punto de control de seguridad. Además, los ingenieros de redes sólo tienen que hacerse expertos en una tecnología, en lugar de tener que aprender a administrar un firewall y la VPN de forma separada.

Entre los inconvenientes se puede mencionar que tener la VPN en un firewall convierte al dispositivo en algo más complejo, por lo que se debe ser más cuidadoso en su configuración o de lo contrario cualquier intruso podría tener acceso no autorizado a la red.

Otra desventaja ocurre debido a que tener firewall y VPN juntos, se ejerce presión al rendimiento del firewall.

Esto ocurre principalmente si se tienen conectados cientos o incluso miles de usuarios.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes



VPN de sistema operativo

Los sistemas operativos como Windows de Microsoft, Netware de Novell o Linux en sus diferentes distribuciones (Red Hat, Debian,...) ofrecen servicios de VPN ya integrados. La principal ventaja de esta solución es que resulta ser económica ya que en un mismo sistema operativo se pueden contar con una gran variedad de servicios (servidor Web, de nombres de dominio, acceso remoto, VPN) y además mejora los métodos de autenticación y la seguridad del sistema operativo. Tiene la desventaja de que es vulnerable a los problemas de seguridad del propio sistema operativo. Estas VPN se utilizan más para el acceso remoto.

VPN de aplicación

Este tipo de VPN es poco común. Una VPN de aplicación es un programa que añade posibilidades VPN a un sistema operativo. Sin embargo, este programa no queda integrado con el sistema operativo. La ventaja de este tipo de VPN es que la aplicación añade seguridad extra a la que podría ofrecer una VPN integrada al sistema operativo. Un ejemplo de esta VPN es el programa OpenVpn sobre el cual vamos a hacer la práctica.

La desventaja es que estas VPN no soportan una gran cantidad de usuarios y son mucho más lentas que una VPN basada en hardware. Si se utilizan en Internet, son vulnerables a las fallas de seguridad del sistema operativo que contiene a la aplicación.

VPN de proveedor de servicios

Este tipo de VPN es proporcionada por un proveedor de servicios. Al principio las VPN de proveedor de servicios se basaban en tecnologías tales como X.25 y Frame Relay, posteriormente ATM y SMDS y finalmente se ofrecen redes basadas en IP. El proveedor de

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

servicios es la empresa propietaria de la infraestructura tales como equipos y líneas de transmisión que ofrece líneas dedicadas virtuales a sus clientes.

El cliente se conecta a la red del proveedor de servicios a través de un dispositivo de equipo terminal del cliente (CPE) como puede ser un router. El CPE se conecta a través de medios de transmisión al equipo del proveedor de servicios, que puede ser X.25, Frame Relay, un conmutador ATM o un router IP. La línea virtual que se le proporciona al cliente mediante el proveedor de servicios se le llama circuito virtual (VC).

El proveedor de servicios puede cargar o una tarifa plana para el servicio VPN, que habitualmente depende del ancho de banda disponible para el cliente, o una tarifa basada en el uso, que puede depender del volumen de datos intercambiados o de la duración del intercambio de datos.

Acuerdos a nivel del servicio (SLA, Service Level Agreements).

Los SLA son contratos negociados entre proveedores VPN y sus abonados en los que se plantean los criterios de servicio que el abonado espera tengan los servicios específicos que reciba. La SLA es el único documento que está a disposición del abonado para asegurar que el proveedor VPN entrega el servicio o servicios con el nivel y calidad acordados. Si se ha de implementar una VPN basada en proveedor de servicios, este documento es de vital importancia para asegurar un buen servicio.

Requerimientos de una VPN

Una VPN debe de contar con ciertos requerimientos que permitan que valga la pena el uso de esta tecnología. Sin estos requerimientos, las VPN no podrán ofrecer la calidad necesaria que requieren las organizaciones para un desempeño óptimo. Una solución VPN debe ofrecer los siguientes requerimientos:

- Autenticación de usuarios
- Control de acceso
- Administración de direcciones
- Cifrado de datos
- Administración de claves
- Soporte a protocolos múltiples
- Ancho de banda

Autenticación de usuarios

La autenticación es uno de los requerimientos más importantes en una VPN. Cada entidad participante en una VPN debe de identificarse a sí misma ante otros y viceversa. La autenticación es el proceso que permite a los diversos integrantes de la VPN verificar las identidades de todos.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

Existen muchos mecanismos de autenticación pero el más popular de todos ellos es la Infraestructura de Claves Públicas (PKI, Public Key Infraestructure), el cual es un sistema basado en la autenticación por medio de certificados. Cada integrante de una VPN se autentica intercambiando los certificados de cada uno, los cuales están garantizados por una autoridad de certificación (CA, Certification Authority) en la que todos confían.

El proceso de autenticación también involucra el intercambio de información secreta, como una clave o un desafío ante un Servidor de Acceso a Red (NAS, Network Access Server), el cual consultará a un servidor RADIUS. Un servidor RADIUS administra la autenticación en una red que lo requiere.

Control de acceso

El control de acceso en una red está definido como el conjunto de políticas y técnicas que rigen el acceso a los recursos privados de una red por parte de usuarios autorizados. Una vez que un usuario ha sido autenticado, se debe definir a qué recursos de la red puede tener acceso dicho usuario. Los diferentes tipos de VPN, ya sea de firewalls, sistemas operativos, etc; son responsables de gestionar el estado de la conexión del usuario. La VPN debe administrar el inicio de una sesión, permitir el acceso a ciertos recursos, continuar una sesión, impedir el acceso de recursos y terminar una sesión.

El conjunto de reglas y acciones que definen el control de acceso se denomina políticas de control de acceso. Un servidor RADIUS puede administrar el control de acceso basándose en las políticas. Un ejemplo de una regla de control de acceso sería que el servidor permitiera el acceso sólo los usuarios de acceso remoto que no han rebasado un determinado uso de horas de la red.

El principal propósito de una VPN es permitir acceso seguro y selectivo a los recursos de una red. Con un buen sistema de cifrado y autenticación pero sin control de acceso, la VPN sólo protege la integridad del tráfico transmitido y evita que usuarios no autorizados ingresen a

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

la red, pero los recursos de ésta no quedan protegidos. Es por eso que el control de acceso es importante.

Administración de direcciones

Un servidor VPN debe de asignar una dirección IP al cliente VPN y asegurarse de que dicha dirección permanezca privada. Está claro que IP no es un protocolo seguro y se puede ver esto en la inseguridad de Internet. Las direcciones deben ser protegidas con fuertes mecanismos de seguridad, esto es, deben usarse técnicas que permitan la ocultación de la dirección privada dentro de una red pública.

La tecnología más utilizada para ocultar la información es el tunneling. El tunneling es una técnica que encapsula los datos (incluyendo la dirección destino privada) dentro de otro conjunto de datos. Así, el contenido de los paquetes encapsulados se vuelve invisible para una red pública insegura como Internet. Existen muchas tecnologías de tunneling, cada una de ellas con sus ventajas y desventajas. Otra tecnología alterna al tunneling es MPLS, donde se hace uso de un sistema de etiquetas para transmitir información. MPLS es una tecnología que realizará grandes cambios a los métodos tradicionales de enrutamiento y de la forma de crear túneles.

Cifrado de datos

Cifrar o encriptar los datos es una tarea esencial de una VPN. Aunque se puedan encapsular los datos dentro de un túnel, estos todavía pueden ser leídos si no se implementan fuertes mecanismos de cifrado de la información.

Antes de enviar la información, el servidor VPN cifra la información convirtiéndolo en texto cifrado.

El receptor de la información descifra la información y la convierte en texto nativo.

Al principio los algoritmos de encriptación se mantenían en secreto. Sin embargo, cuando el algoritmo era roto, toda la información protegida con dicho algoritmo se volvía vulnerable. Por consiguiente, actualmente los algoritmos se hacen públicos.

Existen muchos tipos de algoritmos de cifrado muy fuertes utilizados en las VPN entre los que podemos encontrar 3DES, Diffie-Hellman, MD5, RSA y SHA-1 los cuales ya debeis conocer ya que los vimos en el tema anterior.

Puesto que el algoritmo de cifrado es conocido por todos, es necesario implementar técnicas para poder mantener los datos seguros. Esto se logra mediante el uso de claves. Una clave es un código secreto que el algoritmo de encriptación utiliza para crear una única versión de texto cifrado. Mientras la longitud en bits de esta clave sea más grande, más difícil será descifrar una información.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

Las VPN requieren del uso de claves con una cierta longitud, de tal manera que resulta prácticamente imposible descifrar los datos (teóricamente tardaría millones de años, a no ser que se posean cientos de procesadores trabajando al mismo tiempo para encontrar la clave y aunque ésta se encontrara, los algoritmos están diseñados de forma que no se garantizaría totalmente el éxito). Aunque de hecho, el uso de claves muy largas no es recomendable porque se afecta mucho el rendimiento de un procesador. Para eso se utilizan métodos como el uso de claves simétricas y asimétricas.

Con una clave simétrica, se usa la misma clave para cifrar y descifrar la información que viaja por un túnel. Tanto el emisor como el receptor de los datos poseen la misma clave privada. Con una clave asimétrica, la información se cifra con una clave y se descifra con otra diferente. Una de las claves sólo es conocida por el usuario, la cual es conocida como clave privada. La otra clave es conocida por todos y se le llama clave pública.

Las claves públicas permiten el uso de firmas digitales para autenticar información. Una clave pública es distribuida libremente a cualquiera que requiera enviar información cifrada o firmada. La clave privada debe ser bien resguardada por el usuario y no darla a conocer nunca.

Administración de claves

En una VPN, es importante la administración de claves. Para asegurar la integridad de una clave pública, ésta es publicada junto con un certificado. Un certificado es una estructura de datos firmada digitalmente por una organización conocida como autoridad de certificación (CA) en la cual todos confían. Una CA firma su certificado con su clave privada. Un usuario que utiliza la clave pública de la CA podrá comprobar que el certificado le pertenece a dicha CA y por lo tanto, la clave pública es válida y confiable.

En una VPN pequeña no es muy necesario establecer una infraestructura de administración de claves. Sin embargo, las grandes compañías obtendrán muchos beneficios si hacen crean una Infraestructura de Claves Públicas (PKI) para poder crear y distribuir certificados. Una corporación puede crear su propia CA o confiar en una CA de terceros. Una PKI es muy útil en aquellas organizaciones que requieren de mucha seguridad y acceso limitado a sus usuarios.

Soporte a protocolos múltiples

Para que una solución VPN sea viable, es necesario también que ésta pueda ofrecer soporte a múltiples protocolos.

Esto incluye el soporte a protocolos de red que no sean IP como pueden ser AppleTalk, IPX y NetBEUI. PPTP soporta varios protocolos de red. IPSec sólo puede ser utilizado en redes basadas en IP, pero siempre es posible encapsular los protocolos no compatibles dentro de un paquete IP, de modo que puedan ser transportados. En cuanto a L2TP, este protocolo VPN no sólo puede ser implementado en redes IP, sino también en ATM y Frame Relay.

Ancho de banda

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

El ancho de banda es también un requerimiento importante en una VPN. En el mundo de las redes existe un concepto que define la forma de administrar el ancho de banda con el fin de que el tráfico de una red fluya de forma eficiente.

Dicho concepto es la Calidad de Servicio (QoS, Quality of Service). La QoS es una característica muy importante de una VPN. Una solución VPN no estará completa si no proporciona formas para el control y administración del ancho de banda.

La calidad del servicio también se refiere al número de conexiones simultáneas (la cantidad de túneles que pueden ser establecidos entre un sitio remoto y el sitio central) que puede soportar una VPN y la forma cono ésta afecta al rendimiento de la VPN.

Es preciso también asegurarse que una VPN puede cifrar y descifrar los paquetes transmitidos a una velocidad adecuada, ya que algunos algoritmos de cifrado son lentos y si no se tiene un buen procesador el rendimiento se verá afectado. Es importante mencionar que el valor nominal de velocidad de los dispositivos de redes (por ejemplo 100 Mbps) nunca se cumple en la realidad y que eso habrá que tomarse en cuenta a la hora de implementar una VPN.

La calidad de las conexiones a Internet también es importante. Las técnicas de encriptación incrementan el deterioro del rendimiento de la comunicación por las sobrecargas. Las pérdidas de paquetes y la latencia en conexiones a Internet de baja calidad afecta más al rendimiento, que la carga añadida por la encriptación.

Tunneling y VPN

Cuando el uso de túneles se combina con el cifrado de los datos, puede utilizarse para proporcionar servicios de VPN. Las VPN utilizan el tunneling para poder ofrecer mecanismos seguros de transporte de datos. Dentro del contexto de las VPN, el tunneling involucra tres tareas principales:

- Encapsulación
- Protección de direcciones privadas
- Integridad de los datos y confidencialidad de éstos

Para que el proceso del tunneling pueda ser llevado a cabo, existen diversos protocolos llamados protocolos de túnel los cuales se encargan de encapsular y desencapsular los datos que viajan dentro de una red privada virtual.

Los protocolos de túnel usados por las VPN como PPTP y L2TP son usados para encapsular tramas de la capa de enlace de datos (PPP). Protocolos de túnel como IP sobre IP e IPSec en modo túnel son utilizados para encapsular paquetes de la capa de red.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

Es posible colocar un paquete que utiliza una dirección IP privada dentro de un paquete que usa una dirección IP global única para poder extender una red privada sobre una red pública como Internet. Puesto que los contenidos del paquete entunelado sólo pueden ser interpretados por las interfaces de túnel, las direcciones IP privadas pueden ser ocultadas completamente de las redes IP públicas.

Los mecanismos de integridad y confidencialidad garantizan que ningún usuario no autorizado pueda alterar los paquetes entunelados durante la transmisión sin que el ataque pueda ser detectado y que los contenidos del paquete permanecen protegidos de acceso no autorizado. Además, el tunneling opcionalmente puede proteger la integridad de la cabecera del paquete IP externo, mediante técnicas de autenticación. Por ejemplo, si se utiliza IPSec los protocolos AH y ESP pueden proporcionar autenticación de los paquetes transmitidos.

Tres protocolos de túnel son los más usados para la creación de una VPN:
- Protocolo de Túnel punto a punto (PPTP)
- Protocolo de Túnel de Capa 2 (L2TP)
- Protocolo de Seguridad IP

Los protocolos PPTP y L2TP se enfocan principalmente a las VPN de acceso remoto, mientras que IPSec se enfoca mayormente en las soluciones VPN de sitio a sitio.

Los túneles se clasifican de acuerdo a cómo se establece la conexión entre dos hosts. En base a esto, existen dos tipos de túneles. Éstos son:
- Túnel voluntario
- Túnel obligatorio

Túnel voluntario

Un equipo usuario o cliente puede emitir una petición VPN para configurar y crear un túnel voluntario. En este caso, el equipo del usuario es un extremo del túnel que funciona como cliente de túnel. El túnel voluntario se produce cuando una estación de trabajo o un router utilizan software de cliente de túnel para crear una conexión VPN con el servidor de túnel de destino. Para ello, debe instalar el protocolo de túnel correspondiente en el equipo cliente. Un túnel voluntario puede ser creado de dos maneras a través de una conexión dial-up o a través de una lan.

- A través de una conexión dial-up: En este caso, el usuario primero hace una llamada a su ISP para conectarse a Internet y entonces posteriormente podrá ser creado el túnel. Esta suele ser la situación más común. La conexión a Internet es un paso preliminar para crear el túnel pero no forma parte del proceso de creación del túnel.

- A través de una LAN: En este caso, el cliente ya posee una conexión a la red, por lo que el túnel puede ser creado con cualquier servidor túnel deseado. Este es el caso de un usuario de una LAN que crea un túnel para acceder a otra LAN.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

Túnel obligatorio

El túnel obligatorio es la creación de un túnel seguro por parte de otro equipo o dispositivo de red en nombre del equipo cliente. Los túneles obligatorios se configuran y crean automáticamente para los usuarios sin que éstos intervengan ni tengan conocimiento de los mismos. Con un túnel obligatorio, el equipo del usuario no es un extremo del túnel. Lo es otro dispositivo entre el equipo del usuario y el servidor de túnel que actúa como cliente de túnel.

Algunos proveedores que venden servidores de acceso telefónico facilitan la creación de un túnel en nombre de un cliente de acceso telefónico. El dispositivo que proporciona el túnel para el equipo cliente se conoce como procesador cliente (FEP) o PAC en PPTP, concentrador de acceso (LAC) de L2TP en L2TP o puerta de enlace (gateway) de Seguridad IP en IPSec. Para realizar su función, el dispositivo que proporciona el túnel debe tener instalado el protocolo de túnel adecuado y debe ser capaz de establecer el túnel cuando el equipo cliente intenta establecer una conexión.

Esta configuración se conoce como túnel obligatorio debido a que el cliente está obligado a utilizar el túnel creado por el dispositivo que proporciona el túnel. Una vez que se realiza la conexión inicial, todo el tráfico de la red de y hacia el cliente se envía automáticamente a través del túnel. En los túneles obligatorios, la computadora cliente realiza una conexión única PPP y, cuando un cliente se conecta en el NAS, se crea un túnel y todo el tráfico se enruta automáticamente a través de éste. Se puede configurar un el dispositivo que proporciona el túnel para hacer un túnel a todos los clientes hacia un servidor específico del túnel. De manera alterna, el dispositivo que proporciona el túnel podría hacer túneles individuales de los clientes basados en el nombre o destino del usuario.

A diferencia de los túneles por separado creados para cada cliente voluntario, un túnel entre el dispositivo que proporciona el túnel y el servidor del túnel puede estar compartido entre varios clientes. Cuando un segundo cliente se conecta al dispositivo que proporciona el túnel para alcanzar un destino para el cual ya existe un túnel, no hay necesidad de crear una nueva instancia del túnel entre el dispositivo que proporciona el túnel y el servidor del túnel. El tráfico de datos para el nuevo cliente se transporta sobre el túnel existente. Ya que puede haber varios clientes en un túnel único, el túnel no se termina hasta que se desconecta el último usuario del túnel.

Una compañía puede contratar a un ISP para que implemente un conjunto de dispositivos que proporcionen túneles por todos los territorios donde existan LAN de la compañía. Estos dispositivos pueden establecer túneles a través de Internet hasta un servidor VPN conectado a la red privada de la organización, consolidando así las llamadas de zonas geográficamente dispersas en una sola conexión a Internet en la red de la organización.

Existen dos formas de crear túneles obligatorios. En la primera forma, el túnel se crea antes de autenticar al cliente de acceso. Una vez creado el túnel, el cliente de acceso se autentica en el servidor de túnel. En la segunda forma, el túnel se crea después de que el dispositivo que proporciona el túnel autentica al cliente de acceso.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

La seguridad de una VPN debe ir más allá que simplemente controlar el acceso seguro a los recursos de una red.

También debe proveer mecanismos para administrar la implementación de pólizas de seguridad que garanticen el desarrollo exitoso de una VPN. La mejor opción es establecer también, antes de que se establezca la conexión cifrada con una oficina o LAN remota, unos niveles de seguridad que deben cumplirse. La comprobación de los niveles de seguridad que debe cumplir el equipo remoto que desea conectarse a la red corporativa debe ser lo más amplia posible.

Sin duda, es necesario establecer un sistema de chequeo del status de seguridad de los equipos remotos conectados mediante VPN a la red corporativa. Y el chequeo debe ser percibido por el usuario remoto como una ayuda a la seguridad general, no como una imposición corporativa y además, debe hacerse con suficiente amplitud como para abarcar productos y sistemas de seguridad no corporativos, sino elegidos por el teletrabajador en su ámbito doméstico.

La autenticación de usuarios y la encriptación de datos son características de seguridad muy fuertes. Y en una VPN la tecnología que podrá ofrecer mejor seguridad será IPSec.

3. Redes inalámbricas

El protocolo 802.1x

La IEEE 802.1X es una norma del IEEE para el control de acceso a red basada en puertos. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto o previniendo el acceso por ese puerto si la autenticación falla. Es utilizado en algunos puntos de acceso inalámbricos cerrados y se basa en el protocolo de autenticación extensible (EAP–RFC 2284). El RFC 2284 ha sido declarado obsoleto en favor del RFC 3748.

802.1X está disponible en ciertos conmutadores de red y puede configurarse para autenticar nodos que están equipados con software suplicante. Esto elimina el acceso no autorizado a la red al nivel de la capa de enlace de datos. Algunos proveedores están implementando 802.1X en puntos de acceso inalámbricos que pueden utilizarse en ciertas situaciones en las cuales el punto de acceso necesita operarse como un punto de acceso cerrado, corrigiendo deficiencias de seguridad de WEP. Esta autenticación es realizada normalmente por un tercero, tal como un servidor RADIUS. Esto permite la autenticación sólo del cliente o, más apropiadamente, una autenticación mutua fuerte utilizando protocolos como EAP-TLS.

Debido a las carencias de 802.11 ha sido necesario establecer una nueva normativa estándar

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

que permita tanto la autenticación como el intercambio dinámico de contraseñas, de forma fácil y segura.

El estándar IEEE 802.1X proporciona un sistema de control de dispositivos de red, de admisión, de tráfico y gestión de claves para dispositivos tos en una red inalámbrica. 802.1X se basa en puertos, para cada cliente dispone de un puerto que utiliza para establecer una conexión punto a punto. Mientras el cliente no se ha validado este puerto permanece cerrado. Cada una de estas funcionalidades se puede utilizar por separado, permitiendo a WPA, por ejemplo, utilizar 802.1X para aceptar a una estación cliente.

Para el control de admisión 802.1X utiliza un protocolo de autenticación denominado EAP y para el cifrado de datos CCMP y esto es lo que se conoce como RSN (Robust Secure Network) o también WPA2. No todo el hardware admite CCMP.

Autenticación en redes inalámbricas con 802.1x, WPA y WPA2

Las redes WiFi están afectadas por problemas de acceso no autorizado, mucho más que las redes de cable. Esto es obvio si piensas que para acceder a un punto de acceso físico es necesario (conector RJ45), en las redes inalámbricas sólo tienes que estar dentro del rango de cobertura para acceder a ella.

Una primera solución al problema fue WEP (Wired Equivalent Privacy). Sin embargo, este método, asociado con la presencia de claves cifradas simétricas en ambos los puntos de acceso y todos los clientes autorizados para el acceso, dio a los administradores de red el trabajo de cambiar periódicamente las claves y comunicar el cambio a todos los usuarios. El resultado fue que las claves WEP se mantuvieron sin cambios durante largos períodos de tiempo, haciendo que la red fuese insegura.

Desde el punto de vista práctico, el protocolo 802.1x es otro que el protocolo EAP (Extensible Authentication Protocol) de autenticación utilizado para autenticar conexiones punto a punto, adaptado para funcionar en las tramas Ethernet en lugar de paquetes PPP. Por esta razón el protocolo 802.1x es también conocido como EAPoL (EAP sobre LAN).

En la terminología EAP las entidades que juegan un papel durante el proceso de autenticación se incluyen: el suplicante, es decir, el cliente pide que acceder a la red, el autenticador que en las redes inalámbricas coincide con el Punto de acceso, servidor de la autenticación que verifica si los usuarios son realmente quienes dicen ser.

El servidor de autenticación es a menudo uno y el mismo que el servidor RADIUS, mientras que el autenticador es lo que se define como NAS (Network Access Server) en el protocolo RADIUS.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

Como se mencionó anteriormente EAP es sólo un protocolo de autenticación que ofrece el servidor de autenticación suplicante y la tarea de establecer el método de autenticación real de uso. Puede verse que el punto de acceso es transparente desde este punto de vista, ya que su único trabajo consiste en reenviar los paquetes a través de la suplicante EAPoL con el servidor RADIUS y los encapsula en IP (el servidor RADIUS se puede llegar por la parte cableada de la AP) y viceversa.

La suite de protocolos EAP

Autentificación en redes Wifi: EAP, EAP-MD5, LEAP

Vamos a ver los mecanismos de seguridad de las redes wifi, donde trataremos sus puntos fuertes y los potenciales puntos vulnerables. Las redes Wifi tienen dos mecanismos de seguridad, que son los mismos que llevamos repitiendo a lo largo de todos los temas:

- La autentificación: que permite el acceso a redes Wlan únicamente al personal autorizado para ello
- La encriptación: que permite que la información no sea interceptada por terceros y la integridad de la misma

AUTENTIFICACIÓN: Existen distintos tipos de autentificación en las conexiones wireless y casi todas ellas tienen como base EAP, a continuación se tratan aquellos que son más habituales, sus ventajas, sus inconvenientes y los fallos de seguridad reportados a día de hoy.

EAP (Extensible Authentication Protocol)

EAP realmente no es un mecanismo de autentificación. Más bien es una estructura que da soporte a los mecanismos de autentificación como Kerberos, certificados, LADP… Puede ser utilizado para redes cableadas y para redes inalámbricas, aunque su uso es más habitual en redes wireless. Descrito en el RFC 2284 (RFC2284)

Fue creado como una extensión para conexiones PPP, protocolo punto a punto que acabamos de ver. EAP no de depende del protocolo de IP, por lo tanto no necesita de conectividad IP proporcionando un método flexible de control que opera en la capa de enlace de datos. Asimismo EAP tiene soporte para la retransmisión de paquetes, aunque no soporta fragmentación ni reensamblaje, trabaja con 4 tipos de paquetes:

- petición o request identity
- respuesta o identity response
- éxito o success
- fallo o failure

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

El mecanismo de autentificación y de cifrado son independientes. EAP lleva a cabo una autentificación mutua entre el cliente y el servidor, ambos están obligados a demostrar su autentificación para prevenir ataques tipo Man In The Middle con excepción de EAP-MD5, en el que el servidor no es autentificado. EAP permite la generación y distribución de claves dinámicas. (El AP cumple con la función de pasarela entre el cliente y el servidor de autentificación).

1. -El cliente solicita conectarse.
2. -El AP solicita al cliente que se identifique (request identity).
3. -El cliente se identifica (identity response).
4. -El AP lo traslada al servidor de autentificación.
5. -El servidor transmite al AP un challenge (reto o método para verificar la identificación) y el AP se lo envía al cliente.
6. -El cliente responde y el servidor lo evalúa enviando un success o un failure.
7. -El servidor envía información sobre las claves de cifrado.
8. -Con esta información el cliente genera las claves de cifrado mediante un mecanismo de cifrado para el tráfico de red.

Dos tipos de clave:
1-Clave de sesión (pairwise key). Únicas para cada cliente y AP, para el tráfico unicast.
2-Clave de grupo (groupwise key). Compartidas para todos los clientes y el AP, tráfico multicast y broadcast.

Los protocolos de autentificación basados en EAP son:
-EAP-MD5
-LEAP
-EAP-TLS
-EAP-TTLS
-EAP-PEAP

EAP-MD5 (EAP Menssage Digest 5)

Es el primer sistema de autentificación basado en EAP y es el más básico de todos. Descrito en el RFC 2284 La autentificación se realiza por usuario y no por dispositivo y se basa en la generación de claves mediante el algoritmo MD5.

El cliente envía un Hash que contiene el nombre de usuario, la contraseña y una cadena arbitraria, el servidor recibe el Hash, crea uno nuevo con la contraseña y con la cadena arbitraria, compara ambos Hash, si coinciden el cliente estará autentificado correctamente. De fácil implementación ya que no requiere servidor Radius. Requiere una clave WEB fija y manual, no permitiendo la distribución automática de claves.

Las credenciales se envían en texto plano, sin ninguna medida de protección, por lo que está expuesto a ataques de fuerza bruta y de diccionario. Algunas de las herramientas que permiten realizar estos ataques son: Eapmd5pass y Eapmd5crack.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

No existe autentificación mutua entre cliente y el AP, únicamente el cliente se autentifica con el AP, existiendo el riesgo de suplantación de la identidad del AP y siendo susceptible a ataques de tipo Man In The Middle, y Hijack Session…

Conclusión: EAP-MD5 no es un mecanismo de autentificación seguro.
LEAP (Ligtheight Extensible Authentication Protocol)EAP Ligero desarrollado por Cisco. Ofrece una autentificación basada en usuarios y no en dispositivos.

LEAP proporciona un mecanismo de autentificación mutua basado en contraseñas, se produce un intercambio de valores Hash de tipo desafio/respuesta, el servidor envía un desafío que el cliente debe responder con la contraseña tras combinarla con la cadena de desafió creada por el servidor, enviándose en texto plano las credenciales, como todos los sistemas de autentificación basados en contraseñas es vulnerable a ataques de diccionario/fuerza bruta: http://www.securityfocus.com/archive/1/340365/2003-10-03/2003-10-09/2 y http://www.securityfocus.com/archive/1/340565/2003-10-03/2003-10-09/2 por medio de programas como AsLeap.

Asleap tiene las siguientes **funciones**:

- Recuperar contraseñas débiles
- Leer en tiempo real desde cualquier interfaz inalámbrica con la opción RFMON.
- Monitorear un solo canal, o realizar scanning en busca de objetivos.
- Desautentificar a usuarios en redes LEAP, obligándoles a volver a autenticarse. Esto hace que la captura de contraseñas sea muy rápida.
- Leer archivos almacenados libpcap, o AiroPeek archivos de NX (1.X o 2.X).
- Usar una tabla de base de datos dinámica y el índice para realizar búsquedas en archivos de gran tamaño de forma muy rápida. Reduce el tiempo de búsqueda que en ell peor de los casos es del 0,0015% en comparación con las búsquedas en un archivo plano.
- Escribir solo el intercambio de información en un archivo de LEAP libpcap. Esto podría ser utilizado para capturar las credenciales LEAP con un dispositivo con poco espacio en disco (con una Tablet), y luego procesar las credenciales LEAP almacenadas en el archivo libpcap en un sistema con recursos de almacenamiento.

Funciona en sistemas Windows con funcionalidad limitada Leap tiene la ventaja de permitir la utilización de claves dinámicas facultando a los clientes autenticarse con frecuencia, adquiriendo cada vez una nueva clave, además de utilizar MS-CHAP v2 (un protocolo de autentificación de contraseñas de cifrado por desafió mutuo que es irreversible), aunque los dos primeros bits del hash no contienen salt. (salt es un conjunto de datos que se añaden cuando se crea el Hash e impide que se utilicen tablas pre-calculadas, las rainbow tables).

Tiene el inconveniente de necesitar de infraestructura Cisco, así como de un servidor de autentificación que soporte certificados Cisco. Cisco sigue implementándolo en sus

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

dispositivos a día de hoy, aquí el link a Cisco LEAP donde se puede encontrar más información.

Conclusión: LEAP no es seguro, por mucho que diga Cisco que si lo es. Cisco sigue implementándolo en sus dispositivos. Existen empresas que aún utilizan LEAP. Con una buena rainbow table y con Asleap en muy poco tiempo se consigue las credenciales.

4. Firewalls

Introducción

Concepto y origen

El concepto de firewall o muro de fuego, proviene de la mecánica automotriz, donde se lo considera una lámina protectora / separadora entre el habitáculo de un vehículo y las partes combustibles del motor, que protege a sus pasajeros en caso de incendio.

Análogamente, un firewall, en un sentido más informático, es un sistema capaz de separar el habitáculo de nuestra red, o sea, el área interna de la misma, del posible incendio de crackers que se produciría en ese gran motor que es internet.

El primer documento publicado para la tecnología firewall data de 1988, cuando el equipo de ingenieros Digital Equipment Corporation (DEC) desarrolló los sistemas de filtro conocidos como cortafuegos de filtrado de paquetes. Este sistema, bastante básico, fue la primera generación de lo que se convertiría en una característica más técnica y evolucionada de la seguridad de Internet. En AT&T Bell, Bill Cheswick y Steve Bellovin, continuaban sus investigaciones en el filtrado de paquetes y desarrollaron un modelo de trabajo para su propia empresa, con base en su arquitectura original de la primera generación.

Durante 1989 y 1990, tres colegas de los laboratorios AT&T Bell, Dave Presetto, Janardan Sharma, y Nigam Kshitij, desarrollaron la segunda generación de servidores de seguridad. Esta segunda generación de cortafuegos tiene en cuenta, además, la colocación de cada paquete individual dentro de una serie de paquetes. Esta tecnología se conoce generalmente como la inspección de estado de paquetes, ya que mantiene registros de todas las conexiones que pasan por el cortafuegos, siendo capaz de determinar si un paquete indica el inicio de una nueva conexión, es parte de una conexión existente, o es un paquete erróneo. Este tipo de cortafuegos pueden ayudar a prevenir ataques contra conexiones en curso o ciertos ataques de denegación de servicio.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

Tercera generación - cortafuegos de aplicación

Son aquellos que actúan sobre la capa de aplicación del modelo OSI. La clave de un cortafuegos de aplicación es que puede entender ciertas aplicaciones y protocolos (por ejemplo: protocolo de transferencia de ficheros, DNS o navegación web), y permite detectar si un protocolo no deseado se coló a través de un puerto no estándar o si se está abusando de un protocolo de forma perjudicial.

Un cortafuegos de aplicación es mucho más seguro y fiable cuando se compara con un cortafuegos de filtrado de paquetes, ya que repercute en las siete capas del modelo de referencia OSI. En esencia es similar a un cortafuegos de filtrado de paquetes, con la diferencia de que también podemos filtrar el contenido del paquete. El mejor ejemplo de cortafuegos de aplicación es ISA (Internet Security and Acceleration)

Acontecimientos posteriores

En 1992, Bob Braden y DeSchon Annette, de la Universidad del Sur de California (USC), dan forma al concepto de cortafuegos. Su producto, conocido como "Visas", fue el primer sistema con una interfaz gráfica con colores e iconos, fácilmente implementable y compatible con sistemas operativos como Windows de Microsoft o MacOS de Apple.

En 1994, una compañía israelí llamada Check Point Software Technologies lo patentó como software denominándolo FireWall-1.

La funcionalidad existente de inspección profunda de paquetes en los actuales cortafuegos puede ser compartida por los sistemas de prevención de intrusiones (IPS). Actualmente, el Grupo de Trabajo de Comunicación Middlebox de la Internet Engineering Task Force (IETF) está trabajando en la estandarización de protocolos para la gestión de cortafuegos.

Otro de los ejes de desarrollo consiste en integrar la identidad de los usuarios dentro del conjunto de reglas del cortafuegos. Algunos cortafuegos proporcionan características tales como unir a las identidades de usuario con las direcciones IP o MAC. Otros, como el cortafuegos NuFW, proporcionan características de identificación real solicitando la firma del usuario para cada conexión.

¿Qué es un firewall?

Un firewall es un sistema o un grupo de sistemas que implementan una política de control de acceso entre dos o más redes. Podemos imaginarlo como compuesto por dos grandes módulos; uno destinado a bloquear los accesos y el otro a permitirlos.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

¿Por qué un firewall?

Básicamente la razón para la instalación de un firewall es casi siempre la misma: proteger una red privada contra intrusos dentro de un esquema de conectividad a Internet.

En la mayoría de los casos, el propósito es prevenir el acceso de usuarios no autorizados a los recursos computacionales en una red privada y a menudo prevenir el tráfico no autorizado de información propietaria hacia el exterior.

Objetivo de un Firewalls

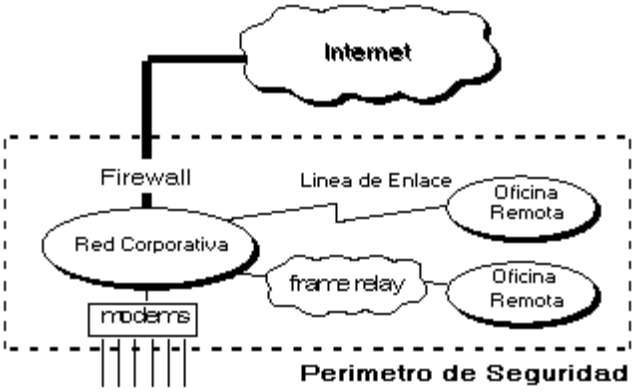
Un firewall sirve para múltiples propósitos, entre otros podemos anotar los siguientes:

- Restricción de entrada de usuarios a puntos cuidadosamente controlados de la red interna.
- Prevención ante los intrusos que tratan de ganar espacio hacia el interior de la red y los otros esquemas de defensas establecidos.
- Restricción de uso de servicios tanto a usuarios internos como externos.
- Determinar cuáles de los servicios de red pueden ser accedidos dentro de ésta por los que están fuera, es decir, quién puede entrar a utilizar los recursos de red pertenecientes a la organización.

Todo el tráfico que viene de la Internet o sale de la red corporativa interna pasa por el firewall de tal forma que él decide si es aceptable o no.

El firewall determina cual de los servicios de red pueden ser accedidos dentro de esta por los que están fuera, es decir quién puede entrar para utilizar los recursos de red pertenecientes a la organización.

Para que un firewall sea efectivo, todo tráfico 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 tráfico, 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 en torno a éste.



El firewall permite al administrador de la red definir un "choke point" (envudo), manteniendo al margen los usuarios no-autorizados 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 es que ayuda a simplificar los trabajos de administración. El firewall ofrece un punto donde

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

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 tránsito de los datos.

Tipos básicos de firewalls

Conceptualmente hay dos tipos de firewalls, nivel de red y nivel de aplicación aunque los firwalls pueden ser físicos o lógicos, esto quiere decir que pueden ser máquinas reales compradas para tal propósito incluso routers con estas características o pueden ser aplicaciones que forman parte de nuestro sistema operativo o que instalamos para este fin.

- **Firewall de red**: Los firewalls de nivel de red toman sus acciones en función del origen, la dirección de destino y el port en cada paquete IP. Los modernos firewalls de este tipo se han sofisticado y mantienen información respecto del estado de las conexiones que están activas a través de él, etc.. Este tipo de firewall tienden a ser muy rápidos y son transparentes al usuario.
- **Firewall de aplicación**: Los firewalls de nivel de aplicación por lo general son hosts corriendo proxy servers, que no permiten el tráfico directo entre redes, manteniendo una elaborada auditoría y logeo del tráfico que pasa a través de él. Este tipo de firewall puede ser utilizado para realizar las tareas relativas al NAT, debido a que como las comunicaciones van de un lado hacia el otro se puede enmascarar la ubicación original. Este tipo tiende a proveer una auditoría más detallada y un mayor grado de seguridad que los de nivel de red

Políticas de diseño de firewalls

Las políticas de accesos en un Firewalls se deben diseñar poniendo principal atención en sus limitaciones y capacidades pero también pensando en las amenazas y vulnerabilidades presentes en una red externa insegura. Conocer los puntos a proteger es el primer paso a la hora de establecer normas de seguridad. También es importante definir los usuarios contra los que se debe proteger cada recurso, ya que las medidas diferirán notablemente en función de esos usuarios. Generalmente se plantean algunas preguntas fundamentales que debe responder cualquier política de seguridad:

- ¿Qué se debe proteger? Se deberían proteger todos los elementos de la red interna (hardware, software, datos, etc.).
- ¿De quién protegerse? De cualquier intento de acceso no autorizado desde el exterior y contra ciertos ataques desde el interior que puedan preverse y prevenir. Sin embargo, podemos definir niveles de confianza, permitiendo selectivamente el acceso de determinados usuarios externos a determinados servicios o denegando cualquier tipo de acceso a otros.
- ¿Cómo protegerse? Esta es la pregunta más difícil y está orientada a

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

establecer el nivel de monitorización, control y respuesta deseado en la organización. Puede optarse por alguno de los siguientes paradigmas o estrategias:

Paradigmas de seguridad

- Se permite cualquier servicio excepto aquellos expresamente prohibidos.
- Se prohíbe cualquier servicio excepto aquellos expresamente permitidos. La más recomendada y utilizada aunque algunas veces suele acarrear problemas por usuarios descontentos que no pueden acceder a tal cual servicio.

Estrategias de seguridad

- Paranoica: se controla todo, no se permite nada.
- Prudente: se controla y se conoce todo lo que sucede.
- Permisiva: se controla pero se permite demasiado.
- Promiscua: no se controla (o se hace poco) y se permite todo.

¿Cuánto costará? Estimando en función de lo que se desea proteger se debe decidir cuánto es conveniente invertir.

Tipos de firewall por funcionalidad

De acuerdo a las técnicas de filtrado de tráfico que se implementan, los firewalls pueden clasificarse en diferentes tipos:

Filtrado de paquetes stateless (sin estado):

Es la forma más básica de filtrado de tráfico. Usualmente se aplica en dispositivos de capa de red e implementa conjuntos de reglas estáticas que examinan los encabezados de cada paquete para permitir o denegar el tráfico, sin ninguna relación con los flujos de tráfico precedentes. Trabajan bien cuando el objetivo filtra aplicaciones basadas en TCP que no utilizan negociación dinámica de puertos.

Filtrado de paquetes statefull (con estado):

Es un método de filtrado de paquetes que trabaja a nivel de flujo o conexión, con ocasionales intervenciones a nivel de la aplicación. Mantienen una tabla de estado que hace seguimiento de las sesiones que atraviesan el firewall y en función de ella hace inspección de cada paquete que atraviesa el dispositivo. El mecanismo asume que si se permite el inicio de la conexión, cualquier conexión adicional que requiera esa aplicación será permitida. Es un mecanismo confiable para filtrar tráfico de red entre dominios de seguridad.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

Filtrado de paquetes stateful con inspección (SPI (Stateful Packet Inspection)) y control de aplicaciones:

Se trata de firewalls stateful que incorporan motores de análisis de tráfico que suman servicios adicionales que reciben la denominación de AIC (Application Inspection and Control) o DPI (Deep Packet Inspection). Estos sistemas reensamblan en memoria las sesiones de capa de transporte para realizar inspección de protocolos de capa de aplicación y decodifican los protocolos de capa de aplicación para permitir filtrado de protocolos y contenidos. Pueden verificar los protocolos de capa de aplicación para eliminar paquetes que no se conformen con el funcionamiento estándar del protocolo.

Sistemas de prevención de intrusos en la red: NIPS (Network Intrusion Prevention Systems):

También conocidos como IDS/IPS o IDPS (Intrusion Detection Prevention System), los vamos a tratar en detalle en el siguiente tema. Son sistemas que analizan el tráfico de la red con el propósito de bloquear tráfico malicioso conocido. Se asienta en una base de datos de ataques que debe ser actualizada periódicamente. Son mecanismos permisivos y usualmente no pueden detectar amenazas nuevas a menos que hayan sido incluidas en las actualizaciones.

Gateways de aplicaciones (proxies):

Es un sistema de software diseñado para actuar como intermediario y reenviar requerimientos de capa de aplicación y respuestas entre los clientes y los servidores. En términos de control de acceso, permite un filtrado y seguimiento muy granular tanto de las solicitudes como de las respuestas. Brindan opciones de control de acceso confiables para los protocolos soportados. Sin embargo, hay que tener presente que no hay proxies disponibles para todas las aplicaciones corporativas y no se aplican a aplicaciones de tiempo real.

Tipos de arquitecturas de firewalls

Firewall de filtrado de paquetes

Se utilizan Routers con filtros y reglas basadas en políticas de control de acceso. El Router es el encargado de filtrar los paquetes (un Choke) basados en cualquiera de los siguientes criterios:

1. Protocolos utilizados.
2. Dirección IP de origen y de destino.
3. Puerto TCP–UDP de origen y de destino.

Estos criterios permiten gran flexibilidad en el tratamiento del tráfico. Restringiendo las comunicaciones entre dos computadoras (mediante las direcciones IP) se permite determinar entre cuales máquinas la comunicación está permitida. El filtrado de paquetes mediante puertos y protocolos permite establecer que servicios estarán disponibles al

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

usuario y por que puertos.
Se puede permitir navegar en la WWW (puerto 80 abierto) pero no acceder a la transferencia de archivos vía FTP (puerto 21 cerrado). Debido a su funcionamiento y estructura basada en el filtrado de direcciones y puertos este tipo de Firewalls trabajan en los niveles de Transporte y de Red del Modelo OSI y están conectados a ambos perímetros (interior y exterior) de la red. Tienen la ventaja de ser económicos, tienen un alto nivel de desempeño y son transparentes para los usuarios conectados a la red. Sin embargo presenta **debilidades** como:

1. No protege las capas superiores a nivel OSI.
2. Las necesidades aplicativas son difíciles de traducir como filtros de protocolos y puertos.
3. No son capaces de esconder la topología de redes privadas, por lo que exponen la red al mundo exterior.
4. Sus capacidades de auditoría suelen ser limitadas, al igual que su capacidad de registro de actividades.
5. No soportan políticas de seguridad complejas como autentificación de usuarios y control de accesos con horarios prefijados.

Cualquier router ip utiliza reglas de filtrado para reducir la carga de la red, por ejemplo, se descartan paquetes cuyo ttl (time to live o tiempo de vida) ha llegado a cero, paquetes con un control de errores erróneos, o simplemente tramas de broadcast. Además de estas aplicaciones, el filtrado de paquetes se puede utilizar para implementar diferentes políticas de seguridad en una red. El objetivo principal de todas ellas suele ser evitar el acceso no autorizado entre dos redes, pero manteniendo intactos los accesos autorizados. Su funcionamiento es habitualmente muy simple: se analiza la cabecera de cada paquete, y en función de una serie de reglas establecidas de antemano la trama es bloqueada o se le permite seguir su camino. Estas reglas suelen contemplar campos como el protocolo utilizado (tcp, udp, icmp. . .), las direcciones fuente y destino, y el puerto destino, lo cual ya nos dice que el firewall ha de ser capaz de trabajar en los niveles de red (para discriminar en función de las direcciones origen y destino) y de transporte (para hacerlo en función de los puertos usados). Además de la información de cabecera de las tramas, algunas implementaciones de filtrado permiten especificar reglas basadas en la interfaz del router por donde se ha de reenviar el paquete, y también en la interfaz por donde ha llegado hasta nosotros.

¿Cómo se especifican tales reglas?

Generalmente se expresan como una simple tabla de condiciones y acciones que se consulta en orden hasta encontrar una regla que permita tomar una decisión sobre el bloqueo o el reenvío de la trama, adicionalmente, ciertas implementaciones permiten indicar si el bloqueo de un paquete se notificaría la máquina origen mediante un mensaje icmp.

Siempre hemos de tener presente el orden de análisis de las tablas para poder implementar la política de seguridad de una forma correcta, cuanto más complejas sean las reglas y su

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

orden de análisis, más difícil será para el administrador comprenderlas. Independientemente del formato, la forma de generar las tablas dependerá obviamente del sistema sobre el que trabajemos, por lo que es indispensable consultar su documentación. Algunos ejemplos particulares – pero aplicables a otros sistemas – pueden encontrarse en http://www.fwtk.org/fwtk/docs/overview.pdf

Por ejemplo, imaginemos una hipotética tabla de reglas de filtrado de la siguiente forma:

Origen	Destino	Tipo	Puerto	Acción
158.43.0.0	*	*	*	Deny
*	195.53.22.0	*	*	Deny
158.42.0.0	*	*	*	Allow
*	193.22.34.0	*	*	Allow

Si al cortafuegos donde está definida la política anterior llegara un paquete proveniente de una máquina de la red 158.43.0.0 se bloqueará su paso, sin importar el destino de la trama, de la misma forma, todo el tráfico hacia la red 195.53.22.0 también se detendrá.

Pero, **¿qué sucedería si llega un paquete de un sistema de la red 158.42.0.0 hacia 193.22.34.0?** Una de las reglas nos indica que dejemos pasar todo el tráfico proveniente de 158.42.0.0, pero la siguiente nos dice que si el destino es 193.22.34.0 lo bloqueemos sin importar el origen. En este caso depende de nuestra implementación particular y el orden de análisis que siga.

Si se comprueban las reglas desde el principio, el paquete atravesaría el cortafuegos, ya que al analizar la tercera entrada se finalizarían las comprobaciones. Si operamos al revés, el paquete se bloqueará porque leemos antes la última regla.

Como podemos ver, ni siquiera en nuestra tabla – muy simple – las cosas son obvias, por lo que si extendemos el ejemplo a un firewall real podemos hacernos una idea de hasta que punto hemos de ser cuidadosos con el orden de las entradas de nuestra tabla.

¿Qué sucederá si, con la tabla del ejemplo anterior, llega un paquete que no cumple ninguna de nuestras reglas?

El sentido común nos dice que por seguridad se debería bloquear, pero esto no siempre sucede así diferentes implementaciones ejecutan diferentes acciones en este caso. Algunas deniegan el paso por defecto, otras aplican el contrario de la ultima regla especificada (es decir, si la última entrada era un Allow se niega el paso de la trama, y si era un Deny se permite), otras dejan pasar este tipo de tramas. . . De cualquier forma, para evitar problemas cuando uno de estos datagramas llega al cortafuegos, lo mejor es insertar siempre una regla por defecto al final de nuestra lista – recordemos una vez más la cuestión del orden – con la acción que deseemos realizar por defecto; si por ejemplo deseamos bloquear el resto del tráfico que llega al firewall con la tabla anterior, y suponiendo que las entradas se analizan en el orden habitual, podríamos añadir a nuestra tabla la siguiente

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

regla:

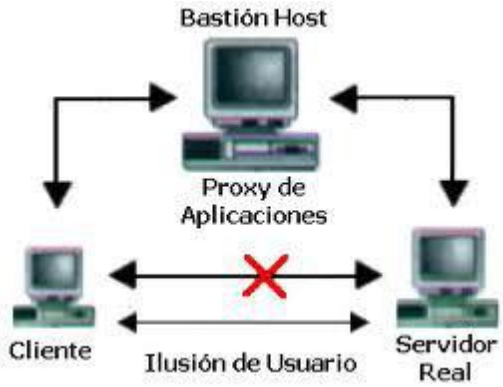
Origen	Destino	Tipo	Puerto	Acción
*	*	*	*	Deny

La especificación incorrecta de estas reglas constituye uno de los problemas de seguridad habituales en los firewalls de filtrado de paquetes, no obstante, el mayor problema es que un sistema de filtrado de paquetes es incapaz de analizar (y por tanto verificar) datos situados por encima del nivel de red Osi. A esto se le añade el hecho de que si utilizamos un simple router como filtro, las capacidades de registro de información del mismo suelen ser bastante limitadas, por lo que en ocasiones es difícil la detección de un ataque.

Se puede considerar un mecanismo de prevención más que de detección. Para intentar solucionar estas – y otras vulnerabilidades – es recomendable utilizar aplicaciones software capaces de filtrar las conexiones a servicios, a dichas aplicaciones se les denomina proxies de aplicación, y las vamos a comentar en el punto siguiente.

PROXY- GATEWAYS DE APLICACIONES

Para evitar las debilidades asociadas al filtrado de paquetes, los desarrolladores crearon software de aplicación encargados de filtrar las conexiones. Estas aplicaciones son conocidas como Servidores Proxy y la máquina donde se ejecuta recibe el nombre de Gateway de Aplicación (pasarela de aplicación) o Bastión Host. El Proxy, instalado sobre el Nodo Bastión, actúa de intermediario entre el cliente y el servidor real de la aplicación, siendo transparente a ambas partes. Cuando un usuario desea un servicio, lo hace a través del Proxy. Este, realiza el pedido al servidor real devuelve los resultados al cliente. Su función fue la de analizar el tráfico de red en busca de contenido que viole la seguridad de la misma.



Los servicios proxy poseen una serie de ventajas de cara a incrementar nuestra seguridad.

En primer lugar, permiten únicamente la utilización de servicios para los que existe un proxy, por lo que si en nuestra organización la pasarela de aplicación contiene únicamente proxies para telnet, http y ftp, el resto de servicios no estarán disponibles para nadie.

Una segunda ventaja es que en la pasarela es posible filtrar protocolos basándose en algo más que la cabecera de las tramas, lo que hace posible por ejemplo tener habilitado un

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

servicio como ftp pero con órdenes restringidas (podríamos bloquear todos los comandos put para que nadie pueda subir ficheros a un servidor).

Además, los gateways de aplicación, permiten un grado de ocultación de la estructura de la red protegida (por ejemplo, la pasarela es el único sistema cuyo nombre está disponible hacia el exterior), facilitaría la autenticación y la auditoría del tráfico sospechoso antes de que alcance el host destino y, quizás más importante, simplifica enormemente las reglas de filtrado implementadas en el router (que como hemos dicho antes pueden convertirse en la fuente de muchos problemas de seguridad):

-Sólo hemos de permitir el tráfico hacia la pasarela, bloqueando el resto.

El principal inconveniente que encontramos a la hora de instalar una pasarela de aplicación es que cada servicio que deseemos ofrecer necesita su propio proxy, además se trata de un elemento que frecuentemente es más caro que un simple filtro de paquetes, y su rendimiento es mucho menor (por ejemplo, puede llegar a limitar el ancho de banda efectivo de la red, si el análisis de cada trama es costoso). En el caso de protocolos cliente–servidor (como telnet) se añade la desventaja de que necesitamos dos pasos para conectar hacia la zona segura o hacia el resto de la red, incluso algunas implementaciones necesitan clientes modificados para funcionar correctamente.

Una variante de las pasarelas de aplicación la constituyen las pasarelas de nivel de circuito

(Circuit- level Gateways) sistemas capaces de redirigir conexiones (reenviando tramas) pero que no pueden procesar filtrar paquetes en base al protocolo utilizado, se limitan simplemente a autenticar al usuario (a su conexión) antes de establecer el circuito virtual entre sistemas. La principal ventaja de este tipo de pasarelas es que proveen de servicios a un amplio rango de protocolos; no obstante, necesitan software especial que tenga las llamadas al sistema clásicas sustituidas por funciones de librerías seguras, como socks.

Monitorización de la actividad

Monitorizar la actividad de nuestro cortafuegos es algo indispensable para la seguridad de todo el perímetro protegido. La monitorización nos facilitará información sobre los intentos de ataque que estemos sufriendo (origen, franjas horarias, tipos de acceso. . .), así como la existencia de tramas que aunque no supongan un ataque a priori sí que son al menos sospechosas.

¿Qué información debemos registrar?

Además de los registros estándar (los que incluyen estadísticas de tipos de paquetes recibidos, frecuencias, o direcciones fuente y destino se recomienda auditar información de la conexión (origen y destino, nombre de usuario – recordemos el servicio ident – hora y duración), intentos de uso de protocolos denegados, intentos de falsificación de dirección por parte de máquinas internas al perímetro de seguridad (paquetes que llegan desde la red externa con la dirección de un equipo interno) y tramas recibidas desde routers desconocidos.

Evidentemente, todos esos registros han de ser leídos con frecuencia (puedes tener un sin fin de alertas en el firewall, pero si no ves los logs del mismo ni te darás cuenta), y el

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

administrador de la red ha de tomar medidas si se detectan actividades sospechosas, si la cantidad de logs generada es considerable nos puede interesar el uso de herramientas que filtren dicha información.

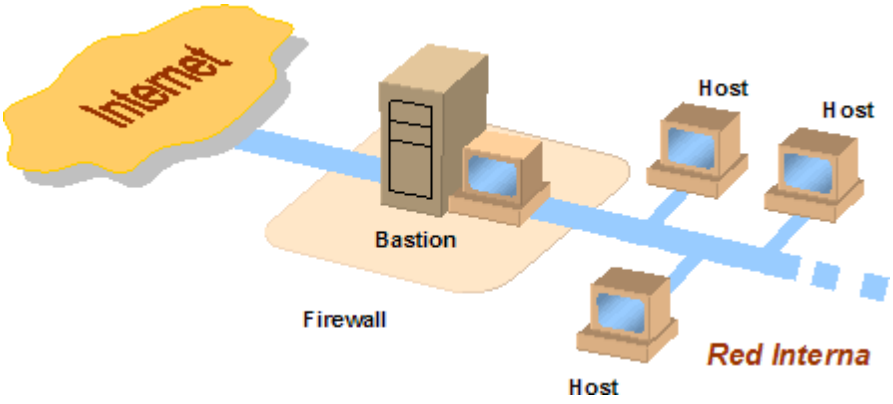
Un excelente mecanismo para incrementar mucho nuestra seguridad puede ser la sustitución de servicios reales en el cortafuegos por programas trampa. La idea es sencilla: se trata de pequeñas aplicaciones que simulan un determinado servicio, de forma que un posible atacante piense que dicho servicio está habilitado y prosiga su 'ataque', pero que realmente nos están enviando toda la información posible sobre el intruso. Este tipo de programas, una especie de troyano, suele tener una finalidad múltiple: aparte de detectar y notificar ataques, el atacante permanece entretenido intentando un ataque que cree factible, lo que por un lado nos beneficia directamente – esa persona no intenta otro ataque quizás más peligroso – y por otro nos permite entretener al intruso ante una posible traza de su conexión.

Evidentemente, nos estamos arriesgando a que nuestro atacante descubra el mecanismo y lance ataques más peligrosos, pero como el nivel de conocimientos de los atacantes de redes habituales en general no es muy elevado, este mecanismo nos permite descubrir posibles exploits utilizados por los intrusos, observar a qué tipo de atacantes nos enfrentamos, e incluso divertirnos con ellos. En la Universidad Politécnica de Valencia existen algunos sistemas con este tipo de trampas, y realmente es curioso observar cómo algunos intrusos siguen intentando aprovechar bugs que fueron descubiertos – y solucionados – hace más de cuatro años (ejemplos típicos aquí son phf y algunos problemas de sendmail).

En un artículo clásico a la hora de hablar de seguridad, se muestra como Bill Cheswick, un experto en seguridad de los laboratorios AT&T estadounidenses, es capaz de analizar detenidamente gracias a estos programas las actividades de un intruso que intenta acceder al gateway de una compañía.

DUAL-HOMEDHOST

Son dispositivos que están conectados a ambos perímetros (interior y exterior) y no dejan pasar paquetes IP (como sucede en el caso del Filtrado de Paquetes), por lo que se dice que actúan con el "IP–Forwarding desactivado" (el ip forwarding es el reenvío de direcciones a través de la red). Un usuario interior que desee hacer uso de un servicio exterior, deberá conectarse primero al Firewall, donde el Proxy atenderá su petición, y en función de la configuración impuesta en dicho Firewall, se conectará al servicio exterior solicitado y hará



El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

de puente entre este y el usuario interior. Es decir que se utilizan dos conexiones. Uno desde la máquina interior hasta el Firewall y el otro desde este hasta la máquina que albergue el servicio exterior.

Este segundo modelo de cortafuegos está formado por simples máquinas Unix equipadas con dos o más tarjetas de red y denominadas anfitriones de dos bases (dual–homed hosts) o multibase (multi–homed hosts), y en las que una de las tarjetas se suele conectar a la red interna a proteger y la otra a la red externa a la organización. En esta configuración el choke y el bastión coinciden en el mismo equipo: la máquina Unix.

El sistema ha de ejecutar al menos un servidor proxy para cada uno de los servicios que deseemos pasar a través del cortafuegos, y también es necesario que el IP Forwarding esté deshabilitado en el equipo, aunque una máquina con dos tarjetas puede actuar como un router, para aislar el tráfico entre la red interna y la externa es necesario que el choke no enrute paquetes entre ellas. Así los sistemas externos 'verán' al host a través de una de las tarjetas y los internos a través de la otra, pero entre las dos partes no puede existir ningún tipo de tráfico que no pase por el cortafuegos: todo el intercambio de datos entre las redes se ha de realizar bien a través de servidores proxy situados en el host bastión o bien permitiendo a los usuarios conectar directamente al mismo.

La segunda de estas aproximaciones es sin duda poco recomendable, ya que un usuario que consiga aumentar su nivel de privilegios en el sistema puede romper toda la protección del cortafuegos, por ejemplo reactivando el IP Forwarding, además – esto ya no relativo a la seguridad sino a la funcionalidad del sistema – suele ser incómodo para los usuarios tener que acceder a una máquina que haga de puente entre ellos e Internet. De esta forma, la ubicación de proxies es lo más recomendable, pero puede ser problemático el configurar cierto tipo de servicios o protocolos que no se diseñaron teniendo en cuenta la existencia de un proxy entre los dos extremos de una conexión.

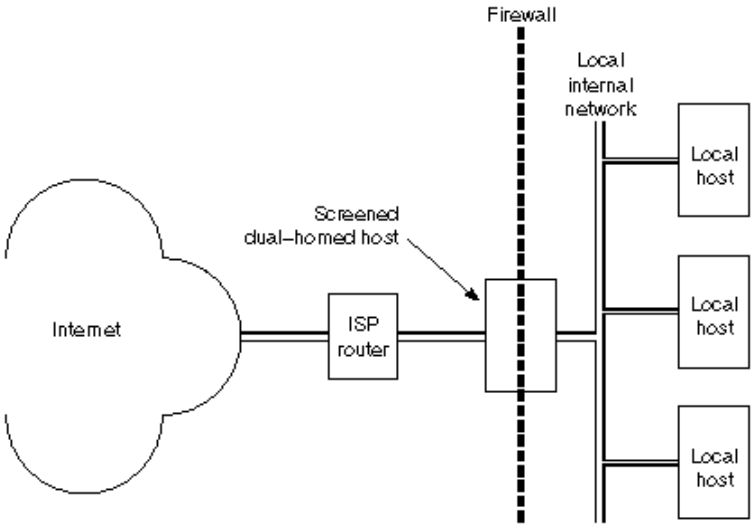
SCREENED HOST

En este caso se combina un Router con un host bastión y el principal nivel de seguridad proviene del filtrado de paquetes. En el bastión, el único sistema accesible desde el exterior, se ejecuta el Proxy de aplicaciones y en el Choke se filtran los paquetes considerados peligrosos y sólo se permiten un número reducido de servicios.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

Un paso más en términos de seguridad de los cortafuegos es la arquitectura screened host o choke- gate, que combina un router con un host bastión, y donde el principal nivel de seguridad proviene del filtrado de paquetes (es decir, el router es la primera y más importante línea de defensa). En la máquina bastión, único sistema accesible desde el exterior, se ejecutan los proxies de las aplicaciones, mientras que el choke se encarga de filtrar los paquetes que se puedan considerar peligrosos para la seguridad de la red interna, permitiendo únicamente la comunicación con un reducido número de servicios.

Pero, **¿dónde situar el sistema bastión, en la red interna o en el exterior del router?** La mayoría de autores recomiendan situar el router entre la red exterior y el host bastión, pero otros defienden justo lo contrario: situar el bastión en la red exterior no provoca aparentemente una degradación de la seguridad, y además ayuda al administrador a comprender la necesidad de un elevado nivel de fiabilidad en esta máquina, ya que está sujeta a ataques externos y no tiene por qué ser un host fiable, de cualquier forma, la 'no degradación' de la seguridad mediante esta aproximación es más que discutible, ya que habitualmente es más fácil de proteger un router que una máquina con un operativo de propósito general, como Unix, que además por definición ha de ofrecer ciertos servicios, no tenemos más que fijarnos en el número de problemas de seguridad que afectan a por ejemplo a IOS (el sistema operativo de los routers Cisco), muy reducido frente a los que afectan a diferentes flavours de Unix. En todo caso, aparte de por estos matices, asumiremos la primera opción por considerarla mayoritaria entre los expertos en seguridad informática, así cuando una máquina de la red interna desea comunicarse con el exterior existen dos posibilidades:



- El choke permite la salida de algunos servicios a todas o a parte de las máquinas internas a través de un simple filtrado de paquetes.
- El choke prohíbe todo el tráfico entre máquinas de la red interna y el exterior, permitiendo sólo la salida de ciertos servicios que provienen de la máquina bastión y que han sido autorizados por la política de seguridad de la organización.

Así estamos obligando a los usuarios a que las conexiones con el exterior se realicen a través de los servidores proxy situados en el bastión.

La primera aproximación entraña un mayor nivel de complejidad a la hora de configurar las listas de control de acceso del router, mientras que si elegimos la segunda la dificultad está

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

en configurar los servidores proxy (recordemos que no todas las aplicaciones soportan bien estos mecanismos) en el host bastión. Desde el punto de vista de la seguridad es más recomendable la segunda opción, ya que la probabilidad de dejar escapar tráfico no deseado es menor. Por supuesto, en función de la política de seguridad que definamos en nuestro entorno, se pueden combinar ambas aproximaciones, por ejemplo permitiendo el tráfico entre las máquinas internas y el exterior de ciertos protocolos difíciles de encaminar a través de un proxy o sencillamente que no entrañen mucho riesgo para nuestra seguridad (típicamente, ntp, dns. . .), y obligando para el resto de servicios a utilizar el host bastión.

La arquitectura screened host puede parecer a primera vista más peligrosa que la basada en una simple máquina con varias interfaces de red, en primer lugar, tenemos no uno sino dos sistemas accesibles desde el exterior, por lo que ambos han de ser configurados con las máximas medidas de seguridad. Además, la mayor complejidad de diseño hace más fácil la presencia de errores que puedan desembocar en una violación de la política implantada, mientras que con un host con dos tarjetas nos aseguramos de que únicamente aquellos servicios con un proxy configurado podrán generar tráfico entre la red externa y la interna (a no ser que por error activemos el IP Forwarding).

Sin embargo, aunque estos problemas son reales, se solventan tomando las precauciones necesarias a la hora de diseñar e implantar el cortafuegos y definiendo una política de seguridad correcta. De cualquier forma, en la práctica esta arquitectura de cortafuegos está cada vez más en desuso debido a que presenta dos puntos únicos de fallo, el choke y el bastión: si un atacante consigue controlar cualquiera de ellos, tiene acceso a toda la red protegida; por tanto, es más popular, y recomendable, una arquitectura screened subnet, de la que vamos a hablar a continuación.

SCREENED SUBNET

En este diseño se intenta aislar la máquina más atacada y vulnerable del Firewall, el Nodo Bastión. Para ello se establece una Zona Desmilitarizada (DMZ) de forma tal que sin un intruso accede a esta máquina no consiga el acceso total a la subred protegida. En este esquema se utilizan dos Routers: uno exterior y otro interior. El Router exterior tiene la misión de bloquear el tráfico no deseado en ambos sentidos: hacia la red interna y hacia la red externa. El Router interior hace lo mismo con la red interna y la DMZ (zona entre el Router externo y el interno).

Es posible definir varios niveles de DMZ agregando más Routers, pero destacando que las reglas aplicadas a cada uno deben ser distintas ya que en caso contrario los niveles se simplificarían a uno solo.

Como puede apreciarse la Zona Desmilitarizada aísla físicamente los servicios internos, separándolos de los servicios públicos. Además, no existe una conexión directa entre la red interna y la externa. Los sistemas Dual–Homed Host y Screned pueden ser complicados de

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

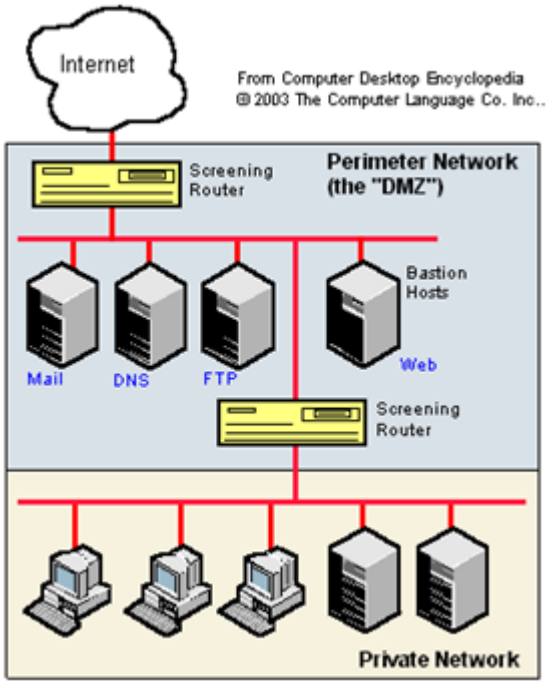
configurar y comprobar, lo que puede dar lugar, paradójicamente, a importantes agujeros de seguridad en toda la red. En cambio, si se encuentran bien configurados y administrados pueden brindar un alto grado de protección y ciertas ventajas:

1. Ocultamiento de la información: los sistemas externos no deben conocer el nombre de los sistemas internos. El Gateway de aplicaciones es el único autorizado a conectarse con el exterior y el encargado de bloquear la información no solicitada o sospechosa.

2. Registro de actividades y autenticación robusta: El Gateway requiere de autenticación cuando se realiza un pedido de datos externos. El registro de actividades se realiza en base a estas solicitudes.

3. Reglas de filtrado menos complejas: Las reglas del filtrado de los paquetes por parte del Router compleja dado a que él sólo debe atender las solicitudes del Gateway. Así mismo tiene la desventaja de ser intrusivos y no transparentes para el usuario ya que generalmente este debe instalar algún tipo de aplicación especializada para lograr la comunicación. Se suma a esto que generalmente son más lentos porque deben revisar todo el tráfico de la red.

La arquitectura Screened Subnet, también conocida como red perimétrica o De-Militarized Zone (DMZ) es con diferencia la más utilizada e implantada hoy en día ya que añade un nivel de seguridad en las arquitecturas de cortafuegos situando una subred (DMZ) entre las redes externa e interna, de forma que se consiguen reducir los efectos de un ataque exitoso al host bastión: como hemos venido comentando, en los modelos anteriores toda la seguridad se centraba en el bastión1 , de forma que si la seguridad del mismo se veía comprometida, la amenaza se extendía automáticamente al resto de la red. Como la máquina bastión es un objetivo interesante para muchos instrusos, la arquitectura DMZ intenta aislarla en una red perimétrica de forma que un intruso que accede a esta máquina no consiga un acceso total a la subred protegida.



Screened subnet es la arquitectura más segura, pero también la más compleja; se utilizan dos routers, denominados exterior e interior, conectados ambos a la red perimétrica como se muestra.

En esta red perimétrica, que constituye el sistema cortafuegos, se incluye el host bastión y también se podrá incluir sistemas que requieran un acceso controlado, como baterías de módems o el servidor de correo, que serán los únicos elementos visibles desde fuera de nuestra red

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

El router exterior tiene como misión bloquear el tráfico no deseado en ambos sentidos (hacia la red perimétrica y hacia la red externa), mientras que el interior hace lo mismo pero con el tráfico entre la red interna y la perimétrica, así un atacante habrá de romper la seguridad de ambos routers para acceder a la red protegida, incluso es posible implementar una zona desmilitarizada con un único router que posea tres o más interfaces de red, pero en este caso si se compromete este único elemento se rompe toda nuestra seguridad, frente al caso general en que hay que comprometer ambos, tanto el externo como el interno.

También podemos, si necesitamos mayores niveles niveles de seguridad, definir varias redes perimétricas en serie, situando los servicios que requieran de menor fiabilidad en las redes más externas: así el atacante habrá de saltar por todas y cada una de ellas para acceder a nuestros equipos; evidentemente, si en cada red perimétrica se siguen las mismas reglas de filtrado, niveles adicionales no proporcionan mayor seguridad.

Esta arquitectura de cortafuegos elimina los puntos únicos de fallo presentes en las anteriores:

Antes de llegar al bastión (por definición, el sistema más vulnerable) un atacante ha de saltarse las medidas de seguridad impuestas por el enrutador externo. Si lo consigue, como hemos aislado la máquina bastión en una subred estamos reduciendo el impacto de un atacante que logre controlarlo, ya que antes de llegar a la red interna ha de comprometer también al segundo router; en este caso extremo (si un intruso logra comprometer el segundo router), la arquitectura DMZ no es mejor que un screened host. Por supuesto, en cualquiera de los tres casos (compromiso del router externo, del host bastión, o del router interno) las actividades de un intruso pueden violar nuestra seguridad, pero de forma parcial, por ejemplo, simplemente accediendo al primer enrutador puede aislar toda nuestra organización del exterior, creando una negación de servicio importante, pero esto suele ser menos grave que si lograra acceso a la red protegida.

Excepto en el primero, compuesto únicamente por un choke Aunque, como hemos dicho antes, la arquitectura DMZ es la que mayores niveles de seguridad puede proporcionar, no se trata de la panacea de los cortafuegos. Evidentemente existen problemas relacionados con este modelo: por ejemplo, se puede utilizar el firewall para que los servicios fiables pasen directamente sin acceder al bastión, lo que puede dar lugar a un incumplimiento de la política de la organización. Un segundo problema, quizás más grave, es que la mayor parte de la seguridad reside en los routers utilizados; como hemos dicho antes las reglas de filtrado sobre estos elementos pueden ser complicadas de configurar y comprobar, lo que puede dar lugar a errores que abran importantes brechas de seguridad en nuestro sistema.

Algo que puede incrementar en gran medida nuestra seguridad y al mismo tiempo facilitar la administración de los cortafuegos es utilizar un bastión diferente para cada protocolo o servicio en lugar de uno sólo, sin embargo, esta arquitectura presenta el grave inconveniente de la cantidad de máquinas necesarias para implementar el firewall, lo que impide que muchas organizaciones la puedan adoptar. Una variante más barata puede consistir en utilizar un único bastión pero servidores proxy diferentes para cada servicio ofertado.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

Cada día es más habitual en todo tipo de organizaciones dividir su red en diferentes subredes, esto es especialmente aplicable en entornos de I+D o empresas medianas, donde con frecuencia se han de conectar campus o sucursales separadas geográficamente, edificios o laboratorios diferentes, etc. En esta situación es recomendable incrementar los niveles de seguridad de las zonas más comprometidas (por ejemplo, un servidor donde se almacenen expedientes o datos administrativos del personal) insertando cortafuegos internos entre estas zonas y el resto de la red. Aparte de incrementar la seguridad, firewalls internos son especialmente recomendables en zonas de la red desde la que no se permite a priori la conexión con Internet, como laboratorios de prácticas: un simple PC con Linux o FreeBSD que deniegue cualquier conexión con el exterior del campus va a ser suficiente para evitar que los usuarios se dediquen a conectar a páginas web o chats desde equipos no destinados a estos usos.

Concretamente en el caso de redes de universidades será muy interesante filtrar las conexiones a irc o a muds, ya sea a nivel de aulas o laboratorios o a nivel de todo el campus, denegando en el router de salida de la red hacia INet cualquier tráfico a los puertos 6667, 8888 y similares, aunque realmente esto no evitaría que todos los usuarios siguieran jugando desde los equipos de la universidad – por ejemplo a través de un servidor que disponga de conexión en otros puertos –, sí conseguirá que la mayor parte de ellos dejara de hacerlo.

RESTRICCIONES EN EL FIREWALL

La parte más importante de las tareas que realizan los Firewalls, la de permitir o denegar determinados servicios, se hacen en función de los distintos usuarios y su ubicación:

1. Usuarios internos con permiso de salida para servicios restringidos: permite especificar una serie de redes y direcciones a los que denomina Trusted (validados). Estos usuarios, cuando provengan del interior, van a poder acceder a determinados servicios externos que se han definido.

2. Usuarios externos con permiso de entrada desde el exterior: este es el caso más sensible a la hora de vigilarse. Suele tratarse de usuarios externos que por algún motivo deben acceder para consultar servicios de la red interna. También es habitual utilizar estos accesos por parte de terceros para prestar servicios al perímetro interior de la red. Sería conveniente que estas cuentas sean activadas y desactivadas bajo demanda y únicamente el tiempo real que sean necesarias.

ACCESS CONTROL LISTS (ACL)

Las Listas de Control de Accesos proveen de un nivel de seguridad adicional a los clásicos provistos por los Sistemas Operativos. Estas listas permiten definir permisos a usuarios y grupos concretos. Por ejemplo pueden definirse sobre un Proxy una lista de todos los

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

usuarios (o grupos de ellos) a quien se le permite el acceso a Internet, FTP, etc. También podrán definirse otras características como limitaciones de anchos de banda y horarios.

Beneficios de un firewall

- Administra los accesos posibles del Internet a la red privada.
- Protege a los servidores propios del sistema de ataques de otros servidores en Internet.
- Permite al administrador de la red definir un "choke point" (embudo), manteniendo al margen los usuarios no-autorizados, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red.
- Ofrece un punto donde la seguridad puede ser monitoreada.
- Ofrece un punto de reunión para la organización. Si una de sus metas es proporcionar y entregar servicios información a consumidores, el firewall es ideal para desplegar servidores WWW y FTP.

Limitación de un Firewalls

- Puede únicamente autorizar el paso del trafico, y él mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece en torno a éste.
- No puede proteger contra aquellos ataques que se efectúen fuera de su punto de operación.
- No puede proteger de las amenazas a que está sometido por traidores o usuarios inconscientes.
- No puede prohibir que los traidores o espías corporativos copien datos sensitivos y los substraigan de la empresa.
- No puede proteger contra los ataques de la "Ingeniería Social", por ejemplo un Hacker que pretende ser un supervisor o un nuevo empleado despistado.
- No puede proteger contra los ataques posibles a la red interna por virus informativos a través de archivos y software.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

5. Sistema de detección de intrusiones (IDS)

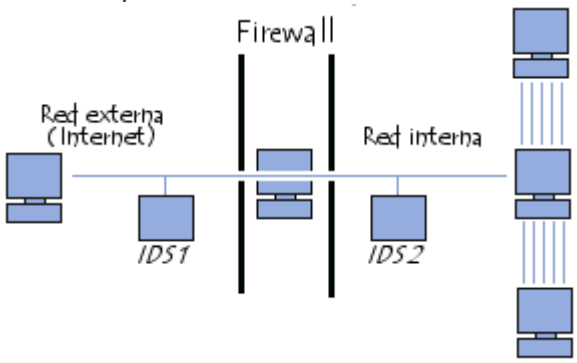
Introducción a los sistemas de detección de intrusiones

El término **IDS** (*Sistema de detección de intrusiones*) hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

Existen dos claras familias importantes de IDS:

- El grupo **N-IDS** (*Sistema de detección de intrusiones de red*), que garantiza la seguridad dentro de la red.
- El grupo **H-IDS** (*Sistema de detección de intrusiones en el host*), que garantiza la seguridad en el host.

Un N-IDS necesita un hardware exclusivo. Éste forma un sistema que puede verificar paquetes de información que viajan por una o más líneas de la red para descubrir si se ha producido alguna actividad maliciosa o anormal. El N-IDS pone uno o más de los adaptadores de red exclusivos del sistema en modo promiscuo. Éste es una especie de modo "invisible" en el que no tienen dirección IP. Tampoco tienen una serie de protocolos asignados.
Es común encontrar diversos IDS en diferentes partes de la red. Por lo general, se colocan sondas fuera de la red para estudiar los posibles ataques, así como también se colocan sondas internas para analizar solicitudes que hayan pasado a través del firewall o que se han realizado desde dentro.



El H-IDS se encuentra en un host particular.
Por lo tanto, su software cubre una amplia gama de sistemas operativos como Windows, Solaris, Linux, HP-UX, Aix, etc.
El H-IDS actúa como un daemon o servicio estándar en el sistema de un host.

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

Tradicionalmente, el H-IDS analiza la información particular almacenada en registros (como registros de sistema, mensajes, lastlogs y wtmp) y también captura paquetes de la red que se introducen/salen del host para poder verificar las señales de intrusión (como ataques por denegación de servicio, puertas traseras, troyanos, intentos de acceso no autorizado, ejecución de códigos malignos o ataques de desbordamiento de búfer).

Técnicas de detección

El tráfico en la red (en todo caso, en Internet) generalmente está compuesto por datagramas de IP. Un N-IDS puede capturar paquetes mientras estos viajan a través de las conexiones físicas a las que está sujeto. Un N-IDS contiene una lista TCP/IP que se asemeja a los datagramas de IP y a las conexiones TCP. Puede aplicar las siguientes técnicas para detectar intrusiones:

1. **Verificación de la lista de protocolos:** Algunas formas de intrusión, como "*Ping de la muerte*" y "*escaneo silencioso TCP*" utilizan violaciones de los protocolos IP, TCP, UDP e ICMP para atacar un equipo. Una simple verificación del protocolo puede revelar paquetes no válidos e indicar esta táctica comúnmente utilizada.
2. **Verificación de los protocolos de la capa de aplicación:** Algunas formas de intrusión emplean comportamientos de protocolos no válidos, como "WinNuke", que utiliza datos NetBIOS no válidos (al agregar datos fuera de la banda). Para detectar eficazmente estas intrusiones, un N-IDS debe haber implementado una amplia variedad de protocolos de la capa de aplicación, como NetBIOS, TCP/IP, etc.
   Esta técnica es rápida (el N-IDS no necesita examinar la base de datos de firmas en su totalidad para secuencias de bytes particulares) y es también más eficiente, ya que elimina algunas falsas alarmas. Por ejemplo, al analizar protocolos, N-IDS puede diferenciar un "Back Orifice PING" (bajo peligro) de un "Back Orifice COMPROMISE" (alto peligro).
3. **Reconocimiento de ataques de "comparación de patrones"**: Esta técnica de reconocimiento de intrusión es el método más antiguo de análisis N-IDS y todavía es de uso frecuente.
   Consiste en la identificación de una intrusión al examinar un paquete y reconocer, dentro de una serie de bytes, la secuencia que corresponde a una firma específica. Por ejemplo, al buscar la cadena de caracteres "cgi-bin/phf", se muestra un intento de sacar provecho de un defecto del script CGI "phf". Este método también se utiliza como complemento de los filtros en direcciones IP, en destinatarios utilizados por conexiones y puertos de origen y/o destino. Este método de reconocimiento también se puede refinar si se combina con una sucesión o combinación de indicadores TCP.

   Esta táctica está difundida por los grupos N-IDS "Network Grep", que se basan en la captura de paquetes originales dentro de una conexión supervisada y en su posterior comparación al

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

utilizar un analizador de "expresiones regulares". Éste intentará hacer coincidir las secuencias en la base de firmas byte por byte con el contenido del paquete capturado.

La ventaja principal de esta técnica radica en la facilidad de actualización y también en la gran cantidad de firmas que se encuentran en la base N-IDS. Sin embargo, cantidad no siempre significa calidad. Por ejemplo, los 8 bytes “CE63D1D2 16E713CF”, cuando se colocan al inicio de una transferencia de datos UDP, indican un tráfico Back Orifice con una contraseña predeterminada. Aunque el 80% de las intrusiones utilicen la contraseña predeterminada, el 20% utilizarán contraseñas personalizadas y no serán necesariamente reconocidas por el N-IDS. Por ejemplo, si la contraseña se cambia a "evadir", la serie de bytes se convertirá en "8E42A52C 0666BC4A", lo que automáticamente la protegerá de que el N-IDS la capture. Además, la técnica inevitablemente conducirá a un gran número de falsas alarmas y falsos positivos.

Existen otros métodos para detectar e informar sobre intrusiones, como el método Pattern Matching Stateful, y/o para controlar el tráfico peligroso o anormal en la red.

En conclusión, un perfecto N-IDS es un sistema que utiliza las mejores partes de todas las técnicas mencionadas anteriormente.

Qué hacen los IDS

Los principales métodos utilizados por N-IDS para informar y bloquear intrusiones son:

- **Reconfiguración de dispositivos externos (firewalls o ACL en routers)**: Comando enviado por el N-IDS a un dispositivo externo (como un filtro de paquetes o un firewall) para que se reconfigure inmediatamente y así poder bloquear una intrusión. Esta reconfiguración es posible a través del envío de datos que expliquen la alerta (en el encabezado del paquete).
- **Envío de una trampa SNMP a un hipervisor externo**: Envío de una alerta (y detalles de los datos involucrados) en forma de un datagrama SNMP a una consola externa como HP Open View Tivoli, Cabletron, Spectrum, etc.
- **Envío de un correo electrónico a uno o más usuarios**: Envío de un correo electrónico a uno o más buzones de correo para informar sobre una intrusión seria.
- **Registro del ataque**: Se guardan los detalles de la alerta en una base de datos central, incluyendo información como el registro de fecha, la dirección IP del intruso, la dirección IP del destino, el protocolo utilizado y la carga útil.
- **Almacenamiento de paquetes sospechosos**: Se guardan todos los paquetes originales capturados y/o los paquetes que dispararon la alerta.
- **Apertura de una aplicación**: Se lanza un programa externo que realice una acción específica (envío de un mensaje de texto SMS o la emisión de una alarma sonora).
- **Envío de un "*ResetKill*"**: Se construye un paquete de alerta TCP para forzar la finalización de una conexión (sólo válido para técnicas de intrusión que utilizan el protocolo de transporte TCP).

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes

- **Notificación visual de una alerta**: Se muestra una alerta en una o más de las consolas de administración.

Desafíos de IDS

En la prensa especializada, cada vez resuena más el término **IPS** (*Sistema de prevención de intrusiones*) que viene a sustituir al IDS "tradicional" o para hacer una distinción entre ellos.
El IPS es un sistema de prevención/protección para defenderse de las intrusiones y no sólo para reconocerlas e informar sobre ellas, como hacen la mayoría de los IDS. Existen dos características principales que distinguen a un IDS (de red) de un IPS (de red):

- El IPS se sitúa en línea dentro de la red IPS y no sólo escucha pasivamente a la red como un IDS (tradicionalmente colocado como un rastreador de puertos en la red).
- Un IPS tiene la habilidad de bloquear inmediatamente las intrusiones, sin importar el protocolo de transporte utilizado y sin reconfigurar un dispositivo externo. Esto significa que el IPS puede filtrar y bloquear paquetes en modo nativo (al utilizar técnicas como la caída de una conexión, la caída de paquetes ofensivos o el bloqueo de un intruso).

El contenido de este tema es de mi Autoría y/o recopilación de diversas fuentes