SEGURIDAD Y ALTA DISPONIBILIDAD UD3

2º ASIR

12/01/2012

VICEN MORALES

INDICE UD3-Implantación de técnicas de acceso remoto. Seguridad perimetral

- Tipos de conexión VPN:

VPN de acceso remoto,
VPN sitio a sitio (tunneling)
VPN sobre LAN.

- Protocolos que generan una VPN: PPTP, L2F, L2TP.

•Técnicas de cifrado. Clave pública y clave privada:

- Pretty Good Privacy (PGP). GNU Privacy Good (GPG).
- Seguridad a nivel de aplicación: SSH (“Secure Shell”).
- Seguridad en IP (IPSEC).
- Seguridad en Web : SSL ("Secure Socket Layer“). TLS ("Transport Layer Security”)

•Servidores de acceso remoto:

- Protocolos de autenticación.

- Protocolos PPP, PPoE, PPPoA
- Autenticación de contraseña: PAP
- Autenticación por desafío mutuo: CHAP
- Autenticación extensible: EAP. Métodos.
- PEAP.
- Kerberos.
- Protocolos AAA:

•Radius

•TACACS+

- Configuración de parámetros de acceso.
- Servidores de autenticación.

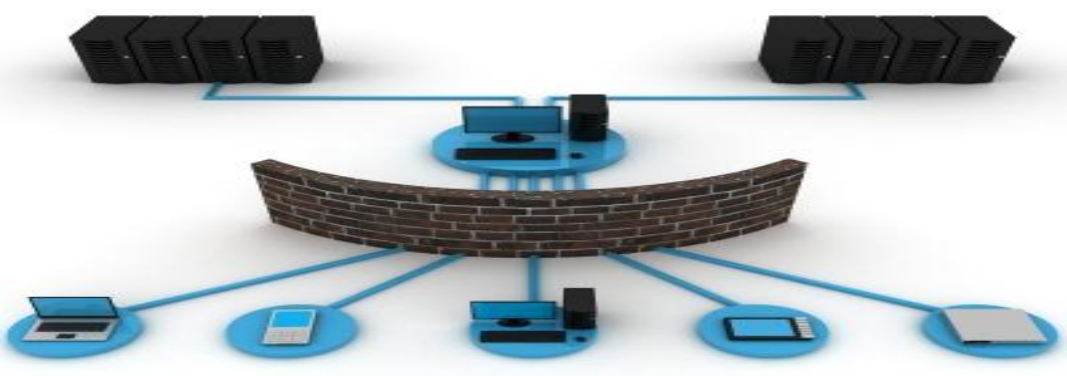
UD 3: Implantación de técnicas de acceso remoto. Seguridad perimetral

•Elementos básicos de la seguridad perimetral:

- Concepto de seguridad perimetral.

La seguridad perimetral es uno de los métodos posibles de defensa de una red, basado en el establecimiento de recursos de segurización en el perímetro externo de la red y a diferentes niveles.

Esto nos permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.



- Objetivos de la seguridad perimetral.

1. **Seguridad de la Red:**
   Asegurar un ambiente estable en términos de red y Pc's. Ya que la mayoría de las amenazas provienen de cómo interactúan los usuarios con internet.
2. **Navegación Segura:**
   Destinadas a proteger al usuario durante la navegación en Internet, controlando los sitios a los que se accede mediante listas negras/blancas (no permitidas/permitidas), sistemas de reputación y otros mecanismos.
3. **Internet libre:**
   Rentabilizar el Recurso Internet para el trabajo, dejándolo libre y con toda su capacidad y velocidad contratada.

4. **Detección de virus:**
   Pronta detección de equipos con brotes de Virus y del uso de programas maliciosos.

5. **Conexiones remotas:**
   Simplificar la conectividad Segura hacia mi red de Oficinas y promoción de la movilidad vía VPN.

- Perímetro de la red:

Se conoce como perímetro de la red a la "frontera" entre el exterior y las computadoras y servidores internas. Este se forma por los equipos que brindan conexión a Internet a las computadoras de la red, así como aquellos que las protegen de accesos externos. Equipos como los Gateway, proxys y firewalls forman parte de este perímetro.

Contar con protección antivirus a este nivel es importante dado que brinda una capa adicional de protección a las que nombramos en series anteriores, protegiendo a nivel de servidores varias de las entradas más comunes de los virus informáticos, antes de que puedan ingresar en la red interna.

Un antivirus en el perímetro de la red debe ser capaz de revisar por la existencia de virus los protocolos más utilizados (HTTP, FTP, POP3, SMTP, IMAP, entre otros).

El protocolo HTTP es el utilizado para la conexión a páginas de Internet; el protocolo FTP es usado para la descarga y transferencia de archivos a servidores que lo soporten; y los protocolos POP3 / IMAP y SMTP son los utilizados para el envío y recepción de correo electrónico.

Estos protocolos también pueden ser protegidos en otros niveles:

- HTTP / FTP: en las estaciones de trabajo y servidores de archivo de la red, los cuales deben contar con una protección antivirus inevitablemente.
- POP3 / IMAP / SMTP: tanto en las estaciones de trabajo y servidores de archivos, como en los propios servidores específicos de correo electrónico.

Existen casos donde no siempre es necesario contar con protección a este nivel, pero lo cierto es que cuantas más capas de seguridad tengamos, más protegidos estaremos.

Un caso donde es altamente deseable contar con una protección antivirus en el

perímetro es cuando se tiene el servidor de correo electrónico fuera, para que sea capaz de analizar tanto el tráfico web como el de correo electrónico que sale y entra a la red interna de la compañía.

La mayor ventaja de utilizar este tipo de herramientas de seguridad antivirus es evitar el ingreso de virus informáticos a nuestra red. Aunque seguramente el antivirus instalado en las estaciones de trabajo y servidores será capaz de detectar las amenazas, frenarlas antes de que estén transmitiéndose internamente evitará picos de saturación de la red (manteniendo el rendimiento normal de la misma), así como no tener que confiar en una sola barrera de protección.

Además, este tipo de antivirus normalmente se integran con otras aplicaciones como firewalls o proxys, lo cual es un valor agregado que nos permite contar con una sola aplicación capaz de brindarnos varios niveles de seguridad.

Una solución integrada a nivel de perímetro, capaz de utilizar más de un antivirus al mismo tiempo proveerá una mayor protección, por lo que es bueno analizar la posibilidad de contar con un software de seguridad capaz de soportar estas configuraciones, y así poder contar con las virtudes propias de varios productos antivirus para proteger la entrada y salida de información de nuestra red.

Aunque existen gran cantidad de soluciones antivirus para estaciones de trabajo y servidores de correo electrónico, la oferta de productos para perímetro es mucho mayor, dado que muchos fabricantes de software que no cuentan con un antivirus propio, ofrecen soluciones capaces de integrarse con otros productos y que incluyen herramientas adicionales (firewalls, filtrado de tráfico y de correo, etc.).

Sintetizando, la protección antivirus a nivel de perímetro es importante, pero no indispensable. Contando con protección en las estaciones de trabajo y los servidores de correo electrónico ya tenemos una fuerte barrera frente a los virus informáticos. Sin embargo, si quiere dormir mucho más tranquilo, tener una capa de seguridad antivirus en el perímetro de la red será un escollo más que los virus deberán cruzar y le dará herramientas adicionales para detenerlo.

-Routers frontera.

Es el último router que controlamos antes de Internet .Primera y última línea de defensa. Filtrado inicial y final.

- Cortafuegos (firewalls).

Los *firewalls* o cortafuegos son una de las herramientas básicas de la seguridad informática. Permiten controlar las conexiones de red que acepta o emite un dispositivo, ya sean conexiones a través de Internet o de otro sistema.
Existen infinidad de variantes de cortafuegos (dedicados, de tipo *appliance*, gestionados, etc.). Este artículo se centrará exclusivamente en los cortafuegos personales (también conocidos como firewalls) y cómo sacarles el mayor provecho.

Los cortafuegos personales son habitualmente programas que, o bien están integrados en el sistema operativo, o bien son aplicaciones de terceros que pueden ser instaladas en ellos.

¿Para qué sirve un cortafuego?

El cortafuego se encarga de controlar puertos y conexiones, es decir, de permitir el paso y el flujo de datos entre los puertos, ya sean clientes o servidores. Es como un semáforo que, en función de la dirección IP y el puerto (entre otras opciones), dejará establecer la conexión o no siguiendo unas reglas establecidas.

De este modo, el firewall controla qué combinaciones "IP Cliente:puerto + IP Servidor:puerto" son válidas o no. Por ejemplo, si el administrador del servidor 222.222.222.222 decide que no quiere que el cliente con dirección IP 111.111.111.111 vea su página web desde casa, podría indicarle a su cortafuegos en el servidor que bloquee esa dirección IP y no le permita acceder a su puerto 80.

Básicamente, los cortafuegos personales es un programa que se interpone entre el sistema operativo y las aplicaciones en la red, y comprueba una serie de parámetros antes de permitir que se establezca una conexión. Cuando se instala un *firewall*, el sistema operativo le cede el control de la gestión de esos puertos virtuales y de las conexiones de red en general, y hará lo que tenga definido como reglas. Las comprobaciones de los cortafuegos están asociadas a unas reglas (que le indican qué debe hacer con esas conexiones). Estas reglas son normalmente "bloquear", "permitir"

o "ignorar". Básicamente, cuando un programa quiere establecer una conexión o reservar un puerto para volcar datos en la red, el *firewall* pregunta:

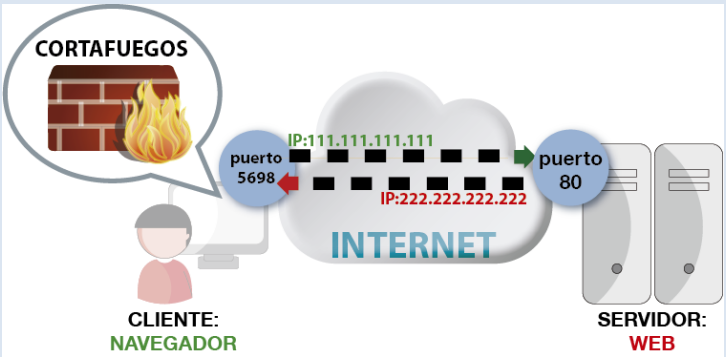
• *¿De qué IP proviene este intento de conexión?*

• *¿Desde qué puerto proviene?*

• *¿A qué IP va destinada este intento de conexión?*

• *¿A qué puerto?*

• *¿Qué debo hacer con ella? (Bloquear, permitir o ignorar)*



Tipos de cortafuegos

Aunque existen sistemas o máquinas específicamente diseñadas para hacer de cortafuegos, nos centramos en este caso en los cortafuegos personales, habitualmente integrados en los sistemas operativos.

- **Entrante**

El cortafuego de tipo entrante es el que controla las conexiones que "entran" en el sistema. Esto quiere decir que está pensado en mayor medida para servidores, para comprobar desde qué direcciones IP se quieren establecer conexiones a sus servicios. Por ejemplo, desde el punto de vista de un servidor que muestra páginas web, un cliente que desee visualizar esa página, será una conexión entrante que deberá verificar en su tabla de reglas.
Este tipo de cortafuegos es muy usado tanto en servidores como en sistemas que habitualmente actúan como clientes. Por ejemplo, Windows XP lo activa por defecto desde su Service Pack 2, publicado en 2004. Desde entonces, todos los sistemas Windows cuentan con unos cortafuegos entrante activado por defecto.

También, la inmensa mayoría de los routers usados para establecer una conexión ADSL tienen un firewall entrante activado por defecto, que protege al ordenador interno.

Ejemplo de conexión entre cliente y servidor, pasando por unos cortafuegos del lado del cliente

- **Saliente**

El cortafuego de tipo saliente controla las conexiones que "salen" del sistema, esto es, las que acuden a un servidor. Está pensado en mayor medida para clientes, para comprobar hacia qué direcciones IP o qué puertos se conecta nuestro ordenador. Este tipo de cortafuegos es mucho menos usado que el entrante, aunque es más seguro, puesto que nos permite tener control total de hacia dónde intentan conectarse los programas y, por tanto, nuestros datos.

Con esta regla, se estaría indicando al cortafuego saliente que, siempre que Internet Explorer se intente conectar desde nuestra dirección IP, desde cualquier puerto y pretenda a ir a cualquier dirección IP de destino, al puerto 81, lo bloquee. Sin embargo, si pretende ir al puerto 80 del servidor, permitirá la conexión normalmente.

Otros tipos de cortafuegos:

Hasta ahora se han visto las funciones básicas de los firewalls y el concepto original para el que fueron creados. Sin embargo, los cortafuegos personales y de servidores han evolucionado para ofrecer funcionalidades avanzadas que han ayudado a proteger aún más los servidores. Veamos algunos ejemplos:

- **Controlar el tipo de conexión**

Las conexiones y flujos de datos entre puertos y direcciones IP pueden establecerse de forma errónea o malintencionada. Existen programas destinados a manipular este tipo

de conexiones e intentar confundir al servidor para violar su seguridad o hacer que deje de responder. Así, pueden intentar establecer conexiones incompletas, confusas, sin sentido, etc. Dependiendo del programa destino, el sistema actuará de una manera u otra.
La mayoría de los cortafuegos ya están preparados para manejar este tipo de conexiones extrañas y no dejarlas pasar para que no causen problemas. Muchos están cargados por defecto con reglas de ataques conocidos que impiden que cualquier establecimiento de conexión que no sea conforme a los estándares, sea descartado.

- **Controlar la denegación de servicio**

La denegación de servicio es un efecto bloqueo que ocurre cuando muchos sistemas intentan acceder a un mismo puerto de un servidor, saturándolo. El programa que escucha en el puerto puede manejar un número limitado de conexiones al mismo tiempo, y si ese número se supera, no permitirá que nuevas conexiones se establezcan. Así, si alguien consigue saturar al servidor e impedir que otras conexiones se establezcan, a través de conexiones que genere él mismo u otros sistemas, estaremos ante una denegación de servicio. Sería como organizar a un grupo de personas para que compren en una misma tienda al mismo tiempo, pero que retrasen el pedido distrayendo al comerciante. Clientes legítimos que quieran comprar algo no podrán realmente acceder a la tienda y por tanto, ésta tendrá un perjuicio.
Los cortafuegos permiten controlar también el número de conexiones que se están produciendo, y en cuanto detectan que se establecen más de las normales desde un mismo punto (o que estas se establecen con demasiada velocidad) pueden añadir reglas automáticamente para bloquearlas y mantener el servicio a salvo.

Controlar las aplicaciones que acceden a internet

Otros cortafuegos permiten controlar, además de qué direcciones IP se conectan a qué puertos, cuáles son las aplicaciones que lo están haciendo. Así, es posible indicar que un programa deje de conectarse a un puerto o una IP en concreto.
Si se realiza una lista blanca de programas que pueden conectarse a ciertos puertos, basados en el uso habitual del sistema, es posible conseguir un nivel de seguridad muy alto. Con esta técnica, se impedirá que programas a los que no hemos permitido explícitamente acceso a Internet, puedan enviar información interna al exterior.

- **Controlar las aplicaciones que acceden a un puerto**

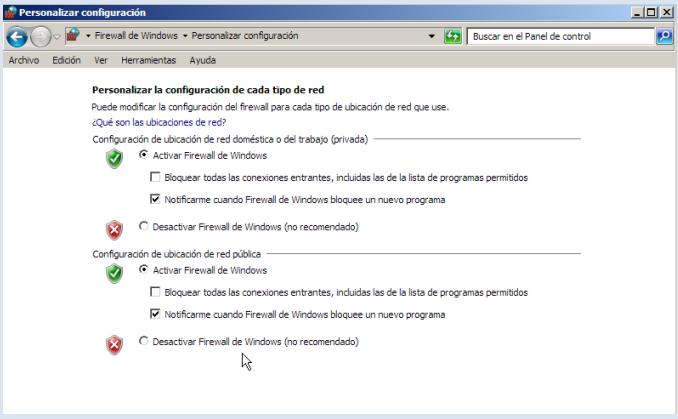
Un cortafuego en el sistema puede también detectar cuándo una aplicación desea hacer uso de un puerto no para establecer una conexión, sino para ponerse a oír en él y esperar conexiones. Este es un comportamiento habitual de los troyanos de hace algunos años. Se conectaban a un puerto (o sea, convertían a la víctima en un servidor) y el atacante, como cliente, se conectaba a ese puerto. Por tanto, los cortafuegos también advierten al usuario cuando una aplicación quiere utilizar un puerto para esperar conexiones entrantes, puesto que puede suponer un riesgo de seguridad.

El firewall de Windows advierte de esta manera de que, en este ejemplo el programa Ccproxy, quiere ponerse a oír en un puerto. Da la oportunidad al usuario de permitir la conexión o no.

Cortafuegos en los distintos tipos operativos:

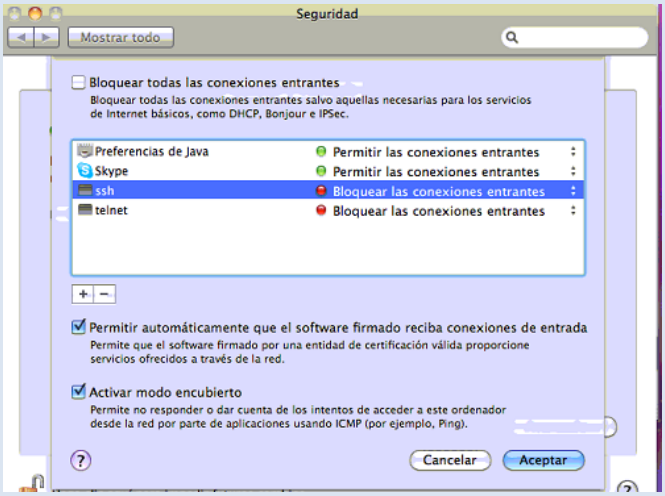
Configuración básica los cortafuegos de Windows en Vista y 7

Windows cuenta con un cortafuegos integrado, tanto entrante como saliente. Su interfaz básica es muy sencilla.



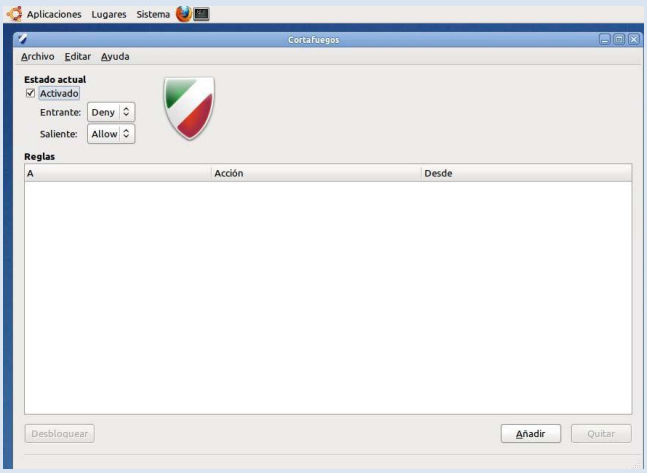
Cortafuegos con configuración típica en Mac OS

Mac OS X cuenta con un cortafuego integrado, sólo para conexiones entrantes.



Interfaz gráfica para cortafuegos en Ubuntu

Para sistemas Linux, es necesario utilizar la línea de comando. Se utilizan reglas llamadas *iptables*, que están implementadas en todos los kernel2 de todos los Linux. Son configurables a través de líneas de comando, y permiten total control de puertos y direcciones (tanto entrantes como salientes).
Sin embargo, existen diferentes "interfaces" gráficas que pueden ser instaladas para manejar de forma más cómoda el cortafuegos y sus reglas *iptables.*



- Sistemas de Detección de Intrusos.

Un sistema de detección de intrusos (o IDS de sus siglas en inglés IntrusionDetectionSystem) es una aplicación usada para detectar accesos no autorizados a un ordenador/servidor o a una red. Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o a través de herramientas automáticas.

Las funciones de un IDS se pueden resumir de la siguiente forma:

- **Detección de ataques** en el momento que están ocurriendo o poco después.
- Automatización de la **búsqueda de nuevos patrones de ataque**, gracias a herramientas estadísticas de búsqueda, y al análisis de tráfico anómalo.
- **Monitorización y análisis** de las actividades de los usuarios. De este modo se pueden conocer los servicios que usan los usuarios, y estudiar el contenido del tráfico, en busca de elementos anómalos.
- **Auditoría** de configuraciones y vulnerabilidades de determinados sistemas.
- **Descubrir sistemas con servicios habilitados** que no deberían de tener, mediante el análisis del tráfico y de los logs.

- **Análisis de comportamiento anormal**. Si se detecta una conexión fuera de hora, reintentos de conexión fallidos y otros, existe la posibilidad de que se esté en presencia de una intrusión. Un análisis detallado del tráfico y los logs puede revelar una máquina comprometida o un usuario con su contraseña al descubierto.

- Automatizar tareas como **la actualización de reglas, la obtención y análisis de logs, la configuración de cortafuegos y otros.**

Un IDS puede compartir u obtener información de otros sistemas como firewalls, routers y switches, lo que permite reconfigurar las características de la red de acuerdo a los eventos que se generan. También permite que se utilicen protocolos como SNMP (Simple Network Management Protocol) para enviar notificaciones y alertas a otras maquinas de la red. Esta característica de los IDS recibe el nombre de **interoperabilidad**.

Básicamente hay tres tipos de IDS:

- ***Network IntrusionDetectionSystem (NIDS):***Es el más común. Su misión principal es vigilar la red (en realidad,el segmento de red que es capaz de ver). Básicamente, pone el interfaz en modopromiscuo y absorbe todo el tráfico, analizándolo posteriormente o en tiempo real.
- ***Network NodeIntrusionDetectionSystem (NNIDS):***Este es un IDS destinado a vigilar el tráfico destinado a un único Host, y no a una subred entera. Por ejemplo, puede servir como vigilante externo de un *HoneyPot*o para vigilar la actividad de una VPN (Virtual Private Network). Dado que solo analiza un host, se puede permitir un análisis mucho más exhaustivo de los paquetes.
- ***Host IntrusionDetectionSystem(HIDS):***Permiten tomar una *instantánea* del sistema, para comprobar más adelante la integridad de la maquina. Entre las técnicas más comunes están las firmas MD5 de los archivos críticos y las copias del registro.

Cortafuegos vs IDS:

Un IDS es un sistema que intenta detectar y alertar sobre las intrusiones intentadas en un sistema o en una red, considerando intrusión a toda actividad no autorizada o no que no debería ocurrir en ese sistema. Según esta definición, muchos podrían pensar que ese trabajo ya se realiza mediante los cortafuegos o firewalls. Pero ahora veremos las diferencias entre los dos componentes y como un IDS es un buen complemento de los cortafuegos.

La principal diferencia, es que un cortafuegos es una herramienta basada en la aplicación de un sistema de restricciones y excepciones sujeta a muchos tipos de

ataques, desde los ataques “tunneling”(saltos de barrera) a los ataques basados en las aplicaciones. Los cortafuegos filtran los paquetes y permiten su paso o los bloquean por medio de una tabla de decisiones basadas en el protocolo de red utilizado. Las reglas verifican contra una base de datos que determina si está permitido un protocolo determinado y permite o no el paso del paquete basándose en atributos tales como las direcciones de origen y de destino, el número de puerto, etc... Esto se convierte en un problema cuando un atacante enmascara el tráfico que debería ser analizado por el cortafuego o utiliza un programa para comunicarse directamente con una aplicación remota. Estos aspectos se escapan a las funcionalidades previstas en el diseño inicial de los cortafuegos. Es aquí donde entran los IDS, ya que estos son capaces de detectar cuando ocurren estos fallos.

- Redes Privadas Virtuales.

Las redes de área local (LAN) son las redes internas de las organizaciones, es decir las conexiones entre los equipos de una organización particular. Estas redes se conectan cada vez con más frecuencia a Internet mediante un equipo de interconexión. Muchas veces, las empresas necesitan comunicarse por Internet con filiales, clientes o incluso con el personal que puede estar alejado geográficamente.

Sin embargo, los datos transmitidos a través de Internet son mucho más vulnerables que cuando viajan por una red interna de la organización, ya que la ruta tomada no está definida por anticipado, lo que significa que los datos deben atravesar una infraestructura de red pública que pertenece a distintas entidades. Por esta razón, es posible que a lo largo de la línea, un usuario entrometido, escuche la red o incluso secuestre la señal. Por lo tanto, la información confidencial de una organización o empresa no debe ser enviada bajo tales condiciones.

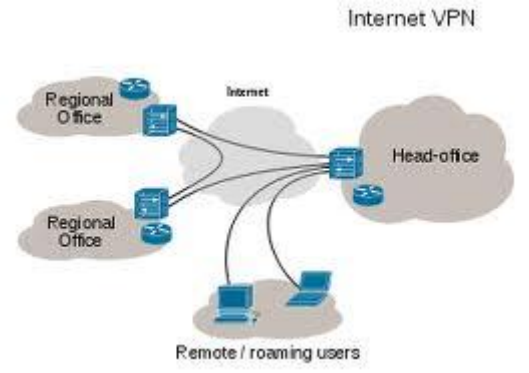
La primera solución para satisfacer esta necesidad de comunicación segura implica conectar redes remotas mediante líneas dedicadas. Sin embargo, como la mayoría de las compañías no pueden conectar dos redes de área local remotas con una línea dedicada, a veces es necesario usar Internet como medio de transmisión.

Una buena solución consiste en utilizar Internet como medio de transmisión con un protocolo de *túnel*, que significa que los datos se encapsulan antes de ser enviados de manera cifrada. El término **Red privada virtual** (abreviado **VPN**) se utiliza para hacer referencia a la red creada artificialmente de esta manera.
Se dice que esta red es *virtual* porque conecta dos redes "físicas" (redes de área local) a través de una conexión poco fiable (Internet) y *privada* porque sólo los equipos que pertenecen a una red de área local de uno de los lados de la VPN pueden "ver" los datos.

Por lo tanto, el sistema VPN brinda una conexión segura a un bajo costo, ya que todo lo que se necesita es el hardware de ambos lados. Sin embargo, no garantiza una calidad de servicio comparable con una línea dedicada, ya que la red física es pública y por lo tanto no está garantizada.

Funcionamiento de una VPN

Una red privada virtual se basa en un protocolo denominado **protocolo de túnel**, es decir, un protocolo que cifra los datos que se transmiten desde un lado de la VPN hacia el otro.



La palabra "túnel" se usa para simbolizar el hecho que los datos estén cifrados desde el momento que entran a la VPN hasta que salen de ella y, por lo tanto, son incomprensibles para cualquiera que no se encuentre en uno de los extremos de la VPN, como si los datos viajaran a través de un túnel. En una *VPN* de dos equipos, el *cliente de VPN* es la parte que cifra y descifra los datos del lado del usuario y el *servidor VPN* (comúnmente llamado **servidor de acceso remoto**) es el elemento que descifra los datos del lado de la organización.

De esta manera, cuando un usuario necesita acceder a la red privada virtual, su solicitud se transmite sin cifrar al sistema de pasarela, que se conecta con la red remota mediante la infraestructura de red pública como intermediaria; luego transmite la solicitud de manera cifrada. El equipo remoto le proporciona los datos al servidor VPN en su red y éste envía la respuesta cifrada. Cuando el cliente de VPN del usuario recibe los datos, los descifra y finalmente los envía al usuario.

- Software y servicios. Host Bastion.

Un **bastión host** (bastion sin acentuar en inglés) es una aplicación que se localiza en un server con el fin de ofrecer seguridad a la red interna, por lo que ha sido especialmente configurado para la recepción de ataques, generalmente provee un solo servicio (como por ejemplo un servidor proxy).

Definición

Históricamente, se le llamaba Bastiones a las altas partes fortificadas de los castillos medievales; puntos que cubrían áreas críticas de defensa en caso de invasión, usualmente teniendo murallas muy fortificadas, salas para alojar tropas, y armas de ataque a corta distancia como ollas de aceite hirviendo para alejar a los invasores cuando ya están por penetrar al castillo. Haciendo una analogía, un bastión host esun sistema identificado por el administrador de firewall como un punto crítico en la

seguridad de la red. Generalmente, los bastion host tendrán cierto grado de atención extra para configurar y diseñar su seguridad, pudiendo tener software modificado para asegurar su buen desempeño.

Diseño

A diferencia del filtro realizado a través de un router, que permite o no el flujo directo de paquetes desde el interior al exterior de una red, los bastión host (también llamados en inglés application-levelgateways) permiten un flujo de información pero no un flujo de paquetes, lo que permite una mayor seguridad de las aplicaciones del host. El diseño del bastión consiste en decidir qué servicios éste incluirá. Se podría tener un servicio diferente por host, pero esto involucraría un costo muy elevado, pero en caso de que se pueda abordar, se podrían llegar a tener múltiples bastión host para mantener seguros múltiples puntos de ataque.

Definida la cantidad de bastión hosts, se debe ahora analizar que se instalará en cada uno de ellos, para esto se proponen distintas estrategias:

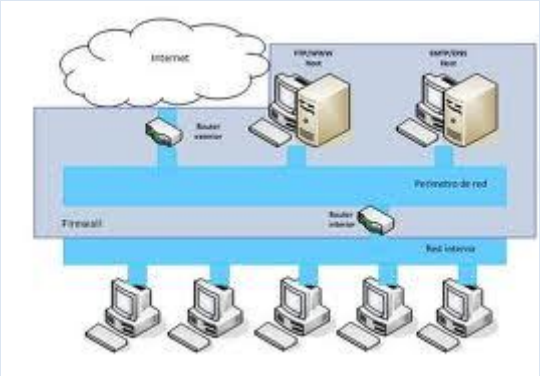
- Que la plataforma de hardware del bastión host ejecute una versión segura de su sistema operativo, diseñado específicamente para proteger al sistema operativo de sus vulnerabilidades y asegurar la integridad del firewall
- Instalar sólo los servicios que se consideren esenciales. La razón de esto es que si el servicio no está instalado, éste no puede ser atacado. En general, una limitada cantidad de aplicaciones proxy son instaladas en un bastión host.
- El bastión host podría requerir autentificación adicional antes de que un usuario ingrese a sus servicios.
- En caso de alojar un proxy, este puede tener variadas configuraciones que ayuden a la seguridad del bastion host, tales como: configurados para soportar sólo un subconjunto de aplicaciones, permitiendo el acceso a determinados hosts y/o proveyendo toda la información de los clientes que se conecten.

Tipos de bastion host

Los bastiones pueden clasificarse en tres tipos: single-homed bastión host, dual-homed bastión host y multihomed bastión host.

Single-homed bastión host

Es un dispositivo con una interfaz única de red, frecuentemente se utiliza para una puerta de enlace en el nivel de aplicación. El router externo está configurado para enviar los datos al Bastión Host y los clientes internos enviar los datos de salida al host. Finalmente el host evaluará los datos según las directrices de seguridad.



Dual-homed bastión host

Es un dispositivo que tiene al menos dos interfaces de red. Sirve como puerta de enlace al nivel de aplicación y como filtro de paquetes. La ventaja de usar este host es crear un quiebre entre las red externa e interna, lo que permite que todo el tráfico de entrada y salida pase por el host. Este host evitará que un hacker intenté acceder a un dispositivo interno.

Multihomed bastión host

Un Bastión host interno puede ser clasificado como multihomed. Cuando la política de seguridad requiere que todo tráfico entrante y salida sea enviado a través de un servidor proxy, un nuevo servidor proxy debería ser creado para la nueva aplicación streaming. Cuando se utiliza un bastión host como interno, debe residir dentro de una organización de la red interna, en general como puerta de acceso para recibir todo el tráfico de un bastión host externo. Lo que agrega un nivel mayor de seguridad.

Aplicaciones

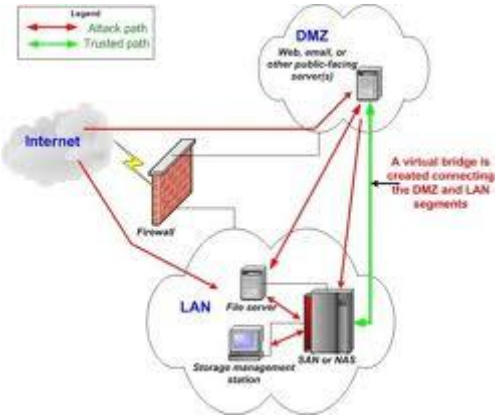
El uso de bastión host puede ser extensible a variados sistemas y/o servicios:

- Webserver.
- DNS (Domain Name System) server.
- Email server.
- FTP (File Transfer Protocol) server.
- Proxy server.
- Honeypot.
- VPN (Virtual Private Network) server.
- Deep-SecureBastion.

A continuación se expone un ejemplo de una red donde se utilizan dos bastiones host, como se observa se forma una capa adicional de seguridad entre el internet y la red interna. Para tener acceso a la red interna, un atacante debe pasar por el router externo, alguno de los bastiones y el router interno. El paso por todas estas etapas como presenta una dificultad para el atacante, es de esperar que por el tiempo que le demore traspasar todas las capas, el administrador de red ya debiese haber reconocido la intrusión y haber tomado una posición defensiva.

- Zonas desmilitarizadas (DMZ) y subredes controladas.

Los sistemas Firewall permiten definir las reglas de acceso entre dos redes. Sin embargo, en la práctica, las compañías cuentan generalmente con varias subredes con diferentes políticas de seguridad. Por esta razón, es necesario configurar arquitecturas de firewall que aíslen las diferentes redes de una compañía. Esto se denomina "**aislamiento de la red**".



Desde un punto de vista conceptual, existen distintas arquitecturas posibles a la hora de realizar la segregación entre la LAN del centro de control y la red corporativa. No obstante, podríamos agruparlas en tres: conexión directa entre ambas, separación en dos zonas con distinto nivel de seguridad, y uso de tres o más zonas con distinto nivel de seguridad. Este último caso es el que contempla la arquitectura basada en zonas desmilitarizadas(DMZs). En una segregación de la LAN del centro de control y la red empresarial, las DMZ se utilizarían para instalar aquellos servicios que requieran comunicación con otros elementos del sistema de control y que además deben ser accesibles desde la red corporativa

Zona desmilitarizada y subred controlada: Pequeñas porciones de la red con servicios accesibles desde el exterior.

Zona desmilitarizada: Situada delante de los cortafuegos, tras el router frontera.

Red controlada: Situada tras los cortafuegos

¿Que es una DMZ?

Una **DMZ** (del inglés *Demilitarizedzone*) o Zona DesMilitarizada. Una **zona desmilitarizada** (DMZ) o **red perimetral** es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

El objetivo de una DMZ es que las conexiones **desde** la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones **desde** la DMZ sólo se permitan a la

red externa, es decir: los equipos locales (hosts) en la DMZ no pueden conectar con la red interna.

Esto permite que los equipos (hosts) de la DMZ's puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de e-mail, Web y DNS.

Las conexiones que se realizan desde la red externa hacia la DMZ se controlan generalmente utilizando portaddresstranslation (PAT).

Habitualmente una configuración DMZ es usar dos cortafuegos, donde la DMZ se sitúa en medio y se conecta a ambos cortafuegos, uno conectado a la red interna y el otro a la red externa. Esta configuración ayuda a prevenir configuraciones erróneas accidentales que permitan el acceso desde la red externa a la interna. Este tipo de configuración también es llamado cortafuegos de subred monitoreada (screened-subnet firewall).

•Arquitecturas de cortafuegos:

- Cortafuego de filtrado de paquetes.

Un *firewall* sencillo puede consistir en un dispositivo capaz de filtrar paquetes, un *choke*: se trata del modelo de cortafuegos más antiguo basado simplemente en aprovechar la capacidad de algunos *routers* - denominados *screeningrouters* - para hacer un enrutado selectivo, es decir, para bloquear o permitir el tránsito de paquetes mediante listas de control de acceso en función de ciertas características de las tramas, de forma que el *router* actue como pasarela de toda la red. Generalmente estas características para determinar el filtrado son las direcciones origen y destino, el protocolo, los puertos origen y destino (en el caso de TCP y UDP), el tipo de mensaje (en el caso de ICMP) y los interfaces de entrada y salida de la trama en el *router*.

En un cortafuegos de filtrado de paquetes los accesos desde la red interna al exterior que no están bloqueados son directos (no hay necesidad de utilizar *proxies*, como sucede en los cortafuegos basados en una máquina con dos tarjetas de red), por lo que esta arquitectura es la más simple de implementar (en muchos casos sobre *hardware* ya ubicado en la red) y la más utilizada en organizaciones que no precisan grandes niveles de seguridad - como las que vemos aquí -. No obstante, elegir unos cortafuegos tan sencillos puede no ser recomendable en ciertas situaciones, o

para organizaciones que requieren una mayor seguridad para su subred, ya que los simples *chokes* presentan más desventajas que beneficios para la red protegida. El principal problema es que no disponen de un sistema de monitorización sofisticado, por lo que muchas veces el administrador no puede determinar si el *router*está siendo atacado o si su seguridad ha sido comprometida. Además las reglas de filtrado pueden llegar a ser complejas de establecer, y por tanto es difícil comprobar su corrección: habitualmente sólo se comprueba a través de pruebas directas, con los problemas de seguridad que esto puede implicar.

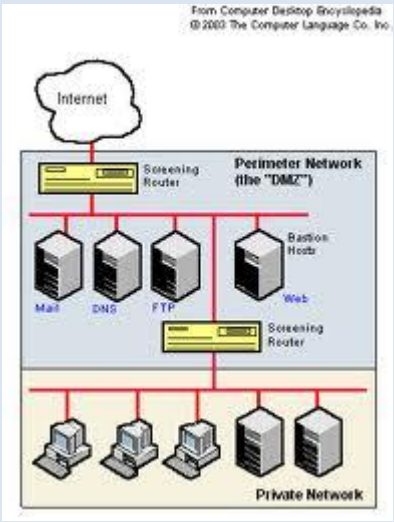
Si a pesar de esto decidimos utilizar un *router* como filtro de paquetes, como en cualquier *firewall* es recomendable bloquear todos los servicios que no se utilicen desde el exterior (especialmente NIS, NFS, X-Window y TFTP), así como el acceso desde máquinas no confiables hacia nuestra subred; además, es también importante para nuestra seguridad bloquear los paquetes con encaminamiento en origen activado.

- Cortafuego Dual-Homed Host.

Dispositivos que están conectados a ambos perímetros (interior y exterior) y no dejan pasar paquetes IP (como sucede en el filtrado de paquetes), por lo que se dice que actúan con el " IP-Forwarding desactivado".

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 conectara al servicio exterior solicitado y hará de puente entre este y el usuario interior.

Es decir que se utilizan dos conexiones. Uno desde la maquina interior hasta el firewall y el otro desde este hasta la maquina que albergue el servicio exterior.



- Screened Host.

Combina un router con un host bastion, 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 maquina bastion, 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.

La mayoría de los autores recomiendan situar el router entre la red exterior y el host bastion, pero otros defienden justo lo contrario: situar el bastion 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 discutible, ya que habitualmente es más fácil de proteger un router que una maquina con un sistema operativo de propósito general, que además por definición ha de ofrecer ciertos servicios: no tenemos más que fijarnos en el numero de problemas de seguridad que afectan a los IOS de los routers cisco, es muy reducido frente a los que afectan a diferentes flavorus 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 maquina 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 maquinas internas a través de un simple filtrado de paquetes.
- El *choke*prohibe 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 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 (DMZ).

La arquitectura *Screened Subnet*, también conocida como red perimétrica o *De-MilitarizedZone* (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 bastión, 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 piratas, 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. En esta red perimétrica, que constituye el sistema cortafuegos, se incluye el *host* bastión y también se podrían 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 *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 habría 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 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 pirata 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 pirata 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.

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 complicados de configurar y comprobar, lo que puede dar lugar a errores que abran importantes brechas de seguridad en nuestro sistema.

- Otras arquitecturas

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 consistiría en utilizar un único bastión pero servidores *proxy* diferentes para cada servicio ofertado.

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 sería 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 conseguiría que la mayor parte de ellos dejara de hacerlo.

•Políticas de defensa en profundidad:

- Defensa perimetral.

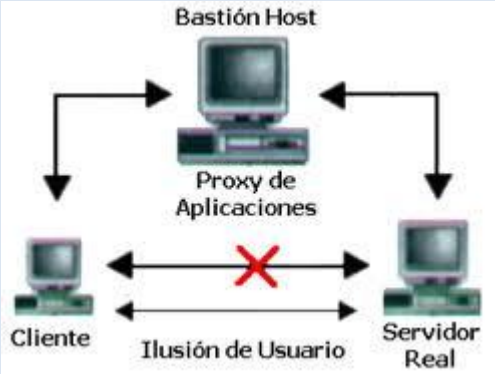
La seguridad perimetral es uno de los métodos posibles de defensa de una red, basado en el establecimiento de recursos de segurización en el perímetro externo de la red y a diferentes niveles.

Esto nos permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

Interacción entre zona perimetral (DMZ) y zona externa.

Una **zona desmilitarizada** o **red perimetral** es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada.

La red exterior sólo permite el tráfico hacia los servidores semi-públicos alojados en la DMZ. La red interior se rige por el "pesimismo", esto es, solo acepta paquetes si responden a una petición originada en el interior de la red o que provienen de uno de los servidores alojados en la DMZ (por defecto guarda toda la información sobre las transacciones).



Monitorización del perímetro: detección y prevención de intrusos

Un IDS es una herramienta de seguridad que intenta detectar o monitorizar los eventos ocurridos en un determinado sistema informático en busca de intentos de comprometer la seguridad de dicho sistema.

Breve introducción a los sistemas IDS y Snort

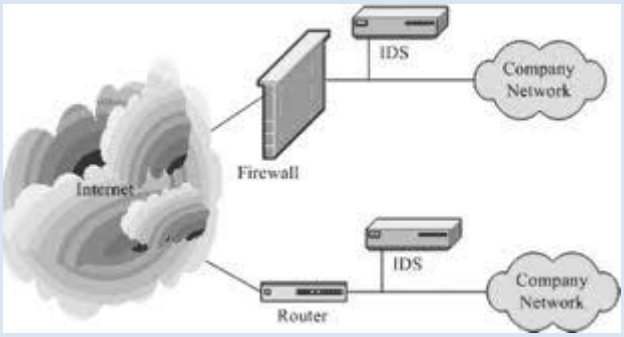
- Un **IDS** o **Sistema de Detección de Intrusiones** es una herramienta de seguridad que intenta **detectar o monitorizar los eventos** ocurridos en un determinado sistema informático o red informática en busca de intentos de comprometer la seguridad de dicho sistema.
- Los **IDS** buscan **patrones previamente definidos** que impliquen cualquier tipo de actividad sospechosa o maliciosa sobre nuestra red o host.
- Los **IDS** aportan a nuestra seguridad una capacidad de **prevención** y de **alerta anticipada** ante cualquier actividad sospechosa. **No** están diseñados para **detener un ataque**, aunque sí pueden generar ciertos tipos de respuesta ante éstos.
- Los **IDS**: aumentan la seguridad de nuestro sistema, vigilan el tráfico de nuestra red, examinan los paquetes analizándolos en busca de datos sospechosos y detectan las primeras fases de cualquier ataque como pueden ser el análisis de nuestra red, barrido de puertos, etc.

Tipos de IDS

1. HIDS (Host IDS)

Protege contra un único Servidor, PC o host. Monitorizan gran cantidad de eventos, analizando actividades con una gran precisión, determinando de esta manera qué procesos y usuarios se involucran en una determinada acción. Recaban información del sistema como ficheros, logs, recursos, etc, para su posterior análisis en busca de posibles incidencias.

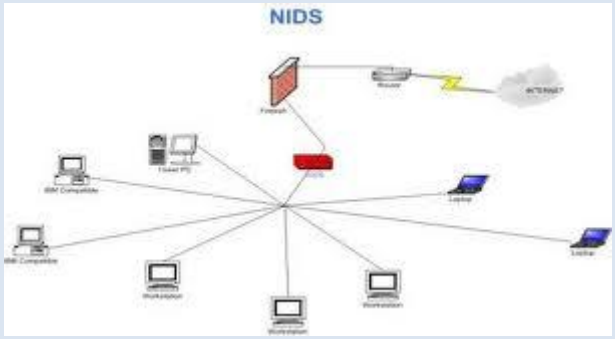
Todo ello en modo local, dentro del propio sistema. Fueron los primeros IDS en desarrollar por la industria de la seguridad informática.



2. NIDS (Net IDS)

Protege un sistema basado en red. Actúan sobre una red capturando y analizando paquetes de red, es decir, son sniffers del tráfico de red. Luego analizan los paquetes capturados, buscando patrones que supongan algún tipo de ataque.

Bien ubicados, pueden analizar grandes redes y su impacto en el tráfico suele ser pequeño. Actúan mediante la utilización de un dispositivo de red configurado en modo promiscuo (analizan, "ven" todos los paquetes que circulan por un segmento de red aunque estos nos vayan dirigidos a un determinado equipo). Analizan el trafico de red, normalmente, en tiempo real. No sólo trabajan a nivel TCP/IP, también lo pueden hacer a nivel de aplicación.



Otros tipos son los híbridos.

Por el tipo de respuesta podemos clasificarlos en:

Pasivos: *Son aquellos IDS que notifican a la autoridad competente o administrador de la red mediante el sistema que sea, alerta, etc. Pero no actúa sobre el ataque o atacante.*

Activos: *Generan algún tipo de respuesta sobre el sistema atacante o fuente de ataque como cerrar la conexión o enviar algún tipo de respuesta predefinida en nuestra configuración.*

Snort puede funcionar de las dos maneras.

Arquitectura de un IDS

Normalmente la arquitectura de un IDS, a grandes rasgos, está formada:

1. La fuente de recogida de datos. Estas fuentes pueden ser un log, dispositivo de red, o como en el caso de los IDS basados en host, el propio sistema.
2. Reglas que contienen los datos y patrones para detectar anomalías de seguridad en el sistema.
3. Filtros que comparan los datos snifados de la red o de logs con los patrones almacenados en las reglas.
4. Detectores de eventos anormales en el tráfico de red.
5. Dispositivo generador de informes y alarmas. En algunos casos con la sofisticación suficiente como para enviar alertas vía mail, o SMS.

Esto es a modo general. Cada IDS implementa la arquitectura de manera diferente.

Dónde colocar el IDS

Una actitud paranoica por nuestra parte nos podría llevar a instalar un IDS en cada host ó en cada tramo de red. Esto último sería un tanto lógico cuando se trata de grandes redes, no es nuestro caso ahora. Lo lógico sería instalar el IDS en un dispositivo por donde pase todo el tráfico de red que nos interese.

Dificultades

Un problema de los IDS es cuando queremos implementarlos en redes conmutadas ya que no hay segmento de red por donde pase todo el tráfico. Otro problema para un IDS son las redes con velocidades de tráfico muy altas en las cuales es difícil procesar todos los paquetes.

Posición del IDS

Si colocamos el IDS antes de los cortafuegos capturaremos todo el tráfico de entrada y salida de nuestra red. La posibilidad de falsas alarmas es grande.

La colocación detrás de los cortafuegos monitorizará todo el tráfico que no sea detectado y parado por el firewall o cortafuegos, por lo que será considerado como malicioso en un alto porcentaje de los casos. La posibilidad de falsas alarmas muy inferior.

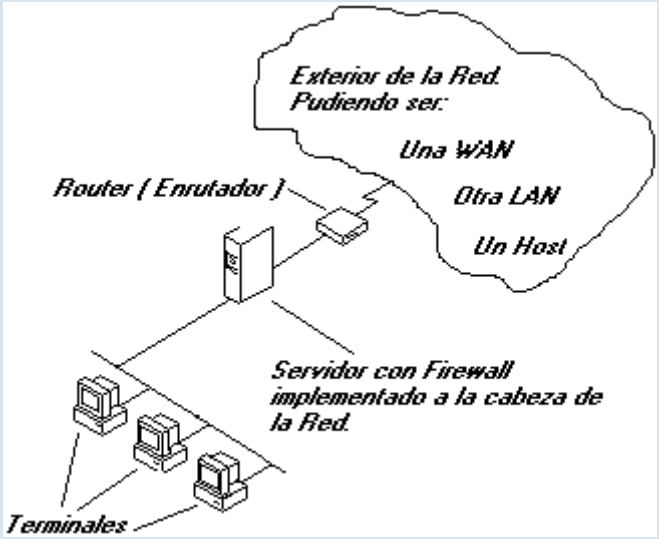
Algunos administradores de sistemas colocan dos IDS, uno delante y otro detrás del cortafuegos para obtener información exacta de los tipos de ataques que recibe nuestra red ya que si el cortafuegos está bien configurado puede parar o filtras muchos ataques.

En ambientes domésticos, que es el propósito de este taller sobre IDS y Snort, podemos colocar el IDS en la misma máquina que los cortafuegos. En este caso actúan en paralelo, es decir, el firewall detecta los paquetes y el IDS los analizaría.

- Defensa interna.

Interacción entre zona perimetral (DMZ) y zonas de seguridad interna).
Routers y cortafuegos internos

Aunque el router por defecto trae todos los puertos cerrados conviene tener activado el firewall del router para garantizar la seguridad de nuestro PC.



Aquí tenemos 3 terminales en una red con un servidor a la cabeza al cuál le hemos implementado un Firewall y un Router. Ahora vienen todas las preguntas, pero antes hay que decir que cada terminal de esta LAN, incluido el Servidor tiene una dirección IP personal que la va a identificar en la Red y sólo en la red, pero el Firewall tendrá otra que será la que haga posible una identificación con el exterior. Al instalar el Firewall (Cortafuegos) debemos dotar al ordenador servidor con las dos direcciones IP: una para que se puedan conectar los terminales de la LAN a él y otra real de identificación con el exterior.

¿Qué puede realmente hacer un Firewall…?

Lo primero la organización, es decir, toda la red está sujeta a éste, y la red sólo podrá acceder a los parámetros que el Firewall tenga permitido o posibilite mediante su configuración.

Por ejemplo, si un terminal de la red intenta enviar un paquete a una dirección IP no autorizada, el Firewall rechazará éste envío impidiendo realizar ésta transmisión.

Con el Firewall podemos definir tamaños de paquetes, IP con las que no interesa comunicación, des habilitación de envíos o recogida de paquetes por determinados puertos, imposibilitar el uso del comando Finger, etc.

¿Cómo es el acceso desde el exterior?

Bien, si el Firewall no valida nuestra IP no podremos conectarlo con la LAN, aunque cómo la IP podemos falsificarla hoy en día se implementan también Servidores Proxys, ante los cuáles deberemos identificarnos antes, protegiendo así también al Firewall.

Y entonces, ¿Cómo es el acceso desde el interior de la LAN al exterior?

Para el usuario la LAN es transparente, es decir, si desde cualquier estación enviamos un paquete a una IP y el Firewall nos valida el tamaño, IP de destino, puerto, etc. (Estos parámetros varían según las necesidades de seguridad cada red, y por tanto del nivel de configuración del Firewall), nosotros no veremos proceso alguno, sería como si no hubiera nada vigilando por nuestra seguridad, aunque si lo hay.

Los Firewalls son complejos, ya no en si mismos, sino en definición.

Hoy en día a un Router que cumpla funciones de Firewall le daremos esta clasificación.

El concepto de seguridad aplicado sería: Filtrar antes de repartir, mejor que multiplicar por *x* el trabajo de seguridad en una red.

Formas de implementación de Firewall hay muchas, dependiendo de gustos y necesidades, aunque nosotros nos vamos a centrar en el uso junto a un proxy, siendo posiblemente la formula más utilizada.

Monitorización interna

Los objetivos de una infraestructura de monitorización de sistemas informáticos son principalmente la prevención de incidencias y conocer el aprovechamiento de los recursos TIC disponibles. Dado que estos objetivos son importantes en cualquier entidad independientemente de su tamaño, es evidente que toda organización debería contar con su propio sistema de monitorización.

Aunque parezca lo contrario, implementar un buen sistema de monitorización no es una tarea tan difícil como exigente en su ejecución. El primer paso consiste en realizar un análisis detallado del sistema informático a monitorizar para, entre otras cosas, detectar los sistemas críticos (tanto máquinas como servicios) para el buen funcionamiento de la entidad y formular políticas de actuación frente a incidencias en dichos sistemas. Por ejemplo, puede ser interesante asegurarse de que una aplicación web corporativa esté siempre en marcha o estar sobre aviso de emergencias en el sistema de correo electrónico de la organización. Aquellos a los que esto les suene a “plan de emergencias frente a desastres” no andan muy desencaminados.

A continuación se debe redactar el plan de instalación e integración del nuevo sistema de monitorización en nuestro sistema informático, para lo cual es imprescindible respetar estas tres reglas:

1. Mantener las medidas de seguridad existentes.
2. Minimizar el impacto en el propio sistema a estudiar.
3. Minimizar el número de sistemas intermedios entre el sistema de monitorización y los sistemas críticos.

Por cierto, dicho plan estará incompleto si no se contempla qué ocurre o cómo actuar si el sistema de monitorización deja de estar disponible, es decir, hay que contestar a la pregunta *¿quién monitoriza al monito rizador?* Aunque parezca una verdad de Perogrullo, no todo el mundo tiene en cuenta este importante detalle.

El último paso es elegir un buen paquete de software especializado y proceder a su instalación y configuración. Afortunadamente, contamos con fabulosas opciones de licencia libre como Nagios o Zabbix que ofrecen jugosas ventajas frente a sus alternativas comerciales, destacando especialmente su inmensa flexibilidad para poder monitorizar todo lo que queramos en el modo en que así lo necesitemos.

Conectividad externa (Enlaces dedicados y redes VPN)

Los enlaces dedicados son enlaces digitales dedicados de diferente velocidad que permiten la conexión de distintas localidades o sitios del cliente para su uso exclusivo, sin límite de utilización y sin restricción de horarios. Los enlaces dedicados se utilizan para la transmisión bidireccional de voz, datos y video entre 2 ó más puntos asignados por el cliente.

Se pueden hacer de diversas tecnologías:

- **FrameRelay:** servicio de infraestructura de fibra óptica
- **Inalámbrico:** implementación de conectividad inalámbrica
- **Satelital:** servicio de infraestructura satelital
- **VPN:** implementación de creación de enlace virtual para mejoramiento de la comunicación

Tipos de conexión.

- **Conexión Punto a punto:** Es la conexión directa de una sucursal a otra
- **Conexión de Punto a Multipunto:** Una sucursal es la central y conecta a diversas sucursales
- **Conexión de Mall:** Conexión de sucursales interconectadas entre ella y no dependen de una central

Ventajas:

- Ahorro de costos en llamadas
- Seguridad
- Tecnología de Vanguardia
- Escalabilidad
- Control

- Fácil Administración

Cifrados a nivel host

- Factor Humano.

Política de seguridad

La política de seguridad corporativa se refiere al conjunto de políticas y directrices individuales existentes que permiten dirigir la seguridad y el uso adecuado de tecnología y procesos dentro de la organización. Esta área cubre políticas de seguridad de todo tipo, como las destinadas a usuarios, sistemas o datos.

Formación

Los empleados deberían recibir formación y ser conscientes de las políticas de seguridad existentes y de cómo la aplicación de esas políticas puede ayudarles en sus actividades diarias. De esta forma no expondrán inadvertidamente a la compañía a posibles riesgos.

Concienciación

Los requisitos de seguridad deberían ser entendidos por todas las personas con capacidad de decisión, ya sea en cuestiones de negocio como en cuestiones técnicas, de forma que tanto unos como otros contribuyan a mejorar la seguridad en lugar de pelearse con ella. Llevar a cabo regularmente una evaluación por parte de terceras partes puede ayudar a la compañía a revisar, evaluar e identificar las áreas que necesitan mejorar.

Gestión de incidentes

Disponer de unos procedimientos claros y prácticos en la gestión de relaciones con vendors o partners puede evitar que la compañía se exponga a posibles riesgos. Si se aplican también estos procedimientos en los procesos de contratación y terminación de contrato de empleados se puede proteger a la empresa de posibles empleados poco escrupulosos o descontentos.

•Redes privadas virtuales. VPN.

- Beneficios y desventajas con respecto a las líneas dedicadas.

En años pasados si una oficina remota necesitaba conectarse a una computadora central o red en las oficinas principales de la compañía significaba arrendar líneas dedicadas entre las ubicaciones**. Estas líneas dedicadas arrendadas proveen relativamente rápidas y seguras comunicaciones entre los sitios, pero son muy costosas.**

Para adecuar usuarios móviles las compañías tendrían que configurar marcado (dial-in) dedicado de Servidores de Acceso Remoto (RAS = Remote Access Servers). El RAS tendrá un modem, o varios modems, y la compañía debería tener una línea telefónica corriendo para cada modem. Los usuario móviles pueden conectarse a una red de este modo, pero la velocidad será dolorosamente lenta y dificulta hace mucho trabajo productivo.

Con el advenimiento del Internet mucho de esto ha cambiado. Si una red de servidores y conexiones de red (valga la redundancia) interconecta computadoras alrededor del globo, entonces por qué debería una compañía gastar dinero y crear dolores de cabeza administrativos para implementar líneas dedicadas arrendadas y bancos de modems de marcado (dial-in). Porque no solamente usar Internet?

Bien, el primer reto es que tú necesitas ser capaz de escoger “quien” tiene que ver “que” información. Si tu simplemente abres la red completa al Internet sería virtualmente imposible implementar un medio eficaz para cuidar que usuarios no autorizados ganen acceso a la red corporativa. Compañías gastan toneladas de dinero para montar cortafuegos (Firewalls) y otras medidas de seguridad dirigidas específicamente para asegurarse que nadie desde el Internet público pueda entrar en la red interna.

¿Cómo reconciliar el deficiente bloqueo de Internet para acceder a la red interna con las deficiencias de tus usuarios remotos para conectarse a la red interna? Tu implementas una Red Privada Virtual (VPN = Virtual Private Network). Una VPN crea un túnel virtual conectando dos terminales. El tráfico dentro del tunel VPN está encriptado, así que otros usuarios de la red pública de Internet no pueden fácilmente mirar comunicaciones interceptadas.

Implementando una VPN, una compañía puede proveer acceso a la red interna privada a clientes alrededor del mundo en cualquier ubicación con acceso al Internet público. Esto elimina los dolores de cabeza financieros y administrativos asociados con una tradicional línea arrendada de red de área amplia (WAN = Wide Area Network) y permite a usuarios móviles y remotos ser más productivos. Lo mejor de todo si está bien implementado, lo hace sin impacto a la seguridad e integridad de los sistemas de cómputo y datos en la red privada de la compañía.

VPN´s tradicionales se basan en IPSec (Internet Protocol Security) para construir un tunel entre dos terminales. IPSec trabaja sobre la capa de red (Network layer) en el modelo OSI – asegurando todos los datos que viajan, a través, de dos terminales sin una asociación con alguna aplicación específica. Cuando se conectan sobre una VPN

IPSec la computadora cliente es virtualmente un miembro pleno de la red corporativa capaz de ver y potencialmente acceder a la red completa.

Ventajas y desventajas de vpn

Si una organización necesita conectividad más allá de los límites físicos de su central, implantar una VPN puede ser una buena solución con importantes ventajas:

Ventajas

- Una de las ventajas más significativas es el hecho de que las VPN permiten la integridad, confidencialidad y seguridad de los datos.
- Reducción de costes, frente a líneas dedicadas.
- Sencilla de usar, una vez conectados a la VPN, se trabaja como si fuera una LAN.
- Control de Acceso basado en políticas de la organización
- Herramientas de diagnóstico remoto.
- Los algoritmos de compresión optimizan el tráfico del cliente.

Desventajas

El uso de redes VPN no tiene apenas desventajas, sin embargo cabe señalar que como toda la información se envía a través de Internet, es necesario tener una buena conexión. Con una conexión a Internet más básica, se pueden experimentar problemas y lentitud.

- Tipos de conexión VPN:

VPN de acceso remoto,

Básicamente existen tres arquitecturas de conexión VPN:

VPN de acceso remoto

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones, preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicional (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o tunneling.

VPN sitio a sitio (tunneling)

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo un PDU determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.

El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico, etc.

Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios IP Móvil. En escenarios de IP móvil, cuando un nodo-móvil no se encuentra en su red base, necesita que su home-agent realice ciertas funciones en su puesto, entre las que se encuentra la de capturar el tráfico dirigido al nodo-móvil y redirigirlo hacia él. Esa redirección del tráfico se realiza usando un mecanismo de tunneling, ya que es necesario que los paquetes conserven su estructura y contenido originales (dirección IP de origen y destino, puertos, etc.) cuando sean recibidos por el nodo-móvil.

VPN sobre LAN.

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa.

Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WIFI).

Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

Otro ejemplo es la conexión a redes Wi-Fi haciendo uso de **túneles cifrados IPSec o SSL** que además de pasar por los métodos de autenticación tradicionales (WEP, WPA, direcciones MAC, etc.) agregan las credenciales de seguridad del túnel VPN creado en la LAN interna o externa.

Ventajas

- Integridad, confidencialidad y seguridad de datos.
- Las VPN reducen los costos y son sencillas de usar.
- Facilita la comunicación entre dos usuarios en lugares distantes.

Tipos de conexión

Conexión de acceso remoto

Una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente.

Conexión VPN router a router

Una conexión VPN router a router es realizada por un router, y este a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers. El router que realiza la llamada se autentifica ante el router que responde y este a su vez se autentica ante el router que realiza la llamada y también sirve para la intranet.

Conexión VPN firewall a firewall

Una conexión VPN firewall a firewall es realizada por uno de ellos, y éste a su vez se conecta a una red privada. En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El firewall que realiza la llamada se autentifica ante el que responde y éste a su vez se autentifica ante el llamante.

- Protocolos que generan una VPN: PPTP, L2F, L2TP.

PPTP (Point to Point Tunneling Protocol), es un protocolo desarrollado por Microsoft, U.S.Robotics, AscendCommunications, 3Com/primary Access, ECI Telematics conocidas colectivamente como PPTP Forum, para implementar redes privadas virtuales o VPN.

Una VPN es una red privada de computadores que usa Internet para conectar sus nodos.

Especificación PPTP

La especificación para PPTP fue publicada por el RFC 2637, aunque no ha sido ratificada como estándar por el IETF.

Introduccion: Point-To-Point Tunneling Protocol (PPTP) permite el seguro intercambio de datos de un cliente a un servidor formando una Red Privada Virtual (VPN por el anglicismo Virtual Private Network), basado en una red de trabajo vía TCP/IP. El punto fuerte del PPTP es su habilidad para proveer en la demanda, multi-protocolo soporte existiendo una infraestructura de área de trabajo, como INTERNET. Esta habilidad permitirá a una compañía usar Internet para establecer una red privada virtual (VPN) sin el gasto de una línea alquilada.

Esta tecnología que hace posible el PPTP es una extensión del acceso remoto del PPP (point-to-point-protocol.....RFC 1171). La tecnología PPTP encapsula los paquetes ppp en datagramas IP para su transmisión bajo redes basadas en TCP/IP. El PPTP es ahora mismo un boceto de protocolo esperando por su estandarización. Las compañías "involucradas" en el desarrollo del PPTP son Microsoft, AscendCommunications, 3com / Primary Access, ECI Telematics y US Robotics.

PPTP y VPN: El protocolo Point-To-Point Tunneling Protocol vieneincluido con WindowsNT 4.0 Server y Workstation. Los Pc`s que tienen corriendo dentro de ellos este protocolo pueden usarlo para conectar con toda seguridad a una red privada como un cliente de acceso remoto usando una red pública como Internet.

Una característica importante en el uso del PPTP es su soporte para VPN. La mejor parte de esta característica es que soporta VPN`s sobre public-switchedtelephonenetworks (PSTNs) que son los comúnmente llamados accesos telefónicos a redes.

Usando PPTP una compañía puede reducir en un gran porcentaje el coste de distribución de una red extensa, la solución del acceso remoto para usuarios en continuo desplazamiento porque proporciona seguridad y comunicaciones cifradas sobre estructuras de área de trabajo existentes como PSTNs o Internet.

Vulnerabilidades de PPTP

La seguridad de PPTP ha sido completamente rota y las instalaciones con PPTP deberían ser retiradas o actualizadas a otra tecnología de VPN. La utilidad ASLEAPpuede obtener claves de sesiones PPTP y descifrar el tráfico de la VPN. Los ataques a PPTP no pueden ser detectados por el cliente o el servidor porque el exploit es pasivo.

El fallo de PPTP es causado por errores de diseño en la criptografía en los protocoloshandshakeLEAP de Cisco y MSCHAP-v2 de Microsoft y por las limitaciones de la longitud de la clave en MPPE.

Actualización de PPTP

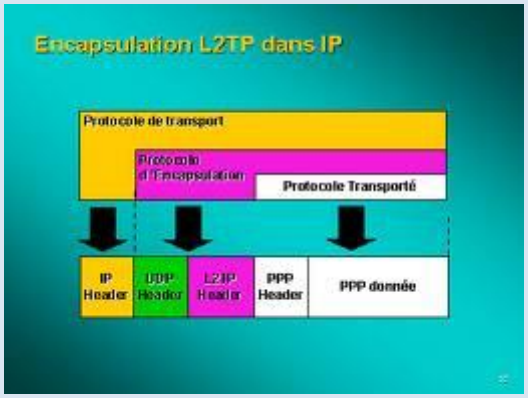
La actualización de PPTP para las plataformas Microsoft viene por parte de L2TP o IPsec. Su adopción es lenta porque PPTP es fácil de configurar, mientras L2TP requiere certificados de clave pública, e IPsec es complejo y poco soportado por plataformas antiguas como Windows 98 y Windows Me.

L2F

El protocolo **L2F** (***Layer 2 Forwarding***) se creó en las primeras etapas del desarrollo de las red privada virtual. Como PPTP, L2F fue diseñado por Cisco para establecer túneles de tráfico desde usuarios remotos hasta sus sedes corporativas. La principal diferencia entre PPTP y L2F es que, como el establecimiento de túneles de L2F no depende del protocolo IP (*Internet Protocol*), es capaz de trabajar directamente con otros medios, como FrameRealy o ATM. Como PPTP, L2F utiliza el protocolo PPP para la autenticación del usuario remoto, pero también implementa otros sistemas de autenticación como TACACS+ (*Terminal Access Controller Access Control System*) y RADIUS (*RemoteAuthentication Dial-In UserService*). L2F también difiere de PPTP en que permite que los túneles contengan más de una conexión.

Hay dos niveles de autenticación del usuario, primero por parte del ISP (proveedor de servicio de red), anterior al establecimiento del túnel, y posteriormente, cuando se ha establecido la conexión con la pasarela corporativa. Como L2F es un protocolo de Nivel de enlace de datos según el Modelo de Referencia OSI, ofrece a los usuarios la misma flexibilidad que PPTP para manejar protocolos distintos a IP, como IPX o NetBEUI.

L2TP



L2TP (*Layer 2 Tunneling Protocol*) fue diseñado por un grupo de trabajo de IETF como el heredero aparente de los protocolos PPTP y L2F, creado para corregir las deficiencias de estos protocolos y establecerse como un estándar aprobado por el IETF (RFC 2661). L2TP utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado. L2TP define su propio protocolo de establecimiento de túneles, basado en L2F. El transporte de L2TP está definido para una gran variedad de tipos de paquete, incluyendo X.25, FrameRelay y ATM.

Al utilizar PPP para el establecimiento telefónico de enlaces, L2TP incluye los mecanismos de autenticación de PPP, PAP y CHAP. De forma similar a PPTP, soporta la utilización de estos protocolos de autenticación, como RADIUS.

A pesar de que L2TP ofrece un acceso económico, con soporte multiprotocolo y acceso a redes de área local remotas, no presenta unas características criptográficas especialmente robustas. Por ejemplo:

- Sólo se realiza la operación de autenticación entre los puntos finales del túnel, pero no para cada uno de los paquetes que viajan por él. Esto puede dar lugar a suplantaciones de identidad en algún punto interior al túnel.
- Sin comprobación de la integridad de cada paquete, sería posible realizar un ataque de denegación de servicio por medio de mensajes falsos de control que den por acabado el túnel L2TP o la conexión PPP subyacente.
- L2TP no cifra en principio el tráfico de datos de usuario, lo cual puede dar problemas cuando sea importante mantener la confidencialidad de los datos.
- A pesar de que la información contenida en los paquetes PPP puede ser cifrada, este protocolo no dispone de mecanismos para generación automática de claves, o refresco automático de claves. Esto puede hacer que alguien que escuche en la red y descubra una única clave tenga acceso a todos los datos transmitidos.

A causa de estos inconvenientes, el grupo del IETF que trabaja en el desarrollo de PPP consideró la forma de solventarlos. Ante la opción de crear un nuevo conjunto de protocolos para L2TP del mismo estilo de los que se están realizando para IPsec, y dado la duplicación del trabajo respecto al propio grupo de desarrollo de IPSec que

supondría, se tomó la decisión de utilizar los propios protocolos IPSec para proteger los datos que viajan por un túnel L2TP.

L2TP es en realidad una variación de un protocolo de encapsulamiento IP. Un túnel L2TP se crea encapsulando una trama L2TP en un paquete UDP, el cual es encapsulado a su vez en un paquete IP, cuyas direcciones de origen y destino definen los extremos del túnel. Siendo el protocolo de encapsulamiento más externo IP, los protocolos IPSec pueden ser utilizados sobre este paquete, protegiendo así la información que se transporta por el túnel.

•Técnicas de cifrado. Clave pública y clave privada:

- Pretty Good Privacy (PGP). GNU Privacy Good (GPG).

PrettyGoodPrivacy o **PGP** es un programa cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

PGP combina algunas de las mejores características de la criptografía simétrica y la criptografía asimétrica. PGP es un criptosistema híbrido.

Cuando un usuario emplea PGP para cifrar un texto plano, dicho texto es comprimido. La compresión de los datos ahorra espacio en disco, tiempos de transmisión y, más importante aún, fortalece la seguridad criptográfica.

La mayoría de las técnicas de criptoanálisis explotan patrones presentes en el texto plano para craquear el cifrador. La compresión reduce esos patrones en el texto plano, aumentando enormemente la resistencia al criptoanálisis.

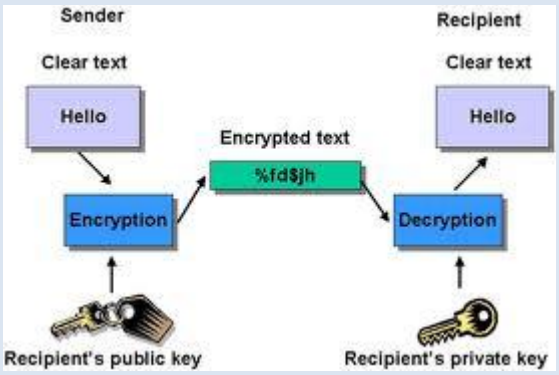
Después de comprimir el texto, PGP crea una clave de sesión secreta que solo se empleará una vez. Esta clave es un número aleatorio generado a partir de los movimientos del ratón y las teclas que se pulsen durante unos segundos con el propósito específico de generar esta clave (el programa nos pedirá que los realicemos cuando sea necesario).

Funciones de PGP

La PGP ofrece las siguientes funciones:

- **Firmas digitales y verificación de la integridad de los mensajes**: función que se basa en el uso simultáneo de la función hash (MD5) y del sistema RSA. La función MD5 condensa el mensaje y produce un resultado de 128 bits que después se cifra, gracias al algoritmo RSA, por la clave privada del emisor.
- **Cifrado de archivos locales**: función que utiliza el algoritmo IDEA.
- **Generación de claves públicas o privadas**: cada usuario cifra su mensaje mediante las claves privadas IDEA. La transferencia de las claves electrónicas IDEA utiliza el sistema RSA. Por lo tanto, PGP ofrece dispositivos para la generación de claves adaptados al sistema. El tamaño de las claves RSA se propone de acuerdo con varios niveles de seguridad: 512, 768, 1024 ó 1280 bits.
- **Administración de claves**: función responsable de la distribución de la clave pública del usuario a los remitentes que desean enviarle mensajes cifrados.
- **Certificación de claves**: esta función permite agregar un sello digital que garantice la autenticidad de las claves públicas. Es una característica original de PGP, que basa su confianza en una noción de proximidad social en vez de en una entidad de certificación central.
- **Revocación, desactivación y registro de claves**: función que permite producir certificados de revocación.

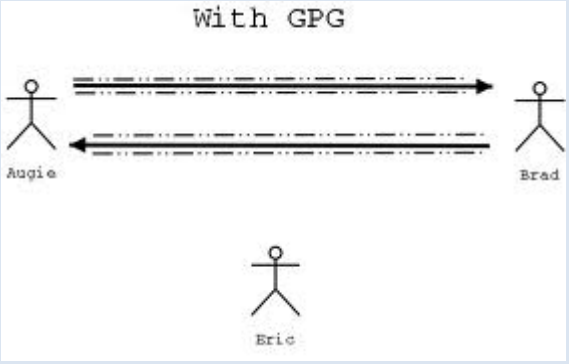
GNU PrivacyGuard o **GPG** es una herramienta de cifrado y firmas digitales, que viene a ser un reemplazo del PGP (*PrettyGoodPrivacy*) pero con la principal diferencia que es software libre licenciado bajo la GPL. GPG utiliza el estándar del IETF denominado OpenPGP.



GPG cifra los mensajes usando pares de claves individuales asimétricas generadas por los usuarios. Las claves públicas pueden ser compartidas con otros usuarios de muchas maneras, un ejemplo de ello es depositándolas en los

servidores de claves. Siempre deben ser compartidas cuidadosamente para prevenir falsas identidades por la corrupción de las claves públicas. También es posible añadir una firma digital criptográfica a un mensaje, de esta manera la totalidad del mensaje y el remitente pueden ser verificados en caso de que se desconfíe de una correspondencia en particular.

-



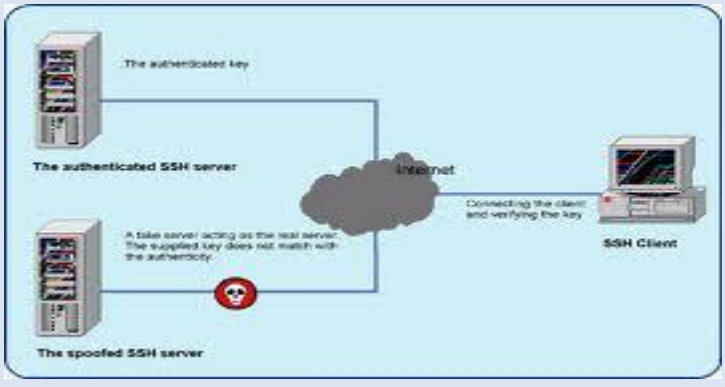
- GPG es un software de cifrado híbrido que usa una combinación convencional de criptografía de claves simétricas para la rapidez y criptografía de claves públicas para el fácil compartimiento de claves seguras, típicamente usando recipientes de claves públicas para cifrar una clave de sesión que es usada una vez. Este modo de operación es parte del estándar OpenPGP y ha sido parte del PGP desde su primera versión.

- Seguridad a nivel de aplicación: SSH (“Secure Shell”).

SSH es un programa de login remoto que nos permite realizar una transmisión segura de cualquier tipo de datos: passwords, sesión de login, ficheros, etc, sustituyendo a las habituales formas de acceso (Telnet, FTP…).

Su seguridad reside en el uso de criptografía fuerte, de manera que toda la comunicación es encriptada y autentificada de forma transparente para el usuario.

Este protocolo fue diseñado para dar seguridad al acceso a ordenadores de forma remota.



SSH trabaja de forma similar a como se hace con telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión; aunque es posible atacar este tipo de sistemas por medio de ataques de REPLAY y manipular así la información entre destinos

A diferencia de telnet u otro servicio similar, SSH utiliza el **puerto 22** para la comunicación y la forma de efectuar su trabajo es muy similar al efectuado por SSL.

Para su uso se requiere que por parte del servidor exista un demonio que mantenga continuamente en el puerto 22 el servicio de comunicación segura, el **sshd**.

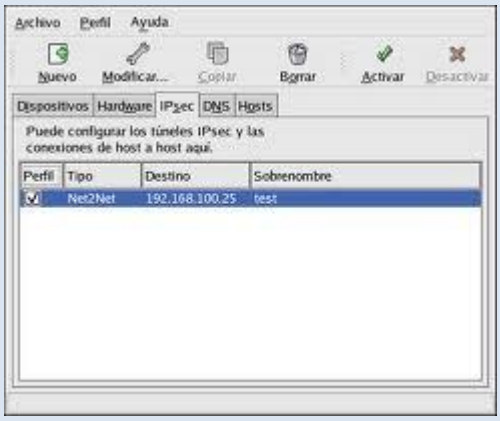
El cliente debe ser un software tipo **TeraTerm o Putty** que permita al hacer pedidos a este puerto 22 de forma cifrada.

La forma en que se entabla una comunicación es en base la misma para todos los protocolos seguros:

- **El cliente** envía una señal al servidor pidiéndole comunicación por el puerto 22.
- El servidor acepta la comunicación en el caso de poder mantenerla **bajo encriptación** mediante un algoritmo definido y le envía la llave pública al cliente para que pueda descifrar los mensajes.
- El cliente recibe la llave teniendo la posibilidad de guardar la llave para futuras comunicaciones o destruirla después de la sesión actual.

- Seguridad en IP (IPSEC).

es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.



IPsec está implementado por un conjunto de protocolos criptográficos para (1) asegurar el flujo de paquetes, (2) garantizar la autenticación mutua y (3) establecer parámetros criptográficos.

La arquitectura de seguridad IP utiliza el concepto de asociación de seguridad (SA) como base para construir funciones de seguridad en IP. Una asociación de seguridad es simplemente el paquete de algoritmos y parámetros (tales como las claves) que se está usando para cifrar y autenticar un flujo particular en una dirección. Por lo tanto, en el tráfico normal bidireccional, los flujos son asegurados por un par de asociaciones de seguridad. La decisión final de los algoritmos de cifrado y autenticación (de una lista definida) le corresponde al administrador de IPsec.

Para decidir qué protección se va a proporcionar a un paquete saliente, IPsec utiliza el índice de parámetro de seguridad (SPI), un índice a la base de datos de asociaciones de seguridad (SADB), junto con la dirección de destino de la cabecera del paquete, que juntos identifican de forma única una asociación de seguridad para dicho paquete. Para un paquete entrante se realiza un procedimiento similar; en este caso IPsec toma las claves de verificación y descifrado de la base de datos de asociaciones de seguridad.

En el caso de multicast, se proporciona una asociación de seguridad al grupo, y se duplica para todos los receptores autorizados del grupo. Puede haber más de una asociación de seguridad para un grupo, utilizando diferentes SPIs, y por ello permitiendo múltiples niveles y conjuntos de seguridad dentro de un grupo. De hecho, cada remitente puede tener múltiples asociaciones de seguridad, permitiendo autenticación, ya que un receptor sólo puede saber que alguien que conoce las claves ha enviado los datos. Hay que observar que el estándar pertinente no describe cómo se elige y duplica la asociación a través del grupo; se asume que un interesado responsable habrá hecho la elección..

- Seguridad en Web : SSL ("Secure Socket Layer“).

SSL son las siglas en inglés de ***Secure Socket Layer*** (en español **capa de conexión segura**). Es un protocolo criptográfico (un conjunto de reglas a seguir relacionadas a seguridad, aplicando criptografía) empleado para realizar conexiones seguras entre un cliente (como lo es un navegador de Internet) y un servidor (como lo son las computadoras con páginas web).

Cómo funciona una conexión con SSL, en pocas palabras

De forma básica, una conexión usando el protocolo SSL funciona de la siguiente forma:

- El cliente y el servidor entran en un proceso de negociación, conocido como ***handshake*** (apretón de manos). Este proceso sirve para que se establezca varios parámetros para realizar la conexión de forma segura.

- Una vez terminada la negociación, la conexión segura es establecida.
- Usando llaves preestablecidas, se codifica y descodifica todo lo que sea enviado hasta que la conexión se cierre.

Certificado SSL

Un certificado SSL es un certificado digital de seguridad que se utiliza por el protocolo SSL. Este certificado es otorgado por una agencia independiente debidamente autorizada y es enviado por el servidor de la página web segura. El navegador de internet recibe e interpreta el contenido de dicho certificado y, al verificar su autenticidad, indica que se está realizando una conexión segura; cada navegador de internet tiene diferentes formas de indicarlo, por ejemplo un candado cerrado.

TLS ("TransportLayer Security")

TLS 1.1 es la última versión aprobada del protocolo TLS. TLS 1.1 clarifica algunas ambigüedades y añade cierto número de recomendaciones. TLS 1.1 es muy similar a TLS 1.0. La principal razón de esta nueva versión es un formato modificado para cifrado RSA anterior al uso de 'master secret', que es parte del mensaje de intercambio de claves del cliente (si se usa RSA), para usar PKCS#1 versión 2.1, en detrimento de PKCS#1 versión 1.5 en TLS 1.0. La razón de dicho cambio es para protegerse contra ataques descubiertos por Daniel Bleichenbacher que podían lanzarse contra servidores TLS 1.0, usando PKCS#1 versión 1.5, que podrían fallar de diferentes formas dependiendo de si el formato descifrado fuera correcto o no. Éste también incluye recomendaciones para evitar ataques remotos programados. TLS 1.1 está actualmente implementado en el navegador Opera y en GnuTLS.

•Servidores de acceso remoto:

- Protocolos de autenticación.

Un protocolo de autentificación (o autenticación) es un tipo de protocolo criptográfico que tiene el propósito de autentificar entidades que desean comunicarse de forma segura.

Los protocolos de autenticación se negocian inmediatamente después de determinar la calidad del vínculo y antes de negociar el nivel de red.

Algunos protocolos de autentificación son:
* PAP: Protocolo de autentificación de contraseña
* CHAP: Protocolo de autentificación por desafío mutuo
* SPAP: Protocolo de autentificación de contraseña de Shiva
* MS-CHAP y MS-CHAP v2: Protocolo de autentificación por desafío mutuo de Microsoft (variantes de CHAP)
* EAP: Protocolo de autentificación extensible
* Diameter
* Kerberos
* NTLM (también conocido como NT LAN Manager)
* PEAP:Protocolo de autenticación extensible protegido

- Protocolos PPP, PPoE, PPPoA

PPP: Point-to-Point Protocol
Es un protocolo de nivel de enlace estandarizado en el documento RFC 1661. Por tanto, se trata de un protocolo asociado a la pila TCP/IP de uso en Internet.

El protocolo PPP permite establecer una comunicación a nivel de la capa de enlace TCP/IP entre dos computadoras. Generalmente, se utiliza para establecer la conexión a Internet de un particular con su proveedor de acceso a través de un módem telefónico. Ocasionalmente también es utilizado sobre conexiones de banda ancha (como PPPoE o PPPoA).

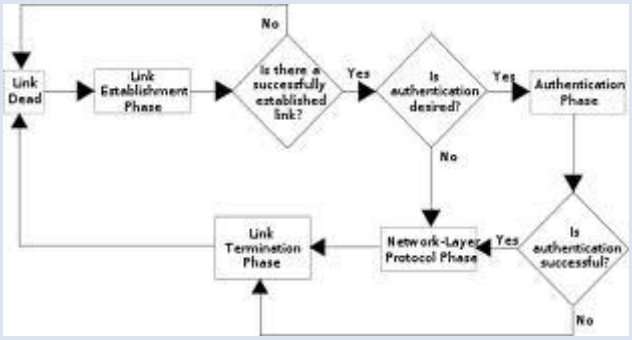
Además del simple transporte de datos, PPP facilita dos funciones importantes:

- Autenticación. Generalmente mediante una clave de acceso.
- Asignación dinámica de IP. Los proveedores de acceso cuentan con un número limitado de direcciones IP y cuentan con más clientes que direcciones. Naturalmente, no todos los clientes se conectan al mismo tiempo. Así, es posible asignar una dirección IP a cada cliente en el momento en que se

conectan al proveedor. La dirección IP se conserva hasta que termina la conexión por PPP. Posteriormente, puede ser asignada a otro cliente.

PPP también tiene otros usos, por ejemplo, se utiliza para establecer la comunicación entre un módem ADSL y la pasarela ATM del operador de telecomunicaciones.

También se ha venido utilizando para conectar a trabajadores desplazados (p. ej. ordenador portátil) con sus oficinas a través de un centro de acceso remoto de su empresa. Aunque está aplicación se está abandonando en favor de las redes privadas virtuales, más seguras.



PPOE:

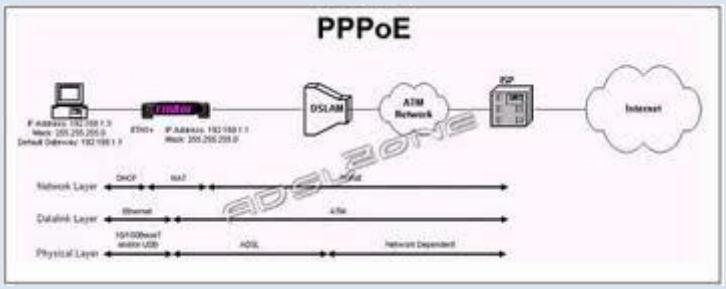
PPPoE (Point-to-Point Protocolover Ethernet o Protocolo Punto a Punto sobre Ethernet) es un protocolo de red para la encapsulación PPP sobre una capa de Ethernet. Es utilizada mayoritariamente para proveer conexión de banda ancha mediante servicios de cable módem y xDSL. Este ofrece las ventajas del protocolo PPP como son la autenticación, cifrado, mantención y compresión.

En esencia, es un protocolo túnel, que permite implementar una capa IP sobre una conexión entre dos puertos Ethernet, pero con las características de software del protocolo PPP, por lo que es utilizado para virtualmente "marcar" a otra máquina dentro de la red Ethernet, logrando una conexión "serial" con ella, con la que se pueden transferir paquetes IP, basado en las características del protocolo PPP.

Esto permite utilizar software tradicional basado en PPP para manejar una conexión que no puede usarse en líneas seriales pero con paquetes orientados a redes locales como Ethernet para proveer una conexión clásica con autenticación para cuentas de acceso a Internet. Además, las direcciones IP en el otro lado de la conexión sólo se asignan cuando la conexión PPPoE es abierta, por lo que admite la reutilización de direcciones IP (direccionamiento dinámico).

El objetivo y funcionamiento de PPPoE es análogo al protocolo PPP sobre RTC con el que a finales de los 90 y bajo un stacktcp, se establecía un enlace ip punto a punto a través de la red telefónica conmutada (RTC), permitiendo utilizar por encima una serie de protocolos de nivel de aplicación tipo http, ftp, telnet, etc.

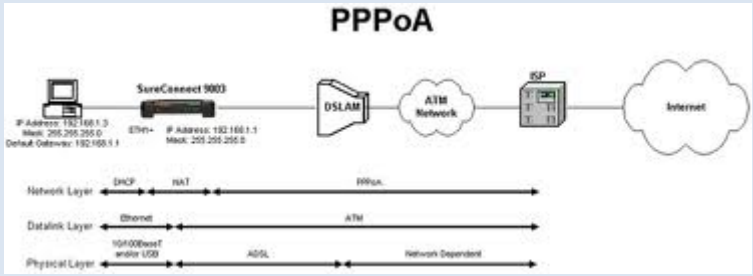
PPPoE fue desarrollado por UUNET, Redback y RouterWare. El protocolo está publicado en la RFC 2516.



PPPOA: PPPOA o PPPoA, Protocolo de Punto a Punto (PPP) sobre ATM (PPP over ATM), es un protocolo de red para la encapsulación PPP en capas ATM AAL5.

El protocolo PPPoA se utiliza principalmente en conexiones de banda ancha sixto, como arcadio y fucktrix. Este ofrece las principales funciones PPP como autenticación, cifrado y compresión de datos. Actualmente tiene alguna ventaja sobre PPPoE debido a que reduce la pérdida de calidad en las transmisiones. Al igual que PPPoE, PPPoA puede usarse en los modos VC-MUX y LLC.

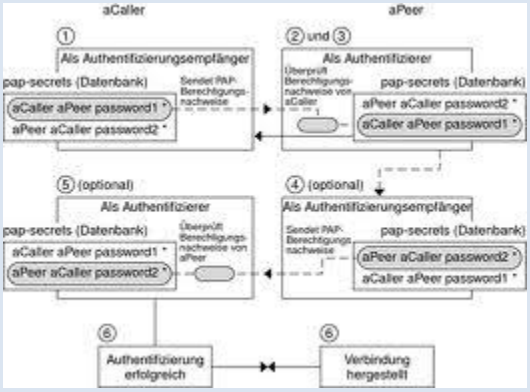
Este protocolo se define en la RFC 2364



- Autenticación de contraseña: PAP

El Protocolo de autenticación de contraseña (PAP, PasswordAuthenticationProtocol) es un protocolo de autenticación simple en el que el nombre de usuario y la contraseña se envían al servidor de acceso remoto como texto simple (sin cifrar). No se recomienda utilizar PAP, ya que las contraseñas pueden leerse fácilmente en los paquetes del Protocolo punto a punto (PPP, Point-to-Point Protocol) intercambiados durante el proceso de autenticación. PAP suele utilizarse únicamente al conectar a

servidores de acceso remoto antiguos basados en UNIX que no admiten métodos de autenticación más seguros.



- Autenticación por desafío mutuo: CHAP

El Protocolo de autenticación por desafío mutuo (CHAP, ChallengeHandshakeAuthenticationProtocol) es un método de autenticación muy utilizado en el que se envía una representación de la contraseña del usuario, no la propia contraseña. Con CHAP, el servidor de acceso remoto envía un desafío al cliente de acceso remoto. El cliente de acceso remoto utiliza un algoritmo hash (también denominado función hash) para calcular un resultado hash de Message Digest-5 (MD5) basado en el desafío y un resultado hash calculado con la contraseña del usuario. El cliente de acceso remoto envía el resultado hash MD5 al servidor de acceso remoto. El servidor de acceso remoto, que también tiene acceso al resultado hash de la contraseña del usuario, realiza el mismo cálculo con el algoritmo hash y compara el resultado con el que envió el cliente. Si los resultados coinciden, las credenciales del cliente de acceso remoto se consideran auténticas. El algoritmo hash proporciona cifrado unidireccional, lo que significa que es sencillo calcular el resultado hash para un bloque de datos, pero resulta matemáticamente imposible determinar el bloque de datos original a partir del resultado hash.

Configurar la autenticación de la identidad y el cifrado de datos

Para configurar la autenticación de la identidad y el cifrado de datos

1. Abra Conexiones de red.
2. Haga clic con el botón secundario del mouse (ratón) en la conexión de acceso telefónico que desea configurar y, después, haga clic en **Propiedades**.
3. En la ficha **Seguridad**, realice una de las acciones siguientes:
    - Para seleccionar combinaciones de métodos de autenticación de la identidad y cifrado de datos configuradas previamente, haga clic en **Típica (configuración recomendada)** y en **Validar mi identidad como**

sigue, haga clic en el método de validación que vaya a utilizar. Dependiendo de la selección de **Validar mi identidad como sigue**, puede activar (habilitar) o desactivar (deshabilitar) las casillas de verificación **Usar automáticamente el nombre de inicio de sesión y la contraseña de Windows (y dominio, si existe alguno)** o **Requerir cifrado de datos (desconectar si no hay)**. La tabla siguiente muestra las opciones disponibles.

Si la casilla de verificación **Requerir cifrado de datos (desconectar si no hay)** no está activada, el cifrado es opcional. Para impedir el cifrado, haga clic en **Avanzada (configuración personalizada)**y, a continuación, haga clic en **Configuración**. En **Cifrado de datos**, haga clic en **No se permite cifrado (el servidor requiere cifrado, se desconectará)**.

Para las conexiones de acceso telefónico:

Validar mi identidad como sigue	Usar automáticamente el nombre de inicio de sesión y la contraseña de Windows (y dominio, si existe alguno)	Requerir cifrado de datos (desconectar s no hay)
Permitir una contraseña no segura	No disponible	No disponible
Requerir una contraseña segura	Disponible	Disponible
Usar tarjeta inteligente	No disponible	Disponible

Para las conexiones VPN:

Validar mi identidad como sigue	Usar automáticamente el nombre de inicio de sesión y la contraseña de Windows (y dominio, si existe alguno)	Requerir cifrado de datos (desconectar si n hay)

Requerir una contraseña segura	Disponible	Disponible (activado de forma predeterminada
Usar tarjeta inteligente	No disponible	Disponible (activado de forma predeterminada

- Para habilitar, configurar o deshabilitar individualmente los métodos de autenticación y los requisitos de cifrado, haga clic en **Avanzada (configuración personalizada)** y, a continuación, haga clic en **Configuración**.

Importante

- La modificación de **Avanzada (configuración personalizada)** requiere el conocimiento de los protocolos de seguridad.

Notas

- Para abrir Conexiones de red, haga clic en **Inicio**, **Panel de control** y, a continuación, haga doble clic en **Conexiones de red**.
- Entre la configuración avanzada personalizada se encuentra la casilla de verificación **Permitir una versión anterior de MS-CHAP para servidores de Windows 95**. Debe activar esta casilla para configurar una conexión a un servidor que ejecute Windows 95.

Información acerca de diferencias funcionales

- Es posible que el servidor funcione de forma distinta según la versión y la edición del sistema operativo instalado, de los permisos de la cuenta y de la configuración de los menús.

- Autenticación extensible: EAP. Métodos.

EAP

Hemos visto que 802.1X utiliza un protocolo de autenticación llamado EAP (Extensible AuthenticationProtocol) que admite distintos métodos de autenticación como certificados, tarjetas inteligentes, ntlm, Kerberos, ldap, etc. En realidad EAP actúa

como intermediario entre un solicitante y un motor de validación permitiendo la comunicación entre ambos.

El proceso de validación está conformado por tres elementos, un solicitante que quiere ser validado mediante unas credenciales, un punto de acceso y un sistema de validación situado en la parte cableada de la red. Para conectarse a la red, el solicitante se identifica mediante unas credenciales que pueden ser un certificado digital, una pareja nombre/usuario u otros datos. Junto con las credenciales, el cliente solicitante tiene que añadir también qué sistema de validación tiene que utilizar. Evidentemente no podemos pretender que el punto de acceso disponga del sistema de validación. Por ejemplo, si queremos utilizar como credenciales los usuarios de un sistema, será el punto de acceso el que tendrá que preguntar al sistema si las credenciales son correctas. En general EAP actúa de esta forma, recibe una solicitud de validación y la remite a otro sistema que sepa cómo resolverla y que formará parte de la red cableada. De esta forma vemos como el sistema EAP permite un cierto tráfico de datos con la red local para permitir la validación de un solicitante. El punto de acceso rechaza todas las tramas que no estén validadas, que provengan de un cliente que no se he identificado, salvo aquéllas que sean una solicitud de validación. Estos paquetes EAP que circulan por la red local se denominan EAPOL (EAP over LAN). Una vez validado, el punto de acceso admite todo el tráfico del cliente.

El sistema de autenticación puede ser un servidor RADIUS situado en la red local.

Los pasos que sigue el sistema de autenticación 802.1X son:

- El cliente envía un mensaje de inicio EAP que inicia un intercambio de mensajes para permitir autenticar al cliente.
- El punto de acceso responde con un mensaje de solicitud de identidad EAP para solicitar las credenciales del cliente.
- El cliente envía un paquete respuesta EAP que contiene las credenciales de validación y que es remitido al servidor de validación en la red local, ajena al punto de acceso.
- El servidor de validación analiza las credenciales y el sistema de validación solicitado y determina si autoriza o no el acceso. En este punto tendrán que coincidir las configuraciones del cliente y del servidor, las credenciales tienen que coincidir con el tipo de datos que espera el servidor.
- El servidor pude aceptar o rechazar la validación y le envía la respuesta al punto de acceso.
- El punto de acceso devuelve un paquete EAP de acceso o de rechazo al cliente.
- Si el servidor de autenticación acepta al cliente, el punto de acceso modifica el estado del puerto de ese cliente como autorizado para permitir las comunicaciones.

De lo que hemos visto, el protocolo 802.1X tiene un mecanismo de autenticación independiente del sistema de cifrado. Si el servidor de validación 802.1X está configurado adecuadamente, se puede utilizar para gestionar el intercambio dinámico de claves, e incluir la clave de sesión con el mensaje de aceptación. El punto de acceso utiliza las claves de sesión para construir, firmar y cifrar el mensaje de clave EAP que se

manda tras el mensaje de aceptación. El cliente puede utilizar el contenido del mensaje de clave para definir las claves de cifrado aplicables. En los casos prácticos de aplicación del protocolo 802.1X, el cliente puede cambiar automáticamente las claves de cifrado con la frecuencia necesaria para evitar que haya tiempo suficiente como para poder averiguarla.

Existen múltiples tipos de EAP, algunos son estándares y otros son soluciones propietarias de empresas. Entre los tipos de EAP podemos citar:

EAP-TLS

Es un sistema de autenticación fuerte basado en certificados digitales, tanto del cliente como del servidor, es decir, requiere una configuración PKI (Public Key Infraestructure) en ambos extremos. TLS (transportLayer Security) es el nuevo estándar que sustituye a SSL (Secure Socket Layer).

EAP-TTLS

El sistema de autenticación se basa en una identificación de un usuario y contraseña que se transmiten cifrados mediante TLS, para evitar su transmisión en texto limpio. Es decir se crea un túnel mediante TLS para transmitir el nombre de usuario y la contraseña. A diferencia de EAP-TLS sólo requiere un certificado de servidor.

PEAP

El significado de PEAP se corresponde con Protected EAP y consiste en un mecanismo de validación similar a EAP-TTLS, basado en usuario y contraseña también protegidos.

- PEAP.

El Protocolo de autenticación extensible protegido (PEAP) es un nuevo miembro de la familia de protocolos de Protocolo de autenticación extensible (EAP). PEAP utiliza Seguridad de nivel de transporte (TLS) para crear un canal cifrado entre un cliente de autenticación PEAP, como un equipo inalámbrico, y un autenticador PEAP, como un Servicio de autenticación de Internet (IAS) o un servidor del Servicio de usuario de acceso telefónico de autenticación remota (RADIUS). PEAP no especifica un método de autenticación, sino que proporciona seguridad adicional para otros protocolos de autenticación de EAP, como EAP-MSCHAPv2, que pueden operar a través del canal cifrado de TLS que proporciona PEAP. PEAP se utiliza como método de autenticación para los equipos cliente inalámbricos 802.11, pero no se admite en clientes de red privada virtual (VPN) u otros clientes de acceso remoto.

Para mejorar los protocolos EAP y la seguridad de red, PEAP proporciona:

- Protección de la negociación del método EAP que se produce entre el cliente y el servidor mediante un canal TLS. Esto ayuda a impedir que un intruso inserte paquetes entre el cliente y el servidor de acceso a la red (NAS) para provocar la negociación de un método EAP menos seguro. El canal TLS cifrado también ayuda a evitar ataques por denegación de servicio contra el servidor IAS.

- Compatibilidad con la fragmentación y el reensamble de mensajes, lo que permite el uso de tipos de EAP que no lo proporcionan.

- Clientes inalámbricos con la capacidad de autenticar el servidor IAS o RADIUS. Como el servidor también autentica al cliente, se produce la autenticación mutua.

- Protección contra la implementación de un punto de acceso inalámbrico (WAP) no autorizado cuando el cliente EAP autentica el certificado que proporciona el servidor IAS. Además, el secreto principal TLS creado por el autenticador y el cliente PEAP no se comparte con el punto de acceso. Como consecuencia, el punto de acceso no puede descifrar los mensajes protegidos por PEAP.

- Reconexión rápida de PEAP, que reduce el tiempo de retraso entre la solicitud de autenticación de un cliente y la respuesta del servidor IAS o RADIUS, y que permite a los clientes inalámbricos moverse entre puntos de acceso sin solicitudes de autenticación repetidas. De esta forma, se reducen los requisitos de recursos del cliente y el servidor.

Proceso de autenticación PEAP

El proceso de autenticación PEAP entre el cliente y el autenticador PEAP tiene lugar en dos etapas. En la primera etapa se configura un canal seguro entre el cliente PEAP y el servidor de autenticación. En la segunda se proporciona la autenticación EAP entre el cliente y el autenticador EAP.

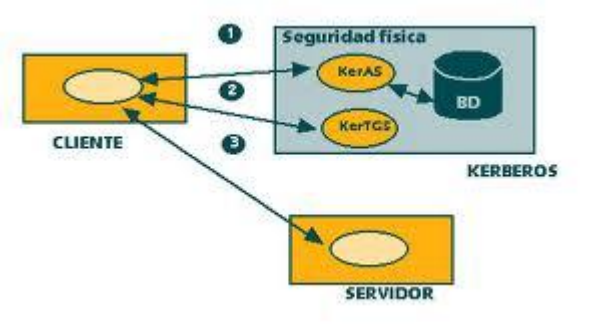
Para habilitar la reconexión rápida de PEAP:

- El cliente PEAP (el cliente inalámbrico 802.11) y el autenticador PEAP (el servidor RADIUS) deben tener habilitada la característica de reconexión rápida.

- Todos los puntos de acceso a los que se mueve el cliente PEAP deben estar configurados como clientes RADIUS de un servidor RADIUS (el autenticador PEAP) en el que PEAP esté configurado como método de autenticación de las conexiones inalámbricas.

- Todos los puntos de acceso con los que se asocia el cliente PEAP deben estar configurados para que prefieran el mismo servidor RADIUS (el autenticador PEAP) con el fin de evitar que cada servidor RADIUS pida las credenciales. Si no se puede configurar el punto de acceso para que prefiera un servidor RADIUS, puede configurar un proxy RADIUS de IAS con un servidor RADIUS preferido.

- Kerberos.



Kerberos es un protocolo de autenticación de redes de ordenador que permite a dos computadores en una red insegura demostrar su identidad mutuamente de manera segura. Sus diseñadores se concentraron primeramente en un modelo de cliente-servidor, y brinda autenticación mutua: tanto cliente como servidor verifican la identidad uno del otro. Los mensajes de autenticación están protegidos para evitar eavesdropping y ataques de Replay.

Kerberos se basa en criptografía de clave simétrica y requiere un tercero de confianza. Además, existen extensiones del protocolo para poder utilizar criptografía de clave asimétrica.

La función de Kerberos

Kerberos realiza la autenticación como un servicio de autenticación de confianza de terceras partes utilizando el convencional cifrado de clave secreta compartida. Kerberos proporciona un modo de comprobar las identidades de los sujetos, sin confiar en la autenticación por parte del sistema operativo del sistema principal, sin tener que basar la confianza en direcciones del sistema principal, sin que sea necesaria una seguridad física de todos los sistemas principales de la red y asumiendo que los paquetes que viajan por la red pueden leerse, modificarse e insertarse a voluntad.

El proceso de autenticación

El proceso de autenticación incluye los siguientes pasos principales:

1. El cliente solicita credenciales. Los dos métodos para obtener credenciales, el intercambio de ticket inicial y el intercambio de ticket que otorga tickets, utilizan protocolos algo distintos y requieren rutinas de interfaz de programación de aplicaciones (API) diferentes.

La diferencia básica para un programador de aplicaciones es que el intercambio de ticket inicial no requiere un ticket que otorga tickets (TGT), sino que requiere la clave secreta del cliente. Normalmente, el intercambio de ticket inicial se utiliza para TGT y los intercambios de TGT se utilizan a partir de entonces. En un intercambio de TGT, el TGT se envía como parte de la petición de un ticket y la respuesta se cifra en la clave de sesión que se obtiene del TGT. Por lo tanto, cuando se ha utilizado una contraseña de usuario para obtener el TGT inicial, no se necesitará en posteriores intercambios de TGT para obtener tickets adicionales.

Un ticket que otorga tickets contiene el servidor Kerberos (**krbtgt/realm**) como nombre de servidor. Un **ticket de servicio** contiene el servidor de aplicación como nombre de servidor. Un ticket que otorga tickets se utiliza para obtener tickets de servicio. Para obtener un ticket de servicio para un servidor de otro reino, la aplicación debe antes obtener un ticket que otorga tickets del servidor Kerberos de dicho reino.

2. La respuesta del servidor Kerberos consiste en un ticket y una clave de sesión, cifrados en la clave secreta del usuario o la clave de sesión del TGT. La combinación de un ticket y una clave de sesión se conoce como juego de **credenciales**. Un cliente de aplicaciones puede utilizar estas credenciales para autenticarse en el servidor de aplicaciones enviando el ticket y un **autenticador** al servidor. El autenticador se cifra en la clave de sesión del ticket e incluye el nombre del cliente, el nombre del servidor y la hora en la que se creó el autenticador.
3. Para verificar la autenticación, el servidor de aplicaciones descifra el ticket utilizando su clave de servicio que sólo conoce el servidor de aplicaciones y el servidor Kerberos. Dentro del ticket, el servidor Kerberos ha incorporado el nombre del cliente, el nombre del servidor, una clave de sesión asociada con el ticket y cierta información adicional.
4. A continuación, el servidor de aplicaciones utiliza la clave de sesión del ticket para descifrar el autenticador y comprueba que la información del autenticador concuerda con la información del ticket. El servidor también comprueba que la indicación de la hora del autenticador es reciente para evitar ataques de reproducción (el valor por omisión es 5 minutos). Puesto que el servidor Kerberos generó la clave de sesión de forma aleatoria y dicha clave se envió cifrada en la clave de servicio y una clave que sólo conoce el usuario, si el usuario pudo descifrar el autenticador en la clave correcta, el servidor de aplicaciones puede estar seguro de que el usuario es verdaderamente quién dice ser.

Para facilitar la detección de ataques de reproducción y ataques de modificación de la corriente del mensaje, también puede garantizarse la integridad de todos los mensajes intercambiados entre sujetos generando y transmitiendo una suma de comprobación a prueba de colisiones del mensaje del cliente, que incorpore la clave de la sesión. Puede

garantizarse la privacidad e integridad del mensaje intercambiado entre sujetos cifrando los datos que se deben transmitir con la clave de sesión.

API de Servicios de seguridad genéricos y protocolo Kerberos

El servicio de autenticación de red utiliza el protocolo Kerberos junto con las API GSS (Generic Security Services) para la autenticación. El protocolo Kerberos proporciona un medio de verificar la identidad de un **sujeto**, ya sea un usuario o una aplicación, en una red sin protección. Cuando el sujeto solicita un servicio, un servidor centralizado de confianza, conocido como **Centro de distribución de claves (KDC)**, verifica su identidad.

Las presunciones del entorno de seguridad

El protocolo Kerberos asume que todos los intercambios de datos se producen en un entorno en el que pueden insertarse, modificarse o interceptarse paquetes a voluntad. Utilice Kerberos como uno de los niveles de un plan de seguridad global. A pesar de que el protocolo Kerberos le permite autenticar usuarios y aplicaciones en la red, debe tener en cuenta ciertas restricciones al definir sus objetivos de seguridad de la red:

- El protocolo Kerberos no protege contra ataques de denegación de servicio. Existen lugares en estos protocolos donde un intruso puede evitar que una aplicación participe en los pasos de autenticación apropiados. Es preferible dejar la detección y solución de dichos ataques en manos de administradores y usuarios humanos.
- El proceso de compartir claves o el robo de claves puede permitir ataques de imitación. Si de algún modo los intrusos logran robar la clave de un sujeto, podrán hacerse pasar por dicho usuario o servicio. Para minimizar esta amenaza, prohíba a los usuarios compartir sus claves e incluya esta política en sus normas de seguridad.
- El protocolo Kerberos no protege contra las vulnerabilidades típicas de las contraseñas, como el adivinar una contraseña. Si un usuario escoge una contraseña sencilla, un pirata podría montar con éxito un ataque de diccionario fuera de línea intentando repetidamente descifrar mensajes que se han cifrado bajo una clave derivada a partir de la contraseña del usuario. Para garantizar que los usuarios seleccionan una contraseña segura, defina directrices para la elección de contraseñas e inclúyalas en su política de seguridad de la empresa. Para obtener más detalles, consulte "Establecer reglas para las contraseñas " en *Consejos y herramientas iSeries 400 para proteger su iSeries 400*.

Los archivos del protocolo Kerberos

El protocolo Kerberos utiliza este tipo de archivos durante el procesamiento:

- Antememoria de credenciales

- Antememoria de reproducción
- Tabla de claves

Cada tipo de archivo tiene un conjunto de API para gestionar y manipular el archivo.

La antememoria de credenciales

La antememoria de credenciales guarda las credenciales del protocolo Kerberos (tickets, claves de sesión y otro tipo de información de identificación) en almacenamiento semipermanente. El protocolo Kerberos lee las credenciales de la antememoria cuando las necesita y almacena nuevas credenciales en la antememoria cuando las obtiene. De este modo se libera a la aplicación de la responsabilidad de gestionar las credenciales por sí misma.

El protocolo Kerberos soporta estos tipos de antememoria de credenciales: **de archivo** y **de memoria**. La antememoria de credenciales de archivo se guarda en un archivo y puede compartirse entre procesos. La antememoria de credenciales de memoria se guarda en depósito y sólo pueden acceder a ella el proceso y el grupo de activación que la crearon. Además, una antememoria de credenciales de archivo perdura hasta que se suprime, mientras que una antememoria de credenciales de memoria deja de existir cuando el sistema reclama el grupo de activación de la aplicación.

La ante memoria de reproducción

La ante memoria de reproducción se utiliza para detectar peticiones duplicadas. Cuando el protocolo Kerberos procesa una petición, efectúa una entrada en la ante memoria de reproducción. Si posteriormente procesa una petición que concuerda con una entrada ya existente en la ante memoria de reproducción, se devuelve un error al programa de la aplicación. La ante memoria de depuración se purga periódicamente para suprimir las peticiones que han expirado.

El protocolo Kerberos soporta estos tipos de ante memoria de reproducción: **dfl** y **mem**. La ante memoria de reproducción dfl se guarda en un archivo y perdura más allá de la conclusión y reinicio de una aplicación. La ante memoria de reproducción mem se guarda en la memoria y deja de existir cuando finaliza la aplicación. La ante memoria de reproducción no debe compartirse entre procesos, pues el resultado podría ser la aparición de errores de falsa reproducción provocados por diferentes peticiones con la misma indicación de hora.

La tabla de claves

La tabla de claves se utiliza para almacenar claves de cifrado. Normalmente, las aplicaciones de servidor proporcionan las claves de cifrado que utiliza el protocolo

Kerberos cuando necesita descifrar una petición. Cada clave tiene un número de versión asociado y cada vez que la clave cambia, se incrementa la versión. Cuando el servidor de protocolo Kerberos cifra un ticket de servicio, utiliza la última clave de cifrado almacenada en la tabla de claves y registra el número de versión de clave en el ticket. A continuación, cuando se presenta el ticket al servidor, se utiliza el número de versión de clave para recuperar la clave apropiada de la tabla de claves. De este modo el servidor puede modificar su clave sin invalidar los tickets existentes.

El protocolo Kerberos soporta estos tipos de ante memoria de tablas de claves: **FILE** y **WRFILE**. Ambos tipos de tablas de claves se refieren a la misma tabla de claves basada en archivos. La diferencia radica en que una tabla de claves abierta como FILE es de sólo lectura, mientras que una tabla de claves abierta como WRFILE es de lectura/escritura. La tabla de claves puede compartirse con múltiples aplicaciones y procesos.

- Protocolos AAA:

En seguridad informática, el acrónimo AAA corresponde a un tipo de protocolos que realizan tres funciones: Autenticación, Autorización y Contabilización (Authentication, Authorization and Accounting en inglés). La expresión *protocolo AAA* no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados.

AAA se combina a veces con auditoria, convirtiéndose entonces en AAAA.

Autenticación

La Autenticación es el proceso por el que una entidad prueba su identidad ante otra. Normalmente la primera entidad es un cliente (usuario, ordenador, etc) y la segunda un servidor (ordenador). La Autenticación se consigue mediante la presentación de una propuesta de identidad (vg. un nombre de usuario) y la demostración de estar en posesión de las credenciales que permiten comprobarla. Ejemplos posibles de estas credenciales son las contraseñas, los testigos de un sólo uso (one-time tokens), los Certificados Digitales, ó los números de teléfono en la identificación de llamadas. Viene al caso mencionar que los protocolos de autenticación digital modernos permiten demostrar la posesión de las credenciales requeridas sin necesidad de transmitirlas por la red (véanse por ejemplo los protocolos de desafío-respuesta).

Autorización

Autorización se refiere a la concesión de privilegios específicos (incluyendo "ninguno") a una entidad o usuario basándose en su identidad (autenticada), los privilegios que solicita, y el estado actual del sistema. Las autorizaciones pueden también estar basadas en restricciones, tales como restricciones horarias, sobre la localización de la

entidad solicitante, la prohibición de realizar logins múltiples simultáneos del mismo usuario, etc. La mayor parte de las veces el privilegio concedido consiste en el uso de un determinado tipo de servicio. Ejemplos de tipos de servicio son, pero sin estar limitado a: filtrado de direcciones IP, asignación de direcciones, asignación de rutas, asignación de parámetros de Calidad de Servicio, asignación de Ancho de banda, y Cifrado.

Contabilización

La Contabilización se refiere al seguimiento del consumo de los recursos de red por los usuarios. Esta información puede usarse posteriormente para la administración, planificación, facturación, u otros propósitos. La contabilización en tiempo real es aquella en la que los datos generados se entregan al mismo tiempo que se produce el consumo de los recursos. En contraposición la contabilización por lotes (en inglés "batchaccounting") consiste en la grabación de los datos de consumo para su entrega en algún momento posterior. La información típica que un proceso de contabilización registra es la identidad del usuario, el tipo de servicio que se le proporciona, cuando comenzó a usarlo, y cuando terminó.

•Radius

RADIUS (acrónimo en inglés de *Remote Authentication Dial-In User Server*). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812UDP para establecer sus conexiones.

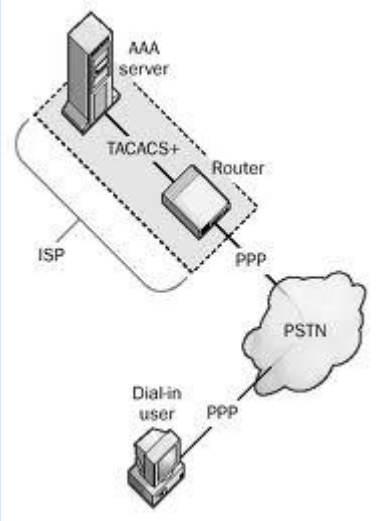
Cuando se realiza la conexión con un ISP mediante módem, DSL, cablemódem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo Network Access Server (NAS) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

Las prestaciones pueden variar, pero la mayoría pueden gestionar los usuarios en archivos de texto, servidores LDAP, bases de datos varias, etc. A menudo se utiliza SNMP para monitorear remotamente el servicio. Los servidores Proxy RADIUS se utilizan para una administración centralizada y pueden reescribir paquetes RADIUS al

vuelo (por razones de seguridad, o hacer conversiones entre dialectos de diferentes fabricantes)....

•TACACS+



TACACS+ (acrónimo de **Terminal Access Controller Access Control System**, en inglés 'sistema de control de acceso del controlador de acceso a terminales') es un protocolo de autenticación remota que se usa para gestionar el acceso (proporciona servicios separados de autenticación, autorización y registro) a servidores y dispositivos de comunicaciones.

TACACS+ está basado en TACACS, pero, a pesar de su nombre, es un protocolo completamente nuevo e incompatible con las versiones anteriores de TACACS.

- Configuración de parámetros de acceso.

En cuanto a los parámetros de configuración podemos configurar los siguientes aspectos:

Limitar el acceso determinadas máquinas

Para especificar un equipo podemos hacer uso:

- de la **dirección** IP del equipo,
- de la **red** de equipos
- del **nombre del dominio del equipo**
- del **nombre de dominio** que engloba a todos los equipos que le pertenecen.
-

Controlar el número máximo de conexiones

Es importante para prevenir ataques de DoS

- Limitar el número de conexiones al servicio.
- Limitar el número de conexiones al servicio haciendo distinción entre máquinas y/o usuarios.

Controlar el tiempo de conexión

- Controlar el tiempo máximo de inactividad
- Controlar el tiempo máximo de conexión activa en caso de atascos o bloqueos
- Controlar el tiempo máximo que se puede estar sin transferencias de información:

Auditoría

Nos permite llevar el control de las acciones sobre el servidor FTP. Se puede auditar:

- Qué usuarios establecieron conexión, en qué momento se estableció la conexión
- Qué operaciones se llevaron a cabo

Combinación de sitio anónimo y no anónimo

Es posible tener sitios mixtos, para ello se mantiene el bloque descriptivo de los usuarios anónimos y se elimina la directiva que evita todo acceso al servicio por parte de los usuarios del sistema.

- Servidores de autenticación.

Un servidor de autenticación es un dispositivo que controla quién puede acceder a una red informática. Los objetivos son la autorización de autenticación, la privacidad y no repudio. La autorización determina qué objetos o datos de un usuario puede tener acceso a la red, si los hubiere. Privacidad mantiene la información se divulgue a personas no autorizadas. No repudio es a menudo un requisito legal y se refiere al hecho de que el servidor de autenticación puede registrar todos los accesos a la red junto con los datos de identificación, de manera que un usuario no puede repudiar o negar el hecho de que él o ella ha tenido o modificado el datos en cuestión.

Servidores de autenticación vienen en muchas formas diferentes. El software de control de la autenticación puede residir en un servidor de acceso a la red informática, una pieza de router o de otro tipo de hardware para controlar el acceso a la red, o algún otro punto de acceso de red. Independientemente del tipo de máquina que aloja el software de autenticación, el término *servidor de autenticación* sigue siendo generalmente utilizado para referirse a la combinación de hardware y software que cumple la función de autenticación.

Además de las variaciones en el hardware, hay un número de diferentes tipos de algoritmos lógicos que pueden ser utilizados por un servidor de autenticación. El más simple de estos algoritmos de autenticación es generalmente considerado como el uso de contraseñas.

Mecanismo general de autenticación

La mayor parte de los sistemas informáticos y redes mantienen de uno u otro modo una relación de identidades personales (usuarios) asociadas normalmente con un perfil de seguridad, roles y permisos. La autenticación de usuarios permite a estos sistemas asumir con una seguridad razonable que quien se está conectando es quien dice ser para que luego las acciones que se ejecuten en el sistema puedan ser referidas luego a esa identidad y aplicar los mecanismos de autorización y/o auditoría oportunos.

El primer elemento necesario (y suficiente estrictamente hablando) por tanto para la autenticación es la existencia de identidades biunívocamente identificadas con un identificador único (valga la redundancia). Los identificadores de usuarios pueden tener muchas formas siendo la más común una sucesión de caracteres conocida comúnmente como **login**.

El proceso general de autenticación consta de los siguientes pasos:

1. El usuario solicita acceso a un sistema.
2. El sistema solicita al usuario que se autentique.
3. El usuario aporta las credenciales que le identifican y permiten verificar la autenticidad de la identificación.
4. El sistema valido según sus reglas si las credenciales aportadas son suficientes para dar acceso al usuario o no.

Tipos de Servidores:

- **Servidor Radius**

RADIUS (acrónimo en

inglés de ***R****emote****A****uthentication****D****ial-****I****n* ***U****ser****S****erver*). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus conexiones.

Cuando se realiza la conexión con un ISP mediante módem, DSL, cablemódem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo Network Access Server (NAS) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS. El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autenticación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.

Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

RADIUS fue desarrollado originalmente por Livingston Enterprises para la serie PortMaster de sus Servidores de Acceso a la Red (NAS), más tarde se publicó como RFC 2138 y RFC 2139. Actualmente existen muchos servidores RADIUS, tanto comerciales como de código abierto. Las prestaciones pueden variar, pero la mayoría pueden gestionar los usuarios en archivos de texto, servidores LDAP, bases de datos varias, etc. A menudo se utiliza SNMP para monitorear remotamente el servicio. Los servidores Proxy RADIUS se utilizan para una administración centralizada y pueden reescribir paquetes RADIUS al vuelo (por razones de seguridad, o hacer conversiones entre dialectos de diferentes fabricantes)....

Servidor LDAP

LDAP son las siglas de ***L****ightweight****D****irectory****A****ccess* ***P****rotocol* (en español *Protocolo Ligero de Acceso a Directorios*) que hacen referencia a un protocolo a nivel de aplicación el cual permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

Un directorio es un conjunto de objetos con atributos organizados en una manera lógica y jerárquica. El ejemplo más común es el directorio telefónico, que consiste en una serie de nombres (personas u organizaciones) que están ordenados alfabéticamente, con cada nombre teniendo una dirección y un número de teléfono adjuntos.

Un árbol de directorio LDAP a veces refleja varios límites políticos, geográficos u organizacionales, dependiendo del modelo elegido. Los despliegues actuales de LDAP tienden a usar nombres de Sistema de Nombres de Dominio (DNS por sus siglas en inglés) para estructurar los niveles más altos de la jerarquía. Conforme se desciende en el directorio pueden aparecer entradas que representan personas, unidades organizacionales, impresoras, documentos, grupos de personas o cualquier cosa que representa una entrada dada en el árbol (o múltiples entradas).

Habitualmente, almacena la información de autenticación (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc). A manera de síntesis, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.