Implementación de técnicas de seguridad remota. Seguridad perimetral.

Seguridad y Alta Disponibilidad

Autor: Miguel Ángel García Felipe

I.E.S GREGORIO PRIETO

ÍNDICE:

- 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.

1- Elementos básicos de la seguridad perimetral:

La **seguridad perimetral** es un concepto emergente asume la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusión y/o disuasión de intrusos en instalaciones especialmente sensibles. Entre estos sistemas cabe destacar los radares tácticos, videosensores, vallas sensorizadas, cables sensores, barreras de microondas e infrarrojos, concertinas, etc.

Los sistemas de seguridad perimetral pueden clasificarse según la geometría de su cobertura (volumétricos, superficiales, lineales, etc.), según el principio físico de actuación (cable de fibra óptica, cable de radiofrecuencia, cable de presión, cable microfónico, etc.) o bien por el sistema de soportación (autosoportados, soportados, enterrados, detección visual, etc.).

También cabe destacar la clasificación dependiendo del medio de detección. En esta se clasificarían en:

- **Sistemas Perimetrales Abiertos:** Los que dependen de las condiciones ambientales para detectar. Como ejemplo de estos son la video vigilancia, las barreras infrarrojas, las barreras de microondas. Esta característica provoca falsas alarmas o falta de sensibilidad en condiciones ambientales adversas.
- **Sistemas Perimetrales Cerrados:** Los que no dependen del medio ambiente y controlan exclusivamente el parámetro de control. Como ejemplo de estos son los antíguos cables microfónicos, la fibra óptica y los piezo-sensores. Este tipo de sensores suelen ser de un coste más elevado.

Su aplicación destaca principalmente en Seguridad Nacional (instalaciones militares y gubernamentales, fronteras, aeropuertos, etc.) e instalaciones privadas de alto riesgo (centrales nucleares, sedes corporativas, residencias VIP, etc.).

Entre los fabricantes internacionales más prestigiosos destacan:

- RBtec Perimeter Solutions (EE.UU)
- Magal Security Systems (Israel),
- Senstar Corporation (Canada),
- Opgal Optronic Systems (Israel),
- Delta Scientific (EE.UU.) y
- Allied Tube & Conduit (EE.UU.).

- Concepto de seguridad perimetral.

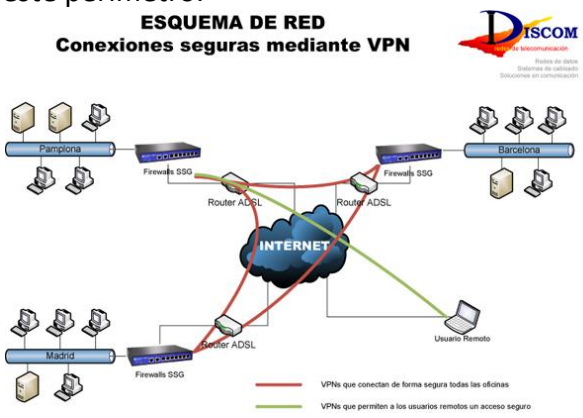
La seguridad perimetral es uno de los métodos posibles de defensa de una red, basado en el establecimiento de recursos de segurización en el perímetro externo de la red y a diferentes niveles.
Esto nos permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos 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 gateways, 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).

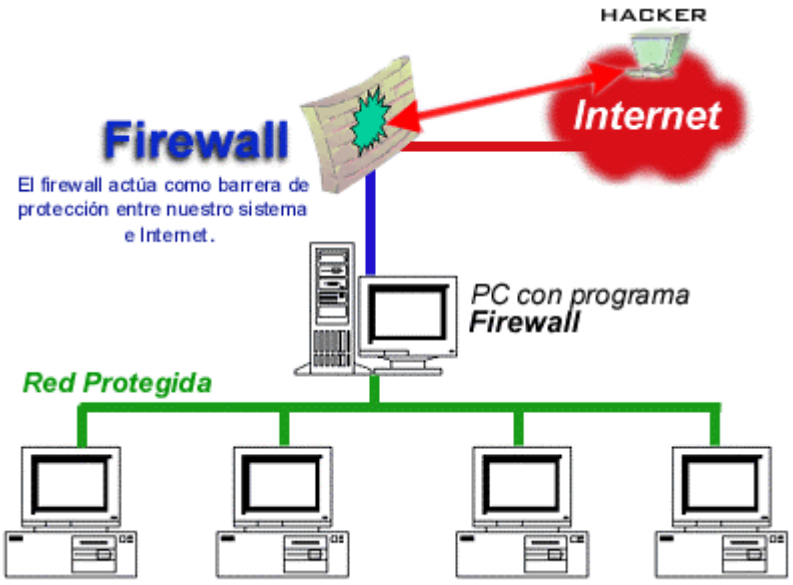
- Routers frontera.

Un router de frontera es un dispositivo situado entre la red interna de y las redes de otros proveedores que intercambian el tráfico con nosotros y que se encarga de dirigir el tráfico de datos de un lado a otro. 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.



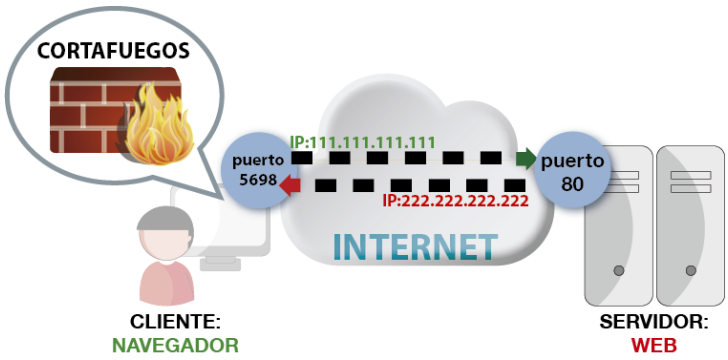
¿Para qué sirve un cortafuegos?

El cortafuegos 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, el cortafuegos personal 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 del 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)*



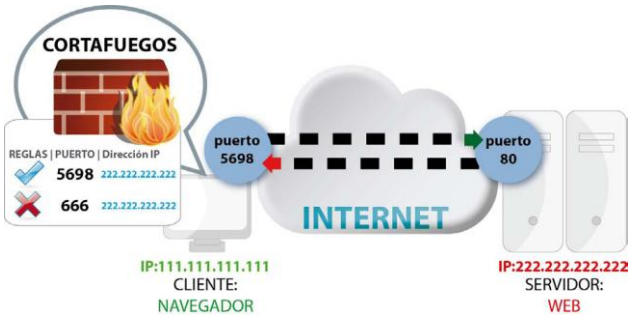
Ejemplo de conexión entre cliente y servidor con cortafuegos

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 cortafuegos 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 un 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 un cortafuegos del lado del cliente

- **Saliente**

El cortafuegos 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 un cortafuegos saliente se podría, por ejemplo, establecer reglas como estas:

CLIENTE (origen)				SERVIDOR (destino)		
IP	Programa	Puerto Origen	Cortafuegos	IP	Programa	Puerto Destino
Nuestra	Internet Explorer	Cualquiera	Bloquear	Cualquiera	Servidor Web	81
Nuestra	Internet Explorer	Cualquiera	Dejar pasar	Cualquiera	Servidor Web	80

Fuente: INTECO

Ejemplo de reglas de un cortafuegos desde el punto de vista del cliente, para el tráfico saliente

Con esta regla, se estaría indicando al cortafuegos 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.

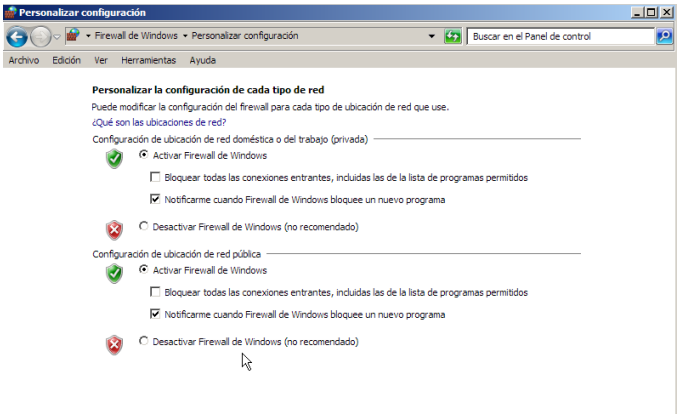
- **Controlar las aplicaciones que acceden a un puerto**

Un cortafuegos 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:

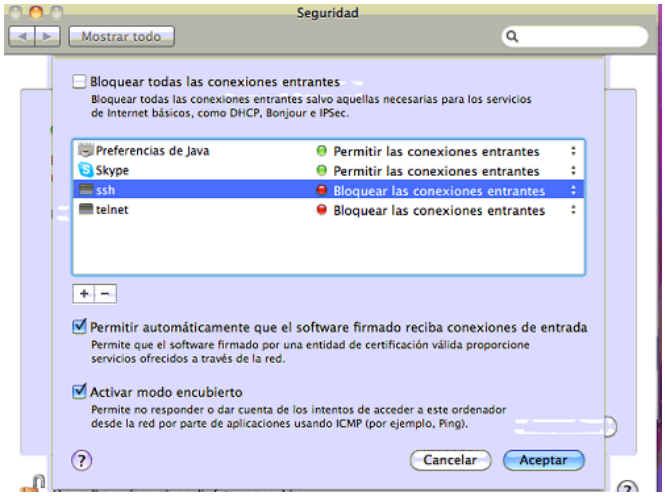
Configuración básica del cortafuegos de Windows en Vista y 7

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



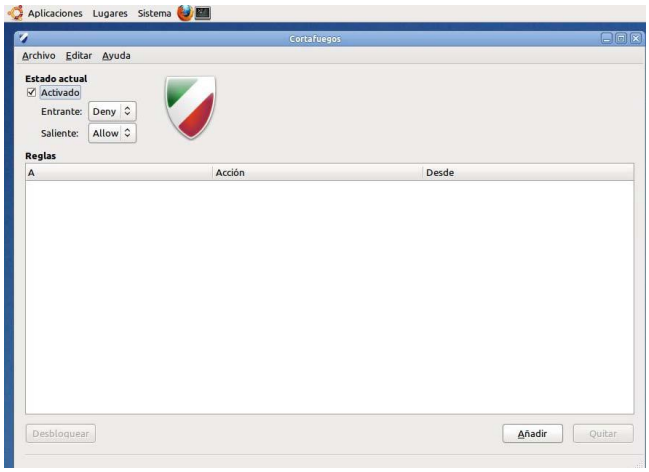
Cortafuegos con configuración típica en Mac OS

Mac OS X cuenta con un cortafuegos 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.*



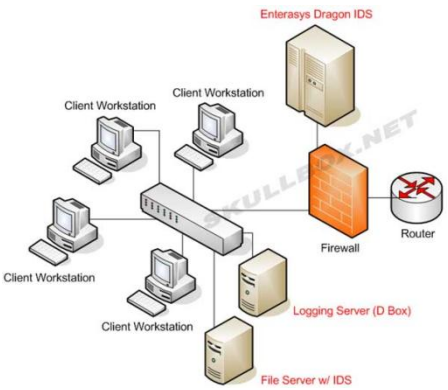
- Sistemas de Detección de Intrusos (IDS).

Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) 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 Intrusion Detection System (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 Node Intrusion Detection System (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 Intrusion Detection System(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 cortafuegos 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.

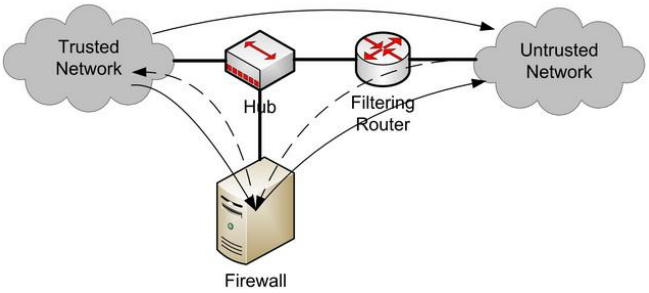
Por lo tanto, el sistema VPN brinda una conexión segura a un bajo costo, ya que todo lo que se necesita es el hardware de ambos lados. Sin embargo, no garantiza una calidad de servicio comparable con una línea dedicada, ya que la red física es pública y por lo tanto no está garantizada.

- 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).

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.

- Zonas desmilitarizadas (DMZ) y subredes controladas.

Una **zona desmilitarizada** (DMZ, demilitarized zone) 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. 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 correo electrónico, Web y DNS.

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

Una DMZ se crea a menudo a través de las opciones de configuración del cortafuegos, donde cada red se conecta a un puerto distinto de éste. Esta configuración se llama

cortafuegos en trípode (three-legged firewall). Un planteamiento más seguro 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).

2- Arquitecturas de cortafuegos:

- Cortafuegos de filtrado de paquetes.

El modelo de cortafuegos más antiguo consiste en un dispositivo capaz de filtrar paquetes, lo que se denomina *choke*. Está basado simplemente en aprovechar la capacidad que tienen algunos *routers* para bloquear o filtrar paquetes en función de su protocolo, su servicio o su dirección IP.

Esta arquitectura es la más simple de implementar y la más utilizada en organizaciones que no precisan grandes niveles de seguridad, donde el *router* actúa como de*pasarela* de la subred y no hay necesidad de utilizar *proxies*, ya que los accesos desde la red interna al exterior no bloqueados son directos. Resulta recomendable bloquear todos los servicios que no se utilicen desde el exterior, así como el acceso desde máquinas que no sean de confianza hacia la red interna.

Sin embargo, los *chokes* presentan más desventajas que beneficios para la red protegida, puesto que no disponen de un sistema de monitorización sofisticado y el administrador no distingue entre si el router está siendo atacado o si su seguridad se ha visto comprometida. Por otra parte, las reglas de filtrado pueden llegar a ser complejas de establecer y por lo tanto, se hace difícil comprobar su correción.

- Cortafuegos Dual-Homed Host.

Dispositivos que estan 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 diche Firewall, se conectara al servicio exterior solicitado y hara 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 alvergue el servicio exterior.

- Screened Host.

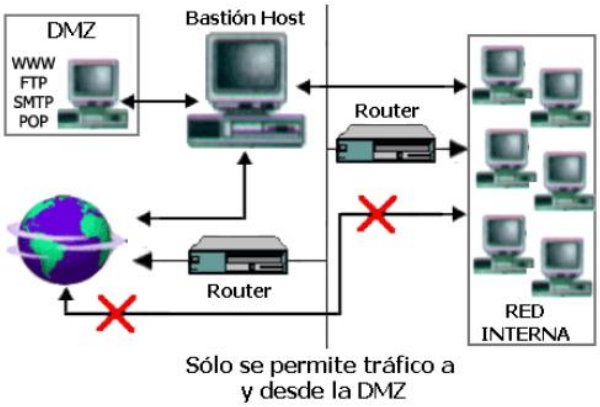
Combina un router con un host bastión, y donde el principal nivel de seguridad proviene del filtrado de paquetes (es decir, el router es la primera y más importante línea de defensa). En la maquina bastión, único sistema accesible desde el exterior, se ejecutan los proxies de las aplicaciones, mientras que el choke se encarga de filtrar los paquetes que se puedan considerar peligrosos para la seguridad de la red interna, permitiendo únicamente la comunicación con un reducido número de servicios.
La mayoría de los autores recomiendan situar el router entre la red exterior y el host bastión, pero otros defienden justo lo contrario: situar el bastión en la red exterior no provoca aparentemente una degradación de la seguridad, y además ayuda al administrador a comprender la necesidad de un elevado nivel de fiabilidad en esta máquina, ya que está sujeta a ataques extern0os 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* prohíbe todo el tráfico entre máquinas de la red interna y el exterior, permitiendo sólo la salida de ciertos servicios que provienen de la máquina bastión y que han sido autorizados por la política de seguridad de la organización. Así, estamos obligando a los usuarios a que las conexiones con el exterior se realicen a través de los servidores *proxy* situados en el bastión.

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

- Screened Subnet (DMZ).

En este diseño se intenta aislar la máquina más atacada y vulnerable del Firewall, el Nodo Bastión. Para ello se establece una Zona Desmilitarizada (DMZ) de forma tal que sin un intruso accede a esta máquina no consiga el acceso total a la subred protegida.
En este esquema se utilizan dos Routers: uno exterior y otro interior. El Router exterior tiene la misión de bloquear el tráfico no deseado en ambos sentidos: hacia la red interna y hacia la red externa. El Router interior hace lo mismo con la red interna y la DMZ (zona entre el Router externo y el interno).
Es posible definir varios niveles de DMZ agregando más Routers, pero destacando que las reglas aplicadas a cada uno deben ser distintas ya que en caso contrario los niveles se simplificarían a uno solo.



Como puede apreciarse la Zona Desmilitarizada aíslafísicamentelos servicios internos, separándolos de los servicios públicos. Además, n o existe una conexión directa entre la red interna y la externa.
Los sistemas Dual-Homed Host y Screnned pueden ser complicados de configurar y comprobar, lo que puede dar lugar, paradójicamente, a importantes agujeros de seguridad en toda la red. En cambio, si se encuentran bien configurados y administrados pueden brindar un alto grado de protección y ciertas ventajas:

1. **Ocultamiento de la información:** los sistemas externos no deben conocer el nombre de los sistemas internos. El Gateway de aplicaciones es el único autorizado a conectarse con el exterior y el encargado de bloquear la información no solicitada o sospechosa.
2. **Registro de actividades y autenticación robusta:** El Gateway requiere de autenticación cuando se realiza un pedido de datos externos. El registro de actividades se realiza en base a estas solicitudes.
3. **Reglas de filtrado menos complejas:** Las reglas del filtrado de los paquetes por parte del Router serán menos compleja dado a que él sólo debe atender las solicitudes del Gateway.

Así mismo tiene la desventaja de ser intrusivos y no transparentes para el usuario ya que generalmente este debe instalar algún tipo de aplicación especializada para lograr

la comunicación. Se suma a esto que generalmente son más lentos porque deben revisar todo el tráfico de la red.

- Otras arquitecturas

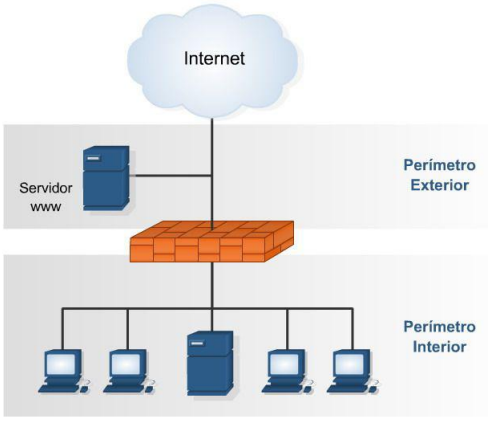
Algo que puede incrementar en gran medida nuestra seguridad y al mismo tiempo facilitar la administración de los cortafuegos es utilizar un bastión diferente para cada protocolo o servicio en lugar de uno sólo; sin embargo, esta arquitectura presenta el grave inconveniente de la cantidad de máquinas 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.

3- Políticas de defensa en profundidad:

- Defensa perimetral.

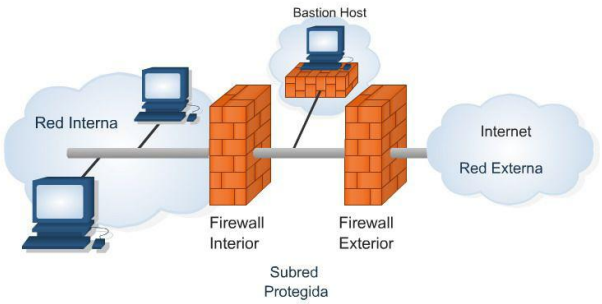
La seguridad perimetral es uno de los métodos posibles de defensa de una red, basado en el establecimiento de recursos de segurización en el perímetro externo de la red y a diferentes niveles.

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

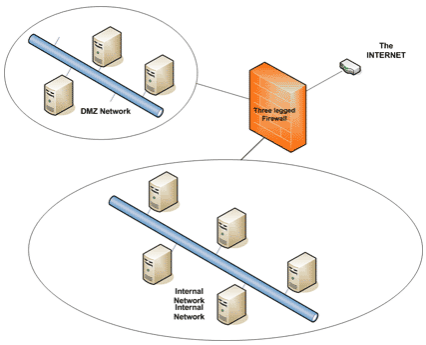
- Un **IDS** o **Sistema de Detección de Intrusiones** es una herramienta de seguridad que intenta **detectar o monitorizar los eventos** ocurridos en un determinado sistema informático o red informática en busca de intentos de comprometer la seguridad de dicho sistema.
- Los **IDS** buscan **patrones 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.

- Defensa interna.

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

En seguridad informática, una **zona desmilitarizada** (DMZ, demilitarized zone) 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. 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 correo electrónico, Web y DNS.



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

Una DMZ se crea a menudo a través de las opciones de configuración del cortafuegos, donde cada red se conecta a un puerto distinto de éste. Esta configuración se llama cortafuegos en trípode (three-legged firewall). Un planteamiento más seguro 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).

Obsérvese que los enrutadores domésticos son llamados "DMZ host", aunque no es una definición correcta de zona desmilitarizada.

ArquitecturaDMZ

Cuando ciertas máquinas de la red interna tienen que ser accesibles desde el exterior (servidor web, un servidor de mensajería, un servidor FTP público, etc.), normalmente es necesario crear una nueva política para una nueva red, accesible tanto desde la red interna como desde el exterior, sin correr el riesgo de comprometer la seguridad de la empresa. Se habla entonces de una "zona desmilitarizada" (DMZ para DeMilitarized Zone) para designar esta zona aislada que aloja aplicaciones a disposición del público. El DMZ sirve como una zona intermedia entre la red a proteger y la red hostil.

DMZ - Zona desmilitarizada

Los servidores situados en la DMZ se llaman "bastiones" debido a su posición anterior en la red de la empresa.

La política de seguridad aplicada en la DMZ, normalmente es la siguiente:

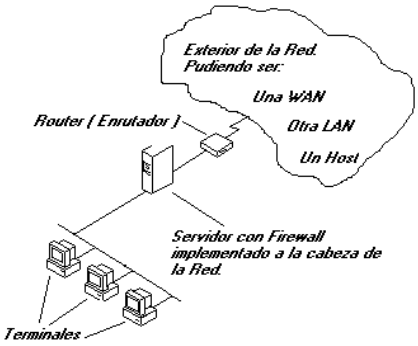
- Tráfico de la red externa hacia la DMZ autorizada;
- Tráfico de la red externa hacia la red interna prohibida;
- Tráfico de la red interna hacia la DMZ autorizada;
- Tráfico de la red interna hacia la red externa autorizada;
- Tráfico de la DMZ hacia la red interna prohibida;
- Tráfico de la DMZ hacia la red externa rechazada.

La DMZ tiene un nivel de protección intermedio. Su nivel de seguridad no es suficiente para almacenar datos críticos de la empresa.

Es necesario notar que es posible instalar una DMZ internamente, para compartir la red interna de acuerdo a los diferentes niveles de protección y así evitar las intrusiones que vienen desde el interior.

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, deshabilitación 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 ántes 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:

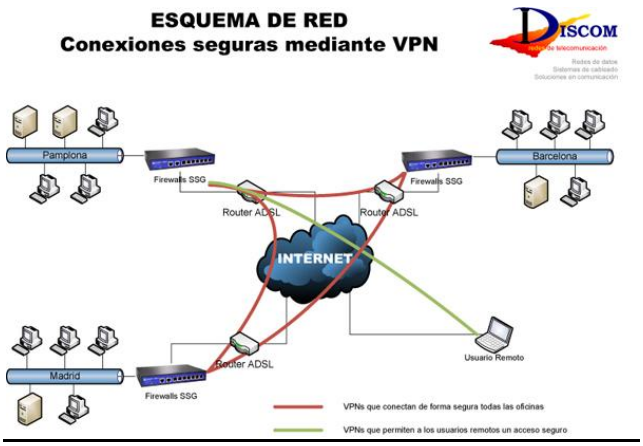
1. Mantener las medidas de seguridad existentes.
2. Minimizar el impacto en el propio sistema a estudiar.
3. Minimizar el número de sistemas intermedios entre el sistema de monitorización y los sistemas críticos.

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 monitorizador?*. 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:

- **Frame Relay:** 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

Los servidores web y los navegadores web emplean el protocolo Secure Sockets Layer (SSL) para crear un canal con un **cifrado** único para las comunicaciones privadas a través de la Internet pública. Los certificados SSL constan de una **clave pública y una clave privada**. La clave pública se utiliza para cifrar la información y la privada para descifrarla. Cuando un navegador web visita un dominio protegido, se establece un nivel de cifrado según el tipo de certificado SSL, así como el navegador web cliente, el sistema operativo y las capacidades del servidor host. Por esta razón, los certificados SSL incluyen varios niveles de cifrado, como por ejemplo "hasta 256 bits".

Un cifrado potente, a 128 bits, puede calcular 2^{88} veces más combinaciones que un cifrado de 40 bits. **Eso es más de un billón por un billón de veces más potente.** A la velocidad de los ordenadores actuales, un pirata con tiempo, herramientas y motivación para atacar utilizando la fuerza bruta necesitaría un billón de años para entrar en una sesión protegida por un certificado con SGC. Para que la mayoría de los visitantes del sitio puedan utilizar un cifrado potente, elija un certificado SSL que permita como mínimo un cifrado de 128 bits para el 99,9% de los visitantes del sitio web. Certificados SSL de 128 bits reales.

- Factor Humano.

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. Este 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.

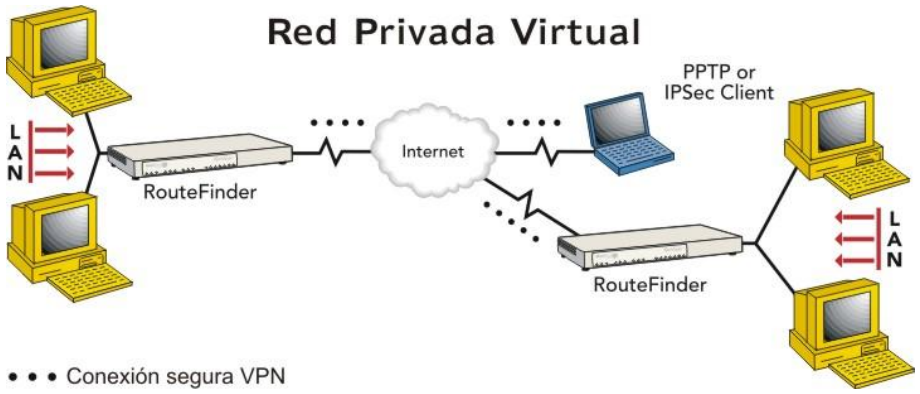
Concienciación

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.

4- 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 que debería una compañía gastar dinero y crear dolores de cabeza administrativos para implementar líneas dedicadas arrendadas y bancos de modems de marcado (dial-in). Por que no solamente usar Internet?

Bien, el primer reto es que tu 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 tunel 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:

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 local 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 tradicionales (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*.

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.

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

Conexión de acceso remoto

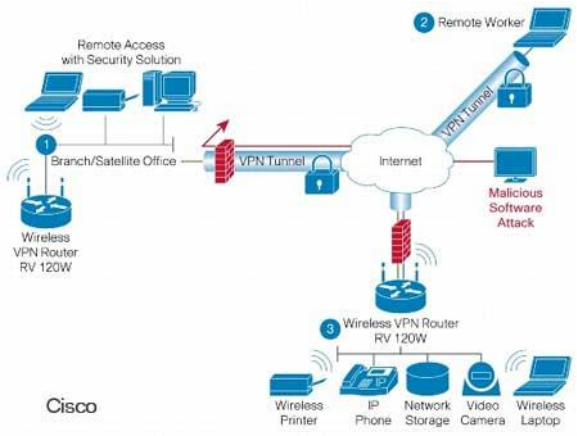
Una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante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



PPTP (Point to Point Tunneling Protocol), es un protocolo de comunicaciones desarrollado por Microsoft, U.S. Robotics, Ascend Communications, 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, Ascend Communications, 3com / Primary Access, ECI Telematics y US Robotics.

PPTP y VPN: El protocolo Point-To-Point Tunneling Protocol viene incluido 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 publica 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-switched telephone networks (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 ASLEAP puede 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 protocolos handshake LEAP 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 Frame Relay 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 (*Remote Authentication Dial-In User Service*). 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, Frame Relay 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 del 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.

5- Técnicas de cifrado. Técnicas de cifrado. Clave pública y clave privada:

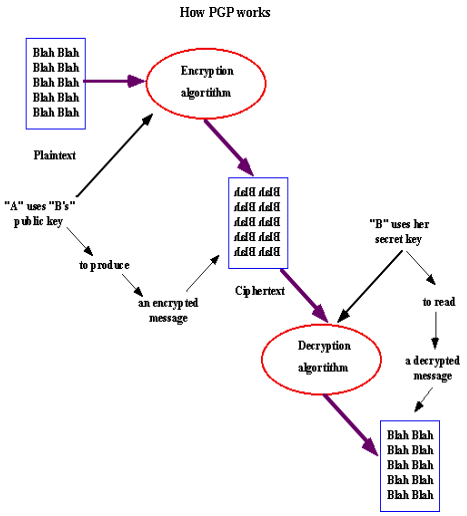
- Pretty Good Privacy (PGP). GNU Privacy Good (GPG).

Pretty Good Privacy 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

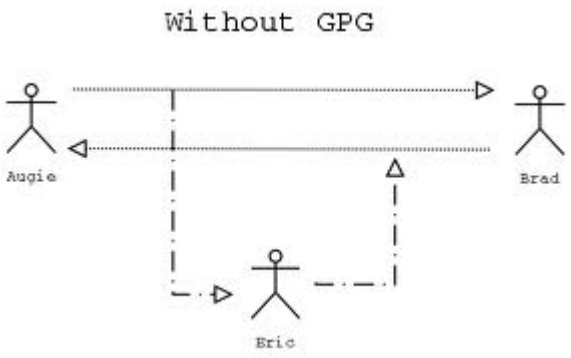
La PGP ofrece las siguientes funciones:

- **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.

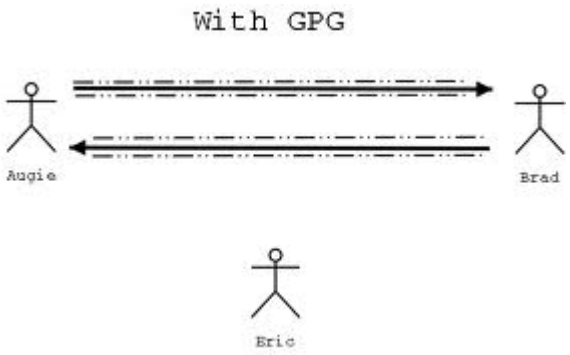
Revocación, desactivación y registro de claves: función que permite producir certificados de revocación.

GNU Privacy Good (GPG).

GNU Privacy Guard o **GPG** es una herramienta de cifrado y firmas digitales, que viene a ser un reemplazo del PGP (*Pretty Good Privacy*) 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 (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.

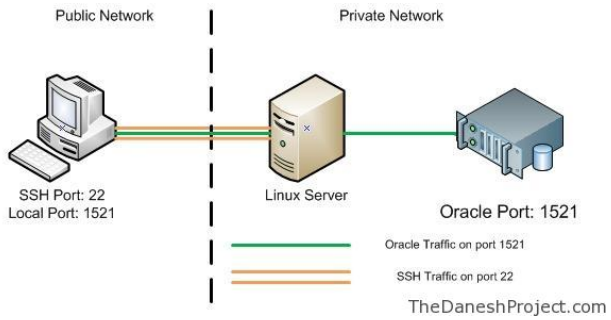
Para su uso se requiere que por parte del servidor exista un demonio que mantenga continuamente en el puerto 22 el servicio de comunicación segura, el **sshd**.

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 publica 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).

IPsec (abreviatura de **Internet Protocol security**) 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.

Los protocolos de **IPsec** actúan en la capa de red, la capa 3 del modelo OSI. Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS y SSH operan de la capa de transporte (capas OSI 4 a 7) hacia arriba. Esto hace que IPsec sea más flexible, ya que puede ser utilizado para proteger protocolos de la capa 4, incluyendo TCP y UDP, los protocolos de capa de transporte más usados. Una ventaja importante de IPsec frente a SSL y otros métodos que operan en capas superiores, es que para que una aplicación pueda usar IPsec no hay que hacer ningún cambio, mientras que para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código.

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.

Como el Protocolo de Internet no provee intrínsecamente de ninguna capacidad de seguridad, IPsec se introdujo para proporcionar servicios de seguridad tales como:

1. Cifrar el tráfico (de forma que no pueda ser leído por nadie más que las partes a las que está dirigido)
2. Validación de integridad (asegurar que el tráfico no ha sido modificado a lo largo de su trayecto)

3. Autenticar a los extremos (asegurar que el tráfico proviene de un extremo de confianza)
4. Anti-repetición (proteger contra la repetición de la sesión segura).

Modos

Así pues y dependiendo del nivel sobre el que se actúe, podemos establecer dos modos básicos de operación de **IPsec**: **modo transporte** y **modo túnel**.

Modo transporte

En **modo transporte**, sólo la carga útil (los datos que se transfieren) del paquete IP es cifrada o autenticada. El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas, ya que eso invalidaría el hash. Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas de ninguna manera (por ejemplo traduciendo los números de puerto TCP y UDP). El **modo transporte** se utiliza para comunicaciones ordenador a ordenador.

Una forma de encapsular mensajes IPsec para atravesar NAT ha sido definido por RFCs que describen el mecanismo de NAT transversal.

Modo túnel

En el **modo túnel**, todo el paquete IP (datos más cabeceras del mensaje) es cifrado o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El **modo túnel** se utiliza para comunicaciones red a red (túneles seguros entre routers, p.e. para VPNs) o comunicaciones ordenador a red u ordenador a ordenador sobre Internet.

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

Secure Sockets Layer (***SSL***; en español «capa de conexión segura») y su sucesor ***Transport Layer Security*** (***TLS***; en español «seguridad de la capa de transporte») son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.

SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.

SSL implica una serie de fases básicas:

- Negociar entre las partes el algoritmo que se usará en la comunicación
- Intercambio de claves públicas y autenticación basada en certificados digitales
- Cifrado del tráfico basado en cifrado simétrico

Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar. Las implementaciones actuales proporcionan las siguientes opciones:

- Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza;
- Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES y AES (Advanced Encryption Standard);
- Con funciones hash: MD5 o de la familia SHA.

Funcionamiento

El protocolo SSL intercambia registros; opcionalmente, cada registro puede ser comprimido, cifrado y empaquetado con un código de autenticación del mensaje (MAC). Cada registro tiene un campo de *content_type* que especifica el protocolo de nivel superior que se está usando.

Cuando se inicia la conexión, el nivel de registro encapsula otro protocolo, el protocolo *handshake*, que tiene el *content_type* 22.

El cliente envía y recibe varias estructuras *handshake*:

- Envía un mensaje *ClientHello* especificando una lista de conjunto de cifrados, métodos de compresión y la versión del protocolo SSL más alta permitida. Éste también envía bytes aleatorios que serán usados más tarde (llamados *Challenge de Cliente* o *Reto*). Además puede incluir el identificador de la sesión.

- Después, recibe un registro *ServerHello*, en el que el servidor elige los parámetros de conexión a partir de las opciones ofertadas con anterioridad por el cliente.

- Cuando los parámetros de la conexión son conocidos, cliente y servidor intercambian certificados (dependiendo de las claves públicas de cifrado seleccionadas). Estos certificados son actualmente X.509, pero hay también un borrador especificando el uso de certificados basados en OpenPGP.

- El servidor puede requerir un certificado al cliente, para que la conexión sea mutuamente autenticada.

- Cliente y servidor negocian una clave secreta (simétrica) común llamada *master secret*, posiblemente usando el resultado de un intercambio Diffie-Hellman, o

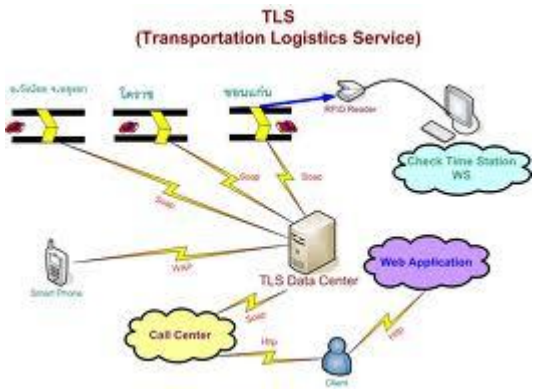
simplemente cifrando una clave secreta con una clave pública que es descifrada con la clave privada de cada uno. Todos los datos de claves restantes son derivados a partir de este *master secret* (y los valores aleatorios generados en el cliente y el servidor), que son pasados a través una *función pseudoaleatoria* cuidadosamente elegida.

TLS/SSL poseen una variedad de medidas de seguridad:

- Numerando todos los registros y usando el número de secuencia en el MAC.
- Usando un resumen de mensaje mejorado con una clave (de forma que solo con dicha clave se pueda comprobar el MAC). Esto se especifica en el RFC 2104).
- Protección contra varios ataques conocidos (incluyendo ataques man-in-the-middle), como los que implican un degradado del protocolo a versiones previas (por tanto, menos seguras), o conjuntos de cifrados más débiles.
- El mensaje que finaliza el protocolo *handshake* (*Finished*) envía un *hash* de todos los datos intercambiados y vistos por ambas partes.
- La función pseudo aleatoria divide los datos de entrada en 2 mitades y las procesa con algoritmos hash diferentes (MD5 y SHA), después realiza sobre ellos una operación XOR. De esta forma se protege a sí mismo de la eventualidad de que alguno de estos algoritmos se revelen vulnerables en el futuro.

-TLS "Transport Layer Security”

El protocolo TLS (*Transport Layer Security*) es una evolución del protocolo SSL (*Secure Sockets Layer*), es un protocolo mediante el cual se establece una conexión segura por medio de un canal cifrado entre el cliente y servidor. Así el intercambio de información se realiza en un entorno seguro y libre de ataques. La última propuesta de estándar está documentada en la referencia RFC 2246.



Normalmente el servidor es el único que es autenticado, garantizando así su identidad, pero el cliente se mantiene sin autenticar, ya que para la autenticación mútua se necesita una infraestructura de claves públicas (o PKI) para los clientes.

Estos protocolos permiten prevenir escuchas (eavesdropping), evitar la falsificación de la identidad del remitente y mantener la integridad del mensaje en una aplicación cliente-servidor.

DESCRIPCIÓN DEL PROTOCOLO

El protocolo SSL/TSL se basa en tres fases básicas:

- **Negociación**: Los dos extremos de la comunicación (cliente y servidor) negocian que algoritmos criptográficos utilizarán para autenticarse y cifrar la información. Actualmente existen diferentes opciones:
- Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm).
- Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard).
- Con funciones hash: MD5 o de la familia SHA.
- **Autenticación y Claves**: Los extremos se autentican mediante certificados digitales e intercambian las claves para el cifrado, según lanegociación.
- **Transmisión Segura**: los extremos pueden iniciar el tráfico de información cifrada y autentica.

OBJETIVOS DEL PROTOCOLO TLS

Los objetivos del protocolo son varios:

- **Seguridad criptográfica**. El protocolo se debe emplear para establecer una conexión segura entre dos partes.
- **Interoperabilidad.** Aplicaciones distintas deben poder intercambiar parámetros criptográficos sin necesidad de que ninguna de las dos conozca el código de la otra.
- **Extensibilidad.** El protocolo permite la incorporación de nuevos algoritmos criptográficos.
- **Eficiencia**. Los algoritmos criptográficos son costosos computacionalmente, por lo que el protocolo incluye un esquema de *cache de sesiones*para reducir el número de sesiones que deben inicializarse desde cero (usando criptografía de clave pública).

FUNCIONAMIENTO DEL PROTOCOLO TLS

El protocolo está dividido en dos niveles:

- **Protocolo de registro TLS** (*TLS Record Protocol*).
- **Protocolo de mutuo acuerdo TLS** (*TLS Handshake Protocol*).

El de más bajo nivel es el ***Protocolo de Registro***, que se implementa sobre un protocolo de transporte fiable como el TCP. El protocolo proporcionaseguridad en la conexión con dos propiedades fundamentales:

- **La conexión es privada**. Para encriptar los datos se usan algoritmos de cifrado simétrico. Las claves se generan para cada conexión y se basan en un secreto

negociado por otro protocolo (como el de mutuo acuerdo). El protocolo también se puede usar sin encriptación.

- **La conexión es fiable**. El transporte de mensajes incluye una verificación de integridad.

El ***Protocolo de mutuo acuerdo,*** proporciona seguridad en la conexión con tres propiedades básicas:

- La identidad del interlocutor puede ser autentificada usando criptografía de clave pública. Esta autentificación puede ser opcional, pero generalmente es necesaria al menos para uno de los interlocutores.
- La negociación de un secreto compartido es segura.
- La negociación es fiable, nadie puede modificar la negociación sin ser detectado por los interlocutores.

6- Servidores de acceso remoto:

- Protocolos de autenticación.

- EAP.
- MS-CHAP.
- MS-CHAP versión 2.
- CHAP.
- SPAP.
- PAP.
- Acceso sin autenticar.

EAP.

Al utilizar el Protocolo de autenticación extensible (EAP, *Extensible Authentication Protocol*), un mecanismo de autenticación arbitrario valida las conexiones de acceso remoto. El cliente de acceso remoto y el autenticador (el servidor de acceso remoto o el servidor del Servicio de autenticación de Internet (IAS, *Internet Authentication Service*)) negocian el esquema de autenticación exacto que se va a utilizar. Puede utilizar EAP a fin de aceptar esquemas de autenticación como Generic Token Card, MD5-Challenge, Seguridad en el nivel de transporte (TLS, *Transport Level Security*) para admitir tarjetas inteligentes y S/Key, así como cualquier tecnología de autenticación futura.

EAP permite que se establezcan conversaciones abiertas entre el cliente de acceso remoto y el autenticador. Esta conversación se compone de las solicitudes de información de autenticación realizadas por el autenticador y las respuestas del cliente de acceso remoto. Por ejemplo, si se utiliza EAP con tarjetas testigos de seguridad, el autenticador puede consultar al cliente de acceso remoto el nombre, el PIN y el valor del testigo de la tarjeta por separado. Con cada consulta realizada y respondida, el cliente de acceso remoto atraviesa otro nivel de autenticación. Una vez que se ha

respondido correctamente a todas las preguntas, se autentica al cliente de acceso remoto.

Los esquemas de autenticación específicos de EAP se denominan tipos de EAP. El cliente de acceso remoto y el autenticador deben admitir el mismo tipo de EAP para que la autenticación se lleve a cabo correctamente.

Infraestructura EAP

El protocolo EAP de Windows 2000 está formado por un conjunto de componentes internos que proporcionan una arquitectura compatible con cualquier tipo de EAP en forma de módulo de complemento. Para que la autenticación se realice correctamente, el cliente de acceso remoto y el autenticador deben tener instalado el mismo módulo de autenticación EAP. Windows 2000 proporciona dos tipos de EAP: EAP-MD5 CHAP y EAP-TLS. También es posible instalar otros tipos de EAP adicionales. Los componentes del tipo de EAP deben estar instalados en todos los autenticadores y clientes de acceso remoto.

EAP-MD5 CHAP

El Protocolo de autenticación por desafío mutuo de síntesis de mensaje 5-EAP (EAP-MD5 CHAP, *EAP-Message Digest 5 Challenge Handshake Authentication Protocol*) es un tipo de EAP requerido que utiliza el mismo protocolo de desafío mutuo que CHAP basado en PPP, con la diferencia de que los desafíos y las respuestas se envían como mensajes EAP.

EAP-MD5 CHAP suele utilizarse para autenticar las credenciales de los clientes de acceso remoto mediante sistemas de seguridad que usan nombres de usuario y contraseñas. También puede utilizarse para probar la interoperabilidad de EAP.

EAP-TLS

El tipo de EAP Seguridad del nivel de transporte EAP (EAP-TLS, *EAP-Transport Level Security*) se utiliza en entornos de seguridad basados en certificados. Si está utilizando tarjetas inteligentes para la autenticación de acceso remoto, debe utilizar el método de autenticación EAP-TLS. El intercambio de mensajes EAP-TLS permite la autenticación y negociación mutua del método de cifrado y el intercambio seguro de claves cifradas entre el cliente de acceso remoto y el autenticador. EAP-TLS proporciona el método de intercambio de claves y autenticación más eficaz.

EAP-TLS sólo se admite en servidores de acceso remoto que ejecutan Windows 2000 y que son miembros de un dominio en modo mixto o modo nativo de Windows 2000. Los servidores de acceso remoto que ejecutan Windows 2000 de forma independiente no admiten EAP-TLS.

Para obtener más información acerca de cómo configurar las tarjetas inteligentes para clientes de acceso remoto, consulte Usar tarjetas inteligentes para el acceso remoto

EAP-RADIUS

EAP-RADIUS no es un tipo de EAP, sino el paso de *cualquier* tipo de EAP a un servidor RADIUS realizada por un autenticador de mensajes EAP para su autenticación. Por ejemplo, si se configura un servidor de acceso remoto para la autenticación RADIUS, los mensajes EAP enviados entre el cliente y el servidor de acceso remoto se encapsulan y formatean como mensajes RADIUS entre el servidor de acceso remoto y el servidor RADIUS.

EAP-RADIUS se utiliza en entornos en los que RADIUS se usa como proveedor de autenticación. La ventaja de utilizar EAP-RADIUS es que no es necesario instalar los tipos de EAP en todos los servidores de acceso remoto, sino sólo en el servidor RADIUS. En el caso de los servidores IAS, sólo debe instalar tipos de EAP en el servidor IAS.

Por lo general, al utilizar EAP-RADIUS, el servidor de acceso remoto Windows 2000 se configura para utilizar EAP y un servidor IAS para la autenticación. Cuando se establece una conexión, el cliente de acceso remoto negocia el uso de EAP con el servidor de acceso remoto. Si el cliente envía un mensaje EAP al servidor de acceso remoto, éste encapsula el mensaje EAP como un mensaje RADIUS y lo envía al servidor IAS configurado. El servidor IAS procesa el mensaje EAP y devuelve un mensaje EAP encapsulado como RADIUS al servidor de acceso remoto. A continuación, el servidor de acceso remoto reenvía el mensaje EAP al cliente de acceso remoto. En esta configuración, el servidor de acceso remoto sólo funciona como dispositivo de paso a través. Todo el procesamiento de los mensajes EAP se lleva a cabo en el cliente de acceso remoto y en el servidor IAS.

MS-CHAP

Windows 2000 incluye compatibilidad con el Protocolo de autenticación por desafío mutuo de Microsoft (MS-CHAP, *Microsoft Challenge Handshake Authentication Protocol*), también conocido comoMS-CHAP versión 1. MS-CHAP es un protocolo de autenticación de contraseñas de cifrado no reversible. El proceso de desafío mutuo funciona de la manera siguiente:

1. El autenticador (el servidor de acceso remoto o el servidor IAS) envía al cliente de acceso remoto un desafío formado por un identificador de sesión y una cadena de desafío arbitraria.
2. El cliente de acceso remoto envía una respuesta que contiene el nombre de usuario y un cifrado no reversible de la cadena de desafío, el identificador de sesión y la contraseña.
3. El autenticador comprueba la respuesta y, si es válida, se autentican las credenciales del usuario.

Si utiliza MS-CHAP como protocolo de autenticación, puede utilizar el Cifrado punto a punto de Microsoft (MPPE, *Microsoft Point-to-Point Encryption*) para cifrar los datos enviados por la conexión PPP o PPTP.

MS-CHAP versión 2

Windows 2000 incluye compatibilidad con la versión 2 del Protocolo de autenticación por desafío mutuo de Microsoft (MS-CHAP v2, *Microsoft Challenge Handshake Authentication Protocol*), que proporciona seguridad de alto nivel para las conexiones de acceso remoto. MS-CHAP v2 resuelve algunos problemas de MS-CHAP versión 1, como se muestra en la siguiente tabla.

MS-CHAP v2 es un proceso unidireccional con contraseña cifrada y autenticación mutua que funciona de la manera siguiente:

1. El autenticador (el servidor de acceso remoto o el servidor IAS) envía un desafío al cliente de acceso remoto que consta de un identificador de sesión y una cadena de desafío arbitraria.

2. El cliente de acceso remoto envía una respuesta que contiene:

   - El nombre del usuario.
   - Una cadena de desafío arbitraria del mismo nivel.
   - Una codificación unidireccional de la cadena de desafío recibida, la cadena de desafío del mismo nivel, el identificador de sesión y la contraseña del usuario.

3. El autenticador comprueba la respuesta del cliente y devuelve una respuesta que contiene:

   - Una indicación del éxito o fracaso del intento de conexión.
   - Una respuesta autenticada basada en la cadena de desafío enviada, la cadena de desafío del mismo nivel, la respuesta codificada del cliente y la contraseña del usuario.

4. El cliente de acceso remoto comprueba la respuesta de autenticación y, si es correcta, utiliza la conexión. Si la respuesta de autenticación no es correcta, el cliente de acceso remoto termina la conexión.

CHAP

El Protocolo de autenticación por desafío mutuo (CHAP, *Challenge Handshake Authentication Protocol*) es un protocolo de autenticación mediante desafío y respuesta que utiliza Síntesis del mensaje 5 (MD5,*Message Digest 5*), un esquema de hash estándar del sector, para cifrar la respuesta. Varios fabricantes de clientes y

servidores de acceso a la red emplean el protocolo CHAP. Los servidores de acceso remoto que ejecutan Windows 2000 admiten CHAP a fin de poder autenticar a clientes de acceso remoto que no son de Microsoft.

SPAP

El Protocolo de autenticación de contraseñas de Shiva (SPAP, *Shiva Password Authentication Protocol*) es un mecanismo de cifrado reversible empleado por Shiva. Al conectarse a un equipo Shiva LAN Rover, los equipos que ejecutan Windows 2000 Professional utilizan SPAP, el mismo protocolo que emplea el cliente Shiva que conecta con el servidor de acceso remoto de Windows 2000. Esta forma de autenticación es más segura que el texto simple pero menos segura que CHAP o MS-CHAP.

PAP

El Protocolo de autenticación de contraseña (PAP, *Password Authentication Protocol*) utiliza contraseñas en texto simple y es el protocolo de autenticación menos sofisticado. Se negocia, normalmente, si el cliente y el servidor de acceso remoto no pueden negociar una forma de validación más segura.

Acceso sin autenticar

Windows 2000 admite el acceso sin autenticar, lo que significa que la persona que llama no requiere las credenciales del usuario (un nombre de usuario y una contraseña). Hay algunas situaciones en las que es aconsejable utilizar el acceso sin autenticar. Esta sección trata:

- Autorización DNIS
- Autenticación ANI/CLI
- Autenticación de invitados

- 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.

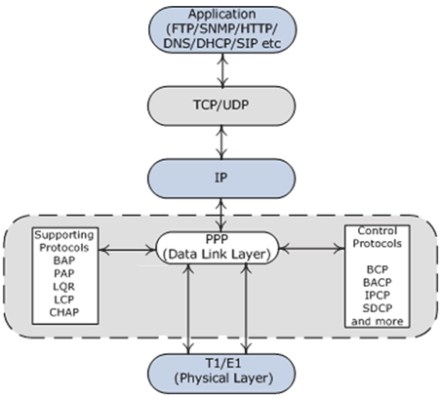
El protocolo PPP permite establecer una comunicación a nivel de la capa de enlace TCP/IP entre dos computadoras. Generalmente, se utiliza para establecer la conexión a Internet de un particular con su proveedor de acceso a través de un módem telefónico. Ocasionalmente también es utilizado sobre conexiones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

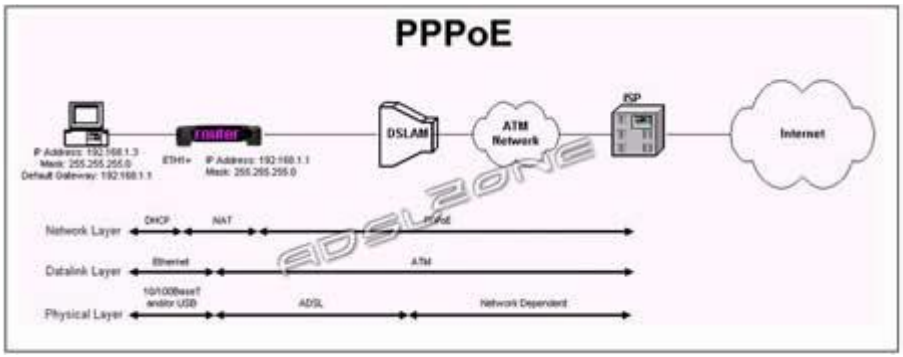
También se ha venido utilizando para conectar a trabajadores desplazados (p. ej. ordenador portátil) con sus oficinas a través de un centro de acceso remoto de su empresa. Aunque está aplicación se está abandonando en favor de las redes privadas virtuales, más seguras.



PPOE:

PPPoE (Point-to-Point Protocol over 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.

Significa "Protocolo de Punto a Punto sobre Ethernet", e implementa una capa IP sobre dos puertos Ethernet, dando la posibilidad de transferir paquetes de datos entre los dispositivos que estén conectados.



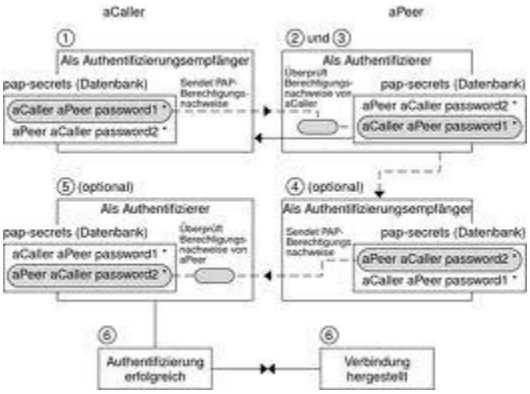
PPPoA

Igual que PPPoE pero, en vez de ser un protocolo sobre una capa Ethernet, se realiza sobre una capa ATM.

Gracias a este protocolos, las señales del router pueden negociar los parámetros de conexión o de red entre el router y el ISP, con lo que sólo necesitas saber tu Identificador de Usuario y tu clave de acceso para poder comenzar a navegar, puesto que el resto de datos se obtienen automáticamente en el momento en que se efectúa la conexión. Con PPPoE, el router efectúa el encaminamiento IP con Network Address Translation (NAT) para la LAN. El router que cuente con PPPoE también es compatible con la asignación dinámica de direcciones IP a nodos de red local. Cuando se use la asignación dinámica, el router actuará como servidor DHCP.

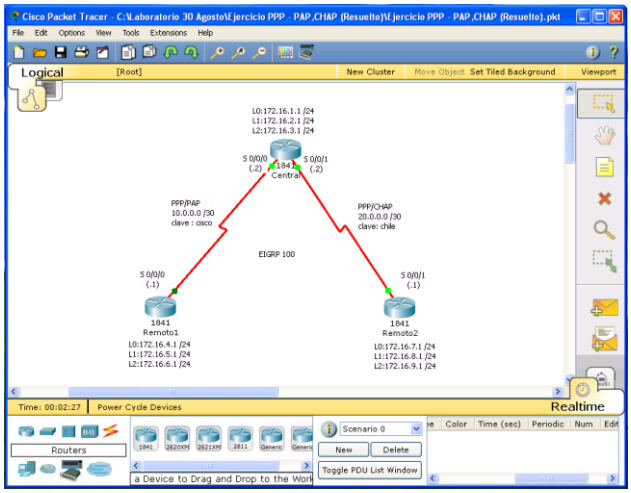
- Autenticación de contraseña: PAP

El Protocolo de autenticación de contraseña (PAP, Password Authentication Protocol) 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, Challenge Handshake Authentication Protocol) 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.



- Autenticación extensible: EAP. Métodos.

Extensible AuthenticationProtocol (EAP) es una autenticaciónframework usada habitualmente en redes WLANPoint-to-Point Protocol. Aunque el protocolo EAP no está limitado a LANinalámbricas y puede ser usado para autenticación en redes cableadas, es más frecuentemente su uso en las primeras. Recientemente los estándares WPA y WPA2 han adoptado cinco tipos de EAP como sus mecanismos oficiales de autenticación.

Es una estructura de soporte, no un mecanismo específico de autenticación. Provee algunas funciones comunes y negociaciones para el o los mecanismos de autenticación

escogidos. Estos mecanismos son llamados métodos EAP, de los cuales se conocen actualmente unos 40. Además de algunos específicos de proveedores comerciales, los definidos por RFC de la IETF incluyen EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, y EAP-AKA.

Los métodos modernos capaces de operar en ambientes inalámbricos incluyen EAP-TLS, EAP-SIM, EAP-AKA, PEAP, LEAP y EAP-TTLS. Los requerimientos para métodos EAP usados en LAN inalámbricas son descritos en la RFC 4017. Cuando EAP es invocada por un dispositivo NAS (Network Access Server) capacitado para 802.1X, como por ejemplo un punto de acceso 802.11 a/b/g, los métodos modernos de EAP proveen un mecanismo seguro de autenticación y negocian un PMK (Pair-wise Master Key) entre el dispositivo cliente y el NAS. En esas circunstancias, la PMK puede ser usada para abrir una sesión inalámbrica cifrada que usa cifrado TKIP o AES.

EAP fue diseñado para utilizarse en la autenticación para acceso a la red, donde la conectividad de la capa IP puede no encontrase disponible. Dado a que EAP no requiere conectividad IP, solamente provee el suficiente soporte para el transporte confiable de protocolos de autenticación y nada más.

EAP es un protocolo lock-step, el cual solamente soporta un solo paquete en transmisión. Como resultado, EAP no pude transportar eficientemente datos robustos, a diferencia de protocolos de capas superiores como TCP.

Aunque EAP provee soporte para retransmisión, este asume que el ordenamiento de paquetes es brindado por las capas inferiores, por lo cual el control de orden de recepción de tramas no está soportado. Ya que no soporta fragmentación y re-ensamblaje, los métodos de autenticación de basados en EAP que generan tramas más grandes que el soportado por defecto por EAP, deben aplicar mecanismos especiales para poder soportar la fragmentación (Por ejemplo EAP-TLS). Como resultado, puede ser necesario para un algoritmo de autenticación agregar mensajes adicionales para poder correr sobre EAP. Cuando se utiliza autentificación a base de certificados, el certificado es más grande que el MTU de EAP, por lo que el número de round-trips (viaje redondo de paquetes) entre cliente y servidor puede aumentar debido a la necesidad de fragmentar dicho certificado.

Se debe considerar que cuando EAP corre sobre una conexión entre cliente y servidor donde se experimenta una significante pérdida de paquetes, los métodos EAP requerirán muchos round-trips y se reflejará en dificultades de conexión.

Proceso de Intercambio de Autenticación EAP

1.- El Servidor de Autenticación envía un Request (Solicitud) de Autenticación al cliente, el mensaje de Request tiene un campo de Tipo, en el cual el cliente debe responder que es lo que está solicitando, los tipos existentes son: Identidad, Notificación, Nak, MD5-Challenge, One-Time Password (OTP), GenericToken-Card (GTC), Tipos Expandidos y Experimental.

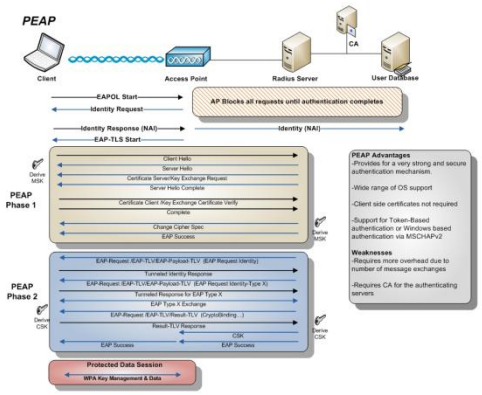
2.- El Cliente envía un paquete Response (Respuesta) al Servidor. Al igual que en el paquete Request, el paquete Response contiene un campo de Tipo, el cual corresponde al campo de Tipo en el paquete de Request.

3.- El Servidor de autenticación envía un paquete Request adicional, al cual el cliente envía un Response. La secuencia de Request y Response continua según sea necesario. Como se mencionó, EAP es un protocolo lock-step, por lo que no se puede enviar el siguiente paquete sin haber recibido uno válido antes. El servidor es responsable de transmitir las solicitudes de retrasmisión, dichos métodos se describen en el RFC de EAP, el RFC 3748. Después de un número de retransmisiones, el Servidor PUEDE terminar la conversación EAP. El Servidor NO PUEDE enviar un paquete de Success o Failure cuando se retransmite o cuando falla en recibir una respuesta a dichos paquetes por parte del cliente.

4.-La conversación continúa hasta que el Servidor no puede autenticar al cliente, y en dicho caso el Servidor DEBE trasmitir un mensaje de Failure. Como alternativa, la conversación de autenticación puede continuar hasta que el Servidor determina que se ha cumplido con una autenticación satisfactoriamente, para dicho caso, el Servidor DEBE enviar un paquete de Success.

- 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

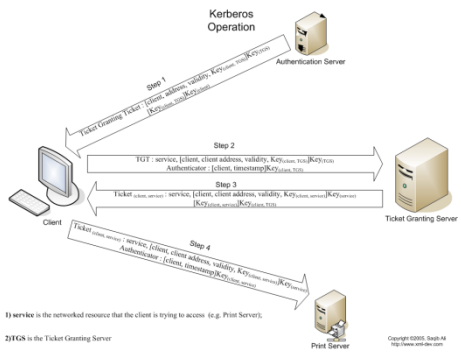
PEAP) con el fin de evitar que cada servidor RADIUS pida las credenciales. Si no se puede configurar el punto de acceso para que prefiera un servidor RADIUS, puede configurar un proxy RADIUS de IAS con un servidor RADIUS preferido.

- 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

- 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

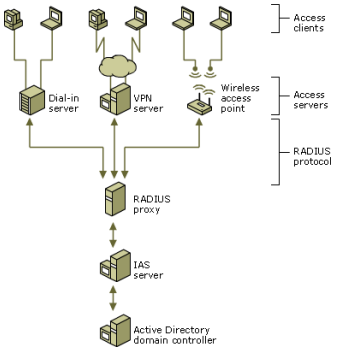
Autorización se refiere a la concesión de privilegios específicos (incluyendo "ninguno") a una entidad o usuario basándose en su identidad (autenticada), los privilegios que solicita, y el estado actual del sistema. Las autorizaciones pueden también estar basadas en restricciones, tales como restricciones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

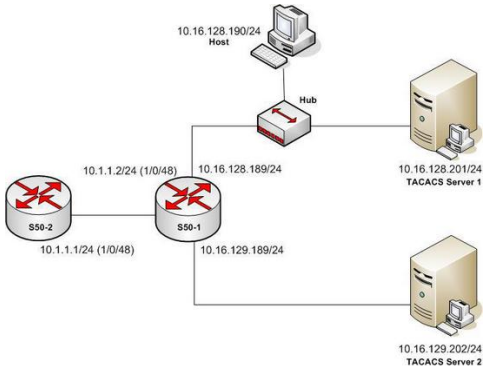


Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.

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 domnio** que engloba a todos los equipos que le pertenecen.

Controlar el número máximo de conexiones

Es impotante para prevenir ataques de DoS

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

Controlar el tiempo de conexión

- Contolar 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

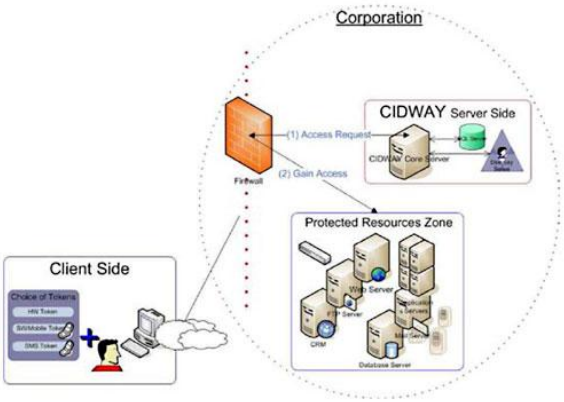
Combinación de sitio anónimo y no anónimo

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. En una aplicación sencilla, el servidor de autenticación sólo puede almacenar una lista de nombres de usuario válido y la contraseña correspondiente, y autenticar todos los usuarios que intentan conectarse a la red de acuerdo a esta lista.

Kerberos es otro tipo de protocolo de autenticación utilizado en muchos sistemas de Windows Server ® de autenticación, por ejemplo, y en algunos de seguridad en línea o sistemas de seguridad de Internet. Hay tres aspectos principales para la autenticación Kerberos: la autenticación de la identidad del usuario, el envasado seguro del nombre del usuario, y la transmisión segura de las credenciales del usuario en la red.

Servidores de autenticación Kerberos en los sistemas operativos Windows ® están disponibles para Windows ® XP, Windows 2000 ®, Windows 2003 ® y sistemas operativos.

Un servidor proxy es un servidor o un equipo que intercepta las peticiones y de una red interna y una red externa, como la Internet. Los servidores proxy a veces actúan como servidores de autenticación, además de un número de otras funciones que pueden cumplir. Hay muchas opciones diferentes que pueden ser utilizados para implementar los servidores de autenticación, incluyendo hardware, sistema operativo, y los requisitos de paquete de software. Como tal, suele ser importante para una organización a analizar a fondo los requisitos de seguridad antes de implementar un servidor de autenticación en el entorno de red.

BIBLIOGRAFÍA

http://www-gris.det.uvigo.es/wiki/pub/Main/PaginaNST/SEC_III_NST.pdf
http://www.inteco.es/Seguridad/Observatorio/Articulos/UD_Cortafuegos
http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos
www.it.uc3m.es/~lmiguel/ids2.pdf
http://technet.microsoft.com/es-es/library/cc757996%28WS.10%29.aspx
http://es.kioskea.net/contents/protect/dmz-cloisonnement.php3
http://seguinfo.wordpress.com/2010/01/07/zonas-desmilitarizadas-y-sistemas-de-control/
http://www.solusan.com/que-es-una-dmz.html
http://es.wikipedia.org/wiki/Protocolo_AAA
http://es.wikipedia.org/wiki/TACACS%2B
http://www.verisign.es/ssl/ssl-information-center/how-ssl-security-works/index.html
http://technet.microsoft.com/es-es/library/cc759573.aspx
http://es.tech-faq.com/tls-transport-layer-security.shtml
http://www.wikilearning.com/articulo/protocolos_seguros_para_el_web
http://leibniz.iimas.unam.mx/~yann/Crypto/Clase08.pdf
http://foro.code-makers.es
http://es.wikipedia.org/wiki/Transport_Layer_Security
http://www.stunnel.org
http://www.ekontsulta.net/ekontsulta/wiki/index.php/VPN#Ventajas_y_desventajas
http://www.angelfire.com/stars4/alemzamayoa/presentacion.htm
http://lular.es/a/Internet/2010/08/Que-es-un-servidor-de-autenticacion.html