UD3: Implantación de técnicas de acceso remoto. Seguridad perimetral

INDICE UD3

-Implantación de técnicas de acceso remoto. Seguridad perimetral

•Elementos básicos de la seguridad perimetral:

- Concepto de seguridad perimetral.

- Objetivos de la seguridad perimetral.

- Perímetro de la red:

-Routers frontera.

- Cortafuegos (firewalls).

- Sistemas de Detección de Intrusos.

- Redes Privadas Virtuales.

- Software y servicios. Host Bastion.

- Zonas desmilitarizadas (DMZ) y subredes controladas.

•Arquitecturas de cortafuegos:

- Cortafuego de filtrado de paquetes.

- Cortafuego Dual-Homed Host.

- Screened Host.

- Screened Subnet (DMZ).

- Otras arquitecturas

•Políticas de defensa en profundidad:

- Defensa perimetral.

Interacción entre zona perimetral (DMZ) y zona externa.

Monitorización del perímetro: detección y prevención de intrusos

- Defensa interna.

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

Routers y cortafuegos internos

Monitorización interna

Conectividad externa (Enlaces dedicados y redes VPN)

Cifrados a nivel host

- Factor Humano.

•Redes privadas virtuales. VPN.

- Beneficios y desventajas con respecto a las líneas

dedicadas.

- Tipos de conexión VPN:

VPN de acceso remoto,

VPN sitio a sitio (tunneling)

VPN sobre LAN.

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

•Técnicas de cifrado. Clave pública y clave privada:

- Pretty Good Privacy (PGP). GNU Privacy Good

(GPG).

- Seguridad a nivel de aplicación: SSH ("Secure

Shell").

- Seguridad en IP (IPSEC).

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

TLS ("Transport Layer Security")

•**Servidores de acceso remoto:**

- Protocolos de autenticación.

- Protocolos PPP, PPoE, PPPoA

- Autenticación de contraseña: PAP

- Autenticación por desafío mutuo: CHAP

- Autenticación extensible: EAP. Métodos.

- PEAP.

- Kerberos.

- Protocolos AAA:

•Radius

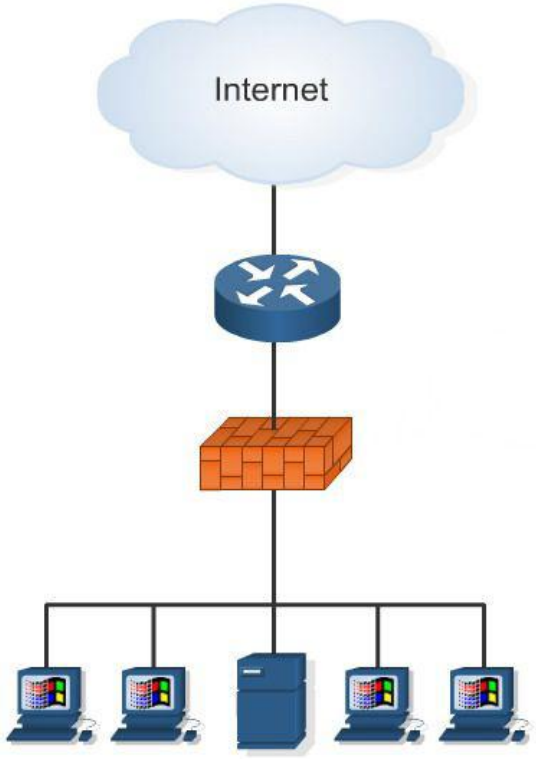
•TACACS+

- Configuración de parámetros de acceso.

- Servidores de autenticación.

1. 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.

2. Perímetro de la red:

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.

La seguridad perimetral:

- No es un componente aislado: es una estrategia para proteger los recursos de una organización conectada a la red
- Es la realización práctica de la política de seguridad de una organización. Sin una política de seguridad, la seguridad perimetral no sirve de nada
- Condiciona la credibilidad de una organización en Internet

Ejemplos de cometidos de la seguridad perimetral:

- Rechazar conexiones a servicios comprometidos
- Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico) o entre ciertos nodos.
- Proporcionar un único punto de interconexión con el exterior
- Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet
- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet
- Auditar el tráfico entre el exterior y el interior

- Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red, cuentas de usuarios internos...

¿Qué es un router de 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.

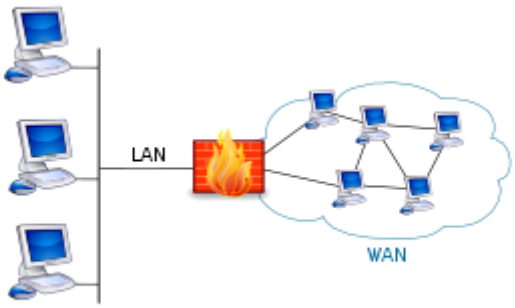
3. Cortafuegos (Firewall)

Un **cortafuegos** (***firewall*** en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al cortafuegos a una tercera red, llamada *Zona desmilitarizada* o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.



Tipos de cortafuegos

- **Nivel de aplicación de pasarela**

Aplica mecanismos de seguridad para aplicaciones específicas, tales como servidores FTP y Telnet. Esto es muy eficaz, pero puede imponer una degradación del rendimiento.

- **Circuito a nivel de pasarela**

Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Una vez que la conexión se ha hecho, los paquetes pueden fluir entre los anfitriones sin más control. Permite el establecimiento de una sesión que se origine desde una zona de mayor seguridad hacia una zona de menor seguridad.

- **Cortafuegos de capa de red o de filtrado de paquetes**

Funciona a nivel de red (capa 3 del modelo OSI, capa 2 del stack de protocolos TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (capa 3 TCP/IP, capa 4 Modelo OSI), como el puerto origen y destino, o a nivel de enlace de datos (no existe en TCP/IP, capa 2 Modelo OSI) como la dirección MAC.

- **Cortafuegos de capa de aplicación**

Trabaja en el nivel de aplicación (capa 7 del modelo OSI), de manera que los filtrados se pueden adaptar a características propias de los

protocolos de este nivel. Por ejemplo, si se trata de tráfico HTTP, se pueden realizar filtrados según la URL a la que se está intentando acceder.

Un cortafuegos a nivel 7 de tráfico HTTP suele denominarse proxy, y permite que los computadores de una organización entren a Internet de una forma controlada. Un proxy oculta de manera eficaz las verdaderas direcciones de red.

- **Cortafuegos personales**

Es un caso particular de cortafuegos que se instala como software en un computador, filtrando las comunicaciones entre dicho computador y el resto de la red. Se usa por tanto, a nivel personal.

Ventajas de un cortafuegos

Bloquea el acceso a personas no autorizadas a redes privadas.

Limitaciones de un cortafuegos

Las limitaciones se desprenden de la misma definición del cortafuegos: filtro de tráfico. Cualquier tipo de ataque informático que use tráfico aceptado por el cortafuegos (por usar puertos TCP abiertos expresamente, por ejemplo) o que sencillamente no use la red, seguirá constituyendo una amenaza. La siguiente lista muestra algunos de estos riesgos:

- Un cortafuegos no puede proteger contra aquellos ataques cuyo tráfico no pase a través de él.
- El cortafuegos no puede proteger de las amenazas a las que está sometido por ataques internos o usuarios negligentes. El cortafuegos no puede prohibir a espías corporativos copiar datos sensibles en medios físicos de almacenamiento (discos, memorias, etc.) y sustraerlas del edificio.
- El cortafuegos no puede proteger contra los ataques de ingeniería social.

3.1 Sistema de detección de intrusos

Un **sistema de detección de intrusos** (o **IDS** de sus siglas en inglés *Intrusion Detection System*) es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.

El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.

Funcionamiento

El funcionamiento de estas herramientas se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. El IDS no sólo analiza qué tipo de tráfico es, sino que también revisa el contenido y su comportamiento.

Normalmente esta herramienta se integra con un firewall. El detector de intrusos es incapaz de detener los ataques por sí solo, excepto los que trabajan conjuntamente en un dispositivo de puerta de enlace con funcionalidad de firewall, convirtiéndose en una herramienta muy poderosa ya que se une la inteligencia del IDS y el poder de bloqueo del firewall, al ser el punto donde forzosamente deben pasar los paquetes y pueden ser bloqueados antes de penetrar en la red.

4. El concepto de las redes privadas virtuales

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

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

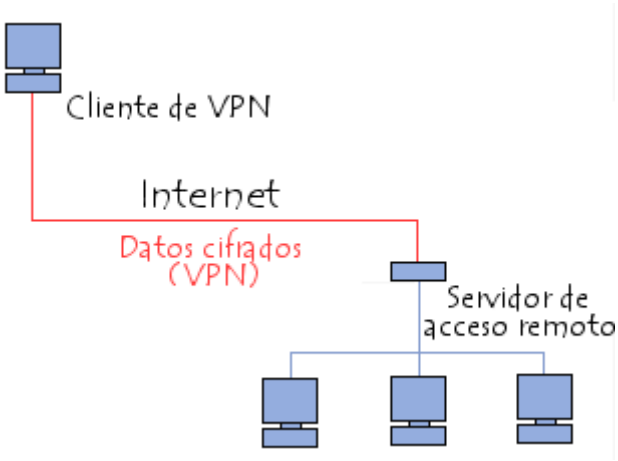
La primera solución para satisfacer esta necesidad de comunicación segura implica conectar redes remotas mediante líneas dedicadas. Sin embargo, como la mayoría de las compañías no pueden conectar dos redes de área local remotas con una línea dedicada, a veces es necesario usar Internet como medio de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

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

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

Funcionamiento de una VPN

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



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

4.1 Software y servicios. Host Bastion.

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

Definición

Históricamente, se le llamaba Bastiones a las altas partes fortificadas de los castillos medievales; puntos que cubrían áreas críticas de defensa en caso de invasión, usualmente teniendo murallas muy fortificadas, salas para alojar tropas, y armas de ataque a corta distancia como ollas de aceite hirviendo para alejar a los invasores cuando ya están por penetrar al castillo.

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-level gateways) 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.

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

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

Tipos de bastion host

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

Single-homed bastión host

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

Dual-homed bastión host

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

Multihomed bastión host

Un Bastión host interno puede ser clasificado como multihomed. Cuando la política de seguridad requiere que todo tráfico entrante y salida sea enviado a través de un servidor proxy, un nuevo servidor proxy debería ser creado para la nueva aplicación streaming.

Aplicaciones

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

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

A continuación se expone un ejemplo de una red donde se utilizan dos bastiones host, como se observa se forma una capa adicional de seguridad entre el internet y la red interna.

5- Zonas desmilitarizadas (DMZ) y subredes controladas.

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

-**Zona desmilitarizada:** Situada delante del cortafuegos, tras el router frontera.

-**Red controlada:** Situada tras el cortafuegos

¿Que es una DMZ?

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

El objetivo de una DMZ es que las conexiones **desde** la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones **desde** la DMZ sólo se permitan a la red externa, es decir: los equipos locales (hosts) en la DMZ no pueden conectar con la red interna.

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

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

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

Habitualmente una configuración DMZ es usar dos cortafuegos, donde la DMZ se sitúa en medio y se conecta a ambos cortafuegos, uno conectado a la red interna y el otro a la red externa. Esta configuración ayuda a prevenir configuraciones erróneas accidentales que permitan el acceso desde la red externa a la interna.

Arquitectura DMZ

Cuando algunas máquinas de la red interna deben ser accesibles desde una red externa (servidores web,servidores de correo electrónico, servidores FTP), a veces es necesario crear una nueva interfaz hacia una red separada a la que se pueda acceder tanto desde la red interna como por vía externa sin correr el riesgo de comprometer la seguridad de la compañía. El término "**zona desmilitarizada**" o **DMZ** hace referencia a esta zona aislada que posee aplicaciones disponibles para el público. La DMZ actúa como una "zona de búfer" entre la red que necesita protección y la red hostil.

Los servidores en la DMZ se denominan "**anfitriones bastión**" ya que actúan como un puesto de avanzada en la red de la compañía.

Por lo general, la política de seguridad para la DMZ es la siguiente:

- El tráfico de la red externa a la DMZ está **autorizado**
- El tráfico de la red externa a la red interna está **prohibido**
- El tráfico de la red interna a la DMZ está **autorizado**
- El tráfico de la red interna a la red externa está **autorizado**
- El tráfico de la DMZ a la red interna está **prohibido**
- El tráfico de la DMZ a la red externa está **denegado**

De esta manera, la DMZ posee un nivel de seguridad intermedio, el cual no es lo suficientemente alto para almacenar datos imprescindibles de la compañía.

Debe observarse que es posible instalar las DMZ en forma interna para aislar la red interna con niveles de protección variados y así evitar intrusiones internas.

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.

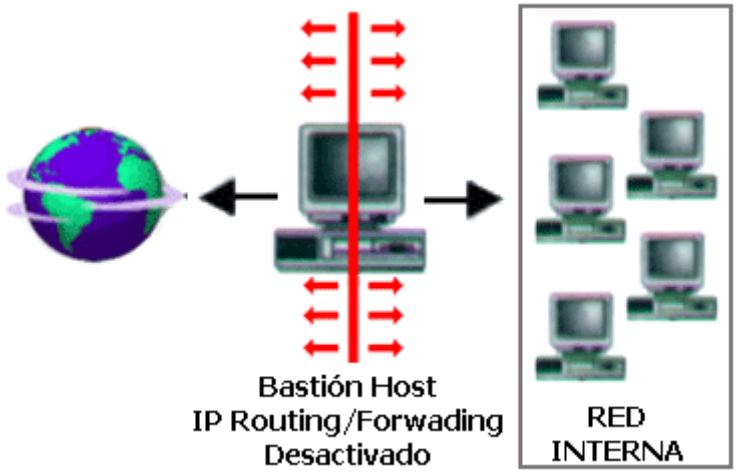
Esta arquitectura es la más simple de implementar y la más utilizada en organizaciones que no precisan grandes niveles de seguridad, donde el *router* actúa como de*pasarela* de la subred y no hay necesidad de utilizar *proxies*, ya que los accesos desde la red interna al exterior no bloqueados son directos. 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.

6 . cortafuego 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.



6.1. screened Host

Combina un router con un host bastion, y donde el principal nivel de seguridad proviene del filtrado de paquetes (es decir, el router es la primera y mas importante línea de defensa). En la maquina bastion, único sistema accesible desde el exterior, se ejecutan los proxies de las aplicaciones, mientras que el choke se encarga de filtrar los paquetes que se puedan considerar peligrosos para la seguirdad de la red interna, permitiendo únicamente la comunicación con un reducido numero de servicios.

La mayoría de los autores recomiendan situar el router entre la red exterior y el host bastion, pero otros defienden justo lo contrario: situar el bastion en la red exterior no provoca aparentemente una degradación de la seguirdad, y además ayuda al administrador a comprender la necesidad de un elevado nivel de fiabilidad en esta maquina, ya que esta sujeta a ataques extern0os y no tiene por que ser un host fiable; de cualquier forma, la `no degradacion' de la seguridad mediante esta aproximación es mas discutible, ya que habitualmente es mas 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 mas 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; asi, cuando una maquina de la red interna desea comunicarse con el exterior existen dos posibilidades:

- El choke permite la salida de algunos servicios a todas o a parte de las maquinas internas a través de un simple filtrado de paquetes.
- El *choke* prohibe todo el tráfico entre máquinas de la red interna y el exterior, permitiendo sólo la salida de ciertos servicios que provienen de la máquina bastión y que han sido autorizados por la política de seguridad de la organización. Así, estamos obligando a los usuarios a que las conexiones con el exterior se realicen a través de los servidores *proxy* situados en el bastión.

-7 Screened Subnet (DMZ).

La arquitectura *Screened Subnet*, también conocida como red perimétrica o *De-Militarized Zone* (DMZ) es con diferencia la más utilizada e implantada hoy en día, ya que añade un nivel de seguridad en las arquitecturas de cortafuegos situando una subred (DMZ) entre las redes externa e interna, de forma que se consiguen reducir los efectos de un ataque exitoso al *host* bastión: como hemos venido comentando, en los modelos anteriores toda la seguridad se centraba en el bastión[16.1], de forma que si la seguridad del mismo se veía comprometida, la amenaza se extendía automáticamente al resto de la red. Como la máquina bastión es un objetivo interesante para muchos piratas, la arquitectura DMZ intenta aislarla en una red perimétrica de forma que un intruso que accede a esta máquina no consiga un acceso total a la subred protegida.

Screened subnet es la arquitectura más segura, pero también la más compleja; se utilizan dos *routers*, denominados exterior e interior, conectados ambos a la red perimétrica como se muestra en la figura 15.2. En esta red perimétrica, que constituye el sistema cortafuegos, se incluye el *host* bastión y también se podrían incluir sistemas que requieran un acceso controlado, como baterías de módems o el servidor de correo, que serán los únicos elementos visibles desde fuera de nuestra red. El *router* exterior tiene como misión bloquear el tráfico no deseado en ambos sentidos (hacia la red perimétrica y hacia la red externa), mientras que el interior hace lo mismo pero con el tráfico entre la red interna y la perimétrica: así, un atacante habría de romper la seguridad de ambos *routers* para acceder a la red protegida; incluso es posible implementar una zona desmilitarizada con un único *router* que posea tres o más interfaces de

red, pero en este caso si se compromete este único elemento se rompe toda nuestra seguridad, frente al caso general en que hay que comprometer ambos, tanto el externo como el interno.

7- Otras arquitecturas

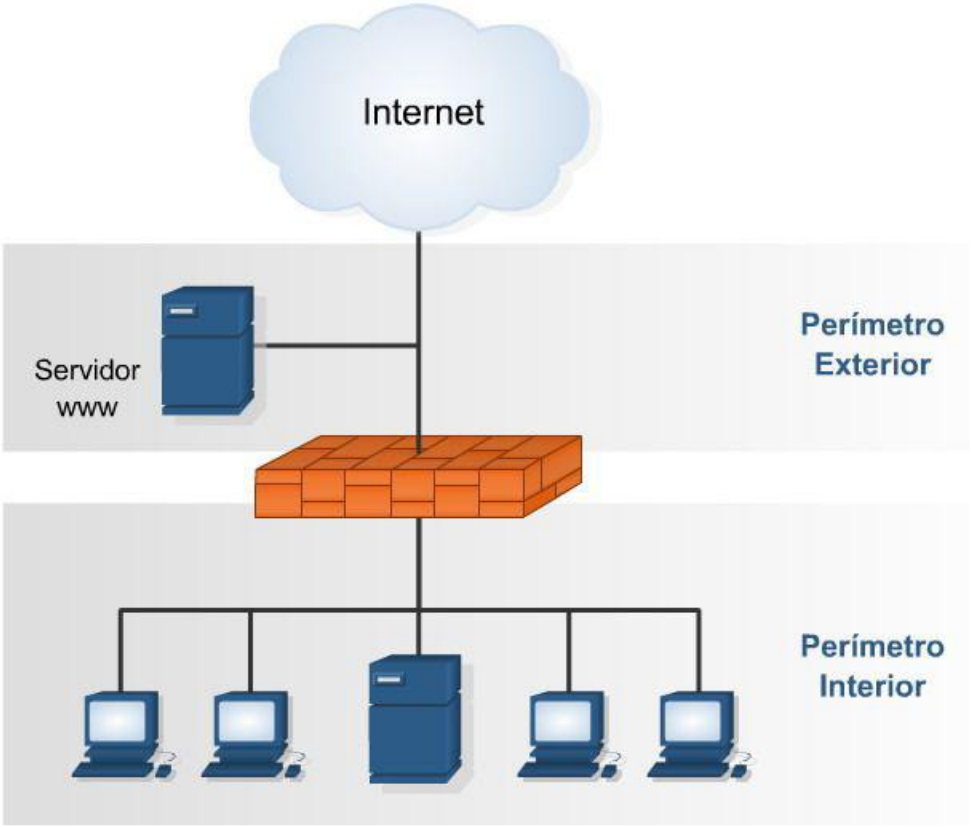
Algo que puede incrementar en gran medida nuestra seguridad y al mismo tiempo facilitar la administración de los cortafuegos es utilizar un bastión diferente para cada protocolo o servicio en lugar de uno sólo; sin embargo, esta arquitectura presenta el grave inconveniente de la cantidad de máquinas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

8- Defensa perimetral.
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.

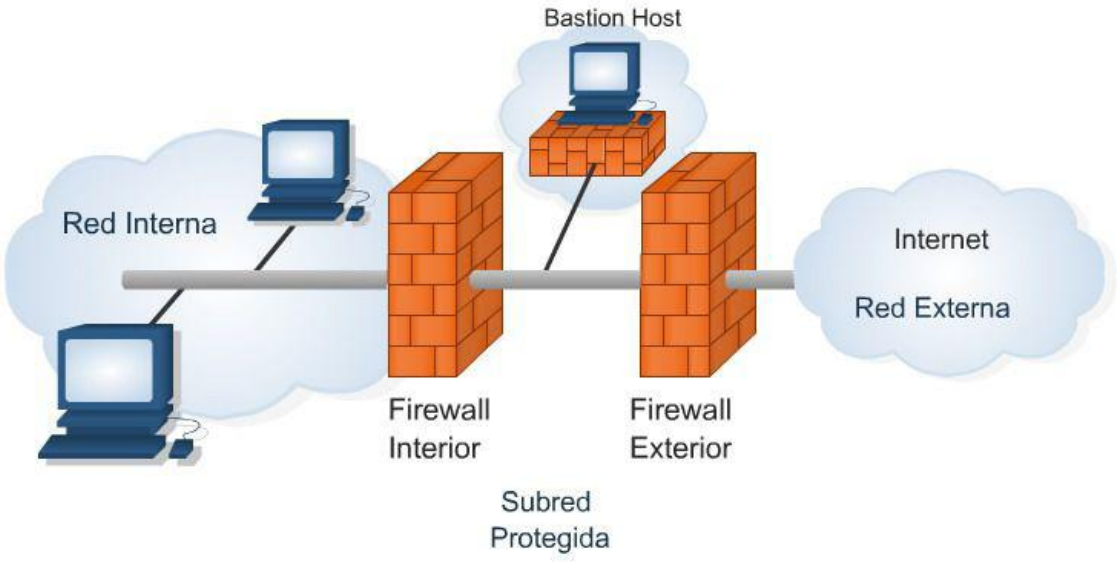
Esto nos permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.



Interacción entre zona perimetral (DMZ) y zona externa.

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

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



Monitorización del perímetro: detección y prevención de intrusos

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

Breve introducción a los sistemas IDS y Snort

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

Tipos de IDS

1. HIDS (Host IDS)

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

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

2. NIDS (Net IDS)

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

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

Otros tipos son los híbridos.

Por el tipo de respuesta podemos clasificarlos en:

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

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

Snort puede funcionar de las dos maneras.

Arquitectura de un IDS

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

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

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

Dónde colocar el IDS

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

Dificultades

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

9. DEFENSA INTERNA:

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

Una zona desmilitarizada (DMZ) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que

las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa -- 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.

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).

Entorno empresarial

En una arquitectura de seguridad con DMZ, se denomina **DMZ host** al ordenador que, situado en la DMZ, está expuesto a los riesgos de acceso desde Internet. Es por ello un ordenador de sacrificio, pues en caso de ataque está más expuesto a riesgos.

Normalmente el **DMZ host** está separado de Internet a través de un router o mejor un cortafuegos. Es aconsejable que en

el cortafuegos se abran al exterior únicamente los puertos de los servicios que se pretende ofrecer con el **DMZ host**.

En una arquitectura de seguridad más simple el router estaría conectado, por un lado a la red externa (usualmente Internet), por otra parte a la red interna, y en una tercera conexión estaría la DMZ, donde se sitúa el **DMZ host**.

Routers y cortafuegos internos

Quizás uno de los elementos más publicitados a la hora de establecer seguridad, sean estos elementos. Aunque deben ser uno de los sistemas a los que más se debe prestar atención, distan mucho de ser la solución final a los problemas de seguridad.

De hecho, los Firewalls no tienen nada que hacer contra técnicas como la Ingeniería Social y el ataque de Insiders.

Un **Firewall** es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

Puede consistir en distintos dispositivos, tendientes a los siguientes objetivos:

1. Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él.
2. Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido.

   Como puede observarse, el Muro Cortafuegos, sólo sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

   Algunos Firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de

ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red. Se entiende que si dos Firewalls están conectados, ambos deben "hablar" el mismo método de encriptación-desencriptación para entablar la comunicación.

3. Routers y Bridges

Cuando los paquetes de información viajan entre su destino y origen, vía TCP/IP, estos pasan por diferentes Routers (enrutadores a nivel de Red).

Los Routers son dispositivos electrónicos encargados de establecer comunicaciones externas y de convertir los protocolos utilizados en las LAN en protocolos de WAN y viceversa.

En cambio, si se conectan dos redes del tipo LAN se utilizan Bridges, los cuales son puentes que operan a nivel de Enlace.

La evolución tecnológica les ha permitido transformarse en computadoras muy especializadas capaz de determinar, si el paquete tiene un destino externo y el camino más corto y más descongestionado hacia el Router de la red destino. En caso de que el paquete provenga de afuera, determina el destino en la red interna y lo deriva a la máquina correspondiente o devuelve el paquete a su origen en caso de que él no sea el destinatario del mismo.

Los Routers "toman decisiones" en base a un conjunto de datos, regla, filtros y excepciones que le indican que rutas son las más apropiadas para enviar los paquetes.

Políticas de Diseño de Firewalls

Las políticas de accesos en un Firewalls se deben diseñar poniendo principal atención en sus limitaciones y capacidades

pero también pensando en las amenazas y vulnerabilidades presentes en una red externa insegura.

Conocer los puntos a proteger es el primer paso a la hora de establecer normas de seguridad. También es importante definir los usuarios contra los que se debe proteger cada recurso, ya que las medidas diferirán notablemente en función de esos usuarios.

Generalmente se plantean algunas preguntas fundamentales que debe responder cualquier política de seguridad:

- ¿Qué se debe proteger?. Se deberían proteger todos los elementos de la red interna (hardware, software, datos, etc.).
- ¿De quién protegerse?. De cualquier intento de acceso no autorizado desde el exterior y contra ciertos ataques desde el interior que puedan preverse y prevenir.

Sin embargo, podemos definir niveles de confianza, permitiendo selectivamente el acceso de determinados usuarios externos a determinados servicios o denegando cualquier tipo de acceso a otros.

- ¿Cómo protegerse?. Esta es la pregunta más difícil y está orientada a establecer el nivel de monitorización, control y respuesta deseado en la organización. Puede optarse por alguno de los siguientes paradigmas o estrategias:
    a. Paradigmas de seguridad
        - Se permite cualquier servicio excepto aquellos expresamente prohibidos.
        - Se prohíbe cualquier servicio excepto aquellos expresamente permitidos. La más recomendada y utilizada aunque algunas veces suele acarrear problemas por usuarios descontentos que no pueden acceder a tal cual servicio.
    b. Estrategias de seguridad
        - Paranoica: se controla todo, no se permite nada.

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

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

Restricciones en el Firewall

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

1. Usuarios internos con permiso de salida para servicios restringidos: permite especificar una serie de redes y direcciones a los que denomina **Trusted (validados)** . Estos usuarios, cuando provengan del interior, van a poder acceder a determinados servicios externos que se han definido.
2. Usuarios externos con permiso de entrada desde el exterior: este es el caso más sensible a la hora de vigilarse. Suele tratarse de usuarios externos que por algún motivo deben acceder para consultar servicios de la red interna.

Beneficios de un Firewall

Los Firewalls manejan el acceso entre dos redes, y si no existiera, todos las computadoras de la red estarían expuestos a ataques desde el exterior. Esto significa que la seguridad de toda la red, estaría dependiendo de que tan fácil fuera violar la seguridad local de cada maquina interna.

El Firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador será el responsable de la revisión de estos monitoreos.

Otra causa que ha hecho que el uso de Firewalls se halla convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones sin clase, las cuales salen a Internet por medio de un "traductor de direcciones", el cual puede alojarse en el Firewall.

Los Firewalls también son importantes desde el punto de vista de llevar las estadísticas del ancho de banda "consumido" por el trafico de la red, y que procesos han influido más en ese trafico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible.

Limitaciones de un Firewall

La limitación más grande que tiene un Firewall sencillamente es el hueco que no se tapa y que coincidentemente o no, es descubierto por un intruso. Los Firewalls no son sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo deja pasar. Más peligroso aún es que ese intruso deje Back Doors, abriendo un hueco diferente y borre las pruebas o indicios del ataque original.

Otra limitación es que el Firewall "NO es contra humanos", es decir que si un intruso logra entrar a la organización y descubrir passwords o los huecos del Firewall y difunde esta información, el Firewall no se dará cuenta.

El Firewall tampoco provee de herramientas contra la filtración de software o archivos infectados con virus, aunque es posible

dotar a la máquina, donde se aloja el Firewall, de antivirus apropiados.

Finalmente, un Firewall es vulnerable, él NO protege de la gente que está dentro de la red interna. El Firewall trabaja mejor si se complementa con una defensa interna. Como moraleja: "cuanto mayor sea el tráfico de entrada y salida permitido por el Firewall, menor será la resistencia contra los paquetes externos.

MONITORIZACION 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.

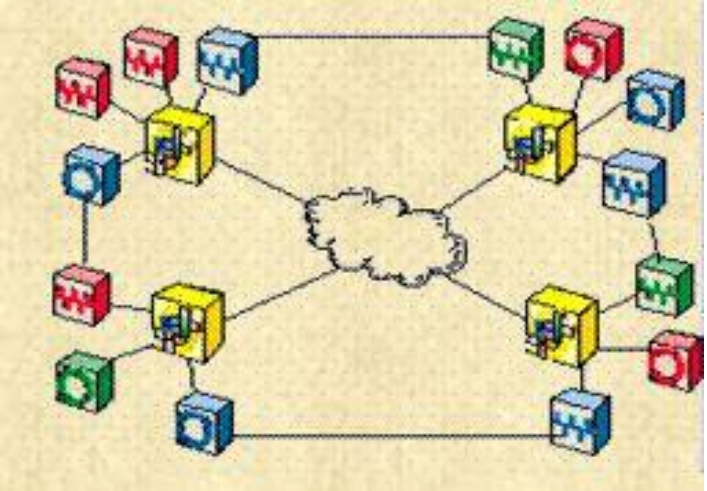
Aunque parezca lo contrario, implementar un buen sistema de monitorización no es una tarea tan difícil como exigente en su ejecución. El primer paso consiste en realizar un análisis detallado del sistema informático a monitorizar para, entre otras cosas, detectar los sistemas críticos (tanto máquinas 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.

Conectividad externa

Que conecta un hipertexto concreto con el resto de hipertextos a través de laWorld Wide Web y las redes telemáticas, es la expresión más potente de la tecnología hipertextual. La conectividad externa es la propiedad de laspáginas web de conducirnos a documentos localizados en espacios distintos al que se ubica el documento de partida. La extensión de cualquier hipertexto concreto a la red, es lo que permite integrar documentos o hiperdocumentos y discursos separados en el espacio, en un todo, y, en ocasiones, la asociación de contenidos puede ser tal que es difícil establecer dónde termina un documento y dónde empieza otro, a no ser que nos fijemos en determinadas marcas que indican su localización, como puede ser la dirección URL o la ruta para ver si se trata de un enlace relativo o absoluto. Se ha llegado a hablar de "documento total" ya que un hipertexto es indefinidamente enlazable y conexionable.

La conectividad externa permite, en teoría, integrar todo el conocimiento y la información humanas en la red. Sin embargo, la

conectividad externa que proporciona la Web sirve más bien para dar/o tener acceso a otros documentos y referencias y no como auguraban los defensores de la narrativa hipertextual para asociar todo un corpus de conocimientos.



En realidad, en la Web prima más la interrogación directa y la visita guiada que la navegación a la deriva, esto es, la Web sirve más para consultar y recuperar información que para navegar por ella sin un rumbo fijo ya que, en tan inmenso océano es casi imposible encontrar lo que nos interesa saltando de enlace en enlace. Se calcula que más del 90 por ciento de los nuevos usuarios acceden a Internet a través de los grandes portales como Google, Yahoo, Altavista, MSN, etc. Los portales, con sus índices y directorios temáticos o a través de los motores de búsqueda, se han convertido en los intermediarios indiscutibles entre la información y el usuario.

La conectividad externa es expansiva e internalizadora a la vez, ya que, por un lado da acceso al conjunto de la comunidad *web* a nuestros propios documentos y contenidos, y por otro, incorpora al propio hipertexto otros hipertextos, documentos e informaciones externas.

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.

Una **red privada virtual**, **RPV**, o **VPN** de las siglas en inglés de ***Virtual Private Network***, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel.

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.

Tipos de conexión

Conexión de acceso remoto

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

Conexión VPN router a router

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

Conexión VPN firewall a firewall

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

10. Políticas de defensa en profundidad

El factor humano

Política de seguridad

La política de seguridad corporativa se refiere al conjunto de políticas y directrices individuales existentes que permiten dirigir la seguridad y el uso adecuado de tecnología y procesos dentro de la organización. 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.

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.

11-Tipos de conexión VPN: VPN de acceso remoto, VPN sitio a sitio (tunneling) VPN sobre LAN.

Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

Tipos de VPN

Básicamente existen tres arquitecturas de conexión VPN:

VPN de acceso remoto

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red 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 puntos 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 over 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.

Tipos de conexión

Conexión de acceso remoto

Una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la

conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente.

Conexión VPN router a router

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

Conexión VPN firewall a firewall

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

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

Protocolos de túnel

Los principales protocolos de túnel son:

- PPTP (*Protocolo de túnel punto a punto*) es un protocolo de capa 2 desarrollado por Microsoft, 3Com, Ascend, US Robotics y ECI Telematics.
- L2F (*Reenvío de capa dos*) es un protocolo de capa 2 desarrollado por Cisco, Northern Telecom y Shiva. Actualmente es casi obsoleto.
- L2TP (*Protocolo de túnel de capa dos*), el resultado del trabajo del *IETF* (RFC 2661), incluye todas las características de *PPTP* y *L2F*. Es un protocolo de capa 2 basado en PPP.
- **IPSec** es un protocolo de capa 3 creado por el IETF que puede enviar datos cifrados para redes IP.

Protocolo PPTP

El principio del PPTP (*Protocolo de túnel punto a punto*) consiste en crear tramas con el protocolo PPP y encapsularlas mediante un datagrama de IP.

Por lo tanto, con este tipo de conexión, los equipos remotos en dos redes de área local se conectan con una conexión de igual a igual (con un sistema de autenticación/cifrado) y el paquete se envía dentro de un datagrama de IP.

De esta manera, los datos de la red de área local (así como las direcciones de los equipos que se encuentran en el encabezado del mensaje) se encapsulan dentro de un mensaje PPP, que a su vez está encapsulado dentro de un mensaje IP.

Protocolo L2F

El protocolo L2F (Layer 2 Forwarding) se creó en las primeras etapas del desarrollo de la 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.

Protocolo L2TP

L2TP es un protocolo de túnel estándar (estandarizado en una RFC, solicitud de comentarios) muy similar al PPTP. L2TP encapsula tramas PPP, que a su vez encapsulan otros protocolos (como IP, IPX o NetBIOS).

Protocolo IPSec

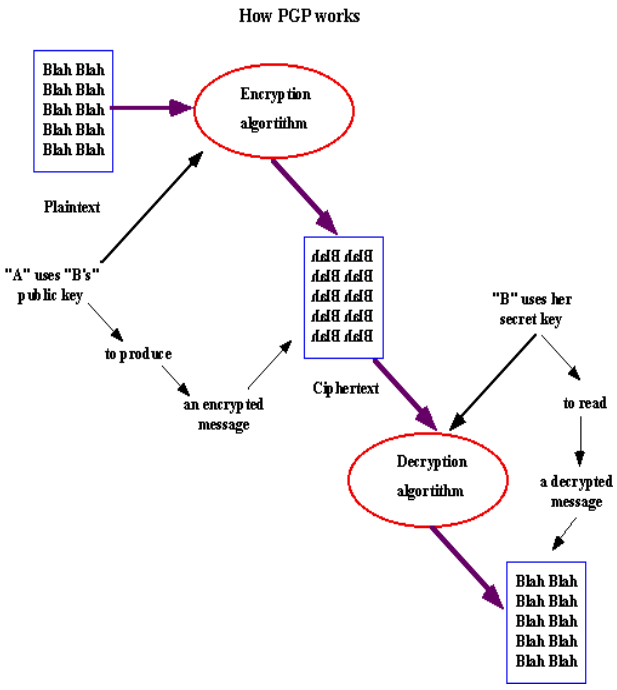
IPSec es un protocolo definido por el IETF que se usa para transferir datos de manera segura en la capa de red. En realidad es un protocolo que mejora la seguridad del protocolo IP para garantizar la privacidad, integridad y autenticación de los datos enviados.

IPSec se basa en tres módulos:

- *Encabezado de autenticación IP* (**AH**), que incluye integridad, autenticación y protección contra ataques de REPLAY a los paquetes.
- *Carga útil de seguridad encapsulada* (**ESP**), que define el cifrado del paquete. ESP brinda privacidad, integridad, autenticación y protección contra ataques de REPLAY.
- *Asociación de seguridad* (**SA**) que define configuraciones de seguridad e intercambio clave. Las SA incluyen toda la información acerca de cómo procesar paquetes IP (los protocolos AH y/o ESP, el modo de transporte o túnel, los algoritmos de seguridad utilizados por los protocolos, las claves utilizadas, etc.). El intercambio clave se realiza manualmente o con el protocolo de intercambio IKE (en la mayoría de los casos), lo que permite que ambas partes se escuchen entre sí.

12-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).

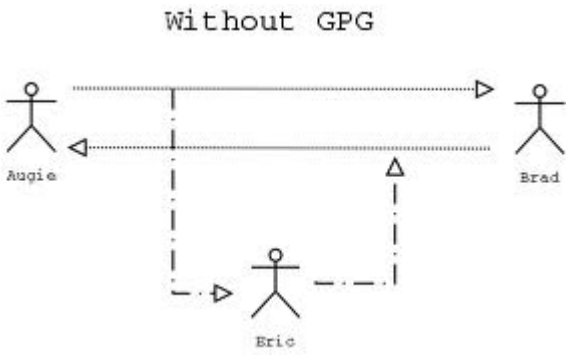
Funciones de PGP

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.

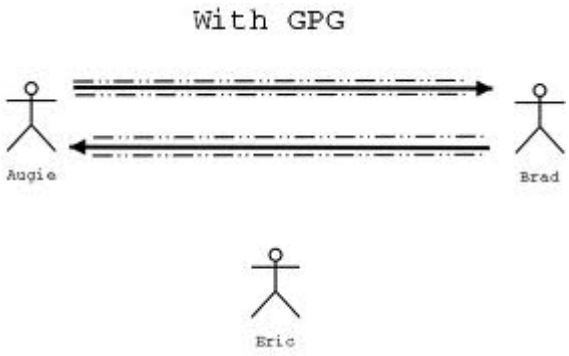
GNU Privacy Good (GPG).

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.

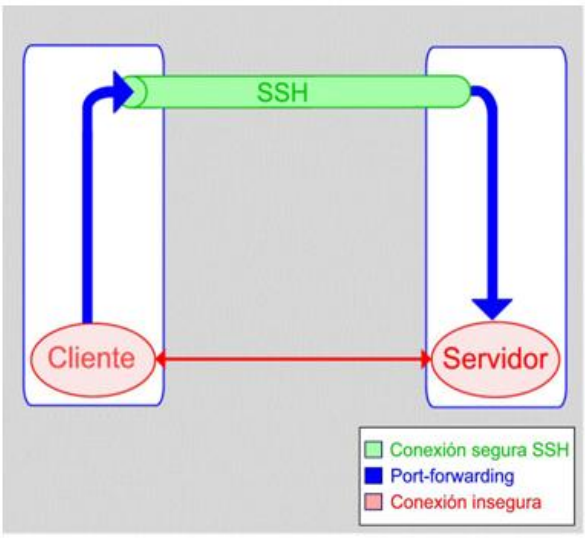
- Seguridad a nivel de aplicación: SSH ("Secure Shell").

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.



Proceso de tunneling SSH.

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

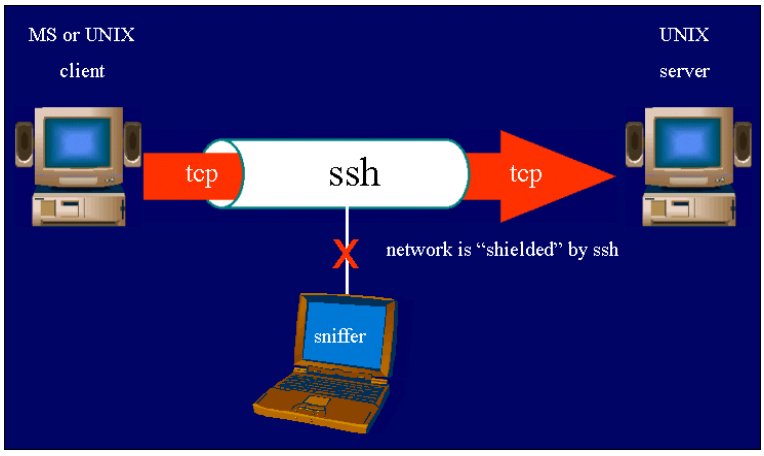
A diferencia de telnet u otro servicio similar, SSH utiliza el **puerto 22** para la comunicación y la forma de efectuar su trabajo es muy similar al efectuado por SSL.

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:

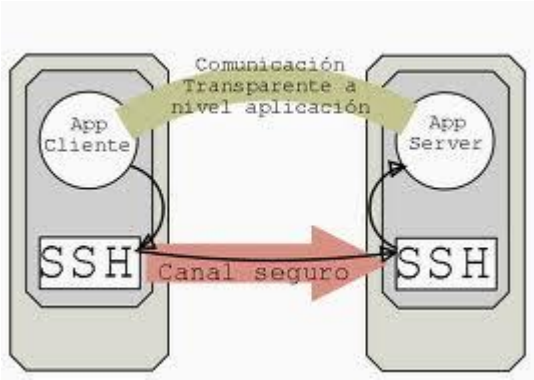
- **El cliente** envía una señal al servidor pidiéndole comunicación por el puerto 22.
- El servidor acepta la comunicación en el caso de poder mantenerla **bajo encriptación** mediante un algoritmo definido y le envía la llave publica al cliente para que pueda descifrar los mensajes.
- El cliente recibe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



Protocolo
El protocolo SSH se establece en tres niveles:
Nivel de transporte

En este nivel se procede a la autenticación del servidor, el establecimiento de un canal cifrado, chequeo de integridad de los mensajes, así como generación de un identificador único de sesión.

En cuanto a los algoritmos empleados se establecen algunos como requeridos y otros como opcionales. Por nombrar:



-Intercambio de claves: Diffie-Hellman
-Algoritmos de clave pública para encriptación y autenticación del servidor: DSA, certificados X.509, certificados PGP etc.
-Algoritmos de clave simétrica: 3Des en modo CBC , blowfish, idea-cbc etc. , todos con claves de 128 bit
-**Algoritmos de integridad**: HMAC-SHA1 , HMAC-MD5 etc.

Nivel de autentificación del usuario

En este nivel se supone establecida la encriptación e integridad del canal, así como la autentificación del servidor.

Para la autentificación del usuario el SSH ofrece varias posibilidades.
La autentificación usando un par de clave pública-privada .

Nivel de conexión
Es el protocolo encargado de simultanear sesiones interactivas de login, ejecución remota de comandos, forwarding de conexiones TCP/IP, forwarding de conexiones X11 etc. SSH está en vía de convertirse en un protocolo estándar de Internet por el IETF más conocido por SECSH.

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

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

Cómo funciona una conexión con SSL, en pocas palabras

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

- El cliente y el servidor entran en un proceso de negociación, conocido como ***handshake*** (apretón de manos). Este proceso sirve para que se establezca varios parámetros para realizar la conexión de forma segura.
- Una vez terminada la negociación, la conexión segura es establecida.
- Usando llaves preestablecidas, se codifica y descodifica todo lo que sea enviado hasta que la conexión se cierre.

Certificado SSL

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

14-TLS ("Transport Layer Security")

INTRODUCCIÓN

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. 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 la negociación.
- **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*).

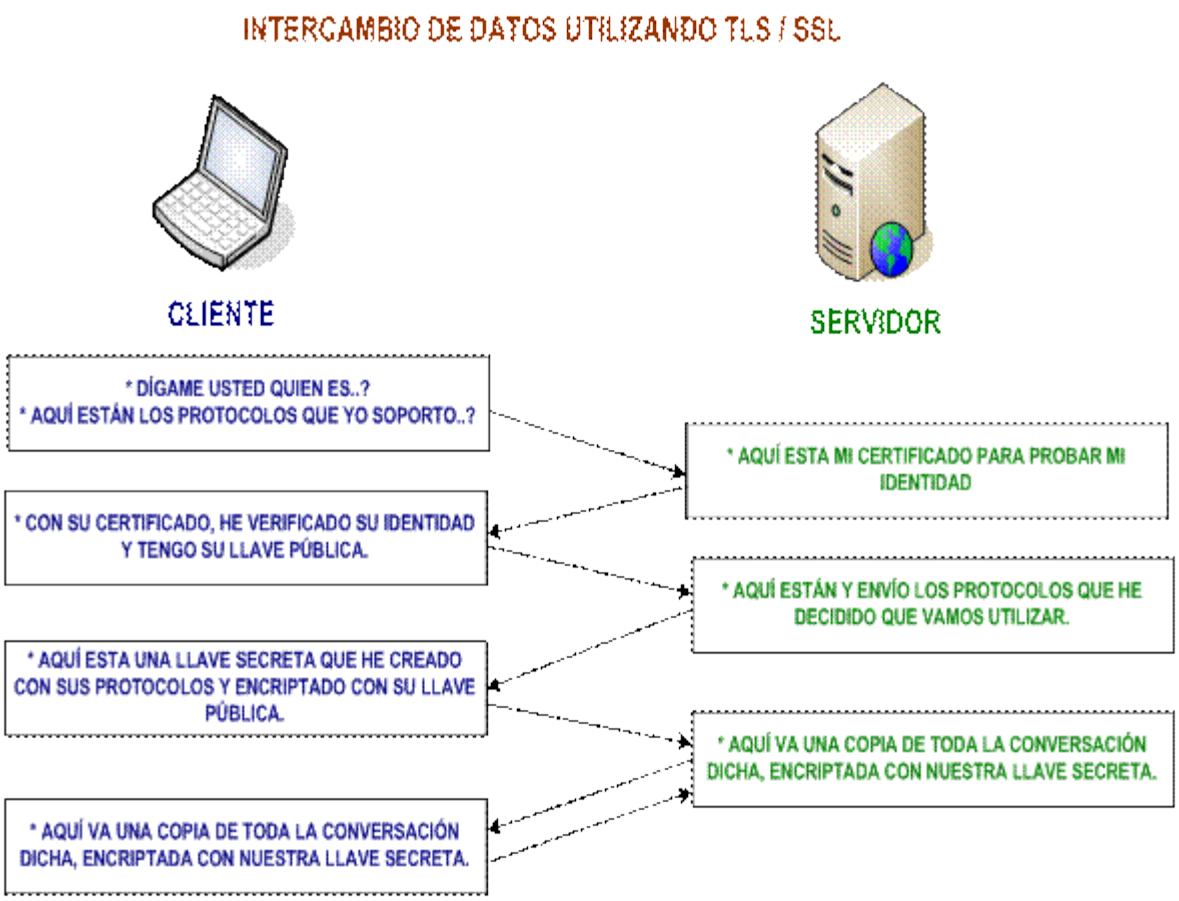
El de más bajo nivel es el ***Protocolo de Registro***, que se implementa sobre un protocolo de transporte fiable como el TCP. El protocolo proporciona seguridad en la conexión con dos propiedades fundamentales:

- **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.

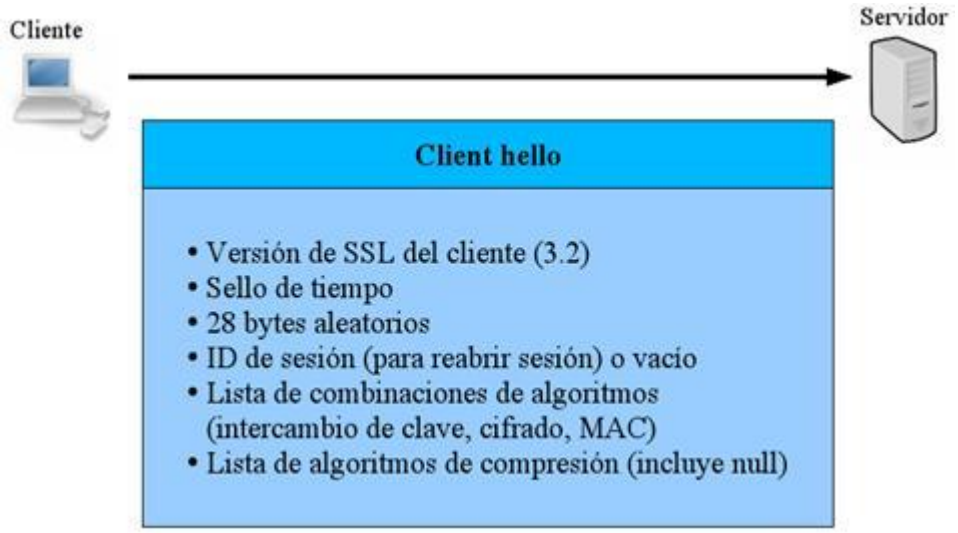
Esquema de operación del protocolo de mutuo acuerdo (*TLS Handshake Protocol*)



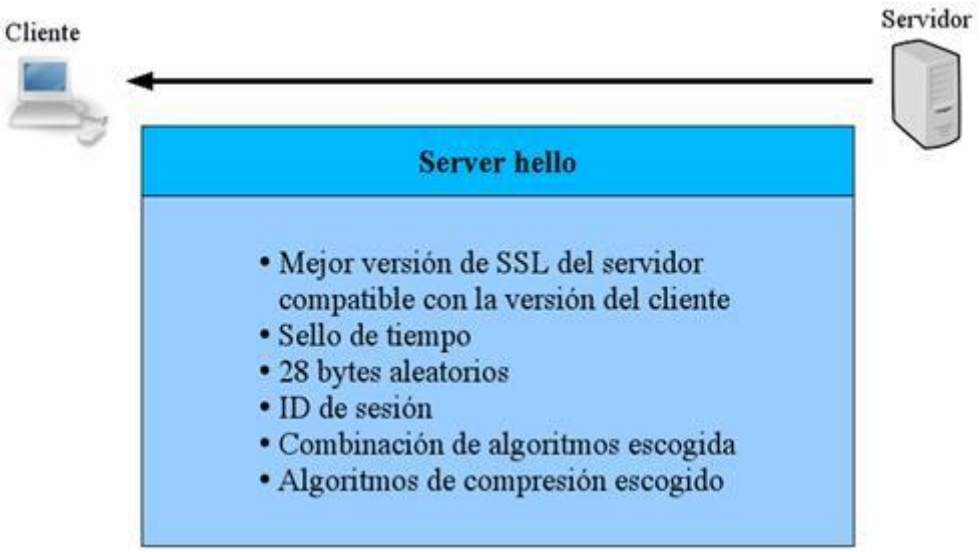
La comunicación entre los nodos CLIENTE y SERVIDOR está basada en el intercambio de mensajes. En cada mensaje existe un campo (content_type) donde se especifica el protocolo de nivel superior utilizado. Estos mensajes puede ser comprimidos, cifrados y empaquetados con un código de autentificación del mensaje (MAC).

En el inicio de un conexión el nivel de mensaje encapsula un protocolo handshake (content_type=22), enviándose diferentes mensajes:

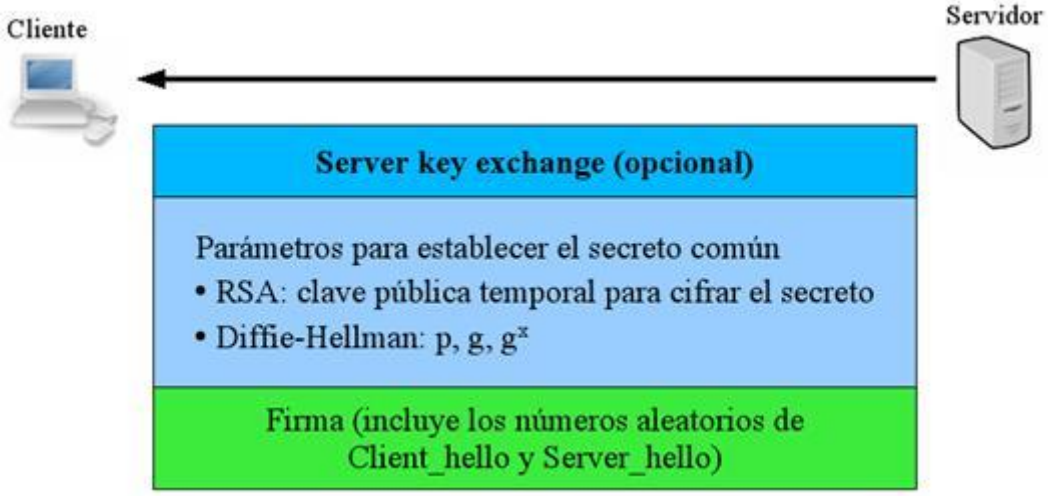
- El cliente inicia la comunicación enviando un mensaje "Client Hello" dónde especifica una lista de conjunto de cifrados, métodos de compresión y la versión del protocolo SSL más alta permitida. A la vez envía una serie de bytes aleatorios (Challenge de Cliente o Reto) que después serán usados. Adicionalmente puede enviar el identificador de la sesión.



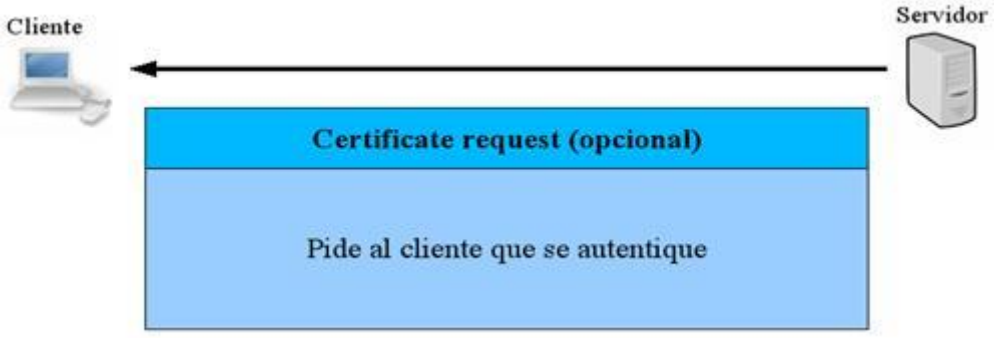
- El servidor responde con un mensaje "Server Hello" donde se indican los parámetros elegidos por el servidor a partir de las opciones ofertadas por el cliente.



- Una vez establecidos los parámetros de la conexión, cliente y servidor intercambian los certificados, según las claves públicas de cifrado seleccionadas. Actualmente son certificados X.509, pero existe un borrador en el que se especifica el uso de certificados basados en OpenPGP.

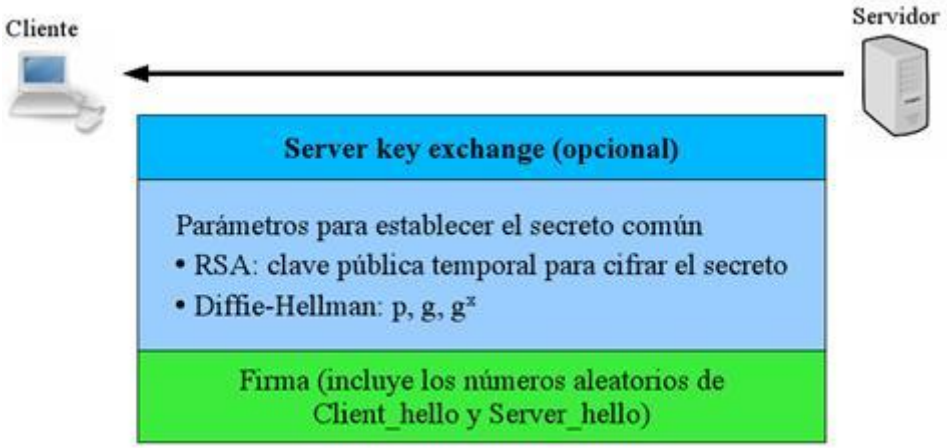


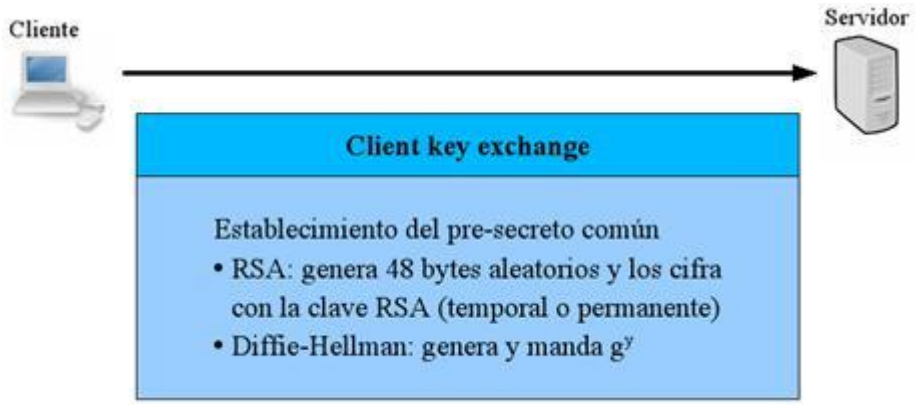
- Si la conexión tiene que ser mutuamente certificada el servidor pide un certificado al cliente y éste se la enviaría.



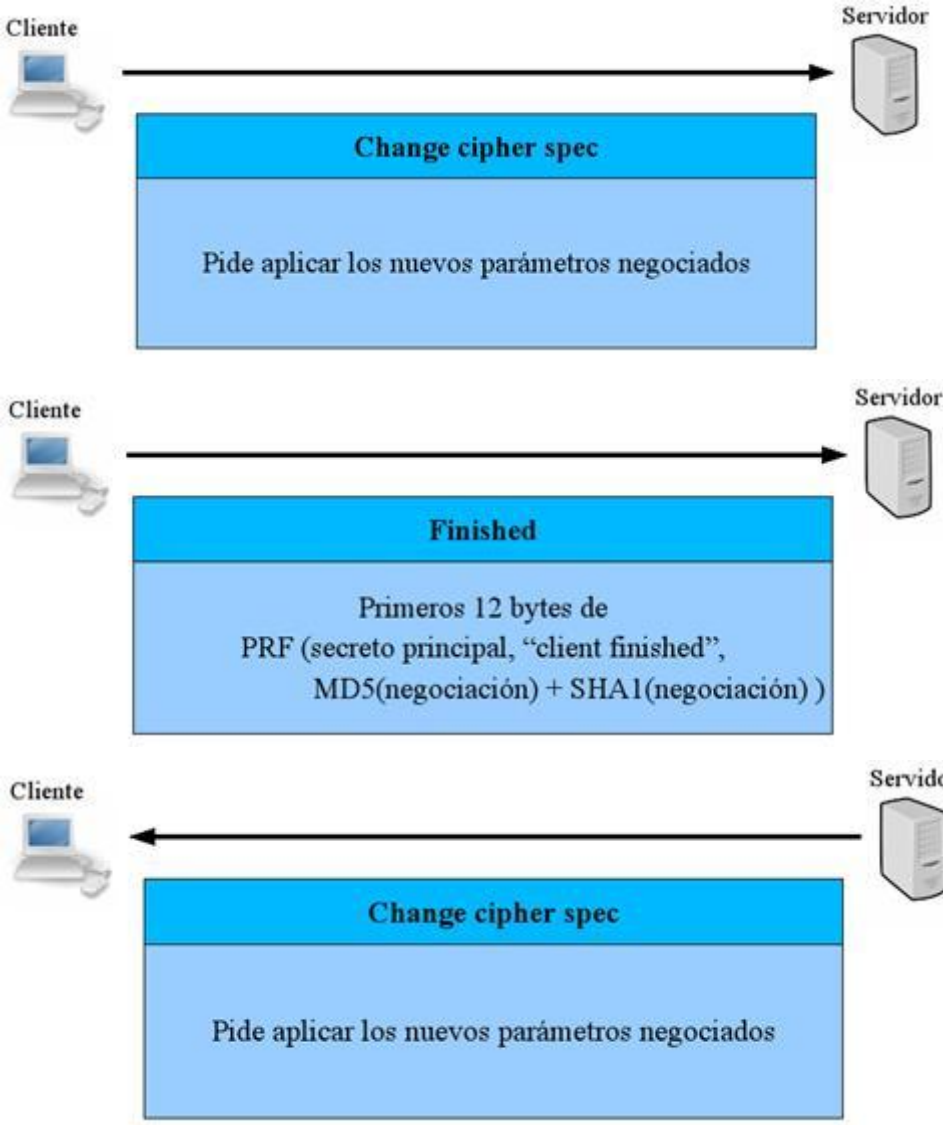
- El cliente verifica la autenticidad del servidor.

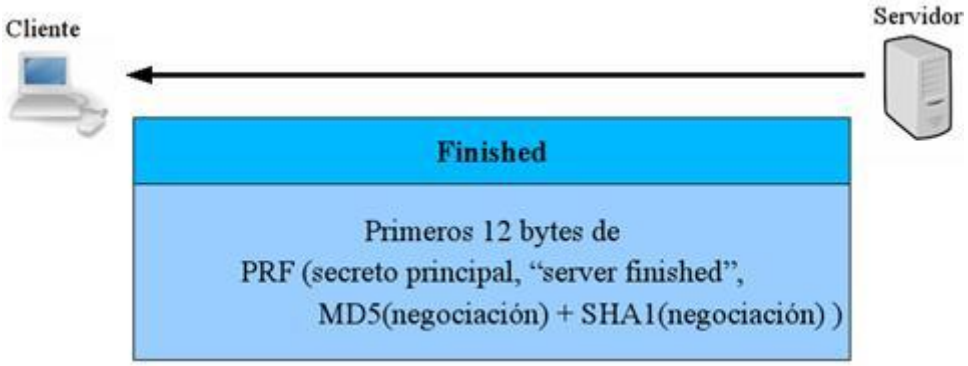
- Cliente y servidor negocian una clave secreta común (master secret), que puede derivarse de un intercambio Diffie-Hellman, o utilizando la clave privada de cada uno para cifrar una clave pública que servirá para cifrar a la vez la clave secreta. El resto de claves son derivadas a partir de este master secret y los valores aleatorios generados en el cliente y el servidor, que son pasados a través una función pseudo-aleatoria.





- Cliente y servidor aplican los parámetros negociados





APLICACIONES DEL PROTOCOLO TLS

El protocolo SSL/TLS tiene multitud de aplicaciones en uso actualmente. La mayoría de ellas son versiones seguras de programas que emplean protocolos que no lo son. Hay versiones seguras de servidores y clientes de protocolos como el http, nntp, ldap, imap, pop3, etc.

El protocolo SSL/TLS se ejecuta en una capa entre los protocolos de aplicación como:

- HTTP sobre SSL/TLS es HTTPS, ofreciendo seguridad a páginas WWW para aplicaciones de comercio electronic, utilizando certificados de clave pública para verificar la identidad de los extremos. Visa, MasterCard, American Express y muchas de las principales instituciones financieras han aprobado SSL para el comercio sobre Internet.
- SSH utiliza SSL/TLS por debajo.
- SMTP y NNTP pueden operar también de manera segura sobre SSL/TLS.
- POP3 i IMAP4 sobre SSL/TLS son POP3S i IMAPS.

Existen múltiples productos clientes y servidores que pueden proporcionar SSL de forma nativa, pero también existen muchos que aún no lo permiten. una solución podría ser usar una aplicación SSL independiente como Stunnel para conseguir el cifrado, pero IETF recomendó en 1997 que los protocolos de aplicación ofrecieran una forma de actualizar a TLS a partir de una conexión sin cifrado (plaintext) en vez de usar un puerto diferente para cifrar las comunicaciones, evitando el uso de envolturas (wrappers) como Stunnel.

SSL también puede ser usado para tunelar una red completa y crear una red privada virtual (VPN), como en el caso de OpenVPN.

Implementaciones del Protocolo TLS

Existen diferentes implementaciones, como por ejemplo:

- **OpenSSL**: es una implementación de código abierto, la más utilizada. Es un proyecto desarrollado por la comunidad Open Source para libre descarga y está basado en SSLeay, que ayuda al sistema a implementar el SSL/TLS ofreciéndole un robusto paquete de herramientas de administración y librerías de criptografía que pueden ser usadas para OpenSSH y navegadores web (acceso seguro a HTTPS).
- **GnuTLS**: es una implementación de código abierto con licencia compatible con GPL.
- **JSSE**: es una implementación realizada en el Java incluida en el Java Runtime Environment.

Estandares y Definiciones RFC del Protocolo TLS

La primera definición de TLS apareció en el RFC 2246: "The TLS Protocol Version 1.0" (El protocolo TLS versión 1.0) y está basada en la versión 3.0 de SSL, siendo prácticamente equivalentes.

- **RFC 2712:** Aparecen las familias de cifrados de 40 bits definidas, para advertir que ya han sido asignadas.
- **RFC 2817:** Explica cómo usar el mecanismo de actualización en HTTP/1.1 para iniciar TLS sobre una conexión TCP existente, permitiendo al tráfico seguro e inseguro HTTP compartir el mismo puerto.
- **RFC 2818:** Diferencia el tráfico seguro e inseguro HTTP usando un puerto de servidor diferente.
- **RFC 3268:** Añade la familia de cifrado AES.
- **RFC 3546:** Añade un mecanismo para negociar extensiones de protocolos durante la inicialización de sesión y define algunas extensiones.
- **RFC 4279:** Añade tres conjuntos de nuevas familias de cifrados para que el protocolo TLS permita la autenticación basada en claves previamente compartidas.

VERSIONAMIENTO DEL PROTOCOLO TLS

El protocolo TLS ha evolucionado desde la versión 1.0 hasta la actual versión que es la 1.1. Esta última versión es muy parecida a la versión anterior (TLS 1.0), pero la principal diferencia es la modificación del formato para cifrado RSA anterior al uso de 'master secret', que es parte del mensaje de intercambio de claves del cliente. En TLS 1.0 se usaba la versión 1.5 del estándar RSA para criptografía de clave pública (PCK#1), pasando a usar ahora la versión 2.1. Con este cambio se consigue protección ante ataques descubiertos por Daniel Bleichenbacher que podían lanzarse contra

servidores TLS 1.0, usando PKCS#1 versión 1.5. También se incluyen recomendaciones para evitar ataques remotos programados. TLS 1.1 está actualmente implementado en el navegador Opera y en GnuTLS.

MEDIAS DE SEGURIDAD DEL PROTOCOLO TLS

- Numera todos los registros y usa el número de secuencia en MAC.
- Usa un resumen de mensaje mejorado con una clave (de forma que solo con dicha clave se pueda comprobar el MAC).
- 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 tornen vulnerables en el futuro.

15- Protocolos PPP, PPoE, PPPoA

Protocolos PPP

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.

Protocolos PPPoe

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 cablemódem y xDSL. Este ofrece las ventajas del protocolo PPP como son la autenticación, cifrado, mantención y compresión.

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

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

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

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

Protocolo de 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.

16 Protocolo de 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 Authentication Protocol (EAP) es una autenticación framework usada habitualmente en redes WLAN Point-to-Point Protocol. Aunque el protocolo EAP no está limitado a LAN inalámbricas 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), Generic Token-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.

17. PEAP: Protocolo de autenticación extensible protegido

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.

17.1 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.

Descripción

Kerberos se basa en el Protocolo de Needham-Schroeder. Usa un tercero de confianza, denominado "centro de distribución de claves" (KDC, por sus siglas en inglés: *Key Distribution Center*), el cual consiste de dos partes lógicas separadas: un "servidor de autenticación" (AS o *Authentication Server*) y un "servidor emisor de tiquets" (TGS o *Ticket Granting Server*). Kerberos trabaja sobre la base de "tickets", los cuales sirven para demostrar la identidad de los usuarios.

Kerberos mantiene una base de datos de claves secretas; cada entidad en la red —sea cliente o servidor— comparte una clave secreta conocida únicamente por él y Kerberos. El conocimiento de esta clave sirve para probar la identidad de la entidad. Para una comunicación entre dos entidades, Kerberos genera una clave de sesión, la cual pueden usar para asegurar sus interacciones.

Cómo funciona

Funcionamiento de Kerberos.

A continuación se describe someramente el protocolo. Se usaran las siguientes abreviaturas:

- AS = Authentication Server
- TGS = Ticket Granting Server
- SS = Service Server.

En resumen el funcionamiento es el siguiente: el cliente se autentica a sí mismo contra el AS, así demuestra al TGS que está autorizado para recibir un ticket de servicio (y lo recibe) y ya puede demostrar al SS que ha sido aprobado para hacer uso del servicio kerberizado.

En más detalle:

1. Un usuario ingresa su nombre de usuario y password en el cliente
2. El cliente genera una clave hash a partir del password y la usará como la clave secreta del cliente.
3. El cliente envía un mensaje en texto plano al AS solicitando servicio en nombre del usuario. Nota: ni la clave secreta ni el password son enviados, solo la petición del servicio.
4. El AS comprueba si el cliente está en su base de datos. Si es así, el AS genera la clave secreta utilizando la función hash con la password del cliente encontrada en su base de datos. Entonces envía dos mensajes al cliente:
    1. Mensaje A: Client/TGS session key cifrada usando la clave secreta del usuario
    2. Mensaje B: Ticket-Granting Ticket (que incluye el ID de cliente, la dirección de red del cliente, el período de validez y el Client/TGS session key) cifrado usando la clave secreta del TGS.
5. Una vez que el cliente ha recibido los mensajes, descifra el mensaje A para obtener el client/TGS session key. Esta session key se usa para las posteriores comunicaciones con el TGS. (El cliente no puede descifrar el mensaje B pues para cifrar éste se ha usado la clave del TGS). En este momento el cliente ya se puede autenticar contra el TGS.
6. Entonces el cliente envía los siguientes mensajes al TGS:

1. Mensaje C: Compuesto del Ticket-Granting Ticket del mensaje B y el ID del servicio solicitado.
2. Mensaje D: Autenticador (compuesto por el ID de cliente y una marca de tiempo), cifrado usando el client/TGS session key.

18 **Protocolo 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.

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.

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.

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.

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.(esta parte no se si este muy bien porque no he encontrado nada por internet)

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.

19. **Servidor 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.

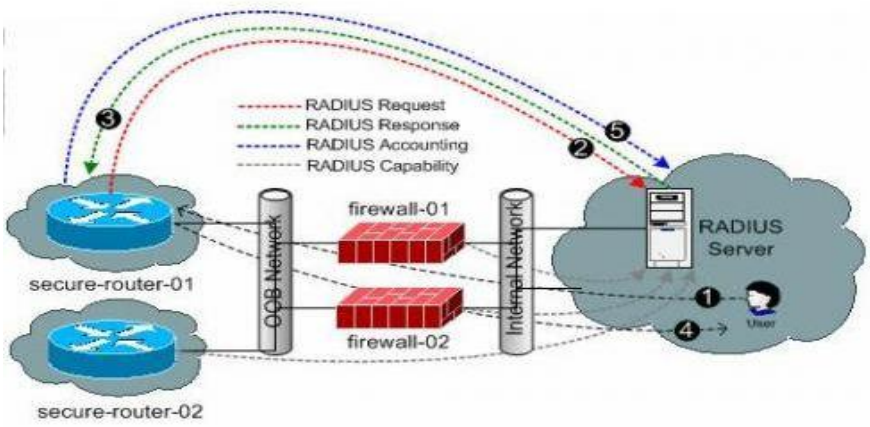
Kerberos es otro tipo de protocolo de autenticación utilizado en muchos sistemas de Windows Server ® de autenticación, por ejemplo, y en algunos de seguridad en línea o sistemas de seguridad de Internet. Hay tres aspectos principales para la autenticación Kerberos: la autenticación de la identidad del 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.

Tipos de Servidores:

Radius: 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.

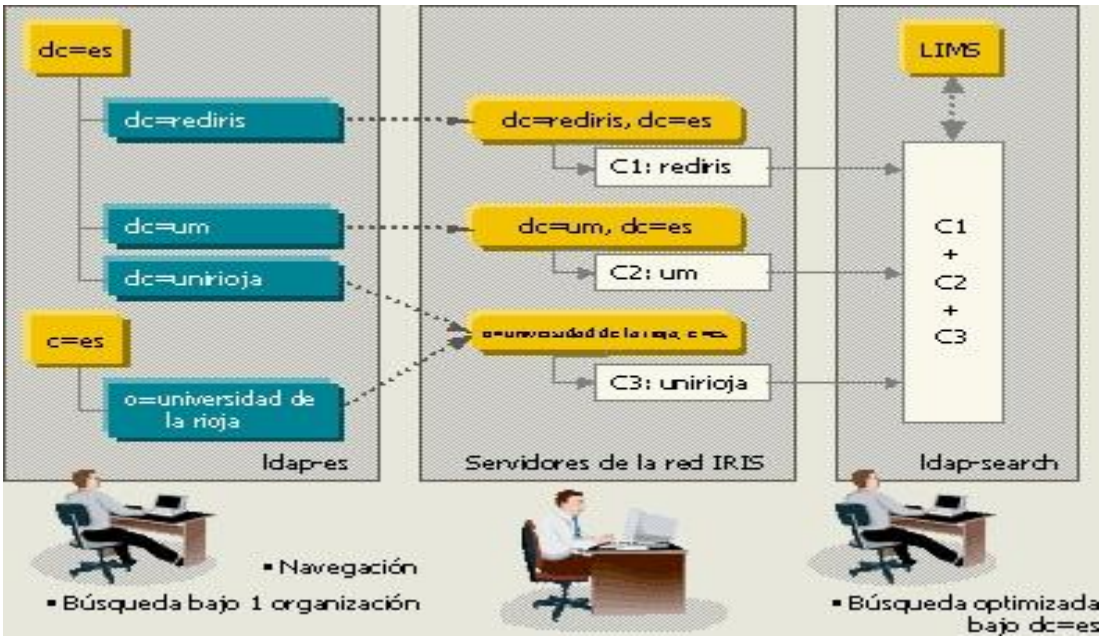
Cuando se realiza la conexión con un ISP mediante módem, DSL, cable módem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo Network Access Server (NAS) sobre el protocolo PPP, quien redirige la petición 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.

LDAP: que hacen referencia a un protocolo a nivel de aplicación el cual permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos a la que pueden realizarse consultas.

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


dc=es
dc=rediris
dc=um
dc=unirioja
c=es
o=universidad de la rioja
ldap-es
dc=rediris, dc=es
C1: rediris
dc=um, dc=es
C2: um
C3: unirioja
Servidores de la red IRIS
LIMS
C1
+
C2
+
C3
ldap-search
• Navegación
• Búsqueda bajo 1 organización
• Búsqueda optimizada bajo dc=es