IMPLANTACIÓN DE TÉCNICAS DE ACCESO REMOTO. SEGURIDAD PERIMETRAL

MARÍA ÁNGELES PEÑASCO SÁNCHEZ- 2º ASIR- TEMA 3 SAD

ÍNDICE

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:

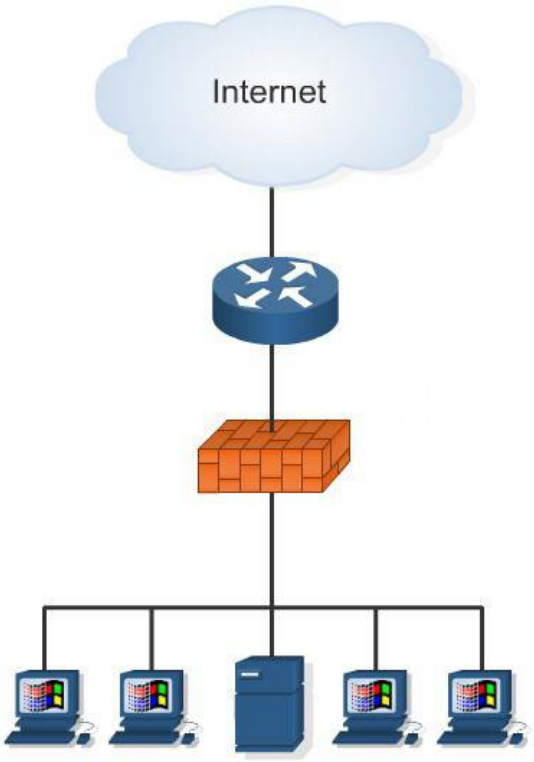
- PROTOCOLOS DE AUTENTICACIÓN
  - PROTOCOLOS PPP, PPPoE, PPPoA
  - AUTENTICACIÓN DE CONTRASEÑA: PAP
  - AUTENTICACIÓN POR DESAFÍO MUTUO: CHAP
  - AUTENTICACIÓN EXTENSIBLE: EAP. MÉTODOS
  - PEAP
  - KERBEROS
  - PROTOCOLOS AAA:
    - RADIUS
    - TACACS+
- CONFIGURACIÓN DE PARÁMETROS DE ACCESO.
- SERVIDORES DE AUTENTICACIÓN.

ELEMENTOS BÁSICOS DE LA SEGURIDAD PERIMETRAL

- **CONCEPTO DE SEGURIDAD PERIMETRAL.**

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

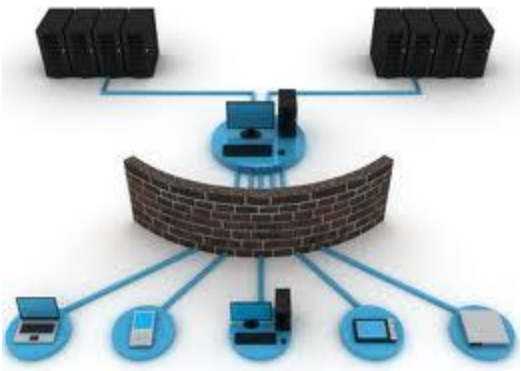
Esto nos permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.



- **OBJETIVOS DE LA SEGURIDAD PERIMETRAL.**
- **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.
- **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.
- **Internet libre:**
  Rentabilizar el Recurso Internet para el trabajo, dejándolo libre y con toda su capacidad y velocidad contratada.
- **Detección de virus:**
  Pronta detección de equipos con brotes de Virus y del uso de programas maliciosos.
- **Conexiones remotas:**
  Simplificar la conectividad Segura hacia mi red de Oficinas y promoción de la movilidad vía VPN.

- **PERÍMETRO DE LA RED:**

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...

○ ROUTERS FRONTERA.

Un router de frontera es un dispositivo situado entre la red interna de y las redes de otros proveedores que intercambian el tráfico con nosotros y que se encarga de dirigir el tráfico de datos de un lado a otro. El último router que controlamos antes de Internet. Primera y última línea de defensa. Filtrado inicial y final.

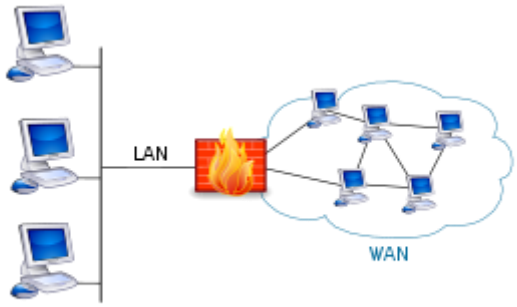
○ CORTAFUEGOS (FIREWALLS).

Un cortafuego (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 de los cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al cortafuego 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.



- **SISTEMAS 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 sniffers 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.

Los IDS suelen disponer de una base de datos de “firmas” de ataques conocidos.

Dichas firmas permiten al IDS distinguir entre el uso normal del PC y el uso fraudulento, y/o entre el tráfico normal de la red y el tráfico que puede ser resultado de un ataque o intento del mismo.

Tipos de IDS

Existen dos tipos de sistemas de detección de intrusos:

1. HIDS (HostIDS): el principio de funcionamiento de un HIDS, depende del éxito de los intrusos, que generalmente dejaran rastros de sus actividades en el equipo atacado, cuando intentan adueñarse del mismo, con propósito de llevar a cabo otras actividades. El HIDS intenta detectar tales modificaciones en el equipo afectado, y hacer un reporte de sus conclusiones.
2. NIDS (NetworkIDS): un IDS basado en red, detectando ataques a todo el segmento de la red. Su interfaz debe funcionar en modo promiscuo capturando así todo el tráfico de la red. Sirve de protección al sistema

- **REDES PRIVADAS VIRTUALES.**

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

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

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

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

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

- **SOFTWARE Y SERVICIOS. HOST BASTION.**

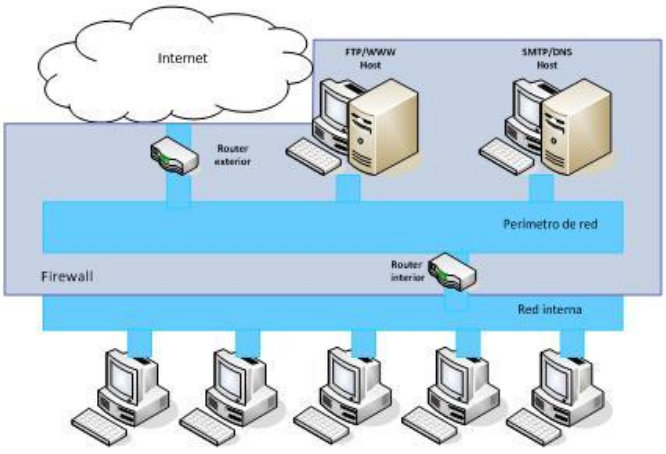
Un bastión host (bastion sin acentuar en inglés) es una aplicación que se localiza en un server con el fin de ofrecer seguridad a la red interna, por lo que ha sido especialmente configurado para la recepción de ataques, generalmente provee un solo servicio (como por ejemplo un servidor proxy).

Diseño

A diferencia del filtro realizado a través de un router, que permite o no el flujo directo de paquetes desde el interior al exterior de una red, los bastión host (también llamados en inglés application-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. Se podría tener un servicio diferente por host, pero esto involucraría un costo muy elevado, pero en caso de que se pueda abordar, se podrían llegar a tener múltiples bastión host para mantener seguros múltiples puntos de ataque.

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

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



ZONAS DESMILITARIZADAS (DMZ) Y SUBREDES CONTROLADAS.

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

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

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

Una DMZ se crea a menudo a través de las opciones de configuración del cortafuegos, donde cada red se conecta a un puerto distinto de éste. Esta configuración se llama cortafuegos en trípode (three-legged firewall). Un planteamiento más seguro es usar dos cortafuegos, donde la DMZ se sitúa en medio y se conecta a ambos cortafuegos, uno conectado a la red interna y el otro a la red externa. Esta configuración ayuda a prevenir configuraciones erróneas accidentales que permitan el acceso desde la red externa a la interna. Este tipo de configuración también es llamado cortafuegos de subred monitoreada (screened-subnet firewall).

Subredes controladas

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

ARQUITECTURAS DE CORTAFUEGOS:

- **CORTAFUEGO DE FILTRADO DE PAQUETES.**

Un firewall sencillo puede consistir en un dispositivo capaz de filtrar paquetes, un choke: se trata del modelo de cortafuegos más antiguo basado simplemente en aprovechar la capacidad de algunos routers - denominados screening routers - para hacer un enrutado selectivo, es decir, para bloquear o permitir el tránsito de paquetes mediante listas de control de acceso en función de ciertas características de las tramas, de forma que el router actúe como pasarela de toda la red.

Generalmente estas características para determinar el filtrado son las direcciones origen y destino, el protocolo, los puertos origen y destino (en el caso de TCP y UDP), el tipo de mensaje (en el caso de ICMP) y los interfaces de entrada y salida de la trama en el router.

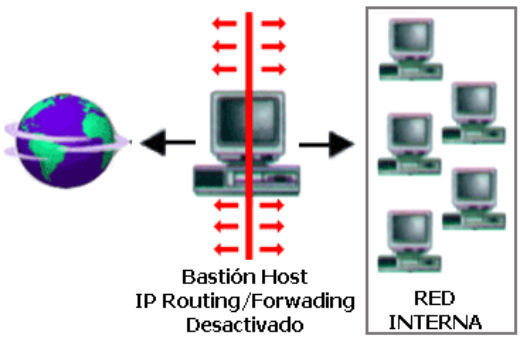
En un cortafuegos de filtrado de paquetes los accesos desde la red interna al exterior que no están bloqueados son directos (no hay necesidad de utilizar proxies, como sucede en los cortafuegos basados en una máquina con dos tarjetas de red), por lo que esta arquitectura es la más simple de implementar y la más utilizada en organizaciones que no precisan grandes niveles de.

- **CORTAFUEGO DUAL-HOMED HOST.**

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

Un usuario interior que desee hacer uso de un servicio exterior, deberá conectarse primero al Firewall, donde el Proxy atenderá su petición, y en función de la configuración impuesta en dicho Firewall, se conectara al servicio exterior solicitado y hará de puente entre este y el usuario interior.

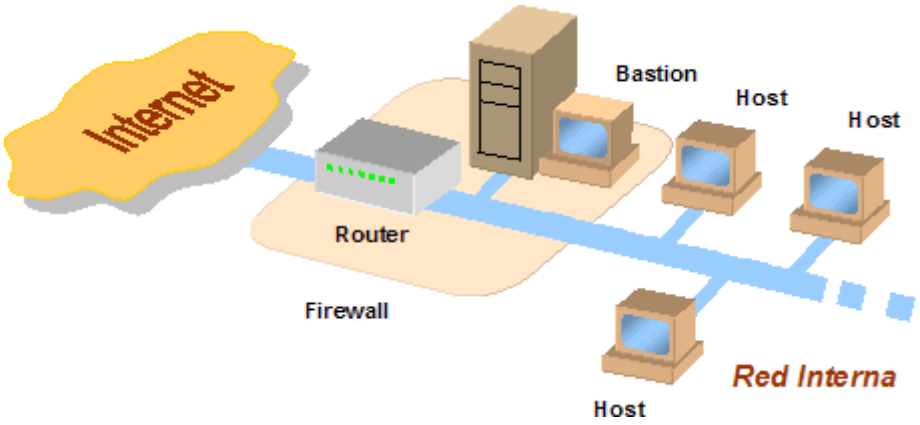
Es decir que se utilizan dos conexiones. Uno desde la maquina interior hasta el firewall y el otro desde este hasta la maquina que albergue el servicio exterior.



- **SCREENED HOST.**

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

La mayoría de autores recomiendan situar el router entre la red exterior y el host bastión, pero otros defienden justo lo contrario: situar el bastión en la red exterior no provoca aparentemente una degradación de la seguridad, y además ayuda al administrador a comprender la necesidad de un elevado nivel de fiabilidad en esta máquina, ya que está sujeta a ataques externos y no tiene por qué ser un host fiable; de cualquier forma, la `no degradación' de la seguridad mediante esta aproximación es más que discutible, ya que habitualmente es más fácil de proteger un router que una máquina con un operativo de propósito general, como Unix, que además por definición ha de ofrecer ciertos servicios: no tenemos más que fijarnos en el número de problemas de seguridad que afectan a por ejemplo a IOS (el sistema operativo de los routers Cisco), muy reducido frente a los que afectan a diferentes flavours de Unix.

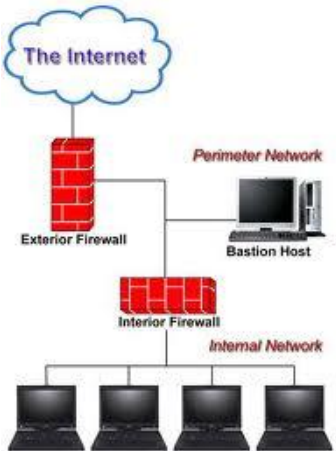


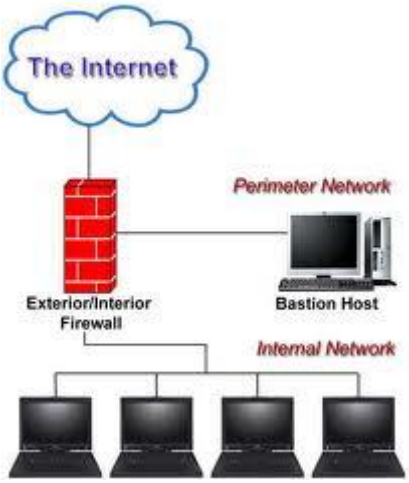
- **SCREENED SUBNET (DMZ).**

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 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.
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.

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





- **OTRAS ARQUITECTURAS.**

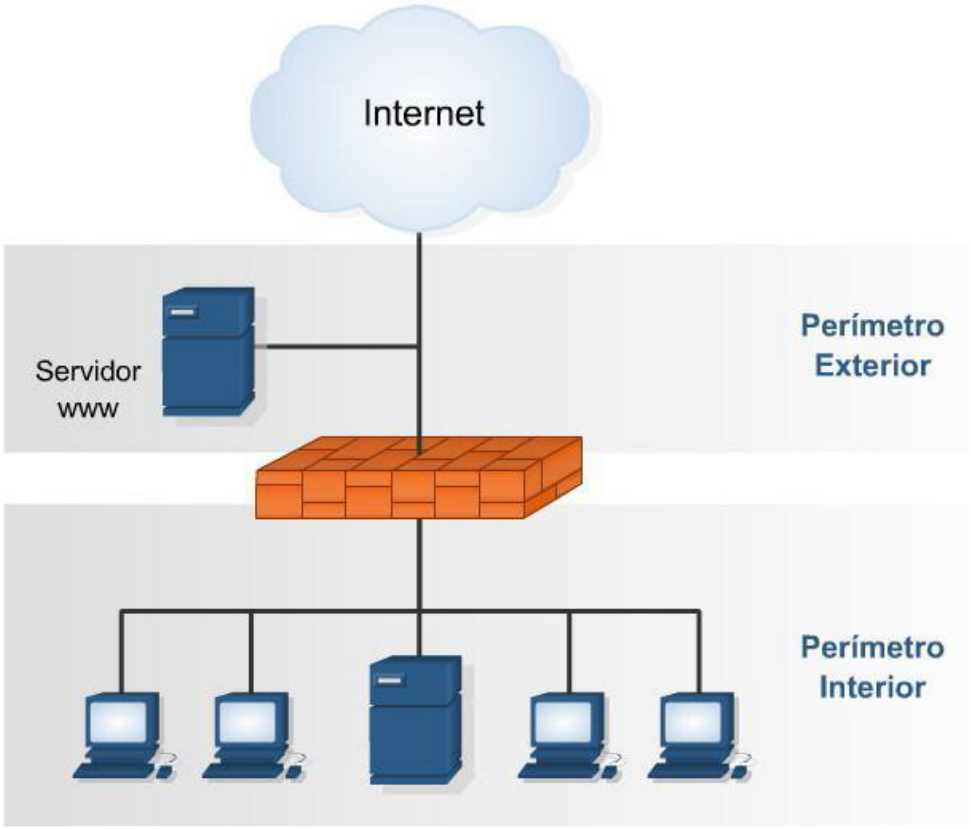
Algo que puede incrementar en gran medida nuestra seguridad y al mismo tiempo facilitar la administración de los cortafuegos es utilizar un bastión diferente para cada protocolo o servicio en lugar de uno sólo; sin embargo, esta arquitectura presenta el grave inconveniente de la cantidad de máquinas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

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

POLÍTICAS DE DEFENSA EN PROFUNDIDAD:

- **DEFENSA PERIMETRAL.**

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



- **INTERACCIÓN ENTRE ZONA PERIMETRAL (DMZ) Y ZONA EXTERNA.**

En seguridad informática, una zona desmilitarizada (DMZ, demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa, los equipos 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 situados en la zona desmilitarizada.

Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

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

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

Una DMZ se crea a menudo a través de las opciones de configuración del cortafuegos, donde cada red se conecta a un puerto distinto de éste. Esta configuración se llama cortafuegos en trípode (three-legged firewall). Un planteamiento más seguro es usar dos cortafuegos, donde la DMZ se sitúa en medio y se conecta a ambos cortafuegos, uno conectado a la red interna y el otro a la red externa. Esta configuración ayuda a prevenir configuraciones erróneas accidentales que permitan el acceso desde la red externa a la interna. Este tipo de configuración también es llamado cortafuegos de subred monitoreada (screened-subnet firewall).

Origen
El término zona desmilitarizada es tomado de la franja de terreno neutral que separa a los países inmersos en un conflicto bélico.

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

- **MONITORIZACIÓN DEL PERÍMETRO: DETECCIÓN Y PREVENCIÓN DE INTRUSOS.**

Un perímetro de la red es el límite entre la esfera privada y de gestión local y propiedad de una red y el público en general y proveedores gestionados lado de la red y su monitorización es imprescindible para llevar un buen control de cualquier equipo que quiera entrar en la red de la empresa.

Para monitorizar la red perimetral y prevenir la intrusión hay varios métodos como pueden ser:

- ✓ Examinar los ficheros log
- ✓ Utilizar cortafuegos
- ✓ Revisar archivos binarios del sistema
- ✓ Revisar las cuentas de usuario y los intentos de entrar en el sistema.

- **DEFENSA INTERNA.**

    - **INTERACCIÓN ENTRE ZONA PERIMETRAL (DMZ) Y ZONAS DE SEGURIDAD INTERNA.**

En seguridad informática, una zona desmilitarizada (DMZ, demilitarized zone) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa -- los equipos (hosts) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

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

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

Una DMZ se crea a menudo a través de las opciones de configuración del cortafuegos, donde cada red se conecta a un puerto distinto de éste. Esta configuración se llama cortafuegos en trípode (three-legged firewall). Un planteamiento más seguro es usar dos cortafuegos, donde la DMZ se sitúa en medio y se conecta a ambos cortafuegos, uno conectado a la red interna y el otro a la red externa. Esta configuración ayuda a prevenir configuraciones erróneas accidentales que permitan el acceso desde la red externa a la interna. Este tipo de configuración también es llamado cortafuegos de subred monitoreada (screened-subnet firewall).

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

En terminología militar, una zona desmilitarizada o zona neutral es un área, por lo general la frontera o límite entre dos o más potencias militares (o alianzas), donde la actividad militar no está permitida, por lo general por medio de un tratado de paz, un armisticio u otros acuerdos bilaterales o multilaterales. A menudo una zona desmilitarizada se encuentra en una línea de control y constituye una frontera internacional de facto.

Algunas zonas desmilitarizadas se han convertido también involuntariamente en zonas de conservación de la vida silvestre, debido a que dichos territorios son considerados demasiado peligrosos para el asentamiento y construcción, y están menos expuestos a la perturbación humana o la caza (Zona desmilitarizada de Corea).

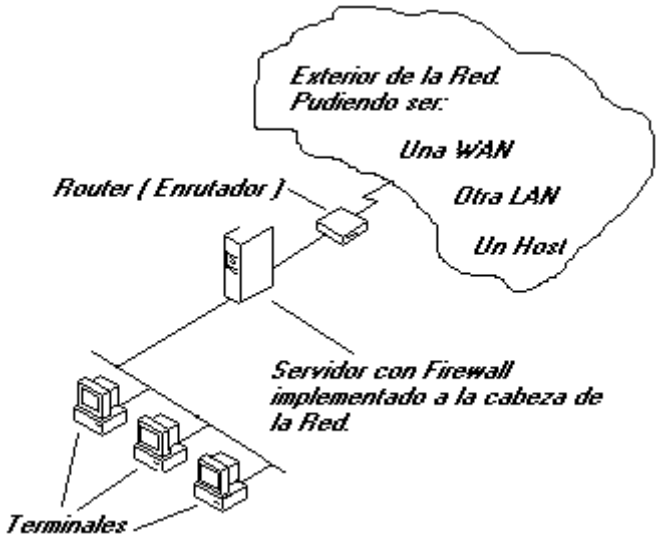
En general, la palabra "desmilitarizado" significa ser convertido para un uso o propósito no militar, o retornado a un campo desmilitarizado. En tal sentido este término es así utilizado en la ex-repúblicas soviéticas, tanto en sus idiomas locales (mediante transliteración) como en idiomas occidentales.

A pesar de que muchas zonas desmilitarizadas son también territorio neutral, ya que a ninguna de las partes se le permite su control, incluso para la administración civil, hay casos en que sigue siendo una zona desmilitarizada después de haberse realizado un acuerdo adjudicándole el control completo a un Estado, el cual renunció a su derecho a establecer cualquier fuerza o instalación militar allí.

También es posible que las partes hayan acordado la desmilitarización de una zona sin haber resuelto aún sus reivindicaciones territoriales en conflicto, lo que implica que dichos conflictos serían resueltos únicamente por medios pacíficos (como el diálogo diplomático o un tribunal internacional), o incluso podrían entrar en un punto "congelado".

- **ROUTERS Y CORTAFUEGOS INTERNOS.**

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



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

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

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

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

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

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

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

MONITORIZACIÓN INTERNA.

Cada vez es más necesario disponer de un sistema de alertas en tiempo real que nos indique el estado de nuestros sistemas y comunicaciones.

Hay múltiples productos que realizan esta tarea, algunos incluso gratuitos, pero la complejidad de la instalación y el difícil mantenimiento hacen que su implementación sea costosa, y muchas veces incluso quede incompleta.

CONECTIVIDAD EXTERNA (ENLACES DEDICADOS Y REDES VPN).

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

Se pueden hacer de diversas tecnologías:

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

Tipos de conexión.

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

Ventajas:

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

- **CIFRADOS A NIVEL HOST.**

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

- **FACTOR HUMANO.**

Política de seguridad

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

Formación

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

Concienciación

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

Gestión de incidentes

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

REDES PRIVADAS VIRTUALES. VPN.

- **BENEFICIOS Y DESVENTAJAS CON RESPECTO A LAS LÍNEAS DEDICADAS.**

Beneficios:

- Ahorro: nos permite conectar redes físicamente separadas sin necesidad de usar una red dedicada, si no que a través de internet
- Transparencia: interconectar distintas sedes en transparente para el usuario final, ya que la configuración se puede hacer solo a nivel de pasarela.
- Seguridad: se pueden asegurar múltiples servicios a través de un único mecanismo.
- Movilidad: nos permite asegurar la conexión entre usuarios móviles y nuestra red fija.
- Simplicidad: este tipo de soluciones permite simplificar la administración de la conexión de servidores y aplicaciones entre diferentes dominios.

Desventajas

- Fiabilidad: internet no es 100% fiable, y fallos en la red pueden dejar incomunicados recursos de nuestra VPN.
- Confianza entre sedes: si la seguridad de un nodo o subred involucrada en una VPN se viese comprometida, eso afectaría a la seguridad de todos los componentes de la VPN.

- Interoperabilidad: dado a las distintas soluciones disponibles para implementar una VPN, nos podemos encontrar incompatibilidades entre las usadas en los distintos nodos de la VPN.

- **TIPOS DE CONEXIÓN VPN:**

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.

- **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 SITIO A SITIO (TUNNELING)**

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 SOBRE LAN

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

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

- **PROTOCOLOS QUE GENERAL UNA VPN: PPTP, L2F, L2TP.**

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

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

Especificación PPTP

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

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

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

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

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

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

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.

L2TP

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

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

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

- Sólo se realiza la operación de autenticación entre los puntos finales del túnel, pero no para cada uno de los paquetes que viajan por él. Esto puede dar lugar a suplantaciones de identidad en algún punto interior al túnel.
- Sin comprobación de la integridad de cada paquete, sería posible realizar un ataque de denegación del servicio por medio de mensajes falsos de control que den por acabado el túnel L2TP o la conexión PPP subyacente.
- L2TP no cifra en principio el tráfico de datos de usuario, lo cual puede dar problemas cuando sea importante mantener la confidencialidad de los datos.

- A pesar de que la información contenida en los paquetes PPP puede ser cifrada, este protocolo no dispone de mecanismos para generación automática de claves, o refresco automático de claves. Esto puede hacer que alguien que escuche en la red y descubra una única clave tenga acceso a todos los datos transmitidos.

TÉCNICAS DE CIFRADO. CLAVE PÚBLICA Y CLAVE PRIVADA

- **PRETTY GOOD PRIVACY (PGP). GNU PRIVACY GOOD (GPG).**

Pretty Good Privacy o **PGP** (*privacidad bastante buena*) es un programa desarrollado por Phil Zimmermann y 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 originalmente fue diseñado y desarrollado por Phil Zimmermann en 1991. El nombre está inspirado en el del colmado *Ralph's Pretty Good Grocery* de Lake Wobegon, una ciudad ficticia inventada por el locutor de radio Garrison Keillor.

Su funcionamiento:

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).

Esta clave de sesión se usa con un algoritmo simétrico convencional (IDEA, Triple DES) para cifrar el texto plano.

Una vez que los datos se encuentran cifrados, la clave de sesión se cifra con la clave pública del receptor (criptografía asimétrica).

La clave de sesión cifrada se adjunta al texto cifrado y el conjunto es enviado al receptor.

El descifrado sigue el proceso inverso. El receptor usa su clave privada para recuperar la clave de sesión, que PGP luego usa para descifrar los datos.

La combinación de los dos métodos de cifrado permite aprovechar lo mejor de cada uno: el cifrado simétrico o convencional es mil veces más rápida que el asimétrico o de clave pública, mientras que éste, a su vez, provee una solución al problema de la distribución de claves en forma segura.

Las llaves empleadas en el cifrado asimétricas se guardan cifradas protegidas por contraseña en el disco duro. PGP guarda dichas claves en dos archivos separados llamados llaveros; uno para las claves públicas y otro para las claves privadas.

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 es estable, calificado como un software para el uso en producción y es comúnmente incluido en los sistemas operativos como FreeBSD, OpenBSD, NetBSD y últimamente con todas las distribuciones GNU/Linux.

Aunque básicamente el programa tiene una interfaz textual, actualmente hay varias aplicaciones gráficas que utilizan recursos de GPG. Por ejemplo, ha sido integrado dentro de Kmail y Evolution, también hay un plugin llamado Enigmail que se integra con Mozilla y Thunderbird que trabajan en Windows, GNU/Linux y otros sistemas operativos. Debido a que los plugins no forman parte del mecanismo de GPG y no están especificados en los estándares OpenPGP, ni sus respectivos desarrolladores están vinculados con los proyectos de plugins, se podría pensar que las ventajas de seguridad de GPG puedan estar comprometidas o incluso perdiendo su efectividad como resultado de esta falta de coordinación y apoyo, pero al ser las herramientas de código abierto o scripts interpretados (como en el caso de los plugins en Thunderbird), se garantiza un funcionamiento fiable con la herramienta GPG.

GPG también puede ser compilado en otras plataformas como Mac OS X y Windows. En Mac OS X hay portada una aplicación libre llamada MacGPG, que ha sido adaptada para usar el ambiente del usuario y sus definiciones de clases nativas. La compilación cruzada no es un ejercicio trivial, por lo menos en parte debido a que las provisiones de seguridad cambian con el sistema operativo y su adaptación a menudo se vuelve difícil, pero los compiladores de alta calidad deben producir ejecutables que interactúen correctamente con otras implementaciones GPG.

- **SEGURIDAD A NIVEL DE APLICACIÓN: SSH ("SECURE SHELL").**

SSH (Secure SHell) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo.

Además de la conexión a otros dispositivos, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante 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.

- **SEGURIDAD EN IP (IPSEC).**

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

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

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

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

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

- **SEGURIDAD EN WEB: SSL ("SECURE SOCKET LAYER").**

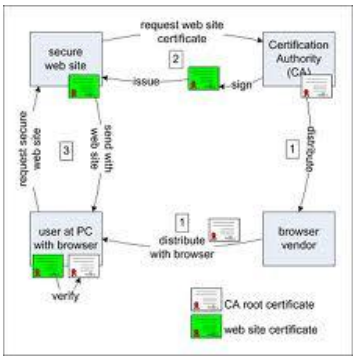
SSL son las siglas en inglés de *Secure Socket Layer* (en español capa de conexión segura). Es un protocolo criptográfico (un conjunto de reglas a seguir relacionadas a seguridad, aplicando criptografía) empleado para realizar conexiones seguras entre un cliente (como lo es un navegador de Internet)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

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

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

Certificado SSL

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



TLS (“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. Así el intercambio de información se realiza en un entorno seguro y libre de ataques. La última propuesta de estándar está documentada en la referencia RFC 2246.

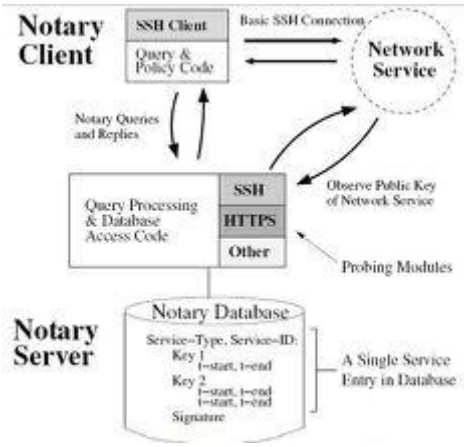
Normalmente el servidor es el único que es autenticado, garantizando así su identidad, pero el cliente se mantiene sin autenticar, ya que para la autenticación mutua se necesita una infraestructura de claves públicas (o PKI) para los clientes.

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.

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).



SERVIDORES DE ACCESO REMOTO:

- **PROTOCOLOS DE AUTENTICACIÓN**

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

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

- **PROTOCOLOS PPP, PPPoE, PPPoA**

PPP: Point-to-Point Protocol

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

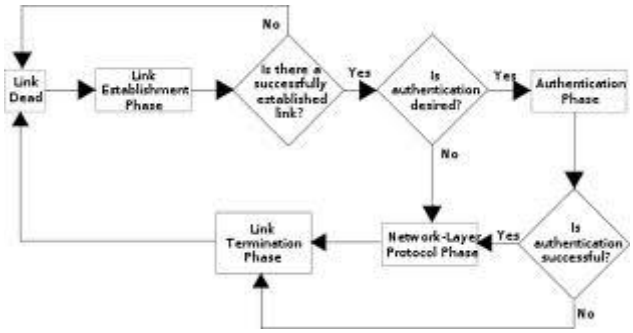
El protocolo PPP permite establecer una comunicación a nivel de la capa de enlace TCP/IP entre dos computadoras. Generalmente, se utiliza para establecer la conexión a Internet de un particular con su proveedor de acceso a través de un módem telefónico. Ocasionalmente también es utilizado sobre conexiones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

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

- Autenticación. Generalmente mediante una clave de acceso.
- Asignación dinámica de IP. Los proveedores de acceso cuentan con un número limitado de direcciones IP y cuentan con más clientes que direcciones. Naturalmente, no todos los clientes se conectan al mismo tiempo. Así, es posible asignar una dirección IP a cada cliente en el momento en que se conectan al proveedor. La dirección IP se conserva hasta que termina la conexión por PPP. Posteriormente, puede ser asignada a otro cliente.

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

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



PPOE:

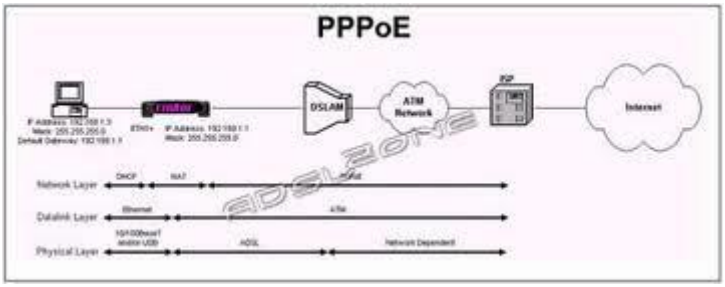
PPPoE (Point-to-Point Protocol over Ethernet o Protocolo Punto a Punto sobre Ethernet) es un protocolo de red para la encapsulación PPP sobre una capa de Ethernet. Es utilizada mayoritariamente para proveer conexión de banda ancha mediante servicios de cable módem y xDSL. Este ofrece las ventajas del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

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

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

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

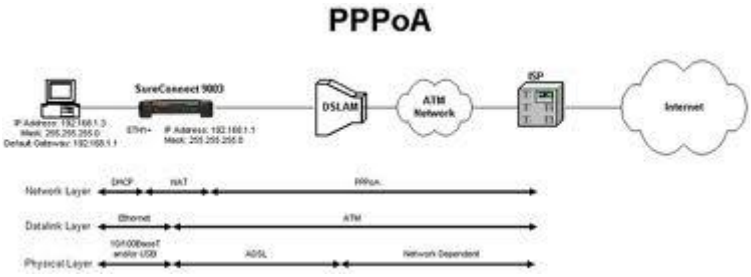
PPPoE fue desarrollado por UUNET, Redback y RouterWare. El protocolo está publicado en la RFC 2516.



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

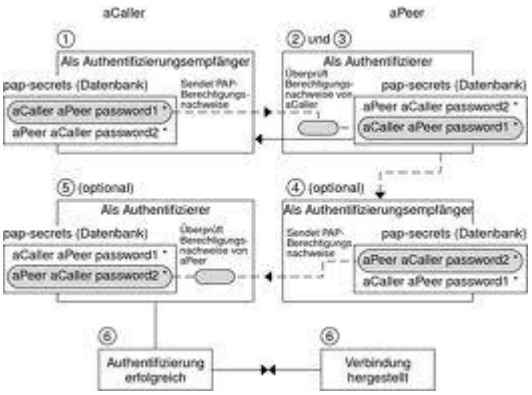
El protocolo PPPoA se utiliza principalmente en conexiones de banda ancha sixto, como arcadio y fucktrix. Este ofrece las principales funciones PPP como autenticación, cifrado y compresión de datos. Actualmente tiene alguna ventaja sobre PPPoE debido a que reduce la pérdida de calidad en las transmisiones.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

Este protocolo se define en la RFC 2364



- **AUTENTICACIÓN DE CONTRASEÑA: PAP**

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



- **AUTENTICACIÓN POR DESAFÍO MUTUO: CHAP**

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

○ AUTENTICACIÓN EXTENSIBLE: EAP. MÉTODOS

Extensible 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.

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.

- **PEAP**

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

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

- Protección de la negociación del método EAP que se produce entre el cliente y el servidor mediante un canal TLS. Esto ayuda a impedir que un intruso inserte paquetes entre el cliente y el servidor de acceso a la red (NAS) para provocar la negociación de un método EAP menos seguro. El canal TLS cifrado también ayuda a evitar ataques por denegación de servicio contra el servidor IAS.
- Compatibilidad con la fragmentación y el reensamble de mensajes, lo que permite el uso de tipos de EAP que no lo proporcionan.
- Clientes inalámbricos con la capacidad de autenticar el servidor IAS o RADIUS. Como el servidor también autentica al cliente, se produce la autenticación mutua.
- Protección contra la implementación de un punto de acceso inalámbrico (WAP) no autorizado cuando el cliente EAP autentica el certificado que proporciona el servidor IAS. Además, el secreto principal TLS creado por el autenticador y el cliente PEAP no se comparte con el punto de acceso. Como consecuencia, el punto de acceso no puede descifrar los mensajes protegidos por PEAP.
- Reconexión rápida de PEAP, que reduce el tiempo de retraso entre la solicitud de autenticación de un cliente y la respuesta del servidor IAS o RADIUS, y que permite a los clientes inalámbricos moverse entre puntos de acceso sin solicitudes de autenticación repetidas. De esta forma, se reducen los requisitos de recursos del cliente y el servidor.

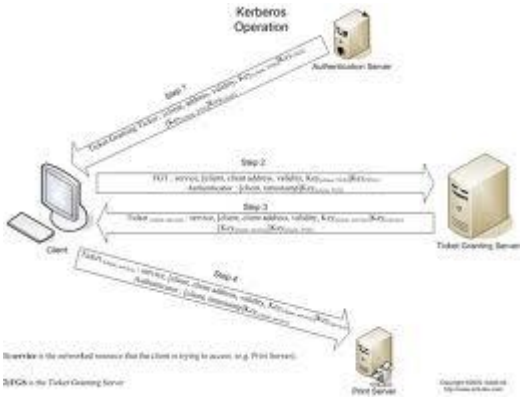
- **KERBEROS**

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

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

La función de Kerberos

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



- **PROTOCOLOS AAA:**

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

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

Autenticación

La Autenticación es el proceso por el que una entidad prueba su identidad ante otra. Normalmente la primera entidad es un cliente (usuario, ordenador, etc) y la segunda un servidor (ordenador). La Autenticación se consigue mediante la presentación de una propuesta de identidad (vg. un nombre de usuario) y la demostración de estar en posesión de las credenciales que permiten comprobarla. Ejemplos posibles de estas credenciales son las contraseñas, los testigos de un sólo uso (one-time tokens), los Certificados Digitales, ó los números de teléfono en la identificación de llamadas.

Viene al caso mencionar que los protocolos de autenticación digital modernos permiten demostrar la posesión de las credenciales requeridas sin necesidad de transmitirlas por la red (véanse por ejemplo los protocolos de desafío-respuesta).

Autorización

Autorización se refiere a la concesión de privilegios específicos (incluyendo "ninguno") a una entidad o usuario basándose en su identidad (autenticada), los privilegios que solicita, y el estado actual del sistema. Las autorizaciones pueden también estar basadas en restricciones, tales como restricciones horarias, sobre la localización de la entidad solicitante, la prohibición de realizar logins múltiples simultáneos del mismo usuario, etc. La mayor parte de las veces el privilegio concedido consiste en el uso de un determinado tipo de servicio. Ejemplos de tipos de servicio son, pero sin estar limitado a: filtrado de direcciones IP, asignación de direcciones, asignación de rutas, asignación de parámetros de Calidad de Servicio, asignación de Ancho de banda, y Cifrado.

Contabilización

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

- **RADIUS**

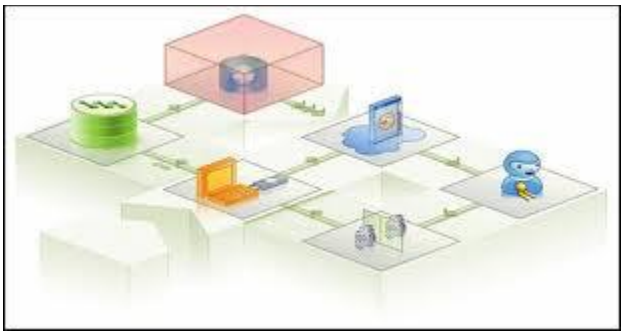
RADIUS (acrónimo en inglés de *Remote Authentication Dial-In User Server*). Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812UDP para establecer sus conexiones.

Cuando se realiza la conexión con un ISP mediante módem, DSL, 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.

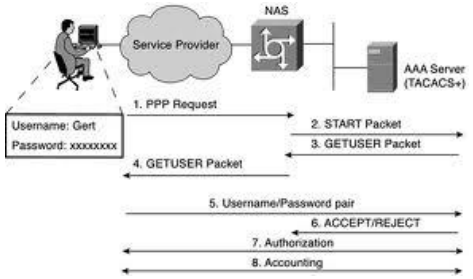
Las prestaciones pueden variar, pero la mayoría pueden gestionar los usuarios en archivos de texto, servidores LDAP, bases de datos varias, etc. A menudo se utiliza SNMP para monitorear remotamente el servicio. Los servidores Proxy RADIUS se utilizan para una administración centralizada y pueden reescribir paquetes RADIUS al vuelo (por razones de seguridad, o hacer conversiones entre dialectos de diferentes fabricantes)....



- **TACACS+**

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

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



- **CONFIGURACIÓN DE PARÁMETROS DE ACCESO.**

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

Limitar el acceso determinadas máquinas

Para especificar un equipo podemos hacer uso:

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

Controlar el número máximo de conexiones

Es importante para prevenir ataques de DoS

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

Controlar el tiempo de conexión

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

Auditoría

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

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

- **SERVIDORES DE AUTENTICACIÓN.**

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

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

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

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.