

UT3: Accesso Remoto con VPN.

SI - 2º CORSO CFGM

SMR

Índice.

1. Arquitecturas de VPN.
2. Beneficios y desventajas frente a las líneas dedicadas.
3. Técnicas de cifrado. Clave pública y clave privada:
 1. VPN a nivel de red: IPSec
 2. VPN a nivel de aplicación: SSL
4. Servidores de acceso remoto.
 1. Protocolos de autenticación.
 2. Configuración de parámetros de acceso.
 3. Servidores de autenticación.

1. Redes privadas virtuales VPN.

Una Virtual Private Network (**VPN**) establece conexiones a modo de túnel seguro sobre una infraestructura de red pública o compartida, asegurando los datos mediante la utilización de **cifrado**, **autorización** y **autenticación**.

Las empresas pueden usar redes privadas virtuales para conectar en forma segura oficinas y usuarios remotos a través de accesos a Internet económicos proporcionados por terceros, en vez de costosos enlaces WAN dedicados o enlaces de marcación remota de larga distancia.

1. Redes privadas virtuales VPN.

Tunneling.

- ✓ La mayoría de las VPNs utilizan el "Tunneling" para comunicarse a través de Internet. En esencia el Tunneling es el proceso de colocación de cada paquete de información que se envía dentro de otro paquete que hace de "envoltorio".
- ✓ El protocolo del paquete que hace de envoltorio solo es entendido por el emisor y por el receptor, en concreto, por el gateway que lo envía y por el gateway que lo recibe.
- ✓ Para los usuarios que utilizan esos routers el proceso es transparente ya que el empaquetamiento y el des-empaquetamiento se realiza en el Gateway o extremo de la VPN y no, normalmente, en el PC.

1. Redes privadas virtuales VPN.

- **Protocolos.**

- La tecnología VPN usa los túneles para crear la conexión y encriptación para proporcionar la parte segura.
- De esa manera usaremos VPN para conectarnos de manera segura al servidor VPN y de esa manera acceder al resto de servidores de la LAN.
- Los cinco protocolos más usados para crear VPNs son:
 - **PPP** Point to Point Protocol, protocolo para conexión serie entre equipos (punto a punto). Funciona a nivel de la capa de enlace.
 - **PPTP** Point to Point Tunneling Protocol expande al protocolo PPP para que pueda ser utilizado a través de Internet. Soporta encriptación y autenciación. Nivel de enlace.
 - **L2TP** Layer 2 Tunneling Protocol, encapsula datos como PPP y mejora PPTP. Nivel de enlace.
 - **IPSec** IP Secure Convierte el protocolo IP en un protocolo seguro. Funciona a nivel de red.
 - **SSL** permite el establecimiento de túneles a nivel de aplicación, que simplifica notablemente el despliegue respecto a IPSec.

1. Redes privadas virtuales VPN.

• Protocolos.

- **PPP** es un protocolo del nivel de enlace que define un mecanismo de encapsulación para transportar paquetes de varios protocolos a través de **enlaces punto a punto**. En el modo tradicional un usuario obtiene una conexión de nivel de enlace a un NAS (Network Access Server) usando alguna de las técnicas disponibles (ADSL, RDSI, ...) y entonces ejecuta PPP a través de dicha conexión. Normalmente el punto de terminación de la conexión PPP es otro dispositivo similar al de origen (ADSL, RDSI,...).
- PPP **no proporciona confidencialidad** de los datos que se envían.
- Funcionamiento de PPP: El establecimiento de un túnel PPP consta de las siguientes fases:
 - Establecimiento de la conexión: los dos extremos que se quieren comunicar negocian parámetros relativos al enlace. El protocolo encargado de esta negociación se llama LCP. Entre otras cosas se ponen de acuerdo sobre el método de autenticación que van a usar los extremos, el tamaño de los datagramas, etc.
 - Autenticación: existen dos posibles métodos a usar en PPP: **PAP y CHAP**. En el apartado de protocolos de autenticación se explican con más detalle.
 - Configuración de la red: se negocian parámetros dependientes del protocolo de red que se vaya a negociar. Para nosotros será IP, por lo que en esta fase se puede **asignar una dirección IP y servidor DNS** al extremo que quiere establecer el túnel.
 - Transmisión: Intercambio de los información de la red.
 - Terminación: finalización de la conexión.

1. Redes privadas virtuales VPN.

• Protocolos.

- **PPTP** es un protocolo desarrollado por Microsoft para implementar VPN. Es una extensión de PPP que permite el intercambio seguro de datos entre un servidor VPN y un cliente VPN. Está en desuso y no recomendado debido a que su seguridad ha sido completamente rota.
- **L2TP** es el protocolo que debería sustituir a PPTP. Se creó para corregir las deficiencias de PPTP y L2F que es otro protocolo de tunelización de Cisco.
- Normalmente lleva conexiones PPP dentro de un túnel L2TP, por eso será necesario configurar un túnel PPP cuando queramos crear una conexión L2TP.
- En cuanto a los mecanismos de autenticación, utiliza PAP o CHAP igual que PPP.
- Los dos extremos del túnel L2TP se llaman LAC (L2TP Access Concentrator) y LNS (L2TP Network Server).
- L2TP no presenta unas características criptográficas especialmente robustas. Por esta razón se recomienda instalar y configurar **L2TP junto con IPSec.**

1. Redes privadas virtuales VPN.

- **Protocolos.**

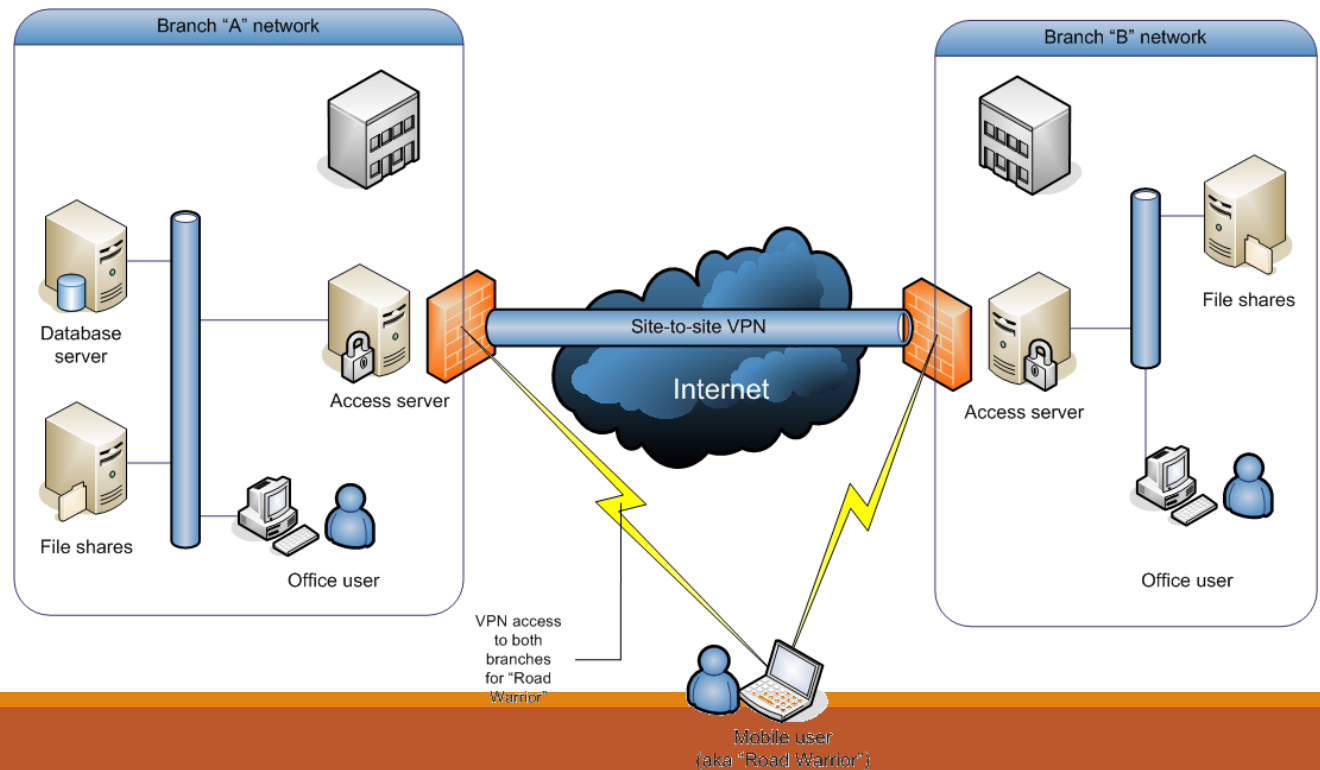
- **L2TP/IPSec** es el protocolo que debería sustituir a PPTP. Se creo para corregir las deficiencias de PPTP y L2F que es otro protocolo de tunelización de Cisco.
- Normalmente lleva conexiones PPP dentro de un túnel L2TP, por eso será necesario configurar un túnel PPP cuando queremos crear una conexión L2TP.
- En cuanto a los mecanismos de autenticación, utiliza PAP o CHAP igual que PPP.
- Los dos extremos del túnel L2TP se llaman LAC (L2TP Access Concentrator) y LNS (L2TP Network Server).
- L2TP no presenta unas características criptográficas especialmente robustas. Por esta razón se recomienda instalar y configurar **L2TP junto con IPSec.**

1. Redes privadas virtuales

Arquitecturas VPN.

Hay tres arquitecturas básicas en la configuración de VPN:

1. **De acceso remoto**, host to gateway, host to LAN o road warrior.
2. **De conexión de sitios**, punto a punto, extremo a extremo o gateway to gateway.
3. **VPN interna o de LAN**. Poco utilizada. Uno de sus usos es acceso Wifi dentro de la propia red.



1. Redes privadas virtuales

Arquitecturas VPN.

1. De acceso remoto, **host to gateway**, host to LAN o **road warrior**.

1. Se utiliza para responder a las necesidades de acceso de empleados trabajando fuera de la empresa (***teletrabajo***), usuarios móviles, tráfico de extranet de cliente a empresa.
2. Cuando se realiza una conexión VPN de este tipo, ***el usuario remoto podría tener acceso a todos los recursos de la red*** (carpetas compartidas, impresoras, llamadas VoIP internas) como si físicamente estuviera en la LAN de la oficina, siempre y cuando la política de control de acceso configurada para la VPN así lo permita.
3. En una VPN de acceso remoto la configuración de la conexión **no es estática**, sino que ***la conexión VPN se puede habilitar y deshabilitar***.
4. La VPN de acceso remoto admite arquitectura cliente/servidor en la que el cliente (host remoto) obtiene acceso seguro a la red corporativa a través de un **servidor VPN** en el perímetro de la red. El cliente requiere:
 1. Conexión a Internet, bien a través de ADSL o a través de la red de telefonía móvil.
 2. En la mayoría de las implementaciones el cliente necesitará un software de **cliente de VPN** en el dispositivo que utilice (ordenador, tablet, móvil, ...).

1. Redes privadas virtuales

Arquitecturas VPN.

1. **De conexión de sitios**, punto a punto, extremo a extremo o gateway to gateway.
 1. Se utiliza para **conectar redes enteras** entres sí, por ejemplo, para conectar una sucursal a la red de la oficina central de una empresa. Antiguamente se utilizaban conexiones punto a punto, líneas alquiladas y que eran privadas. Ahora todas las empresas disponen de acceso a Internet por lo que utilizan una red pública para realizar dichas conexiones.
 2. En este tipo de VPN **requiere de dos dispositivos, gateways VPN**, uno en cada oficina a conectar que se configuran y dicha configuración permanece estática, permanente.
 3. Para los equipos en cada una de las redes a conectar, la existencia de la VPN será transparente.
 4. Cuando un equipo en una red quiera comunicarse con un equipo en la otra red, su gateway VPN será el responsable de encapsular y cifrar el tráfico, colocarlo en el túnel VPN que lo conecta con el otro peer a través de Internet de manera segura. El otro gateway será responsable de descifrar y desencapsular el tráfico y enviarlo al host destino en la red interna.

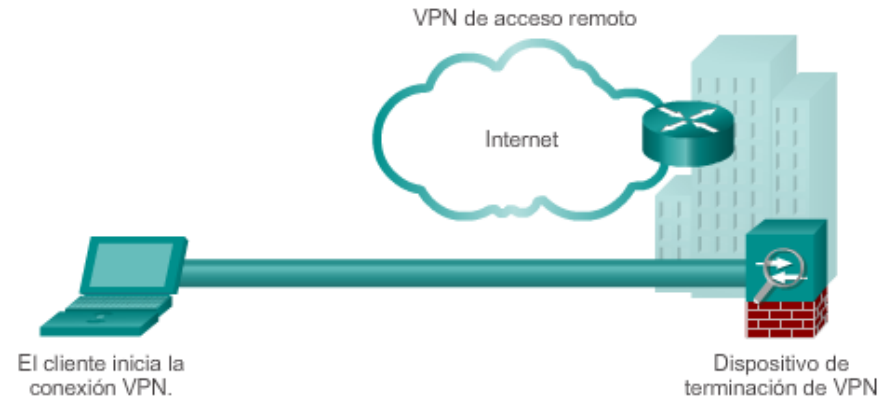
1. Redes privadas virtuales

Arquitecturas VPN.

VPN de sitio a sitio



VPN de acceso remoto



1. Redes privadas virtuales VPN.

Soluciones VPN.

- Existen diferentes formas de que una organización implemente una VPN. Cada fabricante o proveedor ofrece diferentes tipos de soluciones VPN. La empresa tendrá que decidir la que más le conviene. Las opciones son:
 - VPN en Firewall (UTM)
 - VPN de router.
 - VPN en Sistemas Operativos.
 - VPN de aplicación.
 - VPN proporcionada por un proveedor de servicios.

1. Redes privadas virtuales

Soluciones VPN.

- **VPN en Firewall (UTM)**

- Los Firewall además del filtrado de paquetes pueden proporcionar servicios de VPN.
- Simplifica la arquitectura de red al establecer un único punto de control y acceso a la red interna. Tiene la desventaja de que el firewall se convierte en un dispositivo más complejo lo que implica mayor cuidado en su configuración.
- Ejemplos:
 - Libres: IPCop, pfSense, Untangle, Endian, ...
 - Proprietarios: Cisco ASA - Adaptive Sercurity Appliance, Fortigate, ...

- **VPN de router.**

- Muchos modelos de router pueden incluir entre sus funciones la de servidor VPN, tanto en modelos SOHO que lo ofrecen como funcionalidad adicional, como routers empresariales como los de Cisco. Ojo: Cisco ASA es un producto específico de UTM, no sólo router.

1. Redes privadas virtuales VPN.

Soluciones VPN.

- **VPN de Sistema Operativo.**

- Algunos SO como Windows Server incluyen servicios de VPN integrados lo que permite mejorar los sistemas de autenticación por ejemplo, pero por el contrario hacemos que el servicio VPN sea vulnerable a las propias vulnerabilidades del SO.

- **VPN de aplicación**

- Se trata de software de aplicación específico de VPN que se puede instalar en un SO añadiendo al mismo dicha funcionalidad.
- Ejemplos:
 - Software libre: Cloudvpn, Openswan, OpenVPN (muchos de los firewalls mencionados en realidad son distribuciones de GNU/Linux que incorporan este software).
 - Propietarios: CheckPoint VPN-1, MS Frontend Unified Access Gateway.

1. Redes privadas virtuales VPN.

Soluciones VPN.

- **VPN de un proveedor de servicios.**
 - Todas las que hemos mencionado antes son soluciones privadas, que las empresas/particulares deben instalar, configurar y mantener.
 - Una alternativa consistiría en contratar un proveedor de servicio VPN desde Internet.
 - Existen diferentes tarifas en función de la ubicación de la empresa, número de países a conectar, SO de los equipos cliente, o funcionalidades adicionales requeridas.
 - Aquí se pueden ver algunas <http://www.serviciovpn.com/>

1. Redes privadas virtuales VPN.



Soluciones VPN.

- **Clientes VPN.**

- **OpenVPN**, cliente VPN de software libre. No funciona con algunos servidores VPN comerciales propietarios.
- **Cisco AnyconnectVPN**, cliente VPN para conectarse a redes con servidor VPN del fabricante Cisco. El cliente es gratuito.
- **Forticlient**: permite conectarse a remotamente a servidores VPN Fortigate.
- **LogMeIn Hamachi**: permite desplegar de manera casi inmediata conexiones VPN entre dos equipos cualesquiera conectados a Internet. No requiere de la configuración ni contratación de ningún servidor VPN. Las conexiones se realizan a través de los servidores de Hamachi.



1. Redes privadas virtuales VPN.


Soluciones VPN.



Centro de redes y recursos compartidos

Panel de control > Redes e Internet > Centro de redes y recursos compartidos




Conexiones: Ethernet



Cambiar la configuración de red

 **Configurar una nueva conexión o red**
Configurar una conexión de banda ancha, de acceso telefónico o VPN; o bien configurar un enrutador o punto de acceso.








  **Configurar una conexión o red**

Elegir una opción de conexión

-  **Conectarse a Internet**
Configurar conexión a Internet de banda ancha o de acceso telefónico.
-  **Configurar una nueva red**
Configura un enrutador o un punto de acceso nuevos.
-  **Conectarse a un área de trabajo**
Configurar una conexión de acceso telefónico o VPN a su área de trabajo.

  **Conectarse a un área de trabajo**

¿Cómo desea conectarse?

-  **Usar mi conexión a Internet (VPN)**
Conectarse mediante una conexión a una red privada virtual (VPN) a través de Internet.
 —  — 
-  **Llamar directamente**
Conectarse directamente a un número de teléfono sin usar el Internet.
 — 

Cancelar

2. Beneficios y desventajas frente a líneas dedicadas.

Beneficios.

1. Las VPN reducen los costes de explotación al utilizar líneas públicas en vez de alquiladas para realizar conexiones punto a punto.
2. Incrementan la seguridad (CIAN).
3. Son fáciles de desplegar.

Desventajas.

1. Se necesita mayor potencia de cálculo ya que la operación de cifrado consume muchos recursos.
2. Requieren tener acceso a Internet disponible , ya que es la red básica de transporte sobre la que se establece el túnel.
3. Tiene algunos problemas de implementación como, por ejemplo, la convivencia con NAT.
4. Necesita control y supervisión adicional, lo que es más trabajo para el administrador de la red.

Técnicas de cifrado. Clave pública y privada.

Confidencialidad:

- En una VPN los datos privados se están enviando a través de una red pública por lo que la confidencialidad de los mismos es fundamental.

Cifrado:

- La confidencialidad de los datos se consigue como ya sabemos mediante el cifrado, convertir texto legible en texto sólo legible por las entidades que se quieren comunicar.
- El cifrado se consigue con: algoritmos de cifrado + claves.
- El algoritmo es una secuencia matemática de pasos que combina el mensaje en claro con la clave proporcionada, de manera que se obtiene el texto ilegible.
- El grado de seguridad dependerá de la longitud de la clave de cifrado y de la robustez del algoritmo.

Técnicas de cifrado. Clave pública y privada.

Algoritmos de cifrado:

- Cifrado simétrico: recordad que se ambos extremos conocen el algoritmo utilizado y la clave, que será la misma para cifrar y para descifrar. Algoritmos de este tipo: DES, 2DES, AES.
- Cifrado asimétrico: en este caso el algoritmo también es el mismo, pero se dispondrá de una pareja de claves, llamadas pública y privada, y lo si se cifra con una se descifrá con la otra. La clave privada sólo la puede tener el propietario, mientras que la pública la posee cualquiera. Algoritmos de este tipo: RSA, DSA

Intercambio de claves:

- Existía un problema con el intercambio de claves que se resolvía con el algoritmo o método de Diffie-Hellman (DH).
- El grado de seguridad dependerá de la longitud de la clave de cifrado y de la robustez del algoritmo.

Técnicas de cifrado. Clave pública y privada.

Integridad y autenticación de los datos:

- La integridad garantiza que los datos no han sido modificados durante el tránsito por la red pública.
- La autenticación verifica la identidad del origen de los datos que se envían.
- Para verificar ambas se utilizan los algoritmos de hash o resumen: MD5 y SHA.
- El emisor utilizará un algoritmo de hash junto con una clave para generar un resumen de lo que quiera enviar. La clave que se utilizará será la clave privada del emisor. El receptor recibirá dicho resumen y lo recalculará a partir del original utilizando la clave pública del emisor.
- Si obtiene el mismo resumen que el recibido, sabe que solo el emisor lo pudo haber generado. De este modo se garantiza la autenticación del emisor.
- Si el mensaje ha sido modificado, el resumen producido es distinto. De este modo se garantiza la integridad.

VPN a nivel de red: IPSec.

Características de IPSec.

- IPSec es un framework de estándares abiertos que especifica las reglas para realizar comunicaciones seguras, utilizando los algoritmos de seguridad ya existentes.
- IPSec va a proporcionar confidencialidad e integridad de los datos y autenticación del origen (CIA).
- IPSec funciona en la capa de red por lo que protege y autentica paquetes IP.

VPN a nivel de red: IPSec.

Servicios de seguridad de IPSec.

- Confidencialidad (cifrado).
 - En una VPN los datos privados se están enviando a través de una red pública por lo que la confidencialidad de los mismos es fundamental.
- Integridad de los datos.
 - Además es importante garantizar que los datos no han sido modificados durante el tránsito por la red pública.
- Autenticación.
 - Se trata de verificar la identidad del origen de los datos que se envían.
 - IPSec utiliza IKE (Internet Key Exchange) para autenticar a los usuarios.
- Protección antireproducción.
 - Permite descartar paquetes repetidos garantizando que cada paquete es único. Sirve para evitar la suplantación de identidad.

VPN a nivel de red: IPSec.

Protocolos IPSec.

- Los dos protocolos principales del framework IPSec son:
 - Authentication Header (AH)
 - No proporciona confidencialidad.
 - Proporciona integridad y autenticación de los paquetes IP que se transmiten entre dos sistemas.
 - Protección poco eficaz.
 - Encapsulated Secure Payload (ESP)
 - Proporciona confidencialidad mediante el cifrado de paquetes IP.
 - Proporciona autenticación del origen de los paquetes IP además de integridad.

VPN a nivel de red: IPSec.

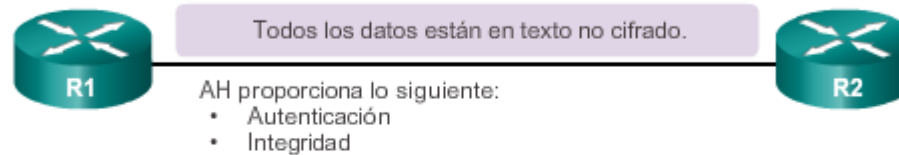
Configuración de protocolos IPSec.

- Los componentes de configuración de IPSec serán :
 - Protocolo IPSec elegido:
 - Se podrá elegir entre: AH, ESP o ESP+AH.
 - Normalmente se seleccionará ESP o ESP+AH pues AH no aporta confidencialidad.
 - Confidencialidad.
 - Se deberá elegir el algoritmo de cifrado para proporcionar esta propiedad.
 - Las opciones suelen ser: DES, 3DES, AES.
 - Integridad.
 - Se selecciona alguno de los algoritmos de hash MD5 o SHA.
 - Autenticación.
 - Se refiere a la manera en la que se autenticarán entre si los extremos participantes en la VPN. Podrá ser PSK o firmas RSA.
 - Grupo Diffie-Hellman.
 - De qué manera se va establecer la clave secreta para cifrado entre peers.

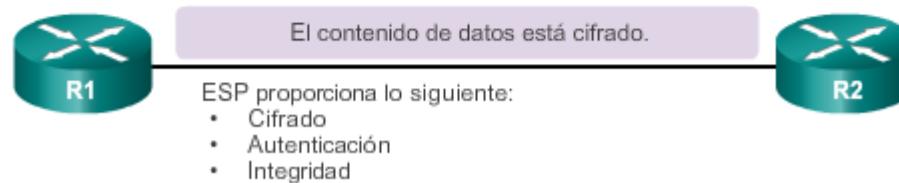
VPN a nivel de red: IPSec.

Marco del protocolo IPSec

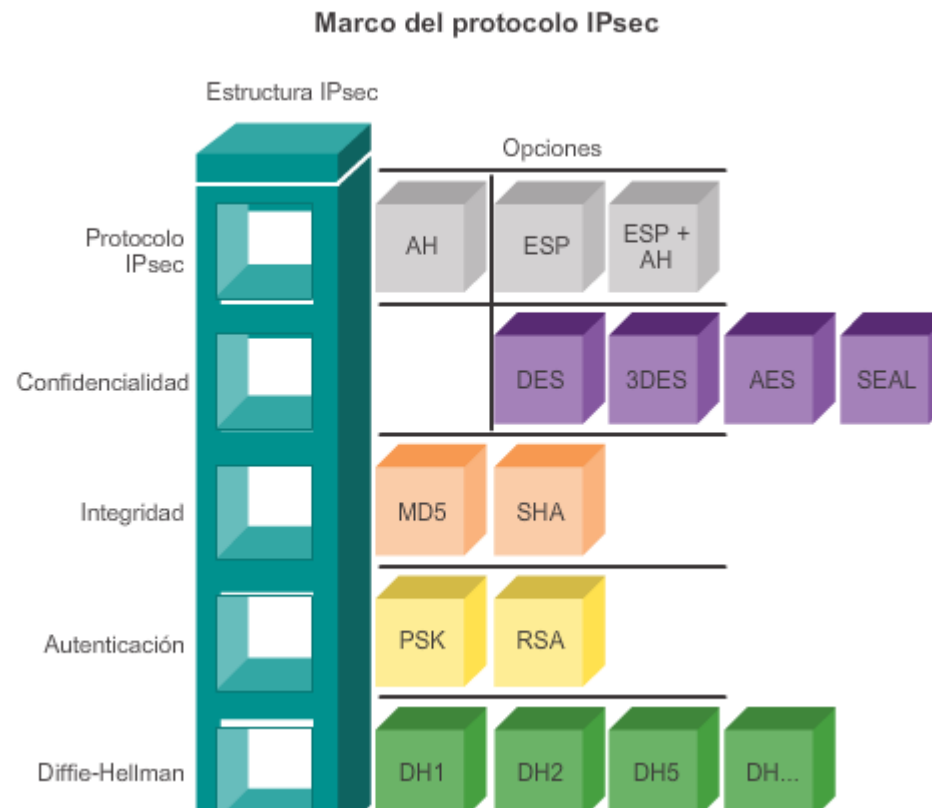
Encabezado de autenticación



Contenido de seguridad encapsulado



VPN a nivel de red: IPSec.



VPN a nivel de red: IPSec.

IKE

- AH y ESP están diseñados para ser independientes de las claves utilizadas en los algoritmos criptográficos.
- IPSec necesita algún mecanismo para la creación y administración de las claves de forma automática. Los participantes en la VPN necesitarán ponerse de acuerdo sobre los tipos de cifrado y los algoritmos de autenticación que van a utilizar para establecer una comunicación segura. Y además deberá autenticarse.
- Todo esto se realizará de manera automática gracias al mecanismo de administración de claves IKE (Internet Key Exchange).
- Cada pareja que participa en una VPN formarán lo que se llama una **SA (Security Association)**.
- IKE se encargará no sólo de la administración de las claves sino que también del establecimiento de la conexión.
- Para el intercambio de claves usará Diffie-Hellman.

VPN a nivel de red: IPSec.

IKF

○



VPN a nivel de red: IPSec.

Autenticación de participantes en la VPN.

- IPSec permite el intercambio y la comprobación de identidades sin exponer la información intercambiada. Existen dos métodos de autenticación de “peers” en IPSec:
 - Pre-shared Key (PSK):
 - Clave secreta compartida entre dos peers.
 - La clave no se envía sino que se envía el hash para que aquella no sea revelada.
 - No es viable cuando hay más de dos participantes en la VPN, ya que cada par necesita su propia clave secreta compartida.

VPN a nivel de red: IPSec.

Autenticación de participantes en la VPN.

- Existen dos métodos de autenticación de “peers” en IPSec:
 - Certificados digitales X.509:
 - Para los escenarios con más de un participante se pueden utilizar certificados digitales, de manera que un participante demuestra quien es con la posesión de una clave privada. Para ello distribuirá su clave pública mediante un certificado digital.
 - Para que se garantice la autenticidad de dicha clave pública y certificado se requiere de la existencia de una PKI por lo que aparecerá la figura de la CA (Autoridad de Certificación).
 - Firmas RSA. Se requerirá de una CA (Autoridad de Certificación) en la que los dos peers confíen y que emitirá certificados digitales para cada uno de ellos.
 - Cada peer generará un hash que cifrará con su clave privada y sólo se podrá descifrar con su clave pública. Este enviará al otro peer su clave pública junto con el certificado digital para garantizar que es él y no otro que le está suplantando.

VPN a nivel de red: IPSec.

Autenticación de participantes en la VPN.

- Certificados digitales X.509 y firmas RSA:
 - Para los escenarios con más de un participante se pueden utilizar certificados digitales, de manera que un participante demuestra quien es con la posesión de una clave privada. Para ello distribuirá su clave pública mediante un certificado digital.
 - Para que se garantice la autenticidad de dicha clave pública y certificado se requiere de la existencia de una PKI por lo que aparecerá la figura de la CA (Autoridad de Certificación).
- Grupos XAuth.:
 - Consiste en añadir un usuario y una contraseña a los certificados digitales anteriores.
 - Necesitaremos un servidor de autenticación, como por ejemplo un Radius para poder autenticar a los usuarios.

VPN a nivel de red: IPSec.

Modos de funcionamiento de IPSec.

- Modo transporte.
 - No se autentica ni cifra la cabecera IP, sólo los datos de las capas superiores.
- Modo túnel.
 - Se autentica y/o cifra el paquete IP completo.

VPN a nivel de red: IPSec.

L2TP/IPSec.

- Como se explicó en el apartado correspondiente, debido a la falta de confidencialidad de L2TP es habitualmente implementado con IPSec. Esto es llamado L2TP/IPSec.
- El proceso para establecer una VPN L2TP/IPSec es el siguiente:
 1. Negociación de asociación de seguridad (SA) utilizando IKE. Para ello se utiliza el puerto **UDP/500**. Se puede usar PSK, claves públicas o certificados X.509.
 2. Establecimiento de la comunicación ESP en modo transporte.
 3. Negociación y establecimiento de un túne L2TP entre los dos extremos de la SA. L2TP usa el puerto **UDP/1701**.

VPN a nivel de red: IPSec.

- **L2TP/IPSec.**

- Cuando el proceso es completado, los paquetes L2TP entre los dos extremos son encapsulados por IPSec. Por lo tanto estos son ocultos por IPSec por lo que no sería necesario abrir el puerto UDP 1701 cuando se usa junto con este último protocolo. (COMPROBAR!!!!)
- Otro punto importante a aclarar es la distinción entre los conceptos de túnel y canal seguro.
 - Túnel: permite que los paquetes de una red sean transportados sobre otra red (Internet en nuestro caso). Aquí el túnel L2TP/PPP transporta paquetes sobre IP.
 - Canal seguro: hace referencia a una conexión con confidencialidad. Así IPSec proporciona un canal seguro y L2TP proporciona el túnel.

Protocolos de autenticación. Servidores de Acceso Remoto.

- PAP (Password Authentication Protocol)
 - Protocolo de autenticación para autenticar un usuario contra un servidor de acceso remoto o contra un ISP.
 - PAP transmite contraseñas en ASCII y sin cifrar por lo que se considera inseguroEnvía usuario y contraseña del usuario
- CHAP (Challenge Handshake Authentication Protocol)
 - Usos similares a los de PAP.
 - Versión de Microsoft MS-CHAP (MS-CHAP2 para Windows 7).
 - CHAP verifica periódicamente la identidad del cliente remoto usando un intercambio de información en tres etapas. La verificación se basa en un secreto compartido (como una contraseña).
 - Tras establecerse el enlace, el agente autenticador solicita autenticación al usuario.
 - El usuario el valor hash del secreto compartido.
 - El autenticador verifica si coincide con su propio cálculo. Si el valor coincide, el autenticador informa de la verificación, de lo contrario terminaría la conexión.
 - A intervalos aleatorios el autenticador manda una nueva «comprobación de veracidad», con lo que se repite el proceso.