español

MOVET

Modernisation of VET through
Collaboration with the Industry

Ivan Pravda

Seguridad de la red

Erasmus+

El presente proyecto ha sido financiado con el apoyo de la Comisión Europea. Esta publicación (comunicación) es responsabilidad exclusiva de su autor. La Comisión no es responsable del uso que pueda hacerse de la información aquí difundida.

Título: Seguridad de la red
Autor: Ivan Pravda
Traducido por: Juan Antonio Ortega
Publicado por: České vysoké učení technické v Praze
Fakulta elektrotechnická
Dirección de contacto: Technická 2, Praha 6, Czech Republic
Número de teléfono: +420 224352084
Print: (only electronic form)
Número de páginas: 41
Edición: Primera edición, 2019

MoVET
Modernisation of VET through
Collaboration with the Industry

https://movet.fel.cvut.cz

El presente proyecto ha sido financiado con el apoyo de la Comisión Europea.
Esta publicación (comunicación) es responsabilidad exclusiva de su autor. La Comisión no es responsable del uso que pueda hacerse de la información aquí difundida.

NOTAS EXPLICATIVAS

	Definición
	Interesante
	Nota
	Ejemplo
	Resumen
	Ventajas
	Desventajas

ANOTACIÓN

Este módulo formativo trata las capacidades de seguridad en la red con un enfoque en Redes Privadas Virtuales (VPN, Virtual Private Networks). Se definen una serie de conceptos básicos, incluyendo la descripción de algunos componentes básicos y conceptos de VPNs. Además, se enfatiza en la explicación del protocolo IPSec y en los mecanismos que permiten la implementación de la seguridad de redes privadas, como el método ISAKMP/IKE y el mecanismo de intercambio de claves Diffie-Hellmann. Por último, pero no por ello menos importante, el módulo contiene una serie de ejemplos prácticos y soluciones para ellos. La parte final del módulo describe la firma electrónica.

OBJETIVOS

Al estudiar el módulo, los lectores tendrán una visión general del problema de la seguridad de las redes informáticas y las soluciones que proporcionan las redes privadas virtuales. El tema es muy actual, ya que el concepto de seguridad está estrechamente relacionado con los delitos cibernéticos. Se hace hincapié no sólo en la aclaración de la terminología en este ámbito, sino también en la explicación de los fundamentos en que se basan los procedimientos básicos y se complementa con ejemplos concretos de aplicación. La parte final explica el concepto de firma electrónica y su aplicación en la vida cotidiana.

LITERATURA

[1] Deal, Richard. The Complete Cisco VPN Configuration Guide. Cisco Press, 2005. 1032 páginas. ISBN: 978-1-58705-204-0.

[2] Cisco Systems. Clientless SSL VPN (WebVPN) on Cisco IOS with SDM Configuration Example. 2009. https://www.cisco.com/c/en/us/support/docs/security/ssl-vpn-client/70663-webvpn.html [online]

[3] RFC4301 - Security Architecture for the Internet Protocol http://tools.ietf.org/html/rfc4301 [online]

[4] RFC4302 - IP Authentication Header http://tools.ietf.org/html/rfc4302 [online]

[5] RFC4303 - IP Encapsulating Security Payload (ESP) http://tools.ietf.org/html/rfc4303 [online]

[6] RFC4308 - Cryptographic Suites for IPsec http://tools.ietf.org/html/rfc4308 [online]

[7] RFC4364 - BGP/MPLS IP Virtual Private Networks (VPNs). http://tools.ietf.org/html/rfc4364 [online]

[8] RFC4835 - Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) http://tools.ietf.org/html/rfc4835 [online]

[9] RFC5246 - The Transport Layer Security (TLS) Protocol Version 1.2. http://tools.ietf.org/html/rfc5246 [online]

Indice

1 Red Privada Virtual - definición de conceptos básicos

DEFINICIÓN FORMAL

Una Red Privada Virtual **VPN** (*Virtual Private Network*) es un entorno de comunicación en el que se controla el acceso a la comunicación entre entidades individuales. El entorno de comunicación se crea sobre la base de una forma predefinida de distribución del medio de comunicación común, que además puede prestar servicios de red de forma no exclusiva.

DEFINICIÓN NO FORMAL

Una Red Privada Virtual **VPN** (*Virtual Private Network*) es una red no pública (informática) construida dentro de una infraestructura de red pública, como Internet. Normalmente, esta red proporciona una conexión segura de sucursales remotas o suscriptores a la red principal.

A partir de las definiciones anteriores, se puede afirmar brevemente que una VPN es esencialmente una red lógica dentro de una infraestructura pública compartida. Proporciona el mismo rendimiento y las mismas reglas que cualquier **LAN** (*red de área local, "Local Area Network"*) privada.

Un problema importante con el uso de las VPN es garantizar su seguridad y la prestación de servicios con la calidad requerida y con respecto a los indicadores de calidad de *servicio* (**QoS**) servicio **QoS** (*Quality of Service*). Ambos requisitos no se refieren a la infraestructura de red basada en **TCP/IP** (*Transmission Control Protocol/Internet Protocol*).

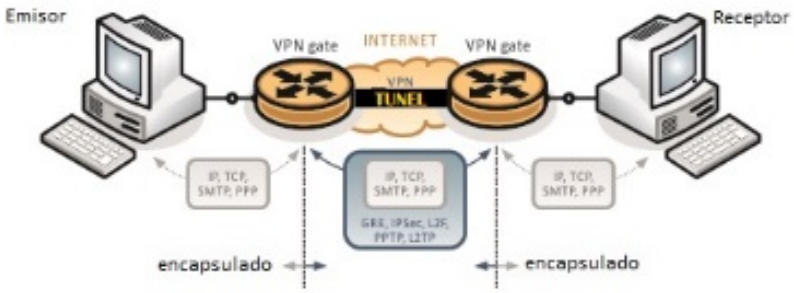
Los requisitos de seguridad se abordan mediante el diseño de la VPN:

- tunelado,
- cifrado,
- autenticación y
- control de acceso.

El término "tunelado" se entiende como un proceso de encapsulación de un paquete original en otro. Ninguno de los dispositivos intermedios puede leer el paquete original durante su transmisión.

La razón del uso de mecanismos de tunelado es garantizar la seguridad y crear un mecanismo de transporte entre lugares geográficamente remotos. La encapsulación puede, por ejemplo, utilizar **GRE** (*Generic Routing Encapsulation*), **IPSec**

(*Internet Protocol Security*), **L2F** (*Layer 2 Forwarding*), **PPTP** (*Point-to-Point Tunneling Protocol*), **L2TP** (*Layer 2 Tunneling Protocol*).



Mecanismo de túnel en VPN

Sin embargo, el tunelado también puede utilizarse para adecuar protocolos incompatibles, como la interconexión LAN con **NetBEUI** (*NetBIOS Extended User Interface*) o **IPX** (*Internetwork Packet Exchange*) a través de Internet (protocolo IP).

En realidad, es posible implementar el llamado Split Tunneling, donde el cliente puede comunicarse simultáneamente dentro de la VPN y con Internet.

El término "cifrado" se refiere al proceso de garantizar la confidencialidad y la integridad de los datos. Técnicamente hablando, significa encapsular los datos en un sobre seguro, es decir, cifrarlos con una clave secreta.

La autenticación dentro de las VPNs asegura la verificación de la autenticidad. Se garantiza que los datos proceden realmente del origen indicado.

Se utilizan esquemas basados en claves compartidas, como **CHAP** (*Challenge Handshake Authentication Protocol*), **RSA** (*Rivest-Shamir-Adleman*) y otros. Más allá de la seguridad, estos sistemas también proporcionan integridad de datos.

El control de acceso permite restringir el acceso o la intrusión de usuarios no autorizados asociados con el proceso de verificación de los derechos de un usuario en particular.

2 Componentes VPN

Las VPNs utilizan protocolos de seguridad de cifrado de túneles para proporcionar protección de rastreo de paquetes, garantizan una autenticación adecuada y declaran la integridad de los mensajes, es decir, la integridad de los mismos.

Los componentes necesarios para construir una conexión VPN son:

- una LAN existente o un terminal independiente (como un PC, un portátil, un netbook, etc.)
- conexión a Internet disponible,
- Gateways (o pasarelas) VPN (por ejemplo, routers, cortafuegos, concentradores VPN), y
- software adecuado (Software) necesario para construir y gestionar los túneles VPN.

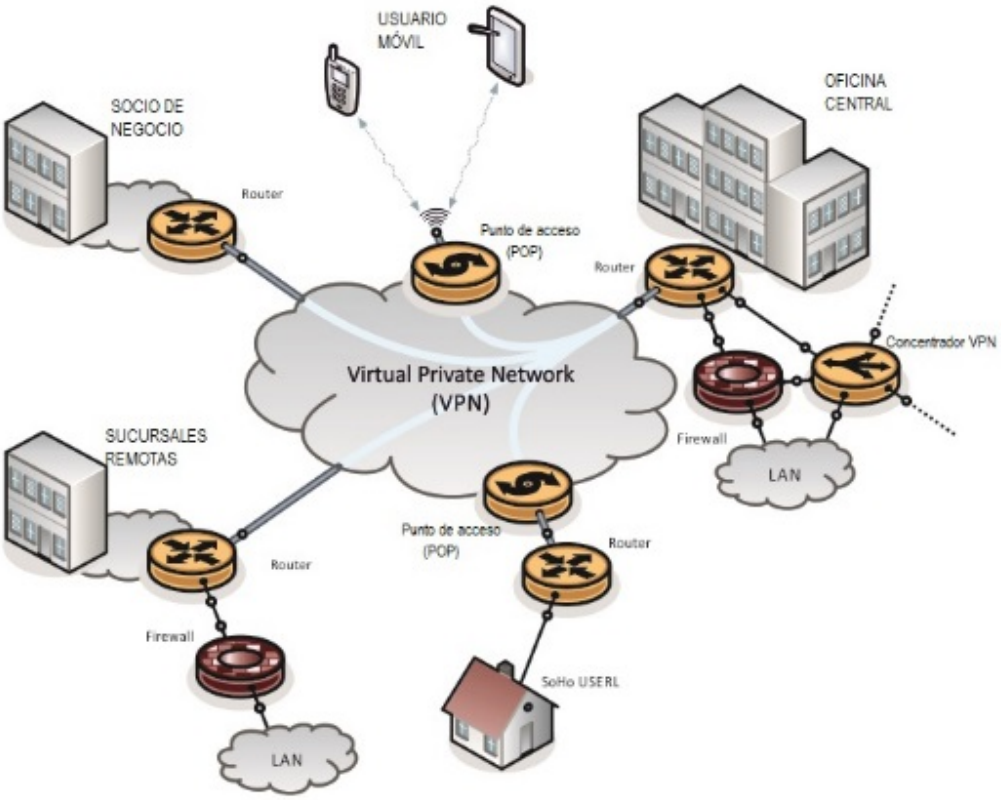
1. Conectividad extremo a extremo o de LAN a LAN

Este tipo de conexión VPN se utiliza para conectar ubicaciones geográficamente dispersas de forma similar a como si estuvieran conectadas por una línea alquilada u otra **WAN** (*red de área extendida, "Wide Area Network"*), (por ejemplo, Frame Relay, **ATM** (*Asynchronous Transfer Mode*)). La ventaja de este enlace es que permite compartir una intranet corporativa o una extranet con una entidad asociada. En esta topología, los usuarios envían y reciben datos a través de un gateway VPN, normalmente un router o un servidor. El gateway VPN es responsable de cifrar el tráfico saliente y enrutarlo al túnel VPN a través de Internet hacia el gateway VPN opuesto de la red destinataria. Este gateway VPN elimina la cabecera del paquete, descifra su contenido y entrega el paquete a un usuario de destino dentro de dicha red de destino.

2. Acceso Remoto

Los teletrabajadores o trabajadores remotos utilizan mucho las conexiones VPN de acceso remoto. En el pasado, estos trabajadores remotos tenían una conexión por líneas telefónicas, lo que significaba una baja tasa de transmisión y con elevados costos de operación. En la actualidad, sin embargo, la mayoría de ellos tienen acceso rápido a Internet directamente desde casa a través de tecnologías de banda ancha y pueden construir conexiones VPN de alta calidad.

Cada usuario suele tener instalado un cliente VPN, es decir, un software que encapsula y cifra los paquetes antes de enviarlos por Internet al gateway VPN de destino. Este software facilita mucho la conexión, ya que el usuario sólo necesita conocimientos básicos para construir una conexión VPN de alta calidad.



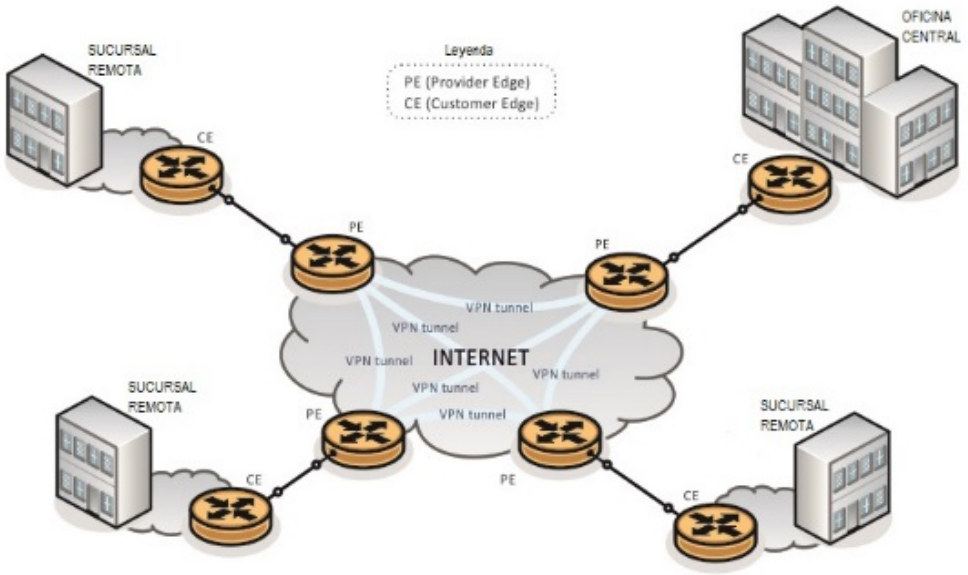
Opciones de conectividad VPN

3 Clasificación de VPN según RM-OSI

1. VPN basada en un dispositivo del proveedor (PE-based VPN)

PE (*Provider Edge*) es el dispositivo límite del **ISP** (*Internet Service Provider*), que incluye routers, conmutadores o dispositivos que son una combinación de ambos.

El dispositivo PE participa en el enrutamiento y reenvío de tráfico basado en el rango de direcciones del cliente. Los datos se transmiten normalmente entre dispositivos PE a través de túneles VPN creados utilizando **MPLS** (*Multi Protocol Layer Switching*), IPSec, L2TPv3 o GRE. En este caso, los dispositivos **CE** (*Customer Edge*) no reconocen que forman parte de una VPN.



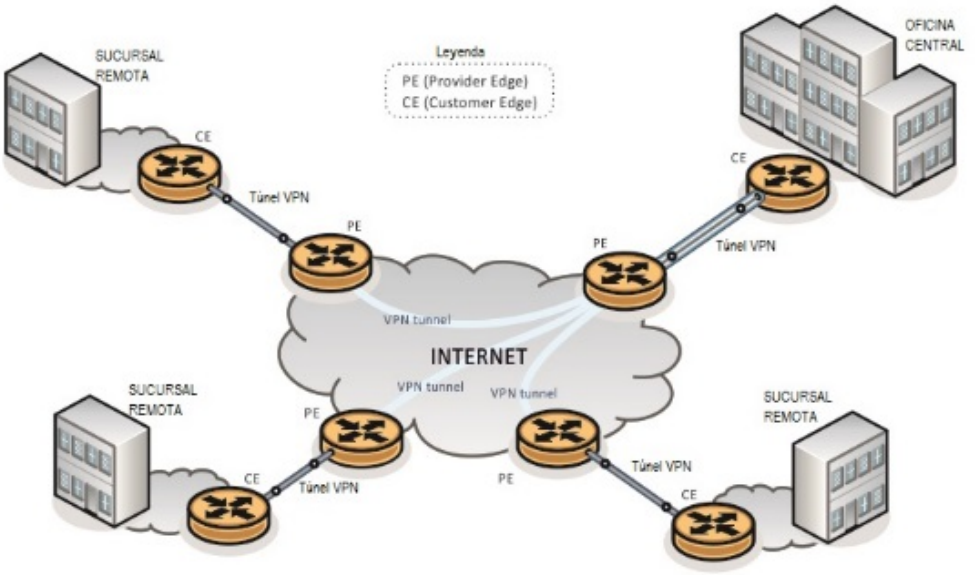
Diseño de VPN basado en el dispositivo del proveedor

Los túneles VPN terminan en el enrutador de frontera PE y normalmente se configuran como permanentes.

2. VPN basada en el equipo del cliente (VPN basada en CE)

El dispositivo CE es un dispositivo de delimitación del cliente conectado al dispositivo PE.

Los dispositivos PE en este modo no distinguen el tipo de tráfico, las conexiones VPN son gestionadas por el dispositivo CE que enruta y envía el tráfico del usuario. Los túneles se crean entre los dispositivos CE basados en IPSec o GRE.



Diseño de VPN basado en el equipo del cliente

Los dispositivos CE (VPN gateway) suelen tener otras características para clientes VPN (como **DHCP** *(Dynamic Host Configuration Protocol)*, **DNS** (*Domain Name Server*)). Esta solución generalmente impone mayores exigencias a la autenticación de clientes, ya que se conectan en cualquier momento y en cualquier lugar.

4 Protocolo IPSec - descripción

El protocolo IPSec es un conjunto completo de protocolos para cifrado, autenticación, integridad de datos y tunelización. La seguridad se implementa en la capa de red de referencia **OSI** (*Open System Interconnection*), por lo que proporciona una seguridad transparente para cualquier aplicación de red o transmisión.

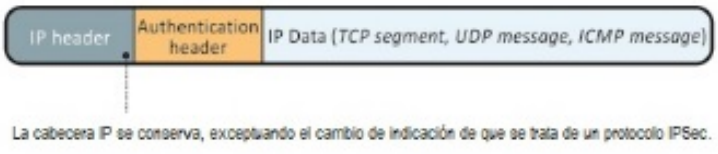
Los componentes básicos de IPSec incluyen:

- protocolos de seguridad - **AH** (*Authentication Header*), **ESP** (*Encapsulating Security Payload*),
- protocolos para el intercambio de claves - **ISAKMP** (*Internet Security Association and Key Management Protocol*), **IKE** (*Internet Key Exchange*),
- Bases de datos de asistencia - **SPD** (*Security Policy Database*), **SAD** (*Security Association Database*), y
- **DOI** (*Dominio de Interpretación*) - contiene diferentes valores, como identificadores e indicadores para **SA** (*Security Association*)

IPSec ofrece dos modos de trabajo:

1. Modo de transporte - para conexión Host-to-Host

En un modo de transporte, sólo el contenido de un determinado paquete IP suele estar cifrado o autenticado. La información de enrutamiento permanece sin cambios, a menos que la cabecera del paquete IP sea modificada o cifrada. Cuando se utiliza un **AH** (*Authentication Header*), las direcciones IP no se pueden traducir, porque el valor hash siempre se pierde. Las capas de transporte y aplicación siempre están protegidas por la función hash, por lo que no pueden modificarse (por ejemplo, cambiando el número de puerto).

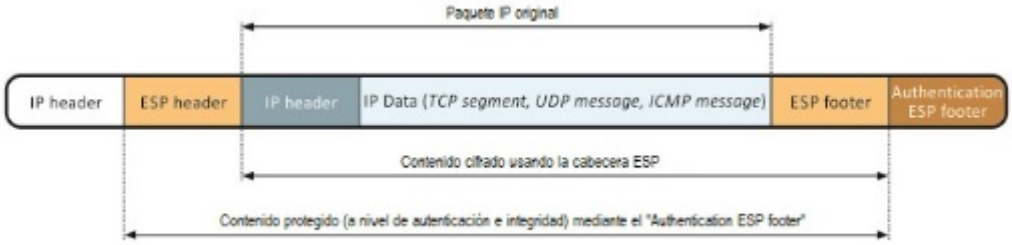


Estructura del paquete IPSec en modo de transporte utilizando el encabezado AH

2. Modo de túnel - diseñado principalmente para conexiones de extremo a extremo

En el modo túnel, todo el paquete IP es encriptado o autenticado por **ESP** (*Encapsulating Security Payload*). Luego se encapsula en un nuevo paquete IP con un nuevo encabezado utilizando el encabezado de autenticación AH. Este modo se utiliza para crear VPNs para la comunicación entre redes extremo a extremo individuales (por ejemplo, entre routers que enlazan diferentes redes),

comunicaciones Host-to-Site (por ejemplo, acceso remoto de usuarios) y comunicaciones Host-to-Host (por ejemplo, chat privado).



Estructura del paquete IPSec en modo túnel utilizando ESP

El modo túnel soporta **NAT** (*Network Address Translation*) y **PAT** (*Port Address Translation*).

IPSec no contiene en su cabecera ningún campo para la especificación de un modo de funcionamiento. El modo de funcionamiento se define en función del valor del campo Next Header (el valor"IP" indica el modo de tunelización; los valores"TCP, UDP, ICMP" (u otros) identifican el modo de transporte).

Los beneficios de IPSec incluyen su transparencia, no hay necesidad de modificar protocolos de capa superior, IPsec puede proteger cualquier protocolo IP, protege protocolos "antiguos" que no son seguros y que son ampliamente soportados por **HW** (*Hardware*) y **SW** (*Software*).

Las desventajas de IPSec incluyen la sobrecarga y la necesidad de instalar el cliente en caso de acceso remoto. No se ocupa de la autenticación de usuarios; NAT y PAT problemáticos (que sólo se pueden utilizar en el modo túnel) y tráfico de multidifusión y difusión.

Protocolo IPSec:

- proporciona tráfico en la capa de red,
- es universal para asegurar cualquier tráfico TCP/IP,
- protege contra el análisis del tráfico de la capa de red de Packet Sniffing,
- es adecuado para usuarios remotos fijos,
- no soporta la transmisión multicast y broadcast,

- muestra los problemas de traducción de direcciones (NAT y PAT) - el campo de dirección protegido por **HMAC-SHA1** (*Hash Message Authentication Code - Secure Hash Algorithm*) es cambiado; la solución es empaquetar el paquete IPSec en el datagrama **UDP** (*User Datagram Protocol*) → el método **NAT-T** (*NAT-Traversal*), y:

- en caso de acceso remoto, se requiere la instalación del cliente (pero puede haber problemas de compatibilidad con diferentes implementaciones).

---

5 Intercambio de claves IPSec - Método ISAKMP/IKE

El intercambio de claves entre clientes antes de iniciar sus propias comunicaciones seguras es importante desde varios puntos de vista. Sin embargo, se plantea la siguiente pregunta: ¿cómo conseguir un intercambio seguro de claves? A efectos de la comunicación, es necesario garantizar:

1. Acuerdo sobre el tipo de clave y la forma en que se crea, es decir, para establecer una clave compartida - **PSK** (*Pre-Shared Key*)
2. Autenticación de los participantes, es decir, autenticación mutua de los participantes en la comunicación.
3. La protección de la identidad de los participantes, es decir, el atacante pasivo no debería poder revelar la identidad de los participantes simplemente monitoreando la comunicación.
4. **DoS** (*Denegación de servicio, "Denial of Service"*), es decir, un usuario malintencionado no debería poder abusar del protocolo para forzar a la contraparte a malgastar recursos (**CPU**, (*Unidad Central de Procesamiento, "Central Processing Unit"*), memoria, capacidad de almacenamiento, ...)

El protocolo ISAKMP está definido por el RFC 2408. Para su funcionamiento hace uso del protocolo de transporte UDP en el puerto 500.

ISAKMP es un protocolo general para generar asociaciones de seguridad *(SA, Security Associations)*, es decir, no se ocupa de cómo reemplazar claves autenticadas. Esta es la tarea del protocolo IKE. El ISAKMP se utiliza para autenticar a las partes comunicantes e intercambiar datos para las claves de cifrado.

No se trata de una comunicación Cliente-Servidor, sino de una comunicación de tipo Llamada-Respuesta. La parte que quiere crear una nueva SA inicia la comunicación con el protocolo ISAKMP.

IKE es un protocolo flexible de "negociación" definido por la Recomendación RFC 2409. Permite la negociación de un método específico de autenticación, cifrado, longitudes de clave y su intercambio seguro. Para ello, utiliza el algoritmo Diffie-Hellman (algoritmo D-H).

El protocolo IKE se utiliza para intercambiar claves de sesión, llamadas claves de sesión. Los mensajes IKE se encapsulan en paquetes ISAKMP.

El protocolo IKE puede dividirse en dos fases independientes. La primera fase construye un canal seguro y autenticado entre entidades comunicantes (ordenadores). En esta fase, la identidad de las partes comunicantes se autentica de forma protegida. Ambas partes en la comunicación acuerdan el uso de SA y realizan un intercambio de claves compartido PSK autenticado. Posteriormente, se establece un túnel seguro para la segunda fase. Hay dos modos disponibles para crear el túnel:

- Modo principal
    - organiza los algoritmos y las funciones de hash, genera el secreto compartido utilizando el algoritmo D-H y verifica la identidad de la contraparte. En total, hay 6 informes.
- Modo Agresivo
    - acorta la negociación en un número menor de paquetes. Hay 3 informes en total.

+ Algunas de las ventajas del modo agresivo son el ahorro de ancho de banda y del tiempo necesario para la transferencia de mensajes.

− Una desventaja del modo agresivo es el intercambio de información importante antes de que se establezca la conexión cifrada, que es susceptible de interceptación, conocida como Sniffing.

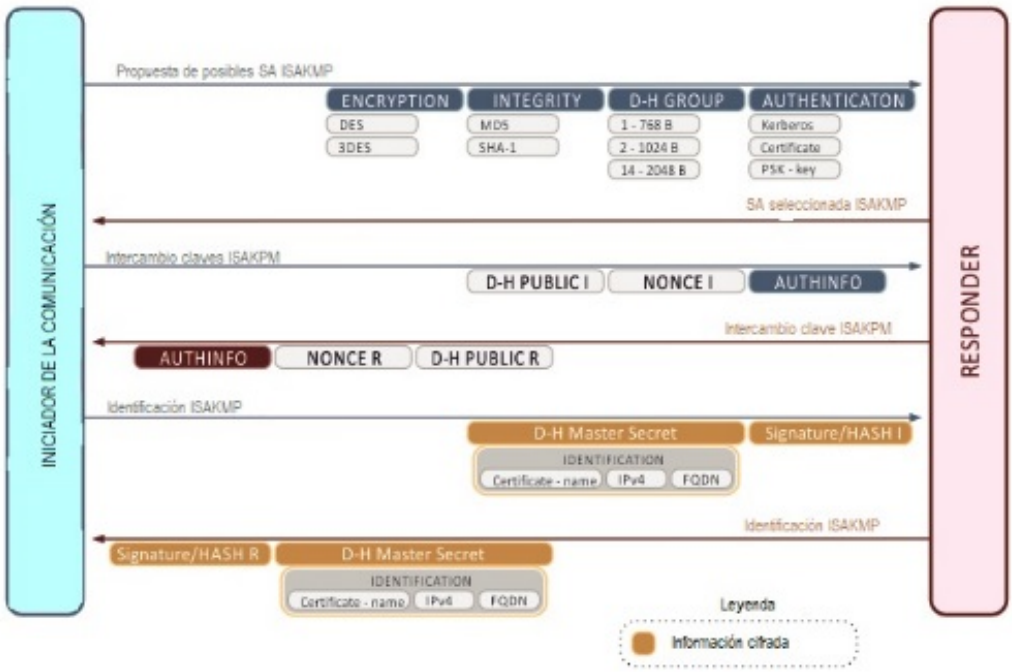


Diagrama de proceso del protocolo IKE etapa 1 (modo principal)

En la primera fase, es posible utilizar 4 formas diferentes de intercambiar la clave PSK:

- cifrado asimétrico de clave pública (versión original)
- cifrado asimétrico de clave pública (versión mejorada)
- firma digital
- clave secreta (algoritmo simétrico)

Cada opción de intercambio de claves se puede utilizar en el modo principal o agresivo, es decir, hay en total 8 opciones diferentes para la primera etapa del protocolo IKE. El modo principal debe ser implementado siempre, el modo agresivo es opcional, es aconsejable que también sea implementado.

El resultado de la primera etapa del protocolo IKE es la autenticación mutua de las partes comunicantes, el intercambio de la clave simétrica compartida PSK y la creación de la IKE Security Association (SA).

La segunda fase (llamada Modo Rápido) crea un SA para la sesión IPSec, es decir, se establecen los parámetros de conexión SA IPsec, IPSec SA se establece para una conexión específica (p. ej. FTP, telnet, etc.) Opcionalmente, se realizan intercambios D-H adicionales y se especifica otro material para la comunicación.

Esta comunicación está protegida desde el principio mediante el uso de algoritmos y claves obtenidos en la primera fase.

Para cifrar la comunicación de tipo convencional, una Clave de Sesión derivada de la Clave Maestra D-H obtenida del Modo Principal SA y del resto establecido en el Modo Rápido SA.

PFS (*Perfect Forward Secrecy*) se refiere a un estado en el que las claves actuales no se utilizan para generar claves adicionales. Si una clave en particular es descifrada accidentalmente, es decir, revelada, no permitirá que el atacante rompa fácilmente las otras claves. Si se utiliza PFS, se generarán nuevos Secretos Compartidos utilizando D-H en Modo Rápido. El uso de PFS es más seguro, pero un poco más exigente en términos de rendimiento y tiempo a la hora de establecer una conexión. La clave de relación se obtiene a partir de la nueva D-H Secret Key y Nonce, obtenida a partir del Modo Rápido SA. Mediante la aplicación de PFS, se garantiza que la clave de sesión nunca se genere a partir del mismo material.

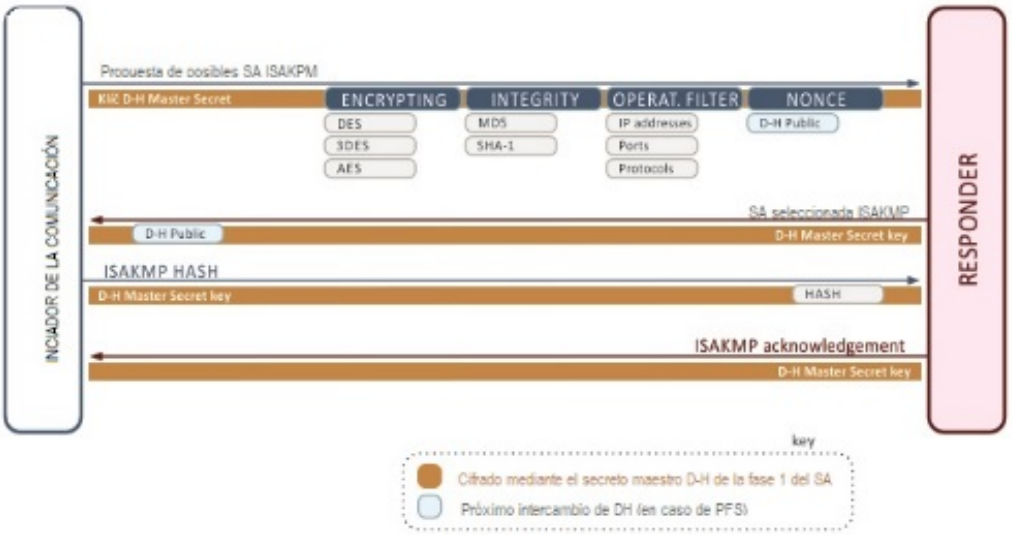


Diagrama de proceso IKE Fase 2 (Modo rápido)

Comparación con SSL/TLS - La sesión SSL se puede comparar con la primera etapa del protocolo IKE; la conexión SSL corresponde a la segunda fase del protocolo IKE.

6 Algoritmo difícil de Hellmann

El algoritmo Diffie-Hellman (algoritmo D-H) es un protocolo criptográfico que se utiliza para crear una conexión cifrada entre partes en comunicación a través de un canal no seguro, sin necesidad de determinar previamente la clave de cifrado. El resultado del algoritmo es una clave de cifrado simétrica, que puede utilizarse para cifrar el resto de la comunicación.

Una ventaja es que un atacante potencial no puede obtener esta clave escuchando a escondidas (intercepción). La clave es creada por todos los participantes en esta comunicación y nunca se envía de forma abierta. Este algoritmo garantiza el intercambio de una clave común de tal manera que si el atacante escucha esta comunicación, no puede reconstruir la clave combinada basada en la información interceptada.

Una desventaja de este protocolo es la indefensión frente a ataques de hombre en el medio "Man in the Middle", porque no permite la autenticación de los participantes. Este protocolo, sin ninguna combinación con otros métodos de autenticación, sólo es apropiado cuando un atacante no puede perturbar la comunicación de forma activa.

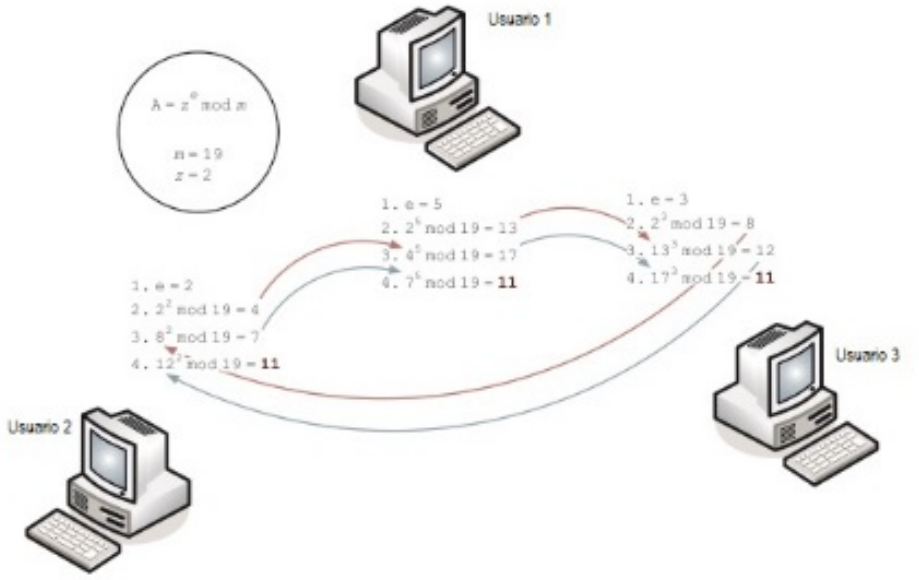
El principio del algoritmo D-H definido por RFC 2409, RFC 3526 a RFC 5114 se basa en la exponencialización de números $(^{AB})^{C} = (^{AC})^{B}$, respectivamente en una opción modular de esta fórmula $(^{AB})^{C|m} = (^{AC})^{B|m}$.

El tamaño del módulo especifica el tipo de grupo. Por lo general, existen estos grupos: 1, 2 y 5. El número de grupo indica la longitud de la clave - DH-1 (768 bits), DH-2 (1024 bits), DH-5 (1535 bits), DH-14 (2048 bits).

El cálculo del valor resultante es muy fácil (rápido), pero es muy difícil encontrar algunos de los valores conocidos sólo por el otro participante. Este principio, que es la base de la seguridad de este algoritmo, se conoce como el problema del logaritmo discreto.

La comunicación mediante el algoritmo D-H se realiza de la siguiente manera:

- Los participantes se ponen de acuerdo públicamente sobre el módulo *m* utilizado (es decir, el tipo de grupo) y la base *z*.
- Cada participante elige su exponente *e* (desacoplado del módulo *m*).
- Cada participante calcula el resultado de la potencia de la base (utilizando su propio exponente) y envía el resultado al siguiente participante.
- El algoritmo termina cuando cada participante procesa cada una de las bases originales.



Principio de comunicación de tres participantes utilizando el algoritmo Diffie-Hellman

7 Ataques a las redes locales - Ejemplos y soluciones

La seguridad de los elementos de red ha sido subestimada durante mucho tiempo y empujada hacia atrás por las empresas. Recientemente, sin embargo, la tendencia ha cambiado y muchas empresas son conscientes de la importancia y las consecuencias de las amenazas potenciales. El número de ataques dentro de la red supera rápidamente al número de ataques desde fuera de la red. Por eso nos ocupamos de la seguridad de los Switches de Acceso, a los que los usuarios tienen acceso directo, donde existe un alto riesgo de diferentes tipos de ataques.

Ejemplos de posibles ataques a interruptores:

- Inundación de direcciones MAC - el **CAM** (*Content Addressable Memory*) → el conmutador actúa como un simple concentrador
- DHCP Spoofing - Denegación de la dirección DHCP por un ataque a un servidor DHCP
- Abuso de puertos troncales: el atacante tiene acceso al tráfico de otra **VLAN** (*LAN virtual*) transmitida.
- Ataques **CDP** (*Cisco Discovery Protocol*): los mensajes CDP no se cifran, se envían periódicamente y proporcionan información detallada sobre el tipo de dispositivo, la versión IOS, entre muchos otros.
- Ataques adicionales, como ataques a contraseñas de acceso remoto, ataques DoS y otros.
- Instalación de puntos de acceso inalámbricos no autorizados (Rogue AP) que el empleado instala para tener Internet disponible para su **PDA** (*Portable Digital Assistant*), lo que puede hacer que la red interna de la empresa esté disponible (abierta) debido a su inadecuada seguridad.

Posibles soluciones:

1. Seguridad de puerto

La seguridad de puerto es la forma más fácil de proteger los puertos para comprobar las direcciones **MAC** (*Medium Access Control*) conectadas a los puertos. En caso de violación de una regla definida, la acción se realiza según la configuración del puerto.

Hay tres respuestas a las violaciones de seguridad:

- Proteger: las direcciones MAC habilitadas pueden seguir comunicándose, la comunicación desde direcciones MAC no autorizadas está bloqueada.
- Restringir - el comportamiento es el mismo que en el modo Proteger, pero se genera un mensaje de error en el registro del dispositivo, y si se configura

SNMP (*Simple Network Management Protocol*), el trap SNMP se envía al servidor SNMP.

- Apagado - se bloquea toda la comunicación (incluso de las direcciones permitidas). El puerto se conmuta a un estado especial de desactivación de errores cuando se requiere la intervención del administrador y el puerto se vuelve a activar manualmente.

De esta manera, un puerto físico determinado se concatena (enlaza) con una red virtual fija (VLAN). Esto crea una conexión fija del grupo de direcciones MAC y una VLAN al puerto de acceso dado.

Para las redes de grandes empresas, la solución anterior no es suficiente. Soluciones integradas complejas como las soluciones basadas en protocolos resultantes de la recomendación IEEE 802.1X.

La seguridad del puerto se realiza en el conmutador Cisco de la siguiente manera. En primer lugar, es necesario activar la función de seguridad de puerto en un puerto determinado, utilizando el comando "switchport port security". El valor por defecto es 1, lo que significa que sólo se puede conectar un dispositivo a ese puerto. Este valor, es decir, el número (cantidad) permitido de direcciones MAC que pueden acceder al puerto, puede cambiarse. Las direcciones con el interruptor también se pueden aprender de forma dinámica o manual. La configuración manual se realiza mediante el comando "port security mac-address MAC-ADDRESS". Este comando puede ampliarse con el llamado parámetro "sticky", que garantiza que la dirección MAC aprendida dinámicamente se almacena en la configuración del dispositivo. Como se mencionó anteriormente, debe preparar una acción que el conmutador ejecuta en caso de violación de las reglas utilizando el comando "switchport port-security violation". Esto se muestra claramente en la siguiente figura.

```
Switch(config)#interface fastethernet 0/1
switch(config-if)#switchport mode access //sets the port to the appropriate mode
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum ADDRESS_AMOUNT
Switch(config-if)#switchport port-security mac-address MAC_DEVICE_ADDRESS //manual addressing
Switch(config-if)#switchport port-security mac-address sticky //dynamic MAC address learning
Switch(config-if)#switchport port-security violation {shutdown | restrict | protect}
```

Ejemplo de la configuración de seguridad de puerto en el conmutador Cisco

2. DHCP Snooping

DHCP Spoofing es un tipo de ataque a la red en el que un atacante (en una red local) falsifica los mensajes del protocolo DHCP (por ejemplo, ejecutando un servidor DHCP personalizado con parámetros de red modificados) para engañar a la víctima, por ejemplo, utilizando otra gateway predeterminada. Esto permite al atacante redirigir el tráfico de la víctima a su ordenador. Posteriormente, pueden interceptar todo el tráfico de salida de la víctima.

Otro tipo de ataque al servidor DHCP es el agotamiento de los rangos de servidores DHCP (DHCP Starvation). En este caso, el atacante genera un gran número de peticiones falsas para asignar una dirección, lo que da como resultado que se queden sin direcciones.

DHCP Snooping es una indicación de cómo defenderse contra DHCP Spoofing. Se configura en los conmutadores que se conectan directamente a las estaciones finales (los llamados conmutadores de acceso). La esencia de todo el proceso de defensa contra el spoofing DHCP es escuchar las consultas DHCP en los puertos de los conmutadores y bloquear la transmisión de respuestas falsas a las consultas. Esto elimina el efecto del servidor DHCP falsificado del atacante. El envío de respuestas desde un servidor DHCP sólo está habilitado en puertos de conmutador de confianza. El puerto de "confianza" es configurado manualmente por el administrador, y normalmente sólo hay un puerto al que está conectado el servidor DHCP correcto. Los conmutadores Cisco le permiten configurar DHCP Snooping para cualquier número de VLAN, configurar puertos de confianza a los que están conectados los servidores DHCP y reducir el número de consultas **PPS** (*paquetes por segundo*) en el servidor DHCP para evitar sobrecargas. Un ejemplo de la configuración de DHCP Snooping se muestra en la siguiente figura.

```
Switch(config)#ip dhcp snooping
switch(config)#no ip dhcp snooping information option
Switch(config)#ip dhcp snooping vlan ONE_VLAN_OR_RANGE
Switch(config)#interface fastethernet NUMBER
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#ip dhcp snooping limit rate PPS //disables option 82 - used for DHCP Relay
```

Un ejemplo de una configuración de DHCP Snooping en un conmutador Cisco

Al habilitar la base de datos DHCP Snooping Binding (ver la figura de abajo), también se puede proteger contra otros tipos de ataques a redes locales. Después de activar esta función, el conmutador crea una tabla que contiene enlaces entre la dirección MAC de la estación, la dirección IP, el tiempo de alquiler de la dirección IP, el puerto desde el que se comunica, la red virtual (VLAN) desde donde se encuentra y la forma en que el elemento se agregó a la tabla (manual o automáticamente). Esta información utiliza **DAI** (*Dynamic ARP Inspection*) para protegerse contra el envenenamiento de la caché ARP.

```
Switch(config)#ip dhcp snooping database flash:/dhcpbind.txt
```

Activación de la función DHCP de Snooping Binding Database en el conmutador Cisco

3. Inspección ARP dinámica

El envenenamiento de la caché ARP es un ataque fácil de implementar y difícil de detectar basado en la falsificación de las respuestas de los mensajes de **ARP** (*Protocolo de resolución de direcciones*). El protocolo ARP proporciona enlaces de direcciones IP y MAC en la red local. Un atacante que utiliza respuestas falsas puede provocar que la comunicación infectada del equipo se redirija a un atacante.

A continuación, puede escuchar la comunicación completa de la víctima con otras estaciones de la red.

Este ataque puede ser detectado (y prevenido) por un interruptor que soporta la función DAI.

El ataque se puede realizar en un PC, por ejemplo utilizando la herramienta Cain&Abel (www.oxid.it) o Ettercap (http://ettercap.sourceforge.net/).

AID es una forma de defenderse contra el envenenamiento de caché ARP. Se utilizan tablas creadas utilizando DHCP Snooping. Si el ARP llega a un paquete desde un puerto de confianza, se envía más lejos. Sin embargo, si el ARP llega a un paquete desde un puerto no confiable, se analiza. En el caso de un mensaje de solicitud ARP, el procesador de red de paquetes detecta si la dirección MAC e IP del ordenador solicitante pertenecen entre sí. Si es así, el paquete es reenviado a la red. De lo contrario, se descarta. En el caso de la Respuesta ARP, también verifica si el MAC y la dirección IP del equipo correspondiente al mensaje de Solicitud ARP están relacionados entre sí. Las combinaciones de direcciones IP y MAC se toman de una base de datos creada por la función DHCP de Snooping. El comando de habilitación DAI se presenta en la siguiente figura.

```
Switch(config)#ip arp inspection vlan Vlan_ID //enables DAI
Switch#show ip arp inspection vlan Vlan_ID //views monitored VLAN
```

Activar la función DAI en el conmutador Cisco

La siguiente figura muestra un comando para desactivar el control DAI en las interfaces de confianza.

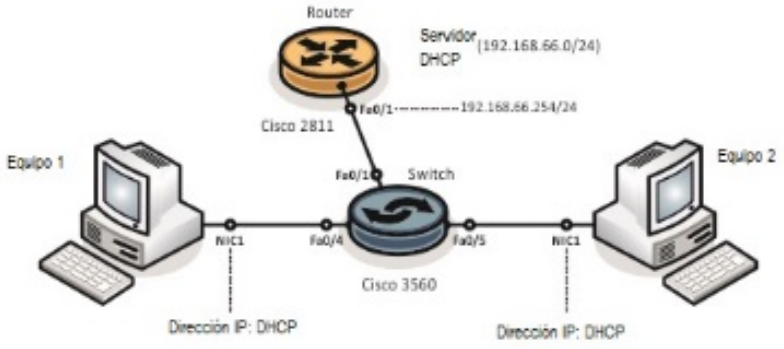
```
Switch(config)#interface fastethernet 0/1
Switch(confid-if)#ip arp inspection trust //tagging the interface as trusted
```

Desactivar el control DAI en la interfaz del conmutador Cisco de confianza

IP Source Guard tiene una función similar a DAI, pero en lugar de detectar direcciones MAC falsas, se detectan direcciones IP de origen falsas. Permite bloquear direcciones IP no autorizadas en los puertos. Está configurado en un puerto específico. Esta función también utiliza la base de datos DHCP Snooping Binding. El comando para activar IP Source Guard se muestra en la siguiente figura.

```
Switch(config)#interface INTERFACE_NAME
Switch(confid-if)#ip verify source port-security //filters by source IP and MAC address
```

Activación de IP Source Guard en el conmutador Cisco



Un ejemplo de topología para activar tareas de simulación de ataques en la red local

8 Construcción de VPN con IPSec - Ejemplos y soluciones

El acceso remoto es ahora una parte indiscutible de la gestión de los dispositivos de red de cualquier vasta red de área local, especialmente en lo que se refiere a la necesidad de una intervención rápida de un administrador de red en caso de que se produzca una situación repentina y en relación con la reducción del coste total de tal acción. Por lo tanto, el administrador de red debe estar conectado a Internet para monitorear y reconfigurar remotamente los elementos individuales de la red.

En el pasado, el protocolo Telnet se utilizaba para el acceso remoto con fines de gestión de elementos de red. Sin embargo, no protegía su propia comunicación, por lo que era relativamente fácil interceptar y capturar la información de inicio de sesión. Al difundir el acceso a Internet, se necesitaba un protocolo que protegiera las comunicaciones contra posibles atacantes. Así, **SSH** (*Secure Shell*), que se comunica con el protocolo de transporte TCP por defecto en el puerto 22, proporciona autenticación segura en ambos lados, asegura su integridad, cifrado de datos transparente y, opcionalmente, compresión sin pérdidas (se puede encontrar más información en RFC 4252 [https://www.ietf.org/rfc/rfc4252.txt]).

Las necesidades de las grandes empresas de interconectar de forma segura sus sucursales han creado redes privadas virtuales que debían proporcionar la conexión de dos o más dispositivos de red en un entorno público de Internet no fiable. Otra razón fue el precio de la interconexión. En el caso de los circuitos dedicados, los costes serían incomparablemente más elevados. Desde la perspectiva del modelo de referencia OSI, las VPNs generalmente se pueden dividir por la capa en la que están trabajando. Las tecnologías VPN más comunes se enumeran en la siguiente tabla.

Las tecnologías más comunes en VPNs

Tipo de VPN	Capa RM-OSI	Descripción
Frame Relay	enlace	Requiere un entorno homogéneo de Frame Relay. Fiable, más seguro, pero también más caro en comparación con la VPN IP.
ATM	enlace	Requiere un entorno ATM homogéneo. Al igual que FR, proporciona canales virtuales con parámetros acordados.
L2TP/PPTP	enlace	L2TP como sustituto de PPTP, que deriva las claves de la contraseña del usuario (potencial debilidad). PPTP utiliza **MPPE** (*Microsoft Point-to-Point Encryption*) y L2TP IPsec para el cifrado. Definido por RFC 2637 [https://www.ietf.org/rfc/rfc2637.txt] y RFC 2661 [https://www.ietf.org/rfc/rfc2661.txt] .
BGP/MPLS	enlace/red	Intercambia información de forma segura entre routers fronterizos **BGP** (Border *Gateway Protocol*) en redes troncales que utilizan túneles MPLS. Definido por RFC 4364 [https://www.ietf.org/rfc/rfc4364.txt] y otros.
IPSec	red	Es una extensión de seguridad del protocolo IP convencional. El cifrado de cada paquete crea una transmisión transparente y segura (el llamado túnel). Definido por varias recomendaciones RFC.
SSL/TLS	transporte y superiores	**SSL** (*Secure Sockets Layer*) es una tecnología que es transparente a la tecnología utilizada en la capa de red OSI. SSL se deriva entonces del protocolo **TLS** (*Transport Layer Security*) definido en RFC 5246 [https://www.ietf.org/rfc/rfc5246.txt] .

La forma más común de conectar sucursales es conectarlas con VPN IPSec cuando se establece un canal unidireccional (virtual) cifrado llamado SA entre routers/firewalls ubicados en la red de área local.

Para la comunicación dúplex (bidireccional), se deben establecer dos SA unidireccionales independientes.

IPSec es un componente obligatorio de IPv6 y, además, también se ha implementado en IPv4.

IPSec permite trabajar en dos modos (túnel - el paquete IP original completamente encapsulado en un nuevo paquete IP, y transporte - la cabecera IPsec se inserta entre la cabecera IP original y la cabecera de la capa superior) y se utiliza para proteger dos protocolos AH y ESP. Ambos protocolos admiten cifrado cero (NULL), **DES** (*Data Encryption Standard*), **3DES** (*Triple DES*), **AES** (*Advanced Encryption Standard*) y Blowfish. El protocolo IPsec está definido en muchas recomendaciones **RFC** (**Request For Comments**), pero el básico es el RFC 4301 [https://www.ietf.org/rfc/rfc4301.txt] . Para garantizar la integridad, se utilizan los algoritmos **MD5** (*Message-Digest 5*) y SHA-1 de HMAC.

8.1 Ejemplo de una configuración de VPN IPSec en dispositivos Cisco

En la primera etapa, es necesario establecer políticas ISAKMP IKE. La política de IKE sirve a IPsec para construir una SA. Sin embargo, debe crearse una clave PSK compartida entre las dos partes, de modo que las claves de cifrado personalizadas se deriven de ella. El mecanismo DH se utiliza normalmente para intercambiar claves. ISAKMP utiliza el protocolo de transporte UDP en el puerto 500. Un ejemplo de configuración de una política (tipo de autenticación, algoritmo de cifrado y hash, grupos DH y duración de vida SA en segundas unidades) puede verse en la siguiente figura.

```
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#encryption {des | 3des | aes 128 | aes 192 | aes 256}
Router(config-isakmp)#hash {md5 | sha}
Router(config-isakmp)#group {1 | 2 | 5}
Router(config-isakmp)#lifetime 86400
```

Configuración de políticas ISAKMP IKE en un router Cisco

Además, se debe configurar una clave PSK compartida para que las partes puedan autenticarse entre sí. Dentro del comando también se define la dirección IP de la otra parte. El ejemplo se muestra en la siguiente figura.

```
Router(config)#crypto isakmp key HEREisTHISsecretKEY address 192.168.0.2
```

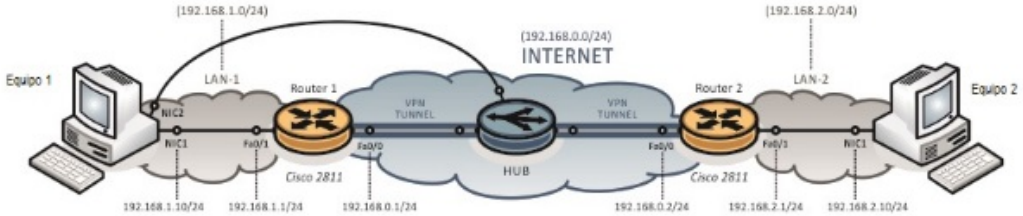
Configuración de la clave compartida PSK en el router Cisco

La segunda etapa configura la configuración personalizada de IPsec. Se define un conjunto de algoritmos para la confidencialidad e integridad de los datos, conocidos como **TS** (*Transform Set*). Por ejemplo, utilizamos el protocolo ESP en combinación con el algoritmo HMAC SHA-1. El router sólo podrá cifrar el tráfico si tiene el llamado "Interesting Traffic" establecido usando la regla convencional del cortafuegos **ACL** (*Access List*). Los parámetros que se definen de esta manera combinan el objeto Crypto Map, que - junto con otros parámetros adicionales, como la dirección por defecto del otro lado (generalmente, se pueden definir múltiples direcciones) y parámetros opcionales como el grupo DH, el tiempo de vida de IPsec SA (en segundos) - se aplica a la interfaz **WAN** (*Wide Area Network*) apropiada. Lo anterior es evidente a partir del ejemplo de la siguiente figura.

```
Router(config)#crypto ipsec transform-set ESP-AES esp-aes 256 esp-sha-hmac
Router(config)#ip access-list extended INTERESTING-OPERATION
Router(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
Router(config)#crypto map IPSEC-MAP 1 ipsec-isakmp
Router(config-crypto-map)#match address INTERESTING-OPERATION
Router(config-crypto-map)#set peer 192.168.0.2 default
Router(config-crypto-map)#set transform-set ESP-AES
Router(config-crypto-map)#set pfs group2
Router(config-crypto-map)#set security-association lifetime seconds 86400
Router(config)#interface fastethernet 0/0
Router(config-if)#crypto map IPSEC-MAP
```

Configuración de VPN IPsec en un router Cisco

Del mismo modo, ambas fases IPsec deben ser configuradas en el otro lado de la comunicación (router)!



Un ejemplo de topología para realizar tareas en VPN IPSec

9 Creación de VPN con SSL/TLS - Ejemplos y soluciones

Una VPN no sólo puede interconectar sucursales individuales, sino que también puede facilitar el acceso del cliente a fuentes ubicadas en partes inaccesibles de la red de la empresa a través del protocolo **HTTPS** (*HyperText Transfer Protocol for Secure*) - **HTTP** (*HyperText Transfer Protocol*) con soporte SSL/TLS para clientes de origen ubicados en partes inaccesibles de la red corporativa. El cliente se conecta a través de un navegador web estándar habilitado para SSL/TLS a la página web de entrada en la que introduce sus datos de acceso. Si son correctos, una página de recursos de red compartidos estará disponible. Todas las conexiones están protegidas por SSL/TLS.

La VPN SSL también soluciona algunos inconvenientes de la VPN IPSec clásica. IPSec VPN tiene problemas para pasar a través de NAT. Esto puede ser pasado por alto por el mecanismo NAT-T, que consiste en empaquetar paquetes IPsec y / paquetes ESP en datagramas UDP, sin embargo, esto aumenta la sobrecarga del protocolo. Otra desventaja es la necesidad de un software especial en el lado del abonado en el caso del acceso remoto a la VPN. La implementación de clientes IPsec de diferentes fabricantes también puede no ser mutuamente compatible, el túnel puede no ser construido debido a las reglas de seguridad en redes extranjeras (por ejemplo, filtrando el tráfico saliente, usando servidores proxy), ...

Algunos de estos problemas pueden evitarse utilizando SSL/TLS VPNs. Este acceso VPN se denomina SSL VPN o VPN sin clientes porque el usuario no necesita un software especial para acceder a las VPN; se puede utilizar un navegador web común con soporte HTTPS.

El término SSL VPN se conoce a menudo como una serie de tecnologías incompatibles entre sí. Sin embargo, todos se basan en la misma idea básica, que es el uso de criptografía asimétrica y bibliotecas SSL/TLS para una comunicación segura. Hoy en día, la tecnología SSL/TLS se utiliza ampliamente para el acceso al servidor web HTTPS cifrado.

El objetivo de SSL VPN es crear un túnel transparente y encriptado basado en SSL/TLS. Debido a la presencia de SSL en los navegadores web comunes, no es necesario instalar ningún software cliente especial en los ordenadores clientes para conseguir la mayor parte de la funcionalidad ofrecida. Las soluciones SSL VPN también se utilizan para pequeñas aplicaciones en forma de applets Java o componentes ActiveX. La abundancia de equipos premium influye significativamente en el valor de las implementaciones SSL VPN de diferentes fabricantes.

La funcionalidad básica de SSL VPN es el acceso seguro a los recursos de información internos de la empresa. Se crea un túnel SSL encriptado entre la gateway SSL VPN y el navegador web del ordenador cliente. En este formulario, SSL VPN puede servir muy bien como una forma fácil de implementar para acceder de forma segura a los portales Web de los sistemas de información de la empresa dentro de Internet. Otra característica común de la solución SSL VPN es la posibilidad de utilizar **CIFS** (*Common Internet File System*) compartido para

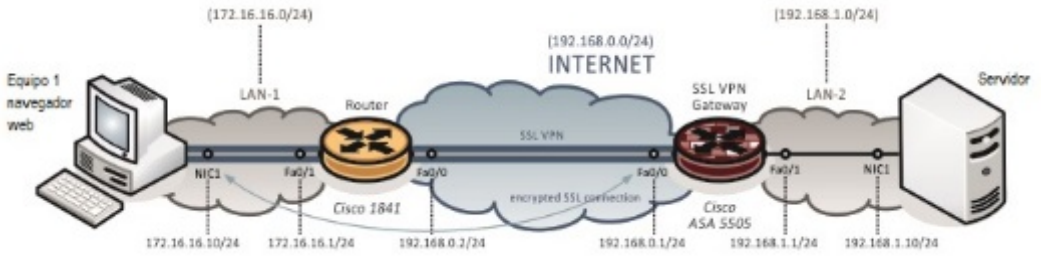
compartir archivos de versiones más recientes de Windows o **NFS** (*Network File System*).

9.1 Tipos de acceso SSL VPN

1. VPN sin clientes

En este modo, el usuario remoto accede a la red interna utilizando un navegador web (FireFox, Chrome, Internet Explorer, Edge, Safari,...) en el ordenador cliente (véase la figura siguiente). Las siguientes aplicaciones están disponibles para el usuario remoto:

- Navegación por Internet (usando HTTPS) - un portal proporciona una lista de URLs de servidores web que un usuario remoto puede ver.
- Compartir archivos (utilizando el sistema de archivos CIFS) - el portal proporciona una lista de servidores de archivos donde el usuario remoto puede hacerlo:
    - ver y descargar archivos compartidos,
    - renombrar y borrar archivos,
    - cargar y descargar archivos, y
    - crear y renombrar nuevos archivos y directorios.



Un ejemplo de topología para realizar una tarea en una VPN IPSec

2. ThinClient

Una condición básica es que la computadora de un usuario remoto debe soportar esta forma de comunicación. El usuario remoto descarga el Java applet desde la página del portal. Este applet funciona en el cliente como un servidor proxy TCP para los servicios que se configuran en la página del portal. Este tipo permite el acceso remoto a aplicaciones estándar basadas en TCP como **POP3** (*Post Office Protocol 3*), **SMTP** (*Simple Mail Transfer Protocol*), **IMAP** (*Internet Message Access Protocol*) o Telnet, así como el acceso a sistemas de información empresariales como **SAP** (*System Application Products*). Las aplicaciones del cliente deben estar configuradas para comunicarse a través de una conexión TCP con un servidor y puerto conocidos. La dirección del servidor es típicamente un loopback (127.0.0.0.1), donde la comunicación es capturada por el servidor proxy TCP y luego enrutada al túnel SSL.

3. Túnel

Este modo muestra la lista más grande de opciones para usuarios remotos. El usuario descarga (manual o automáticamente) un cliente SSL VPN completo después de iniciar sesión en el servidor VPN. Para Cisco, se trata de "Cisco AnyConnect VPN Client". Este programa crea una interfaz de red virtual que proporciona acceso a la capa de red de varias aplicaciones. Este tipo de SSL VPN proporciona opciones comparables a IPsec VPN (Acceso Remoto). Al finalizar la conexión, el cliente Cisco AnyConnect VPN se eliminará de la estación cliente o podrá permanecer instalado en la estación.

Las SSL VPN convencionales no se pueden utilizar para crear VPNs de sitio a sitio, sino que se utilizan principalmente como VPNs de acceso remoto. Una excepción a esta regla es el proyecto OpenVPN que le permite crear VPNs seguras SSL/TLS de sitio a sitio.

10 Firma Electrónica

Existen varias razones para introducir la firma electrónica. Por un lado, era necesario introducir un equivalente a una firma convencional y, por otro, se produce un gran número de documentos en formato electrónico; algunos datos incluso existen sólo en formato digital, pero, sobre todo, su naturaleza limita la fácil falsificación de datos.

En general, las firmas electrónicas requieren la identificación del firmante/entidad, la integridad del documento entregado (integridad de los datos), la innegabilidad y la aceptabilidad legal.

En el caso de un documento firmado electrónicamente, es posible que también tengamos que ocultar el contenido del mensaje (es decir, el cifrado) y determinar si el documento existía en un momento determinado (es decir, el sello de tiempo).

¿Qué es una firma electrónica? La definición de firma electrónica se basa en el Reglamento nº 910/2014 del Parlamento Europeo y del Consejo relativo a los servicios de identificación electrónica y de fideicomiso para las transacciones electrónicas en el mercado interior (abreviado como **eIDAS** (*electronic IDentification, Authentication and trust Services*)).

En el párrafo 10 del artículo 3 del reglamento de eIDAS se define la firma electrónica como los datos en forma electrónica que se adjuntan a un mensaje de datos o que se asocian lógicamente con ese mensaje de datos. Así pues, la firma electrónica sirve como método de verificación inequívoca de la identidad del firmante en relación con el mensaje de datos.

Esta definición muy general también podría referirse a una firma de texto de correo electrónico ordinario.

La firma electrónica representa varias opciones posibles:

- firma electrónica,
- firma electrónica garantizada,
- firma electrónica reconocida,
- firma electrónica cualificada.

El concepto de firma electrónica reconocida es/era específico para la República Checa (hasta el 2 de septiembre de 2008). Es una firma electrónica garantizada basada en un certificado reconocido. Por lo tanto, es aplicable a la comunicación con las autoridades públicas (¡pero sólo en la República Checa!) No existe ningún requisito de un repositorio seguro de HW. Para una firma electrónica cualificada, las llaves deben almacenarse en un lugar "seguro".

En relación con la firma electrónica, también cabe mencionar el término firma digital. Una firma digital utiliza los medios de la criptografía asimétrica. Se trata de una solución técnica específica para la firma electrónica.

La firma digital es la forma más segura de implementar la firma electrónica.

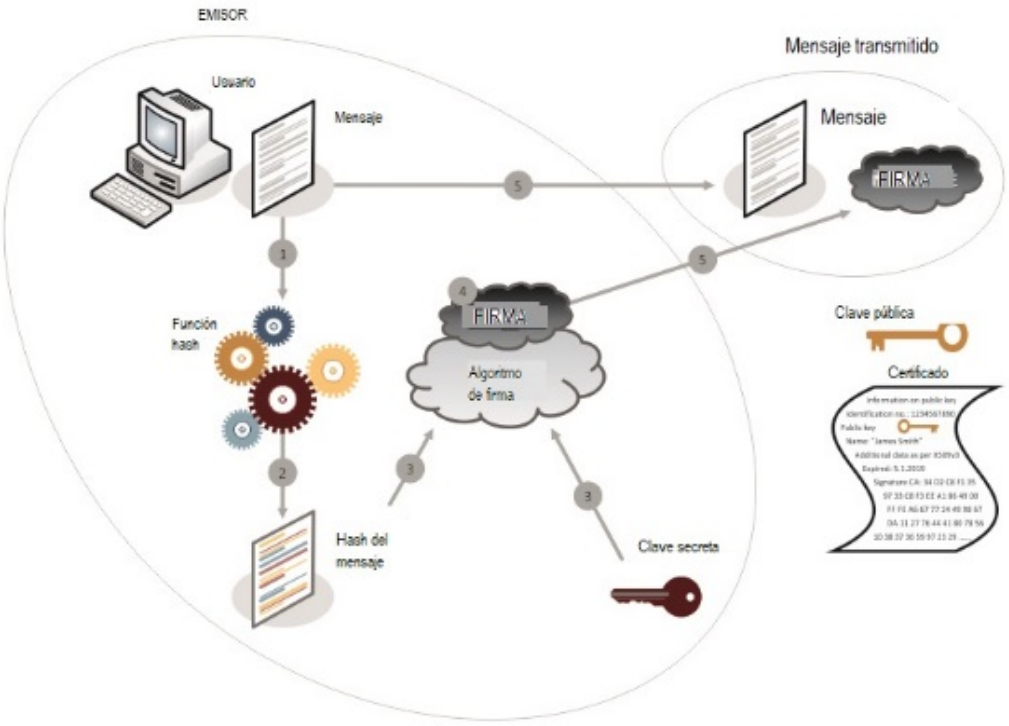
El término firma electrónica es más general en el contexto de la firma digital; es tecnológicamente neutro. Incluye, además de la firma digital, todos los demás métodos que proporcionan las propiedades requeridas (por ejemplo, los métodos biométricos). Por esta razón, también es aplicable a los documentos legislativos.

1. La firma digital es un término criptográfico/matemático.
2. La firma electrónica es, en particular, un término jurídico y normativo.
3. La definición de firma electrónica en sí misma establece los requisitos, pero no se refiere a cómo pueden lograrse.
4. Por el contrario, las herramientas de firma digital se centran plenamente en el cumplimiento de los requisitos.

10.1 Firma electrónica garantizada

Desde el punto de vista criptográfico, una firma electrónica se entiende como un conjunto de funciones criptográficas parciales que garantizan la identificación, autenticación, integridad e innegabilidad. Matemáticamente, la firma electrónica es sólo un gran número.

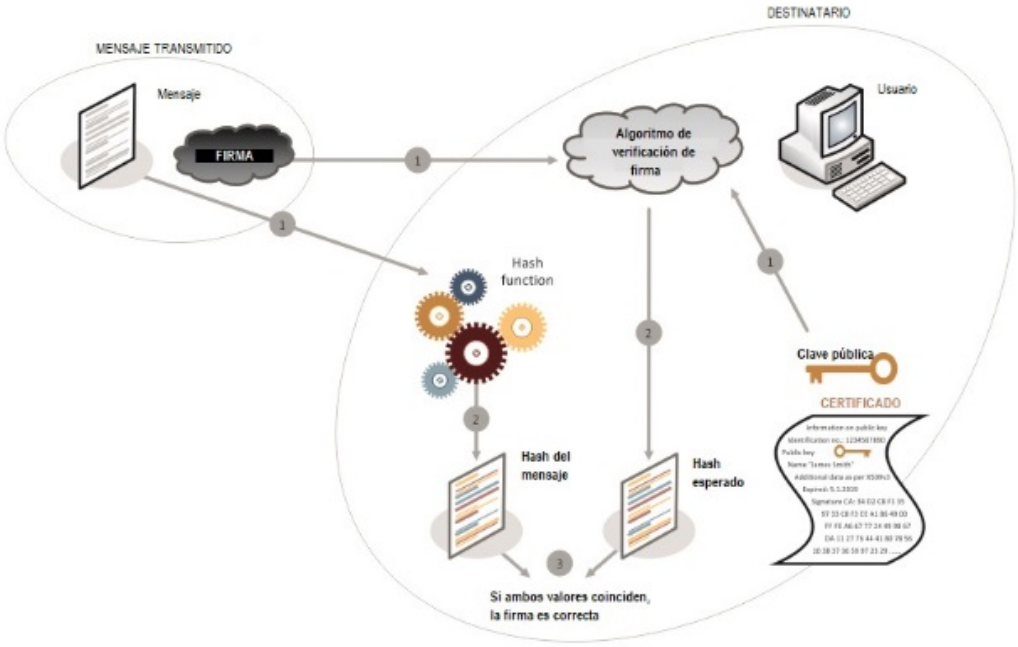
La siguiente figura muestra el proceso de creación de una firma electrónica segura. Los números de la figura indican los pasos del proceso de creación de una firma electrónica garantizada.



El proceso de creación de una firma electrónica garantizada

Cualquier dato digital como texto (PDF, TXT, DOCX, RTF, XLSX, ...), imagen (BMP, JPG, GIF, PNG,...), audio (WAV, MP3, FLAC, (AVI, MPG,...), archivos ejecutables (EXE, COM,...), y más, puede ser firmado electrónicamente. Esencialmente, cualquier cosa puede ser firmada electrónicamente.

La siguiente figura muestra el proceso de verificación de la firma electrónica garantizada. Los números de la figura indican los pasos del proceso de verificación de la firma electrónica garantizada.



Proceso de verificación de la firma electrónica garantizada

+

La firma electrónica segura garantiza la integridad de los mensajes y documentos transmitidos, la identificación de las partes comunicantes, la autenticación de las partes comunicantes (es decir, la verificación de su identificación), la innegabilidad y la irrefutabilidad.

−

Sin embargo, la firma electrónica garantizada no garantiza la aceptabilidad legal de los documentos firmados.

$E=m\cdot c^2$

El Reglamento eIDAS define la firma electrónica garantizada en el apartado 11 del artículo 3, si cumple las condiciones del artículo 26:

1. Está claramente asociado con el firmante.
2. Permite identificar al firmante en relación con el mensaje de datos.
3. Se ha creado (la firma garantizada) y se ha adjuntado al mensaje de datos utilizando instrumentos que el firmante puede mantener bajo su control exclusivo.
4. Se adjunta al mensaje de datos al que se refiere de modo que se pueda detectar cualquier cambio posterior en los datos.

10.2 Firma electrónica reconocida

El Reglamento eIDAS define la firma electrónica reconocida en el apartado 12 del artículo 3 como una firma electrónica garantizada que se crea por un medio cualificado diseñado para crear firmas electrónicas y que se basa en un certificado reconocido para firmas electrónicas.

Tiene la misma validez que una firma manuscrita.

Un certificado reconocido se define en el apartado 15 del artículo 3 de la eIDAS como un certificado de firma electrónica expedido por un proveedor de servicios fiduciarios cualificado que crea certificados de confianza y cumple los requisitos establecidos en el anexo I de dicho Reglamento.

Técnicamente hablando, un certificado reconocido es lo mismo que cualquier certificado convencional.

10.3 Sello electrónico

Tecnológicamente, es lo mismo que en el caso de la firma electrónica segura. La diferencia está en el área de su uso, que se centra en el área legal.

La firma electrónica es utilizada exclusivamente por una persona física, el sello electrónico puede ser utilizado exclusivamente por una persona jurídica o una unidad organizativa del Estado.

Anteriormente, el término etiqueta electrónica se utilizaba para el sello electrónico. Es equivalente a un sello oficial, que garantiza la integridad y el origen de un documento.

El sello calificado se basa en una firma electrónica calificada y es su equivalente con respecto al área de su uso (exclusivamente para personas jurídicas). También requiere un **HSM** (*Hardware Security Module*) específico para almacenar una clave privada (secreta).

Los tipos de certificados en términos de firma electrónica son los siguientes:

1. Personal, es decir, destinado exclusivamente a personas físicas
   a) comercial - la ley no especifica su contenido; se utiliza, por ejemplo, para acceder a los buzones de datos
   b) calificado - la ley no especifica su contenido; se utiliza, por ejemplo, para firmar mensajes y documentos
2. Sistema, es decir, destinado a personas jurídicas, unidades organizativas del Estado o autoridades públicas.
   a) comercial - por ejemplo, para iniciar sesión en un servicio de archivos
   b) cualificado - diseñado para crear sellos electrónicos

10.4 Marca de tiempo

Un sello de tiempo (o sello de tiempo) demuestra la existencia de un documento en una forma dada en un momento dado (específico); no se refiere a cuándo se creó el documento y a quién pertenecía el documento.

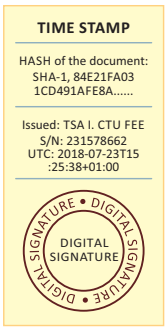
La estructura de datos del cronomarcador es similar a la estructura de los certificados. Técnicamente, un sello de tiempo se implementa como una firma electrónica más derivada de la **TSA** (*Time Stamp Authority*).

También existe el llamado sello de tiempo cualificado, que es el equivalente a un sello electrónico cualificado o a una firma electrónica cualificada. El sello de tiempo calificado es creado por un proveedor de servicio de sello de tiempo calificado.

La estructura firmada electrónicamente de un sello de tiempo incluye, entre otras muchas cosas:

- nombre del editor,
- número de serie único del sello,
- HASH (suma de comprobación) derivada del documento
- momento

TSA, autoridad de sello de tiempo, prueba la sincronización de su fuente de tiempo con **UTC** (*Universal Time Coordinated*).



Ejemplo de cronomarcador