Sistemas de Computación 2

« Redes »

Virtual Private Network

VPN

Una VPN es una conexión virtual entre dos dispositivos que permite el envío de información de manera segura a través de un medio inseguro como lo es Internet.

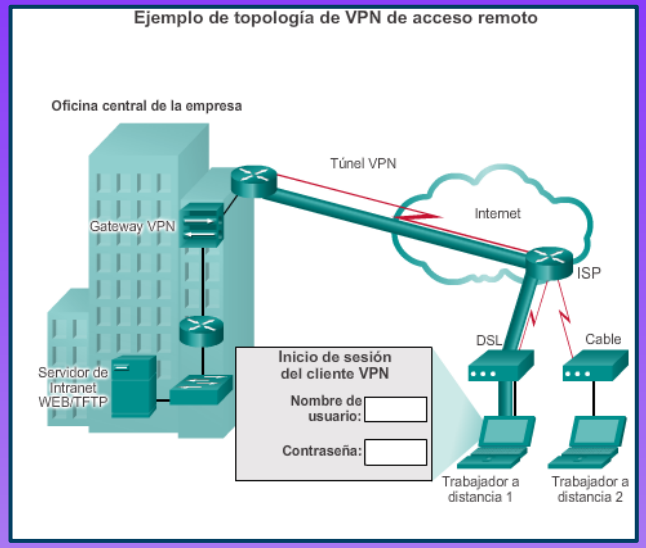
Una VPN es una conexión cifrada entre redes privadas a través de una red pública, como Internet. En vez de usar una conexión dedicada de capa 2, como una línea alquilada (ATM, FrameRelay, etc), una VPN usa conexiones virtuales llamadas “túneles VPN”, que se enrutan a través de Internet desde la red privada de la empresa hasta el host del sitio o del empleado remoto.

Se establece una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifradas o combinación de ambas.

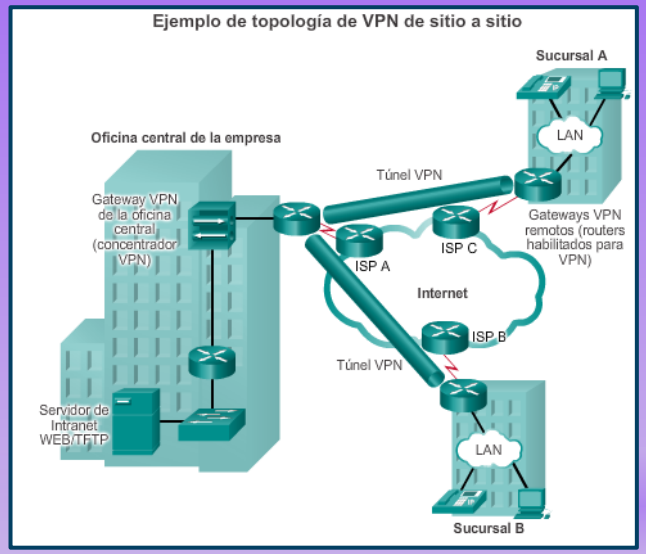
Características

- Autentificación y autorización: usuario/equipo y nivel de acceso.
- Integridad: mediante el uso de funciones de hash.
- No repudio: mensaje firmado.
- Control de acceso: usuarios con acceso solo a aquello que fueron autorizados.
- Auditoria y registro de actividades: correcto funcionamiento.
- Calidad del servicio: rendimiento.

Tipos de VPN



VPN de acceso remoto: las VPN de acceso remoto permiten que los hosts individuales, como los empleados a distancia, los usuarios móviles y los consumidores de extranets, accedan a la red de una empresa de manera segura a través de Internet. Por lo general, cada host tiene cargado un software de cliente VPN o usa un cliente basado en Web.



VPN punto a punto: Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El equipo central VPN, que posee un vínculo a Internet permanente, acepta las conexiones vía Internet provenientes de los sitios y establece el "túnel" VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales, sobre todo en las comunicaciones internacionales.

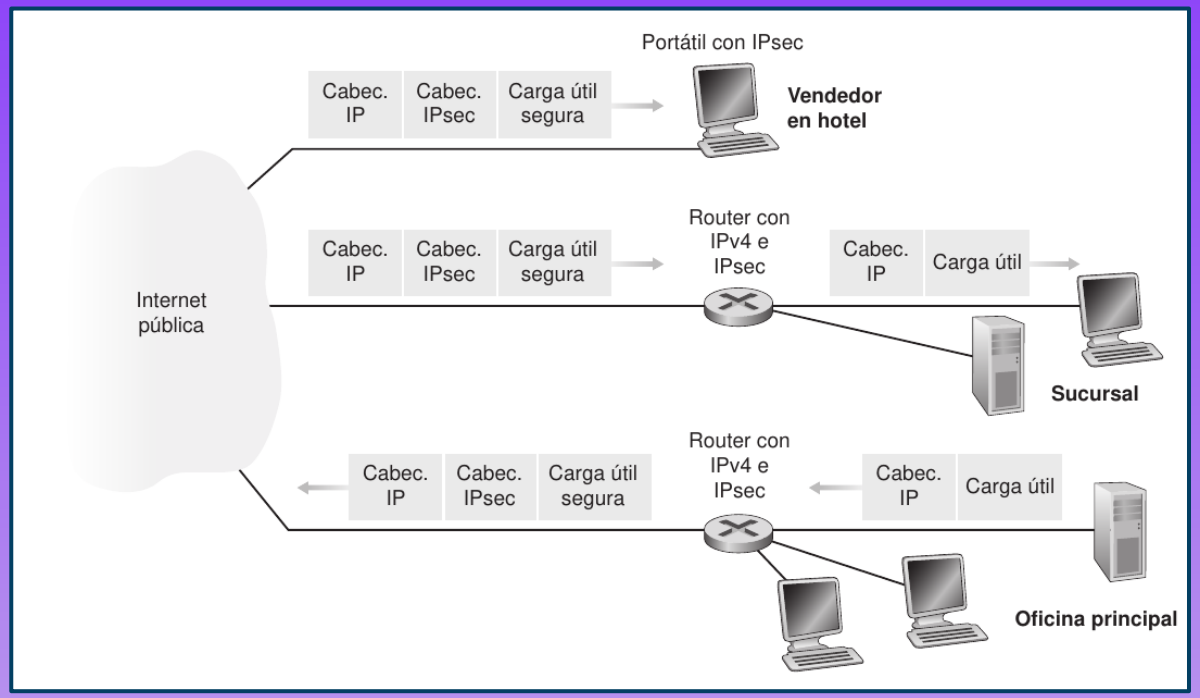
IPsec y redes privadas virtuales

El protocolo de seguridad IP, más conocido como IPsec, proporciona seguridad en la capa de red. IPsec proporciona seguridad a los datagramas IP intercambiados por cualesquiera dos entidades de la una red. Muchas instituciones (corporaciones, agencias gubernamentales, organizaciones, etc.) utilizan IPsec para crear redes privadas virtuales (VPN, Virtual Private Network), que funcionan sobre la red Internet pública.

Normalmente, una empresa que abarque múltiples regiones geográficas deseará disponer de su propia red IP, de modo que sus hosts y servidores puedan intercambiarse datos de forma segura y confidencial. Para conseguir este objetivo, esta empresa podría implantar realmente una red física independiente (incluyendo routers, enlaces y una infraestructura DNS) que esté completamente separada de la red Internet pública. Dicha red separada, dedicada exclusivamente, se denomina red privada. No es sorprendente que tales redes privadas puedan llegar a ser muy costosas, ya que la empresa necesitará comprar, instalar y mantener su propia infraestructura física de red.

En lugar de implantar y mantener una red privada, muchas empresas crean actualmente redes VPN sobre la red Internet pública existente. Con una VPN el tráfico entre sucursales se envía a través de la red Internet pública, en lugar de enviarse a través de una red físicamente independiente. Pero para proporcionar confidencialidad, el tráfico entre sucursales se cifra antes de entrar en la Internet pública.

IPsec y redes privadas virtuales

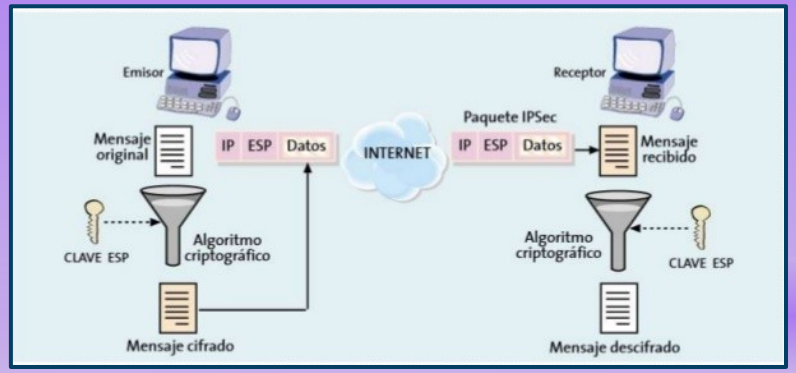


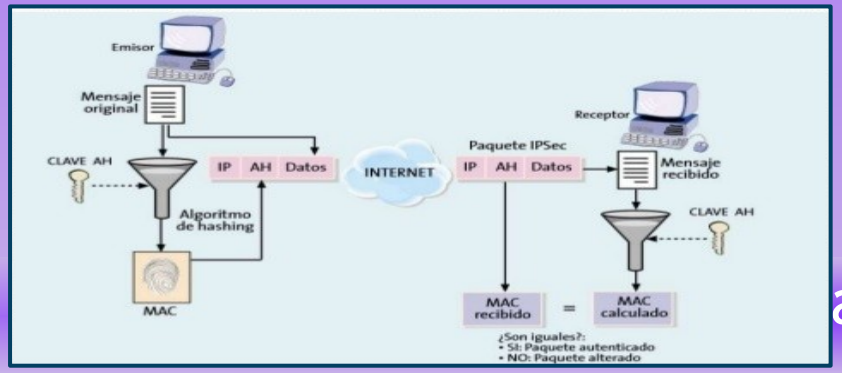
El router gateway de la oficina principal convierte el datagrama IPv4 simple en un datagrama IPsec y luego reenvía dicho datagrama IPsec hacia Internet. Este datagrama IPsec tiene de hecho una cabecera IPv4 tradicional, de modo que los routers de la red Internet pública procesan el datagrama como si se tratara de un datagrama IPv4 normal; para ellos el datagrama es, de hecho, como cualquier otro. Pero como se muestra en la imagen, la carga útil del datagrama IPsec incluye una cabecera IPsec, que es utilizada para el procesamiento IPsec; además, la carga útil del datagrama IPsec está cifrada. Cuando el datagrama IPsec llega al portátil del vendedor, el sistema operativo del equipo descifra la carga útil y proporciona algunos otros servicios de seguridad, como la verificación de la integridad de los datos, y pasa la carga útil descifrada hacia el protocolo de la capa superior (por ejemplo, hacia TCP o UDP) y de ahí a la aplicación que se utilizara para acceder a los datos.

Los protocolos AH y ESP

IPsec es un protocolo bastante complejo que está definido en más de una docena de documentos RFC. Dos documentos importantes son RFC 4301, que describe la arquitectura global de seguridad IP, y RFC 6071, que proporciona una panorámica de la serie de protocolos IPsec.

En la serie de protocolos IPsec hay dos protocolos principales: el protocolo de cabecera de autenticación (AH, Authentication Header) y el protocolo de carga útil de seguridad para encapsulación (ESP, Encapsulation Security Payload). Cuando una entidad IPsec de origen (normalmente un host o un router) envía datagramas seguros a una entidad de destino (también un host o un router) lo hace con el protocolo AH o el protocolo ESP. El protocolo AH proporciona autenticación del origen e integridad de los datos, pero no proporciona confidencialidad. El protocolo ESP proporciona autenticación del origen, integridad de los datos y confidencialidad. Puesto que la confidencialidad a menudo es crítica para las redes VPN y otras aplicaciones IPsec, el protocolo ESP se utiliza mucho más ampliamente que el protocolo AH.





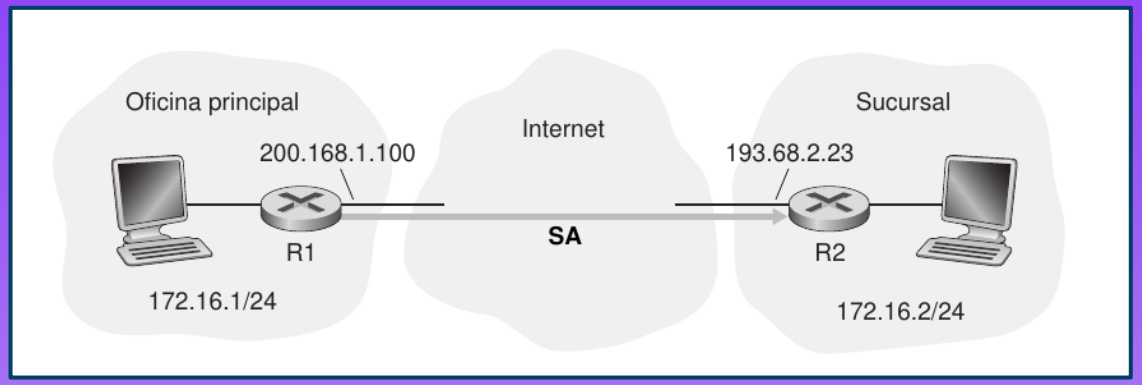
Asociaciones de seguridad

Los datagramas IPsec se intercambian entre parejas de entidades de red, como por ejemplo entre dos hosts, entre dos routers o entre un host y un router. Antes de enviar datagramas IPsec desde la entidad de origen a la de destino, ambas entidades crean una conexión lógica en la capa de red. Esta conexión lógica se denomina asociación de seguridad (SA, Security Association). Una asociación de seguridad es una conexión lógica de tipo simple; es decir, una conexión unidireccional desde el origen al destino. Si ambas entidades desean enviarse datagramas seguros entre sí, entonces será necesario establecer dos SA (es decir, dos conexiones lógicas), una en cada dirección.

Hay que recordar que no todo el tráfico enviado hacia Internet por los routers gateway o por las computadoras estará protegido mediante IPsec. Por ejemplo, un host situado en la oficina principal podría querer acceder a un servidor web (como Amazon o Google) disponible en la red Internet pública. Por tanto, el router (y los equipos) enviará hacia Internet tanto datagramas IPv4 normales como datagramas dotados de seguridad Ipsec.

Cada entidad IPsec (router o host) suele mantener información de estado para muchas asociaciones de seguridad. Cada entidad IPsec almacena la información de estado para todas sus asociaciones de seguridad en su base de datos de asociaciones de seguridad (SAD, Security Association Database), que es una estructura de datos contenida en el kernel del sistema operativo de esa entidad.

Asociaciones de seguridad



En la imagen se observan una asociación de seguridad existente entre el router R1 y el router R2. El router R1 mantendrá una cierta información de estado acerca de esta SA, la cual incluirá:

- Un identificador de 32 bits para la SA, denominado Índice de parámetro de seguridad (SPI, Security Parameter Index).
- La interfaz de origen de la SA (en este caso, 200.168.1.100) y la interfaz de destino de la SA (en este caso 193.68.2.23).
- El tipo de cifrado que se va a utilizar (por ejemplo, 3DES con CBC).
- La clave de cifrado.
- El tipo de comprobación de integridad (por ejemplo, HMAC con MD5).
- La clave de autenticación.

Cada vez que el router R1 necesite construir un datagrama IPsec para reenviarlo a través de esta SA, accederá a esta información de estado para determinar cómo debe autenticar y cifrar el datagrama. De forma similar, el router R2 mantendrá la misma información de estado para esta SA y utilizará esta información para autenticar y descifrar todos los datagramas IPsec que lleguen desde dicha asociación de seguridad.

El datagrama IPsec

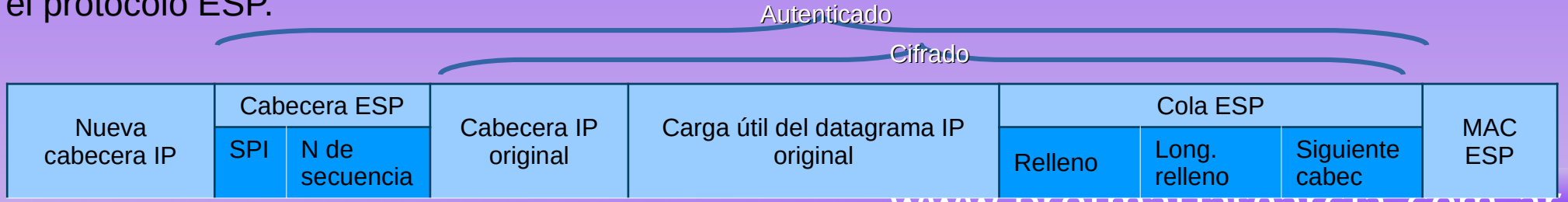
IPsec tiene dos formas distintas de paquete, una para el denominado modo túnel y otra para el denominado modo transporte. El modo túnel, al ser más apropiado para las redes VPN, está más ampliamente implantado que el modo transporte.

Suponga que el router R1 recibe un datagrama IPv4 normal procedente del host 172.16.1.17 (situado en la red de la oficina principal) que está destinado al host 172.16.2.48 (situado en la red de la sucursal). El router R1 utiliza la siguiente receta para convertir este “datagrama IPv4 original” en un datagrama Ipsec:

- Añade al final del datagrama IPv4 original (que incluye los campos originales de cabecera) un campo de “cola ESP”.
- Cifra el resultado utilizando el algoritmo y la clave especificados por la asociación de seguridad.
- Añade al principio de este paquete cifrado un campo denominado “cabecera ESP”.
- Crea un valor MAC de autenticación para toda la enchilada utilizando el algoritmo y la clave especificados en la SA.
- Añade el valor MAC al final de la enchilada formando así la carga útil.
- Por último, crea una nueva cabecera IP con todos los campos clásicos de la cabecera IPv4 y añade dicha cabecera al principio de la carga útil.

El datagrama IPsec

Observe que el datagrama IPsec resultante es un datagrama IPv4 perfectamente normal, con los campos tradicionales de cabecera IPv4 seguidos de una carga útil. Pero en este caso la carga útil contiene una cabecera ESP, el datagrama IP original, una cola ESP y un campo de autenticación ESP (estando cifrados el datagrama original y la cola ESP). El datagrama IP original tiene el valor 172.16.1.17 como dirección IP de origen y el 172.16.2.48 como dirección IP de destino. Puesto que el datagrama IPsec incluye el datagrama IP original, estas direcciones se incluyen (y se cifran) como parte de la carga útil del paquete IPsec. ¿Pero qué sucede con las direcciones IP de origen y de destino contenidas en la nueva cabecera IP, es decir, en la cabecera situada más a la izquierda en el datagrama IPsec? Como cabría esperar, esos valores se configuran con las direcciones de las interfaces de router de origen y de destino situadas en los dos extremos de los túneles, es decir, con los valores 200.168.1.100 y 193.68.2.23. Asimismo, el número de protocolo en este nuevo campo de cabecera IPv4 no se configura con el valor correspondiente a TCP, UDP o SMTP, sino con el valor 50, que indica que se trata de un datagrama IPsec que está empleando el protocolo ESP.



El datagrama IPsec

Después de que R1 envíe el datagrama IPsec hacia la red Internet pública, este pasará a través de muchos routers antes de alcanzar R2. Cada uno de estos routers procesará el datagrama como si fuera un datagrama normal; de hecho, todos esos routers no son conscientes de que el datagrama esté transportando datos cifrados mediante IPsec. Para estos routers de la red Internet pública, puesto que la dirección IP de destino contenida en la cabecera externa es R2, el destino último del datagrama es R2.

La cola ESP está compuesta por tres campos: relleno, longitud de relleno y siguiente cabecera. Hay que recordar que los sistemas de cifrado de bloque requieren que el mensaje que hay que cifrar sea un múltiplo entero de la longitud de bloque. Por ello se emplea un relleno (compuesto por bytes que no tienen ningún significado) para que, al añadirlo al datagrama original (junto con los campos de longitud de relleno y de siguiente cabecera), el “mensaje” resultante tenga un número entero de bloques. El campo de longitud de relleno indica a la entidad receptora cuánto relleno se ha insertado (y, por tanto, cuánto relleno habrá que eliminar). El campo de siguiente cabecera indica el tipo (por ejemplo, UDP) de los datos contenidos en el campo de datos de carga útil. Los datos de carga útil (normalmente, el datagrama IP original) y la cola ESP se concatenan y se cifran.

El datagrama IPsec

Delante de esta unidad cifrada se encuentra la cabecera ESP, que se envía como texto en claro y que consta de dos campos: el SPI y el campo de número de secuencia. El SPI indica a la entidad receptora cuál es la SA a la que pertenece el datagrama; la entidad receptora puede entonces indexar su base de datos SAD con el índice SPI para determinar los algoritmos y claves apropiados de autenticación/descifrado. El campo de número de secuencia se utiliza para defenderse frente a los ataques por reproducción.

La entidad emisora también añade un código MAC de autenticación. Como hemos dicho anteriormente, la entidad emisora calcula un código MAC para toda la enchilada (compuesta por la cabecera ESP, el datagrama IP original y la cola ESP, estando el datagrama y la cola cifrados).

Para calcular un valor MAC, el emisor añade una clave secreta MAC y luego calcula un valor hash de longitud fija para el resultado.

Cuando R2 recibe el datagrama IPsec, observa que la dirección IP de destino del datagrama es el propio R2, por lo que dicho router se encarga de procesar el datagrama. Puesto que el campo de protocolo (en la cabecera IP situada más a la izquierda) tiene el valor 50, R2 ve que debe aplicar el procesamiento ESP de IPsec al datagrama. En primer lugar, analizando la autenticación, R2 utiliza el SPI para determinar a qué asociación de seguridad (SA) pertenece el datagrama.

El datagrama IPsec

En segundo lugar, calcula el valor MAC y verifica que es coherente con el valor contenido en el campo ESP MAC. Si lo es, el router sabrá que el mensaje procede del router R1 y que no ha sido manipulada. En tercer lugar, comprueba el campo de número de secuencia para verificar que el datagrama sea reciente y no un datagrama reproducido. En cuarto lugar, descifra la unidad cifrada utilizando la clave y el algoritmo de descifrado asociados con la SA. En quinto lugar, elimina el relleno y extrae el datagrama IP normal original. Y, finalmente, en sexto lugar, reenvía el datagrama original a la red de la sucursal para que el datagrama llegue a su verdadero destino.

Cuando el router R1 recibe un datagrama (no dotado de seguridad) procedente de un host de la red y dicho datagrama está destinado a alguna dirección IP de destino situada fuera, ¿cómo sabe R1 si ese datagrama debe ser convertido en un datagrama IPsec? Y si tiene que ser procesado por IPsec, ¿cómo sabe R1 qué SA (de las muchas asociaciones de seguridad existentes en su base de datos SAD) hay que utilizar para construir el datagrama Ipsec? Junto con una base de datos SAD, la entidad IPsec también mantiene otra estructura de datos denominada base de datos de políticas de seguridad (SPD, Security Policy Database). La SPD indica qué tipos de datagramas (en función de la dirección IP de origen, de destino y el tipo de protocolo) hay que procesar mediante IPsec; y para aquellos que haya que procesar mediante IPsec, qué SA debe emplearse. En un cierto sentido, la información de una SPD indica “qué” hacer con los datagramas que lleguen, mientras que la información de la SAD indica “cómo” hay que hacerlo.

IKE: gestión de claves en IPsec

Cuando una red VPN tiene un pequeño número de puntos terminales (por ejemplo, solo dos routers, el administrador de la red puede introducir manualmente la información de la SA (claves y algoritmos de cifrado/autenticación y los índices SPI) en las bases de datos SAD de los puntos terminales. Este tipo de “introducción manual” de las claves resulta obviamente poco práctico para una VPN de gran tamaño, que puede constar de centenares o incluso miles de hosts y routers IPsec. Las tareas de implantación de gran envergadura y geográficamente distribuidas requieren un mecanismo automatizado para la creación de las SA. IPsec lleva a cabo este tipo de tarea mediante el protocolo de Intercambio de claves de Internet (IKE, Internet Key Exchange), especificado en RFC 5996.

IKE presenta algunas similitudes con el procedimiento de acuerdo en SSL. Cada entidad IPsec tiene un certificado, que incluye la clave pública de la entidad. Al igual que en SSL, el protocolo IKE exige que las dos entidades intercambien certificados, negocien los algoritmos de autenticación y cifrado e intercambien de modo seguro el material necesario para crear las claves de sesión para las SA de IPsec. A diferencia de SSL, IKE emplea dos fases para llevar a cabo estas tareas.

IKE: gestión de claves en IPsec

La primera fase está compuesta por dos intercambios de parejas de mensajes entre R1 y R2:

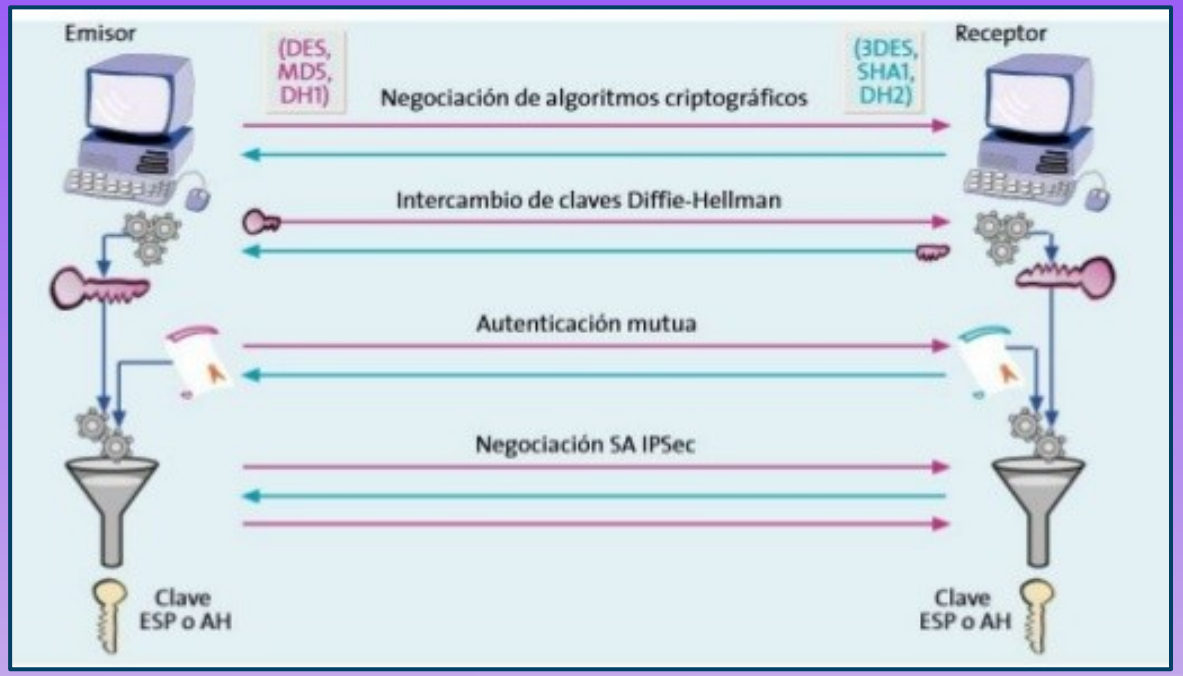
1) Durante el primer intercambio de mensajes los dos lados utilizan Diffie-Hellman para crear una IKE SA bidireccional entre los routers. Esta SA IKE bidireccional es enteramente distinta de las SA IPsec. La IKE SA proporciona un canal autenticado y cifrado entre los dos routers. Durante este primer intercambio de parejas de mensajes se establecen las claves de cifrado y autenticación para la IKE SA. También se establece un valor secreto maestro que se utilizará para calcular las claves IPSec SA posteriormente en la fase 2. Observe que durante este primer paso no se utilizan claves pública y privada RSA. En particular, ni R1 ni R2 revelan su identidad firmando un mensaje con su clave privada.

2) Durante el segundo intercambio de mensajes ambos lados se revelan mutuamente su identidad, firmando sus mensajes. Sin embargo, las identidades no son reveladas a nadie que esté husmeando pasivamente el canal de comunicación, ya que los mensajes se envían a través del canal IKE SA seguro. También durante esta fase los dos lados negocian los algoritmos de cifrado y autenticación IPsec que serán empleados por las asociaciones de seguridad IPsec.

En la fase 2 de IKE los dos lados crean una SA en cada dirección. Al final de la fase 2 las claves de sesión para cifrado y autenticación habrán sido establecidas en ambos terminales para las dos SA.

IKE: gestión de claves en IPsec

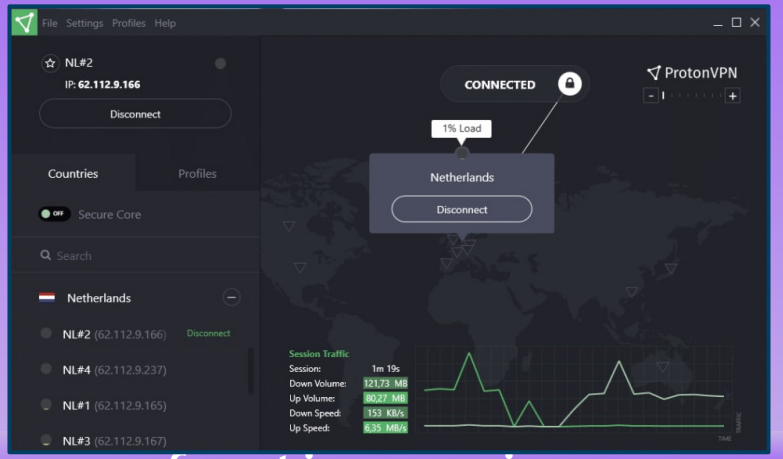
Los dos lados pueden emplear entonces las SA para enviar datagramas seguros. La principal motivación para que existan dos fases en IKE es el coste computacional: puesto que la segunda fase no implica ningún tipo de criptografía de clave pública, IKE puede generar un gran número de asociaciones de seguridad entre las dos entidades IPsec con un coste de computación relativamente bajo.



Acceso del usuario a la VPN

VPN Stand-Alone: Este es el caso en que la VPN es proporcionada por un dispositivo físico. Al conectarse a internet este dispositivo establece una conexión segura con el servidor VPN que le fue configurado. Esto último permite que el usuario del dispositivo se conecte a la red de área local del proveedor del servidor. Es decir, si una empresa le brinda a un empleado uno de estos dispositivos (También conocidos como Routers VPN), el usuario se conectara a internet desde su casa pero al pedir su IP le será asignado uno que corresponde a la red de la oficina. Si bien su posición física esta fuera de la oficina, su máquina tendrá conexión tal y como si estuviera conectado al cable de red de su área de trabajo. Esto se logra hacer de manera segura gracias a que desde el usuario hasta el servidor VPN en la oficina todos los mensajes son encriptados.

VPN Software: Otra solución es que este servicio lo brinde un software. En esta modalidad el usuario ejecuta un programa que intercepta todos los paquetes que el equipo envía, los encripta y los envía al servidor VPN correspondiente. Este servicio hoy en día está disponible no solo para empresas, sino que existen soluciones para cualquier usuario. Un ejemplo de esto es el programa ProtonVPN, este habilita conexiones a distintos servidores VPN de forma gratuita y ofreces opciones pagas.



Bibliografía & Licencia

- CCNA 2 (2017). Switching, Routing and Wireless Essentials. Cisco Press.
- Textos tomados, corregidos y modificados de diferentes páginas de Internet, tutoriales y documentos.

- Autor:

Matías E. García

Prof. & Tec. en Informática Aplicada

www.profmatiasgarcia.com.ar

info@profmatiasgarcia.com.ar