¿Qué problemas resuelve IPsec?

Sin IPsec, los paquetes IP son vulnerables a: • Intercepción (sniffing): Cualquiera puede leer el contenido. • Modificación (man-in-the-middle): Un atacante puede cambiar los datos en el camino. • Suplantación (spoofing): Un atacante puede hacerse pasar por otro. • Ataques de repetición (replay attack): Un atacante puede grabar un paquete y reenviarlo para causar acciones no deseadas.

Psec es un conjunto de protocolos estándar, neutrales respecto al fabricante, que se utiliza para unir dos redes LAN físicamente distintas. Las LAN se conectan como si fueran una única red lógica, a pesar de estar separadas por Internet.

El protocolo IPSEC levanta un túnel seguro entre el usuario y el equipo de borde (firewall), donde el cliente VPN crea una interfaz virtual que cifra todo el tráfico destinado a la empresa

El tráfico que sale de la PC de un usuario conectado a la VPN inicialmente podía pasar completamente por la infraestructura de la empresa, incluso para navegar por internet. Sin embargo, muchas configuraciones modernas utilizan el "split tunnel", que permite que el tráfico destinado a internet salga directamente por la conexión del usuario, mientras que el tráfico para la red corporativa se cifra y se envía por el túnel. Las políticas de navegación y restricciones de seguridad aplicadas a los usuarios conectados a la VPN dependen de la configuración de cada empresa, a menudo para mitigar riesgos de seguridad como la infección por malware que podría propagarse a la red corporativa.

IPSEC trabaja en la capa de red (capa 3 del modelo OSI) y es opcional en IP versión 4, pero es parte integral de IP versión 6. Se identificaron tres casos de uso:

- La conexión de usuarios remotos a un terminador de túneles VPN,
- La conexión de dos edificios (side-to-side) a través de Internet, y
- Topologías más complejas como *Hub and Spoke* (sucursales conectadas a una central) o *Mesh* (comunicación directa entre sucursales).

En el contexto de conectar dos sucursales (side-to-site), se discutieron las opciones de conectividad de red de área amplia (WAN) como Metro Ethernet o MPLS.

Se explicó que Metro Ethernet es más costoso y físicamente limitante,

mientras que MPLS ofrece conectividad privada y garantizada por el proveedor, con un costo intermedio.

La tercera opción es usar dos enlaces de Internet, que es mucho más económico pero requiere el uso de IPSEC para asegurar la comunicación a través de una red insegura.

Cuando se utilizan enlaces de Internet para conectar dos sitios (side-to-site), se establece un único túnel IPSEC entre el firewall de un sitio y el firewall del otro, utilizando sus direcciones IP públicas. Esta configuración es más fácil de administrar que instalar clientes VPN individuales en cada PC y es igual de segura, permitiendo que todo el tráfico interno viaje cifrado por el túnel

IPsec provee servicios de seguridad:

- Negociación de mecanismos de seguridad entre nodos.
- Autenticación, al identificar el origen y el destino de la transmisión en ambas direcciones.
- Confidencialidad, para otorgar privacidad en la transmisión de datos de usuario.
- Integridad, al asegurar la no alteración de los datos durante su envío.
- No repudio, para que el origen no pueda rechazar un envío malicioso.

Esto se logra mediante protocolos criptográficos y la autenticación mutua, utilizando el concepto de "asociación de seguridad" (SA), que combinan algoritmos y claves para cifrar y autentifcar el tráfico.

Para la protección a un paquete saliente, IPsec compone una Asociación de Seguridad (SA) con estos datos:

- Security Parameter Index (SPI): Numero de 32 bits seleccionado para identificar unívocamente una SA en cualquier dispositivo conectado.
- IP Destination Address: La dirección IP destino del extremo donde se establecerá la SA.
- Security Protocol Identifier: Especifica el protocolo de seguridad (AH y/o ESP) que se aplicara al trafico de la SA.

Al llegar el paquete a su destino, el receptor comparara con su Base de Datos de SA local (SADB) la SA que se corresponde al paquete entregado.

Para la protección a un paquete entrante se realiza un procedimiento similar; en este caso IPsec toma las claves de verificación y descifrado de la (SADB).

IPSEC es un conjunto de protocolos, no solo uno. Utiliza ISAKMP (Internet Security Association and Key Management Protocol) para definir el formato de las Security Associations, e IKE (Internet Key Exchange) para gestionar cómo se intercambian las SA y cómo se generan las claves. IKE es fundamental para la autenticación de los nodos, el manejo de las SA y la gestión del intercambio de claves de manera segura, utilizando Diffie-Hellman.

ISAKMP presenta cuatro requisitos básicos:

- Autenticar a los nodos participantes en la comunicación.
- Crear y manejar las Asociaciones de Seguridad (SA).
- Proveer mecanismos para la generación de claves.
- Protección contra amenazas (como ataques de repetición o denegación de servicio).

El protocolo IKE realiza:

- Inserción de las políticas de seguridad que se utilizaran en el intercambio de las SA.
- Gestión de intercambio de las SA.
- Definición del cifrado de llaves.
- Autenticación de la identidad de los extremos.

IKE opera en dos fases. En la Fase Uno, se establece una autenticación (mediante una *pre-shared key*, firmas digitales o clave pública - PKI) y se genera una clave secreta compartida (usando Diffie-Hellman) SA ISAKMP bidireccional para un túnel seguro, utilizando una única clave para cifrar y descifrar el tráfico saliente y entrante.

En la Fase Dos, una vez que el canal se considera seguro, se negocian nuevas Security Associations de IPSEC con dos claves unidireccionales (una para cifrar y otra para descifrar), y si se activa Perfect Forward Secrecy (PFS), se generarán nuevas claves cuando las actuales expiren en la Fase 2.

Existen dos opciones de protocolo de seguridad disponibles para IPsec: Authentication Header (AH) y Encapsulating Security Payload (ESP). Para lograr la integridad se utilizan funciones hash, y la confidencialidad se logra mediante un protocolo de encriptación como AES.

- Authentication Header (AH): AH proporciona integridad, autenticación y no repudio de datos, pero no ofrece confidencialidad, ya que el texto viaja en texto plano. El protocolo utiliza un hash (Hash Message Authentication Code o HMAC) para generar una huella digital y verificar si el paquete ha sido alterado en tránsito, pero la información sigue siendo legible.
- Encapsulating Security Payload (ESP): ESP ofrece integridad y autenticación de origen, y añade confidencialidad mediante algoritmos de cifrado como 3DES o AES, cifrando el contenido del paquete y no solo el encabezado. A diferencia de AH, que solo firma el paquete, ESP crea un contenedor cifrado para la carga útil, por lo cual se está descartando AH en muchas implementaciones de IPsec.

Dependiendo del nivel sobre el que se actúe es posible establecer dos modos básicos de operación: Transporte y Túnel

Modo Transporte: El modo transporte conecta directamente una PC con otra, ofreciendo seguridad de extremo a extremo, donde la carga útil del paquete se cifra y autentica, mientras que el enrutamiento permanece intacto porque las cabeceras IP no se modifican. En este modo, solo existe un único encabezado IP que conecta el origen con el destino.

Modo Túnel: El modo túnel, el más utilizado en la actualidad, establece comunicaciones de red a red, donde los túneles seguros se levantan entre *routers* o *firewalls*. En este modo, todo el paquete IP original (datos y cabeceras del mensaje) es cifrado y autenticado, y se encapsula dentro de un nuevo encabezado IP.

En el modo túnel, el nuevo encabezado IP es necesario debido a los dispositivos intermediarios (*firewall* o *router*) que levantan el túnel IPsec, y estas nuevas cabeceras contienen las IP públicas de origen y destino de los dispositivos de red que establecen el túnel (01:16:24). El dispositivo de red encapsula todo el paquete original, cifrándolo, para que viaje por Internet de forma segura entre las IP públicas, permitiendo que dos redes separadas se comuniquen mediante *routing*

El protocolo IPsec es un conjunto de varios estándares que utilizan diferentes tecnologías para lograr la confidencialidad (cifrado AES), la integridad (hashes como MD5) y la autenticación (RSA o Diffie-Hellman).