Apuntes SinCara Extras IPSec

- IPsec (abreviatura de Internet Protocol security) es un conjunto de protocolos (no especifica algoritmos) cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. Es decir, proporciona servicios de seguridad a la capa IP (capa 3 OSI) y a todos los protocolos superiores, como TCP y UDP (capa de transporte en internet). La gran ventaja de IPsec, es que no hay que hacer ningún cambio en las capas superiores.
- Es parte del estándar IPv6, mientras que en IPv4 es opcional.
- Los estándares IPsec definen dos modos distintos de funcionamiento de IPsec, el modo transporte y el modo túnel. Dichos modos no afectan a la codificación de paquetes. Los paquetes están protegidos por AH, ESP, o ambos en cada modo.

Modos

- Modo Transporte.
  - Generalmente es el modo usado para comunicaciones de ordenador a ordenador, o de ordenador a red.
  - La cabecera IPsec se insertará a continuación de la cabecera IP y justo antes de los datos aportados por la capa de transporte. De esta forma, sólo la carga útil es autenticada y opcionalmente cifrada, y se mantienen las direcciones IP originales.
  - El modo transporte asegura la comunicación extremo a extremo pero los extremos deben saber de la existencia del protocolo IPsec y de la clave para poder entenderse.
- Modo Túnel.
  - Modo de comunicación entre redes, pero también se usa con ordenadores con redes, y ordenadores con ordenadores.
  - Todo el paquete IP (datos más cabeceras del mensaje) es cifrado o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento.
  - Generalmente, esa IP será la de los routers de entrada de cada red, con lo que este modo de funcionamiento facilita que los nodos puedan ocultar su identida

Componentes

- Cabecera de autenticación (AH - Authentication Header).
  - Garantiza la integridad y autenticación del datagram, mediante un hash cifrado, pero no su privacidad, los datos no están cifrados, eso solo lo hace ESP.
  - El enrutamiento permanece intacto, ya que no se modifica la cabecera IP, las direcciones IP no pueden ser traducidas (NAT), ya que eso invalidaría el hash.
  - También ofrece protección opcional contra los llamados «ataques de reinyección» (replay attack), donde se captura un mensaje por un usuario no autorizado y luego es re-enviado.
  - Calcula el Hash del contenido del paquete y de la cabecera original, y se añade a la cabecera AH, y lo cifra con la clave previamente compartida.
  - Cuando llega al destino, compara ese valor con el Hash calculado.
  - Si coincide, el datagrama no ha sido modificado.
  - El Hash (y solo el Hash), va codificado con una clave compartida previamente mediante IKE.
  - https://www.redeszone.net/2011/08/30/ipsec-volumen-ii-ah-cabecera-de-autenticacion/
- Carga de seguridad encapsulada (ESP - Encapsulating Security Payload).
  - La función principal del protocolo ESP es proporcionar confidencialidad a los datos, mediante el cifrado de los mismos, aunque es una función opcional.
  - Con la opción de cifrado activa, cifra el datagrama IP. Garantiza la confidencialidad.
  - Con la opción de autenticación activa, proporciona la misma protección que AH.
  - Con ambas opciones activas, proporciona integridad sólida, autenticación de datos y confidencialidad.

- Protocolo de intercambio de claves en internet (IKE - Internet key exchange).
    - Es una combinación de ISAKMP y de Oakley.
        - ISAKMP (Protocolo de administración de claves y asociaciones de seguridad en Internet) es un protocolo definido por RFC 2408 para establecer asociaciones de seguridad (SA) y claves criptográficas en un entorno de Internet. ISAKMP solo proporciona un marco para la autenticación y el intercambio de claves y este marco es independiente del intercambio de claves.
        - Oakley es un protocolo de acuerdo de claves, de intercambio de claves, que permite que las partes autenticadas intercambien material de claves en una conexión no protegida mediante el algoritmo de intercambio de claves Diffie-Hellman.
    - Este protocolo se utiliza para generar, administrar e intercambiar las claves necesarias para establecer las conexiones AH y ESP.
    - Emplea un intercambio secreto de claves de tipo Diffie-Hellman para establecer el secreto compartido de la sesión. Se suelen usar sistemas de Criptografía de clave pública o clave pre-compartida.
    - IKE no sólo está en IPsec sino que puede ser usado en los distintos algoritmos de enrutamiento como OSPF o RIP.
    - Es compatible con NAT transversal, aunque uno o los dos participantes estén detrás de una NAT, la conexión se podrá realizar.
    - Es resistente a ataques de denegación de servicio. IKE no realiza ninguna acción hasta que determina si el extremo que realiza la petición realmente existe, de esta forma se protege contra ataques desde direcciones IP falsas.

Servicios que proporciona IPsec

- **Confidencialidad**: requiere que la información sea accesible únicamente a las entidades autorizadas
- **Integridad**: incluye códigos detectores de errores y que la información no se vea modificada. IPsec permite al host receptor verificar que los campos de cabecera del datagrama y la carga útil cifrada no han sido modificados mientras el datagrama estaba en ruta hacia el destino.
- **Autenticación**: el usuario es realmente quien dice ser. Cuando el host recibe un datagrama IPsec de un origen, el host está seguro de que la dirección IP de origen del datagrama es el origen real del mismo.
- Permite el **acceso remoto** a ordenadores en distintos lugares como si estuviéramos en la misma red local (redes privadas virtuales). Gracias a esta característica podremos tener redes privadas comunicando diferentes sedes de empresas en Internet, sin necesidad de redes físicas privadas con el coste que estas redes conllevan.
- **Negociación del cifrado**: mecanismos que permiten a los dos host que están se están comunicando acordar las claves y algoritmos de cifrado.
- **Cifrado de la comunicación**: cuando el host emisor recibe un segmento de la capa de transporte, IPsec cifra la carga útil. Estos datos sólo puede ser descifrada por IPsec en el host receptor. Perfecto para el comercio electrónico.

Enlaces

- https://es.wikipedia.org/wiki/IPsec - Wikipedia
- https://es.wikipedia.org/wiki/Diffie-Hellman - Diffie–Hellman
- https://www.redeszone.net/tutoriales/vpn/ipsec-que-es-como-funciona/ - Extenso artículo explicando IPsec
- https://www.tecnodelinglesalcastellano.com/2013/01/protocolos-de-seguridad-ip-ipsec.html - Artículo muy técnico