Seguridad a nivel de red [L3] - IPSec

IPSec busca proveer de un framework de estándares abiertos para securizar comunicaciones sobre IP, protege todos los protocolos corriendo sobre IPv4 e IPv6. Muchas soluciones son específicas para una aplicación (PGP y S/MIM para email, SSHm para login remoto, Kerberos para control de acceso...). IPSec está por debajo de la capa de transporte, es transparente para las aplicaciones. En un router o Firewall IPSec provee seguridad fuerta para todo el tráfico que entra la red sin pasa la seguridad directa a la red interna y workstations, también es transparente para los usuarios. En IPv6 IPSec es requerido y es uno de los factore que aseguran que IPv6 provee más seguridad que IPv4.

Un problema de IPsec es que puede ser demasiado complejo y puede tener conflicto con algunso firewalls. IPSecs necesita los puertos TPC 50/51 y puertos UDP 500/4500 abiertos. TLS sua solo el puerto 443.

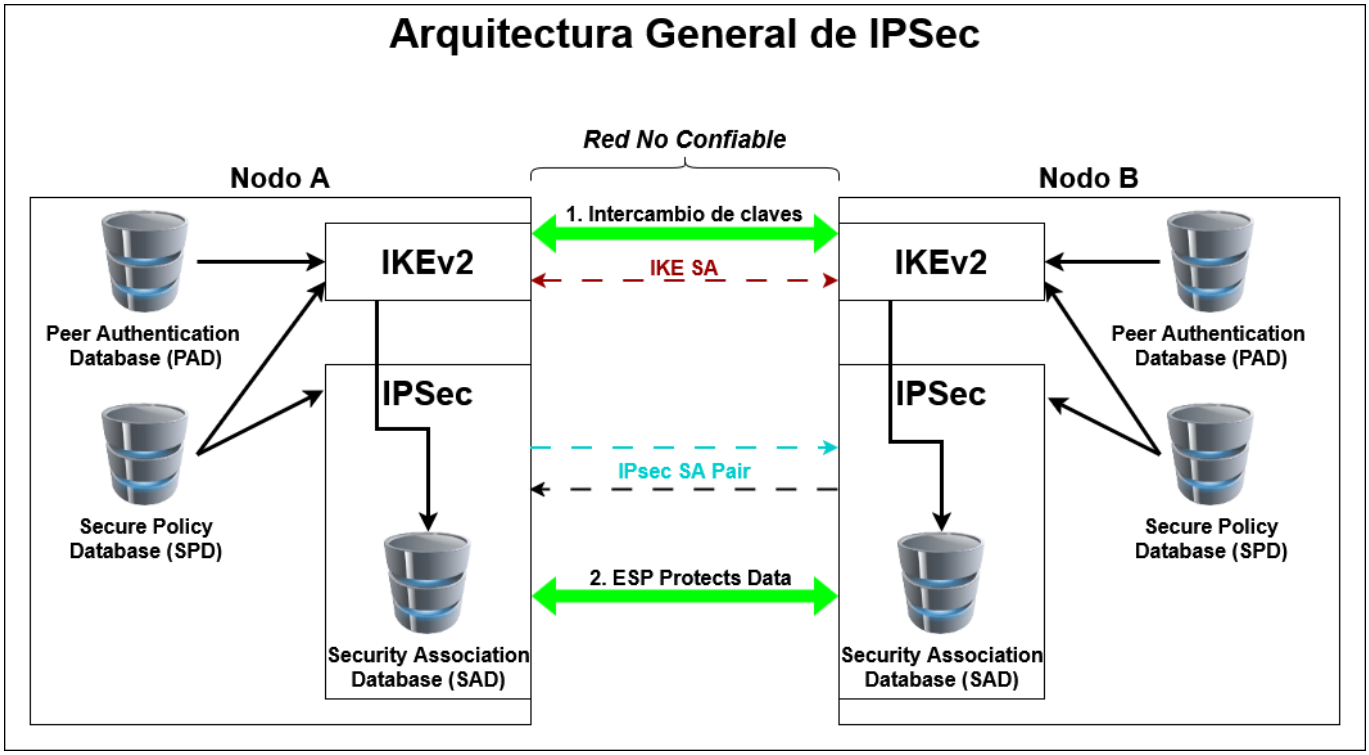
IPSec puede tener los siguientes usos:

- Establecimiento de VPN
- Acceso remoto de bajo coste
- Conectividad desde fuera de la red.

Principales componentes de IPSec

- Protocolos de seguridad:
    - AH - Authentication Header
    - ESP - Encapsulating Security Payload
        - Solo Cifrado
        - Cifrado con autenticación
- Cryptoalgoritmos que sportan el protocolo
- 2 modos de encapsulación
    - Transport Mode
    - Tunnel Mode
- Key distribution and Management Protocol (IKE)
- Security Police Database (SPD): Que paquetes serán protegidos, saltados o descartados
- Security Association Database (SAD): Homo van a ser protegidos lso paquetes por IPSec. Cada Security Asociation almacena todos los parámetros de seguridad del flujo de un paquete unidirecional en un extremo del tunel. Para comunicación bidireccional se necesitan al menos dos Security Association.

Arquitectura IPSec

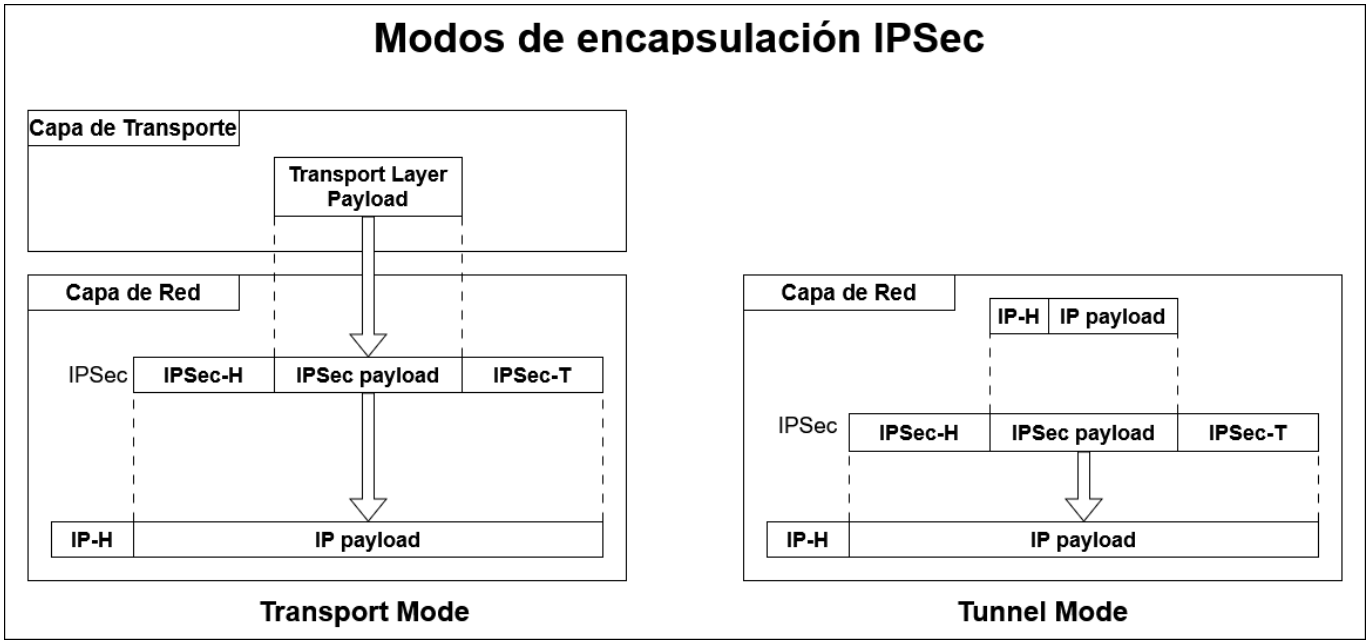


Protocolos y Servicios de IPSec

	AH	ESP (Solo Cifrado)	ESP (Cifrado + Autenticación)
Control de acceso	✔	✔	✔
Integridad sin conexion	✔		✔
Autenticación de origen de datos	✔		✔
Rechazo de paquetes replayed	✔	✔	✔
Confidencialidad		✔	✔
Confidencialidad de flujo de tráfico limitado		✔	✔

Modos de encapsulación de IPSec

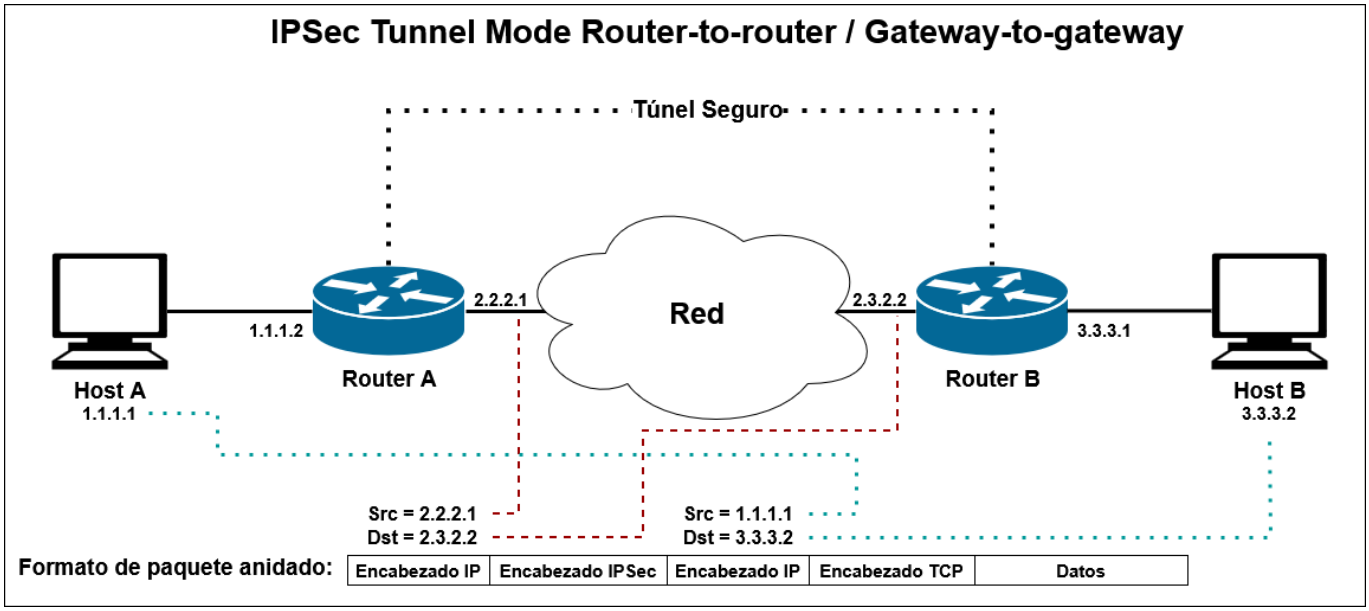
Hay 2 modos de encapsulación en IPSec, Transport Mode, que solo protege los datos de extremo a extremo y Tunnel mode:



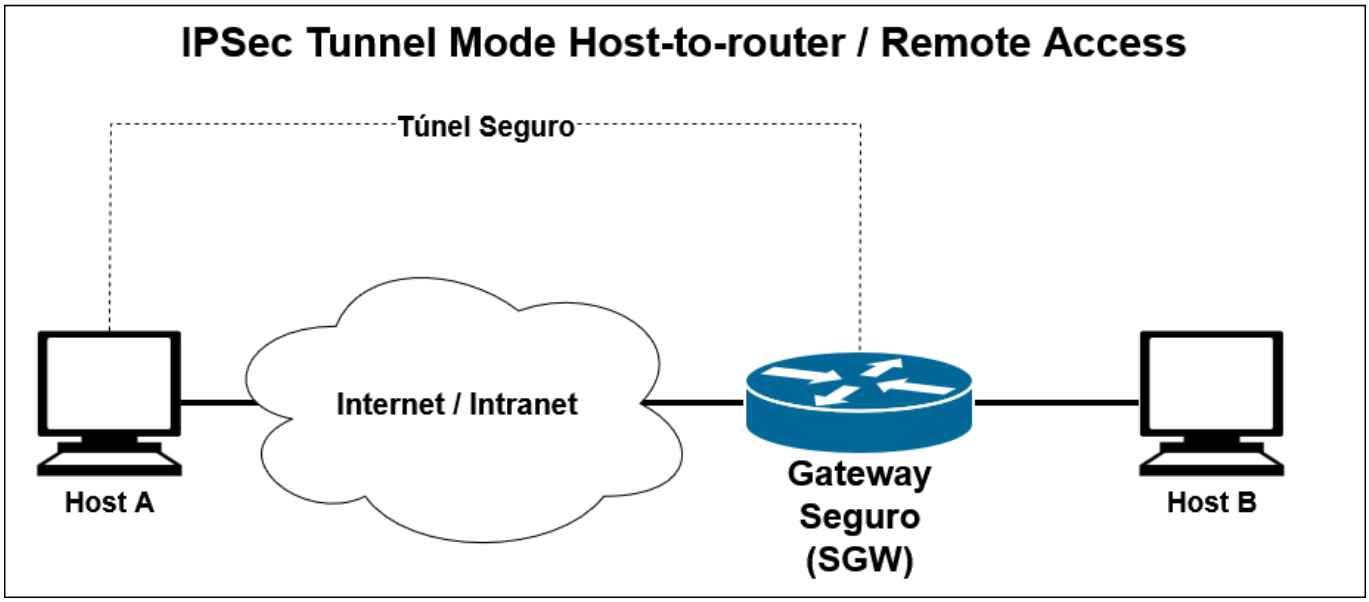
Encapsulación Tunnel Mode

El Tunnel Mode se usa cuando al menos uno de los extremos criptográficos no es un extremo de comunicación del paquete IP securizado. Esto permite gateways que securizan el tráfico IP para otras entidades.

Router-to-Router / Gateway-to-gateway



Host-to-Router / Gateway-to-gateway



Paquetes de IPSec

Formato de Paquete Authentication Header (AH)

- Provee autenticación de mensajes y revisión de integridad de la payload IP.
- Protege el Header IP lo más posible
- Next Header: TCP, UDP, ICMP
- SPI: para identificar SA
- Sequence Number: Para controlar el replay

Formato de paquete Encapsulating Security Payload (ESP)

- Provee confidencialidad y autenticación
- Cuando no se usa, se usa el algoritmo NULL definido en la RFC-2410
- El trailer de autenticación debe ser omitido si no se usa
- Cifrado o autenticación deben estar habilitados (o ambos)

Políticas de seguridad y selectores

Una Security Polocy Database (SPD) especifica que servicios deben ser ofrecidos a los datagramas IP y como.

- El SPD coniene una lista ordenada de entradas de políticas
- Coincide con el subset de tráfico IP preoveido a la SA
- Cada entrada está enlazada a uno o más selectores que definen el set de tráfico IP acompasado por la política de entrada.
- Cada registro incluye también una indicación de que hacer con el tráfico que coincide (Saltarlo, descartarlo o pasarlo por procesado IPSec)
- Una política tiene los siguientes campos:
    - Protocolo

    - IP local
    - Puerto local
    - IP remota
    - Puerto remoto
    - Acción: Bypass, protect + encapsulación o Discard.
    - Comentario

Procesamiento de paquetes de salida

- Coinciden los campos de selector del paquete saliente con las políticas de salida en el SPD:
    - Si no hay política definida para el paquete, se descarta
    - El Procesado IPSec no es requerido por la política
    - El Procesado IPSec es necesario por la política.
- En el último caso anterior, se localiza la primera entrada para el paquete, si no hay SA o gurpo SA especificado en la entrada se usa IKE para establecer el SA y el nuevo SA se almacena en el SAD.
- Cada SA en el SAD está especificado por:
    - Modo de protocolo de IPSec: Tunnel o transporte, AH o ESP
    - Algoritmos y parámetros
        - Algoritmos de autenticación AH
        - Algoritmo de cifrado ESP
        - Algoritmo de autenticación ESP
    - Tiempo de vida del SA
    - Parámetros Anti-Replay
- Si hay una SA o grupo de SA especificado en la entrada:
    - Se va a la entrada correspondiente en el SAD y se realiza el procesado IPSec especificado.

Procesamiento de paquetes de entradda

- Si el paquete de entradda no contiene ninguna cabecera IPSec, la capa IPSec revisa su SPD para determinar como procesar el paquete.
- Si el paquete de entraada contiene una cabecera IPSec:
    - Se usan la IP, el protocolo IPSec y el SPI del destino para reivsar el SA en el SAD, si el paquete no se encuentra se hace un DROP.
    - Se realiza el procesado IPSec de acuerdo al SA del paquete
    - Se busca una política de entrada en el SPD que que coincida con el paquete
    - Se entrega el paquete a la capa de transporte o se le hace forward.

Combinando Security Associations

- Las SA pueden implementar tanto AH como ESP. Para implementar ambos se deben combinar las SA:
    - Formar un grupo de Security Association
    - Puede finalizar en el mismo extremo o en uno diferente
    - Combinado por la adjacencia de transporte o la iteración de tunelado
- Para combianar autenticación y cifrado:
    - ESP con autenticación, ESP interno agrupado con un AH externo, grupo de transporte

interno y ESP externo.

Internet Key Exchange (IKE)

Busca crear una asociaciación de seguridad entre 2 dispositivos IPSec incluyento el establecimiento dinámico de claves compartidas temporales para cifrado y autenticación, el acuerdo de criptoalgoritmos y la utenticacióin mutua de los extremos del túnel. Hay 2 Fases:

- Fase 1: Establece la asociación de seguridad (IKE-SA) para la segunda fase, siempre autenticado por Diffie-Hellman
- Fase 2: Usa IKE-SA para crear una Security association (child-SA) para usar con AH y ESP. Usa claves derivadas en la primera fase para evitar intercambio Diffie-Hellman.

IKEv2

Intergra IKEv1 y características ISAKMP, además de otras extensiones

- Hereda todos los tipos de la payload ISAKMP añadiendo algunos más:
  - Security Association
  - Key Exchange
  - Identification
  - Certificate
  - Certificate request
  - Authentication
  - Nonce
  - Notify
  - Delete
  - Vendor ID
  - Traffic Selector
  - Encrypted
  - Configuration
  - Extensible Autehntication
- La payload tiene una estructura jerárquica compleja
- Puede contener múltiples porposiciones conmúltiples protocolos y múltiples transforms

Intercambios del protocolo IKEv2

- IKE_SA_INIT: Negociación de los algoritmos criptográficos para la Security Association de gestión (IKE_SA)
  - Proposciones en la payload SA:
    - Grupo Diffie-Hellman
    - Función pseudoaleatoria
    - Algoritmo de cifrado
    - Algoritmo de integridad
  - Determinación de material base criptográfico para derivar las claves
  - IKE_SA es bidireccional
- IKE_AUTH:
  - HDR no está cifrado pero tiene protección de integridad

    - Las otras payload estan escondidas
    - Autenticación mutua en los extremos del túnel.
        - Clave compartida
        - Firma Digital (PKI)
        - EAP
    - Negociación y establecimiento del primer child-SA para transmisión de datos.
- CREATE_CHILD_SA
    - Para establecer otras SA y componer un grupo de SA
    - Para regenerar la clave de IKE_SA o cualquier child-SA que haya expirado
    - Cuando se renueva la clave, un nuevo intercambio Diffie-hellman toma lugar
- INFORMATIONAL:
    - Notification
    - Eliminación de SA
    - Configuración de intercambio de Payload
    - Dead Peer Detection
    - NAT keepalive

Ataque Anti Dos Resource-Clogging

Si el responder abre un state para cada intento de conexión, el atacante puede iniciar miles de conexiones con IPs falsas. Las Cookies aseguran que el responder es stateles hasta que el iniciador produce al menos 2 mensajes

- El state del responder se almacena en una cookie y se envia al iniciador
- Una vez el iniciador responde, la cookie se regenera y se compara con la cookie devuelta por el iniciador
- Cuesta 2 mesajes extra en cada ejecución

IPSec AUTH exchange

Para evitar ataques MitM de intercambios Diffie-hellman, las pauload AUTH se construyen usando el paquete enviado durante IKE_SA_INIT, el noce recibido del otro lado y la identidad de propiedad.

- El mecanismo es asimétrico, los extremos no necesitan ser iguales, solo el iniciador puede usar EAP y el respodner tiene que usar firma digital.
- Peer Authorization Database (PAD): Enlaza SPD con IKE. Define una lista de peer IPSec autorizados, identificados por sus identidades IKE, que pueden establecer SA en una instancia local de SPD.
- La autenticación de clave compartida es susceptible a ataques de fuerza bruta: Si el atacante spoofea el responder original en la fase IKE_SA_INT, puede obtener toda la información, salvo la clave compartida para obtener la payload AUTH

IPSec y NAT

- El Authentication Header (AH) y NAT son incompatibles. ESP en transporte, al principio, también.

    - Cambiando ladirección ip de origen requiere el cambio del checksum del encabecado TCP/UDP, el cual o esta cifrado o su modificación puede afectar al valor de revisión de integridad.
- Para Tunnel Mode ESP un dispositivo Nat especial puede usar el SPI de los paquetes ESP para diferenciar flijos IPSec localizados tras el.
- Para correr IPSec con un NAT normal, se usa NAT Transversal, que modifica los paquetes IPSec/IKE usando ecapsulación UDP con origen y destino en el puerto 4500.
- IKE tiene un mencaniso de detección de NAT intriseca que realiza cambios del puerto 500 al 4500