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.

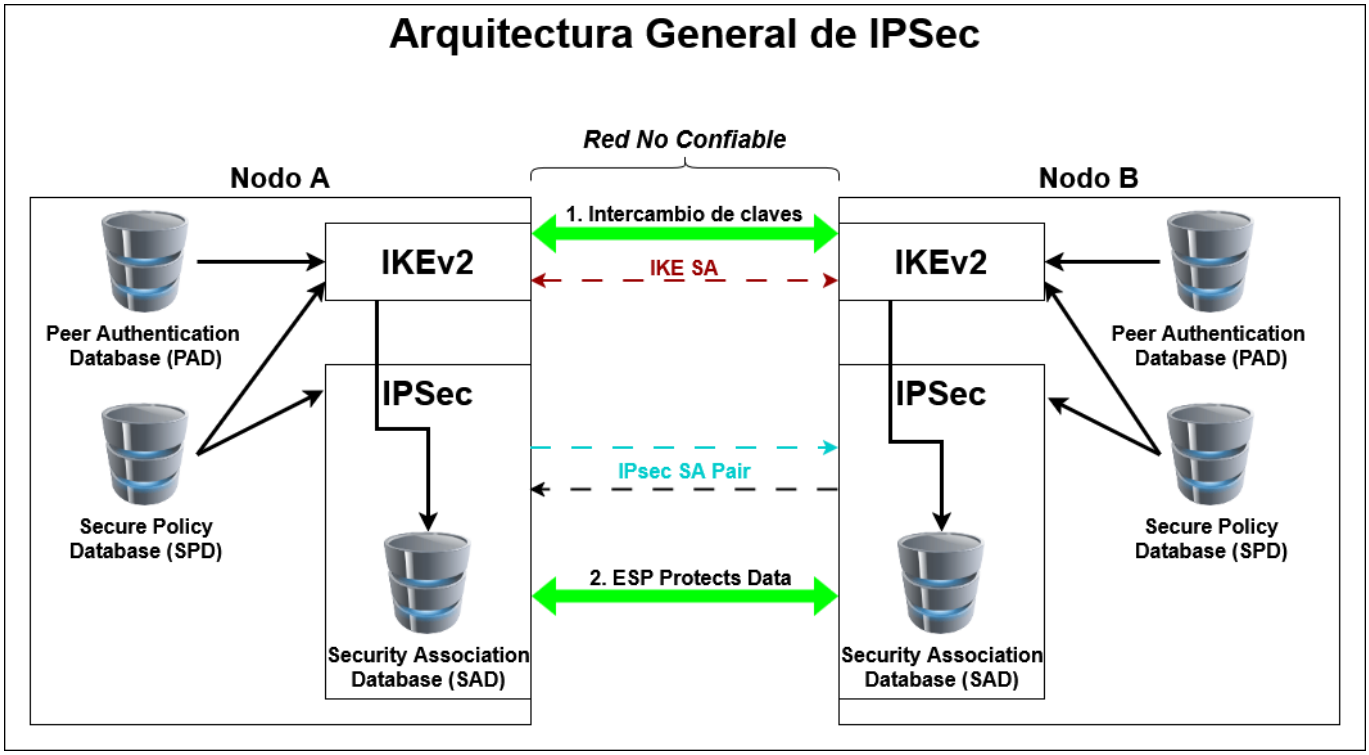
IPSec puede tener los siguientes usos:

- 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

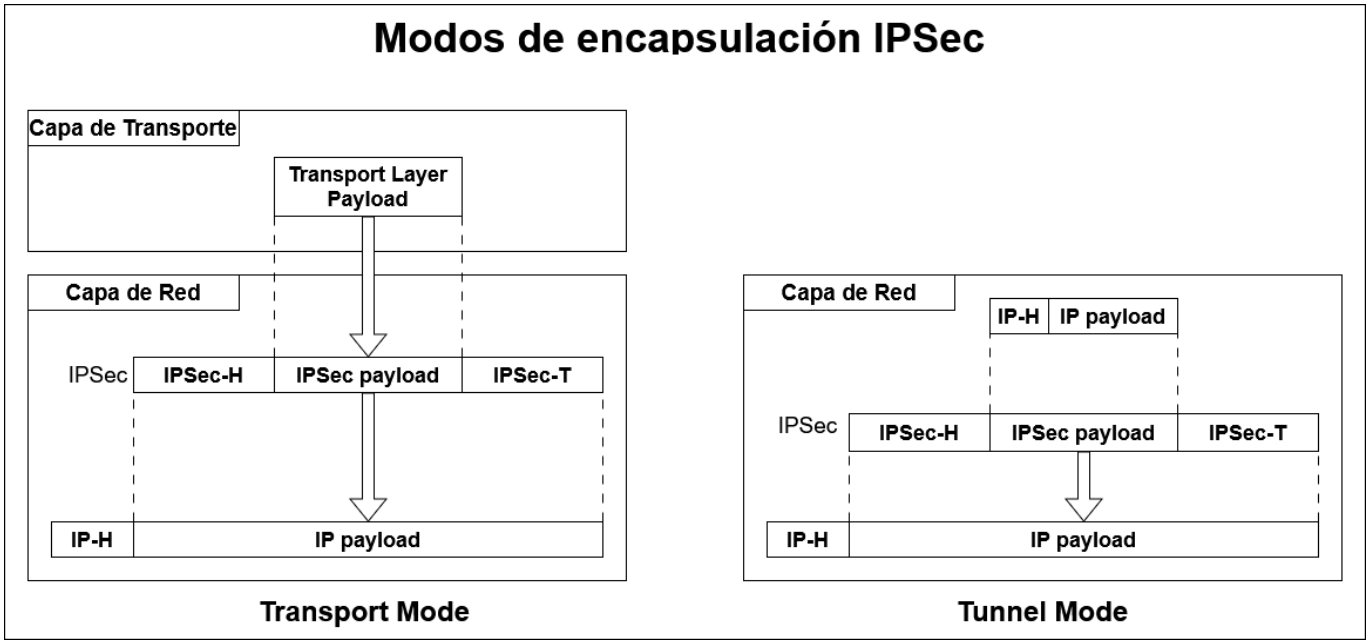


Protocolos y Servicios de IPSec

	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

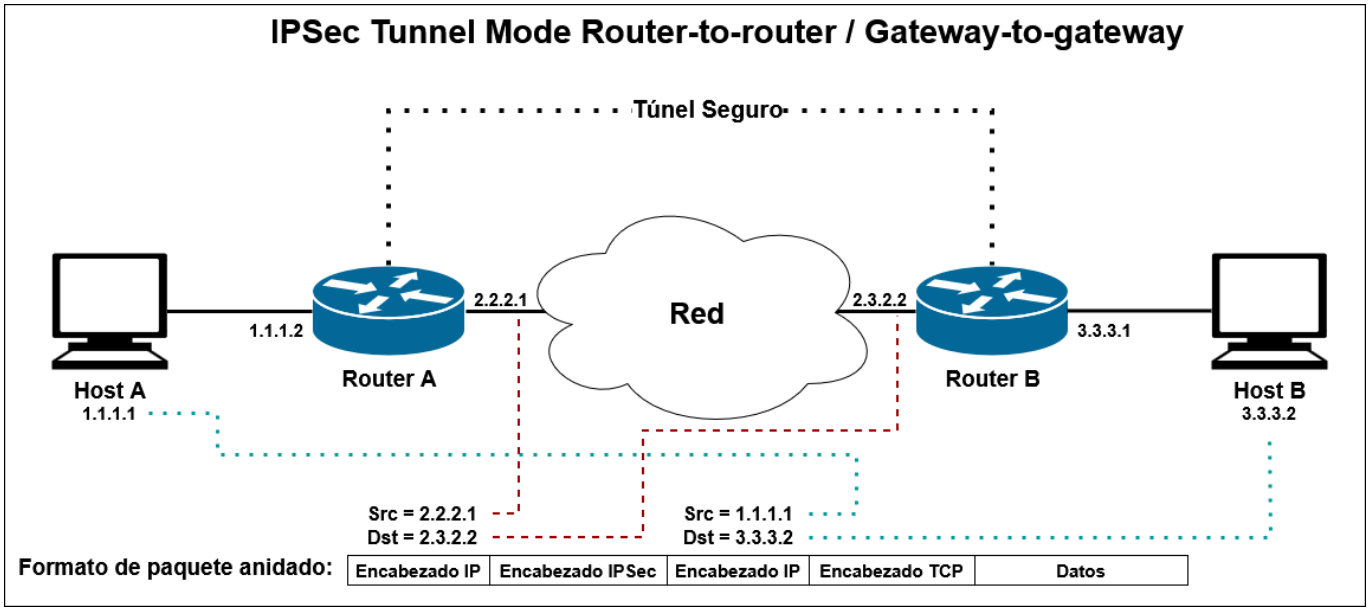
Hay 2 modos de encapsulación en IPSec, Transport Mode, que solo protege los datos de extremo a extremo y Tunnel mode:



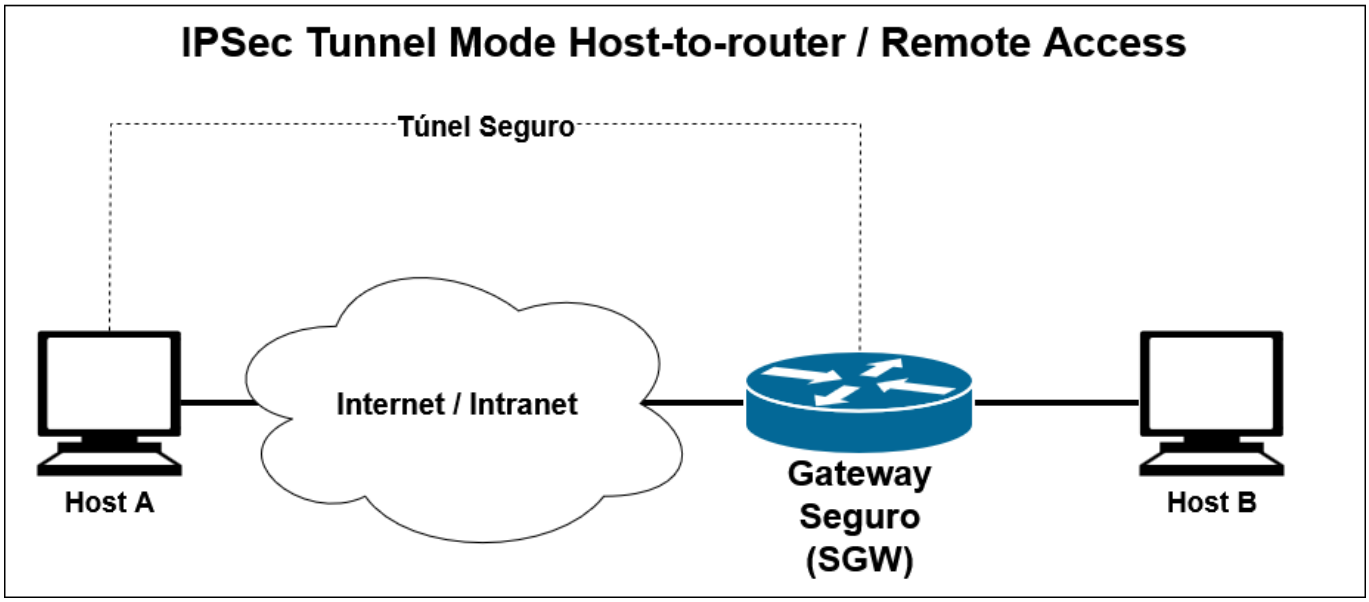
Encapsulación Tunnel Mode

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