

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 fuerte 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 factores que aseguran que IPv6 provee más seguridad que IPv4.

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

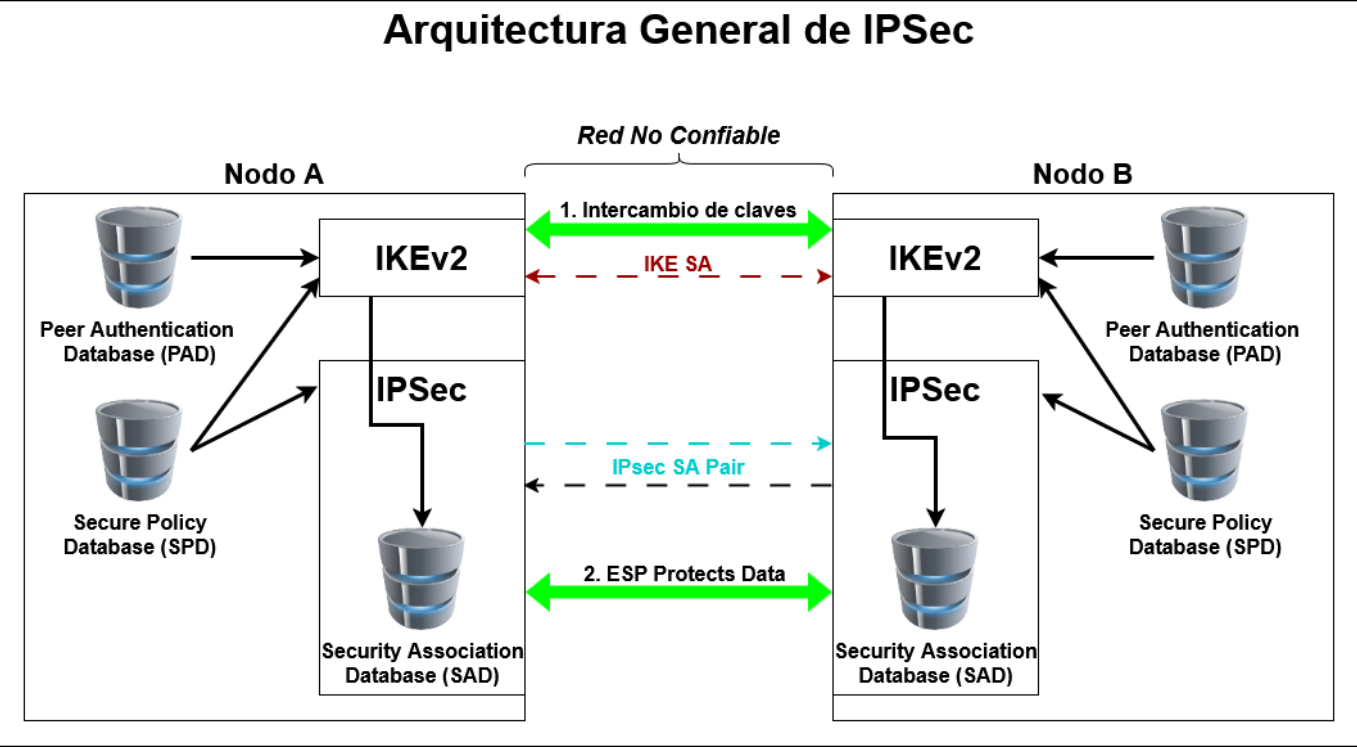
IPSec puede tener los siguientes usos:

- 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 soportan el protocolo
- 2 modos de encapsulación
 - Transport Mode
 - Tunnel Mode
- Key distribution and Management Protocol (IKE)
- Security Policy Database (SPD): Que paquetes serán protegidos, saltados o descartados
- Security Association Database (SAD): Como van a ser protegidos los paquetes por IPSec. Cada Security Association almacena todos los parámetros de seguridad del flujo de un paquete unidireccional en un extremo del túnel. Para comunicación bidireccional se necesitan al menos dos Security Association.

Arquitectura IPSec

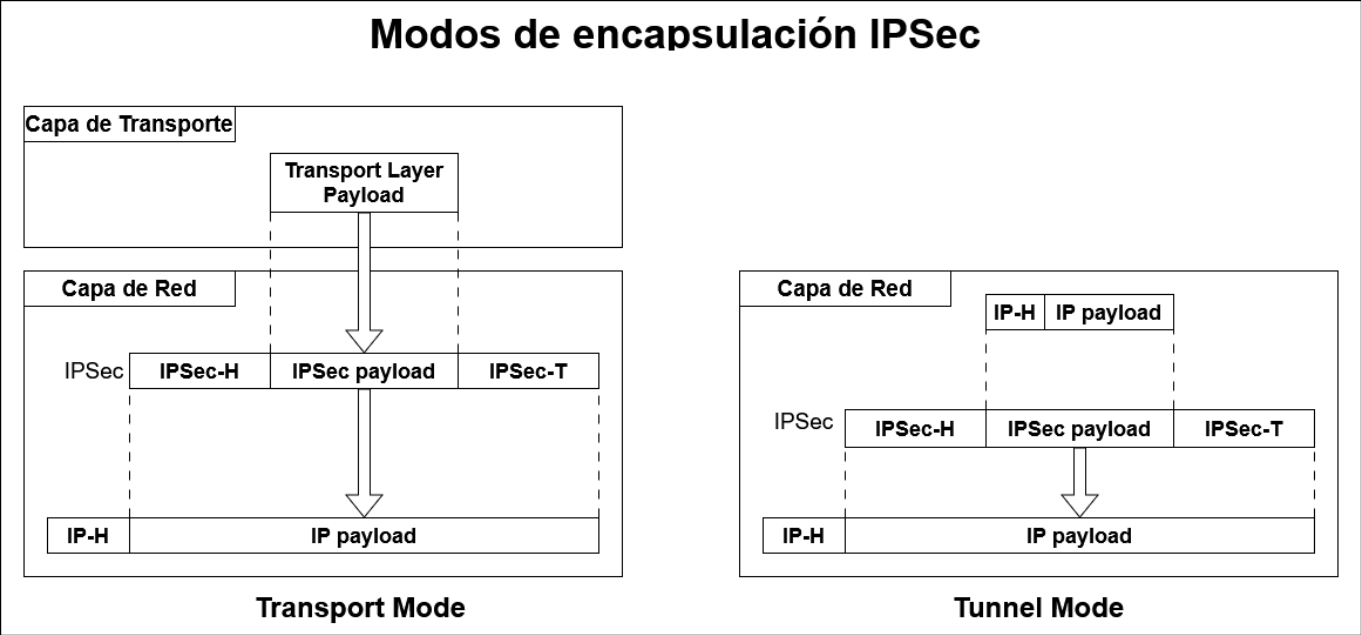


Protocolos y Servicios de IPSec

	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

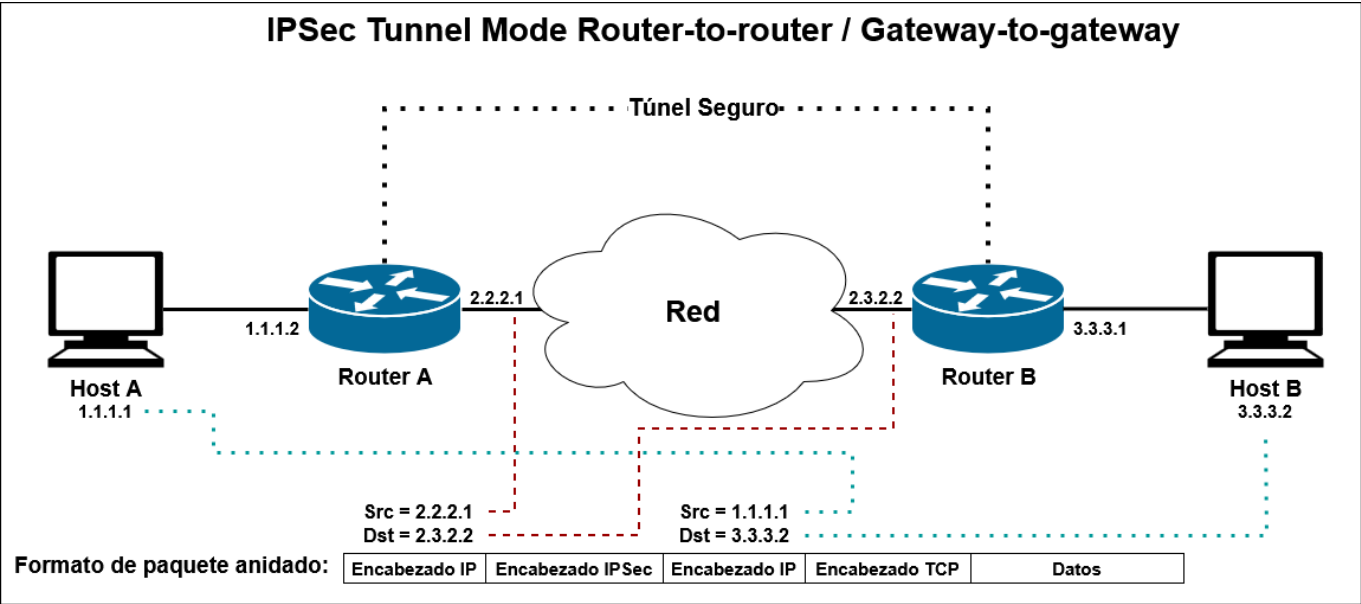
Hay 2 modos de encapsulación en IPSec, Transport Mode, que solo protege los datos de extremo a extremo y Tunnel mode:



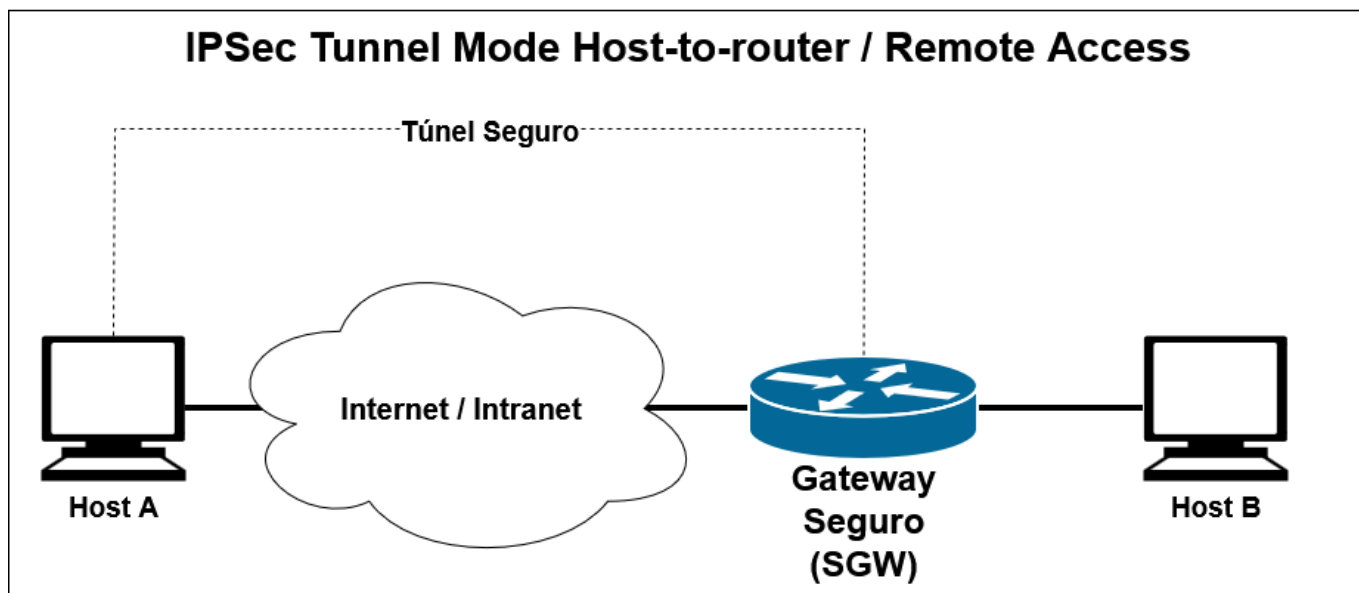
Encapsulación Tunnel Mode

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

- El SPD contiene una lista ordenada de entradas de políticas
- Coincide con el subset de tráfico IP proveído a la SA
- Cada entrada está enlazada a uno o más selectores que definen el set de tráfico IP acompañado 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 grupo 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 entrada

- Si el paquete de entrada no contiene ninguna cabecera IPSec, la capa IPSec revisa su SPD para determinar como procesar el paquete.
- Si el paquete de entrada contiene una cabecera IPSec:
 - Se usan la IP, el protocolo IPSec y el SPI del destino para revisar 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 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 combinar 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 asociación de seguridad entre 2 dispositivos IPSec incluyendo el establecimiento dinámico de claves compartidas temporales para cifrado y autenticación, el acuerdo de criptoalgoritmos y la autenticación 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 Authentication
- La payload tiene una estructura jerárquica compleja
- Puede contener múltiples proposiciones con múltiples protocolos y múltiples transforms

Intercambios del protocolo IKEv2

- IKE_SA_INIT: Negociación de los algoritmos criptográficos para la Security Association de gestión (IKE_SA)
 - Proposiciones 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

From:

<https://knoppia.net/> - **Knoppia**

Permanent link:

https://knoppia.net/doku.php?id=master_cs:secom:tm3_v2&rev=1779924826

Last update: **2026/05/27 23:33**

