IPSEC

Conceptos generales

IPSEC

IPsec (abreviatura de **Internet Protocol security**) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

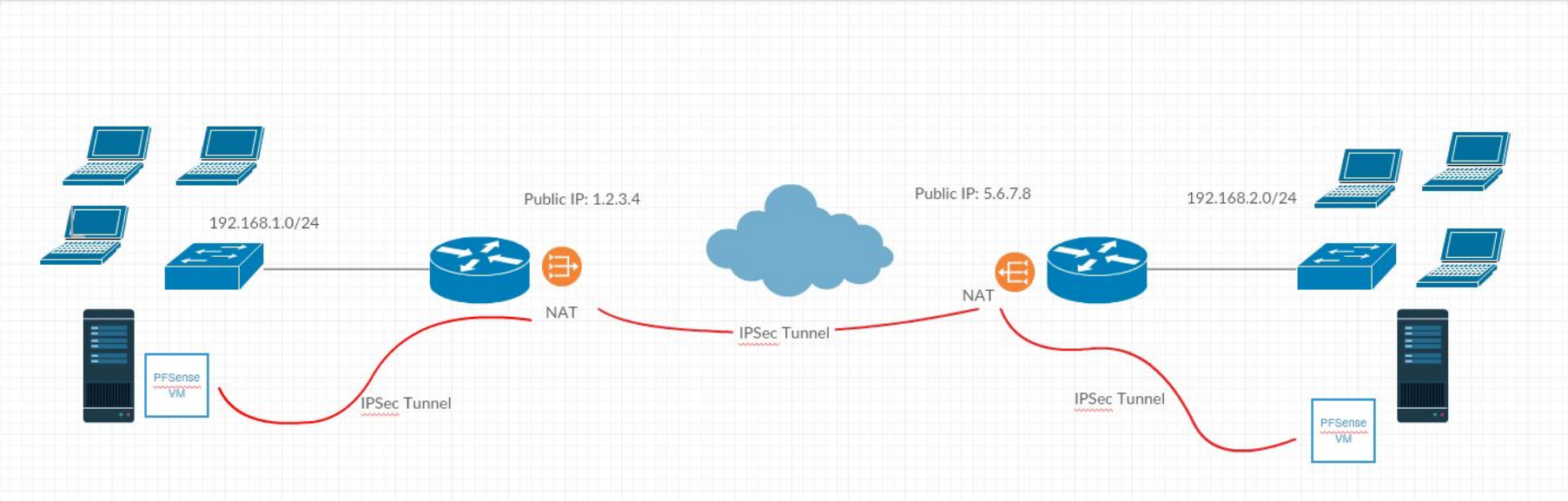
IPsec está implementado por un conjunto de protocolos criptográficos para (1) asegurar el flujo de paquetes, (2) garantizar la autenticación mutua y (3) establecer parámetros criptográficos.

IPSEC

IPSEC fue proyectado para proporcionar seguridad en **modo transporte** (extremo a extremo) del tráfico de paquetes, en el que los ordenadores de los extremos finales realizan el procesado de seguridad, o en **modo túnel** (puerta a puerta) en el que la seguridad del tráfico de paquetes es proporcionada a varias máquinas (incluso a toda la red de área local) por un único nodo.

IPsec puede utilizarse para crear VPNs en los dos modos, y este es su uso principal. Hay que tener en cuenta, sin embargo, que las implicaciones de seguridad son bastante diferentes entre los dos modos de operación.

IPSEC



CANÓ ACADEMY

IPSEC

Dependiendo del nivel sobre el que se actúe, podemos establecer dos modos básicos de operación de **IPsec**: **modo transporte** y **modo túnel**.

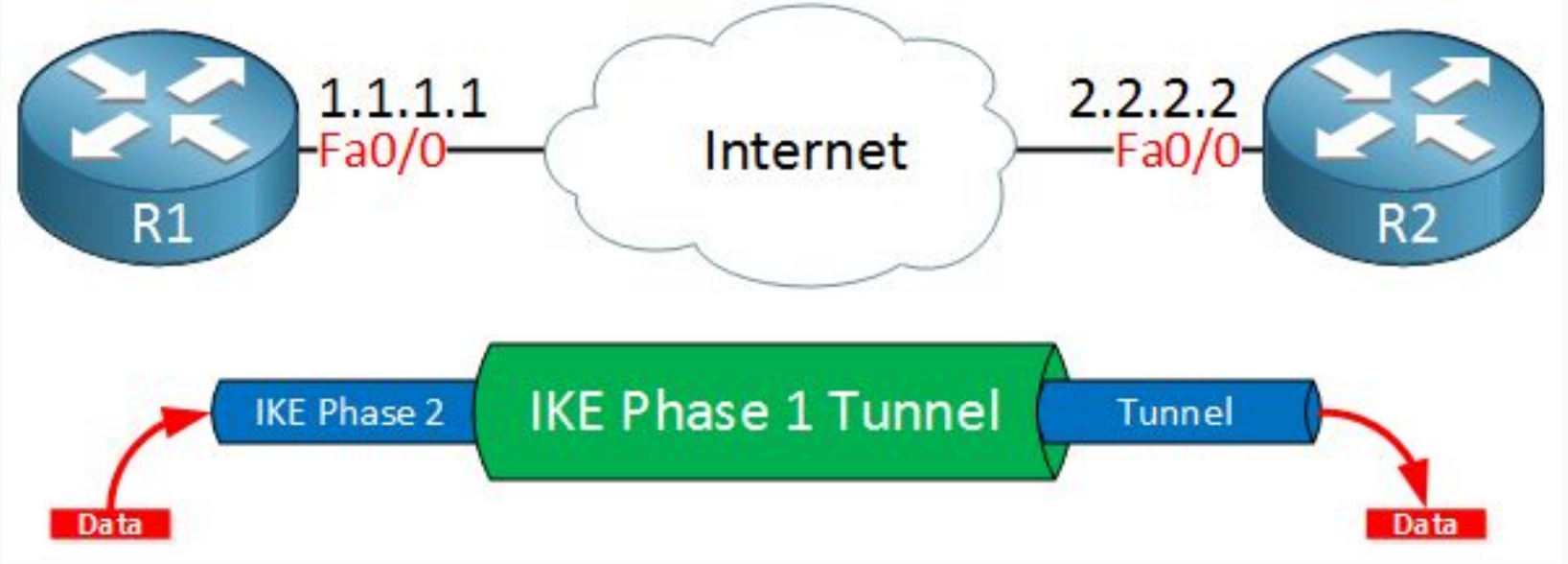
En **modo transporte**, sólo la carga útil (los datos que se transfieren) del paquete IP es cifrada o autenticada. El enrutamiento permanece intacto, ya que no se modifica ni se cifra la cabecera IP; sin embargo, cuando se utiliza la cabecera de autenticación (AH), las direcciones IP no pueden ser traducidas, ya que esto invalidará el hash.

IPSEC

Las capas de transporte y aplicación están siempre aseguradas por un hash, de forma que no pueden ser modificadas de ninguna manera (por ejemplo traduciendo los números de puerto TCP y UDP).

En el **modo túnel**, 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. El **modo túnel** se utiliza para comunicaciones red a red (túneles seguros entre routers - VPNs) o comunicaciones ordenador a red u PC a PC sobre Internet.

IPSEC



CANÓ ACADEMY

Cómo funciona IPSEC

IPSEC trabaja en 5 pasos esenciales

- ***Gestión del "tráfico importante"***
- ***Fase 1 IKE***
- ***Fase 2 IKE***
- ***Transferencia de data***
- ***Terminación del túnel***

Vamos a describir cada paso individual. Atención.

CANÓ ACADEMY

Gestión de tráfico importante

El tráfico importante es determinado por el Header IPSEC que se le agrega a la trama de la comunicación VPN que vamos a iniciar. Esta trama inicia con un **SA(Security Asociation)** entre los 2 extremos del VPN IPSEC.

Esta trama incluye:

Identificador:

IP destino, protocolo de seguridad, SPI(Security Parameter Index)

Párametros:

Algoritmo de autenticación, algoritmo de encriptación, modo de seguridad del protocolo(túnel o transporte).

Fase 1 IKE

El propósito de la fase 1 es proporcional un canal seguro para iniciar el proceso de intercambio del IKE(Internet Key Exchange).

La fase 1 realiza estos pasos:

- Autentica y protege la identidad del peer **IPSEC**
- Negocia una política **IKE SA** para iniciar el intercambio de IKE
- Realiza un intercambio de autenticación **Diffie Hellman** para evaluar el intercambio de IKE correcto de lado y lado.
- Setea el túnel para negociar la fase 2.

Fase 2 IKE

El propósito de la fase 2 es negociar IPSEC SAs para establecer el tunel definitivo.

Esta fase realiza los siguientes pasos:

Negocia los parámetros **IPSEC SA** con un **IKE SA** existente de la fase 1

Establece los **IPSEC SA**

Periódicamente renegocia los **IPSEC SA** para garantizar la seguridad

Realiza de manera opcional un intercambio de **DIFFIE HELLMAN**

Transferencia de DATA

Luego de tener todos los parámetros y la IKE correcta, la data puede intercambiarse por el túnel VPN que hemos creado. Los paquetes son encriptados y desencriptados utilizando la encriptación suministrada en el IPSEC SA.

Terminación del TÚNEL

Los túneles IPSEC pueden **terminar por eliminación o por timeout**. *Esto es muy importante para elegir el tiempo de nuestro timeout.*

Un SA puede expirar después de un tiempo específico o cuando un número de bytes han pasado por el túnel. Cuando un **SA** termina, tambien las **IKE** se descartan.

Cuando se necesita otra vez, se realiza una nueva fase 2 y algunos casos se realiza una fase 1. Esta negociación trae nuevos **SA** y nuevos **IKE**.

Laboratorios IPSEC

Ahora vamos a configurar los laboratorios de IPSEC Site to Site.

Atención especial a estos laboratorios que tienen muchos detalles.

MikroTik

CANÓ ACADEMY