UNIVERSIDAD RAFAEL LANDÍVAR

FACULTAD DE INGENIERÍA

REDES II

SECCIÓN 1 VESPERTINA

MGTR. DENNIS JAVIER DONIS DE LEÓN

IPsec FUNDAMENTALS

Julio Anthony Engels Ruiz Coto 1284719

Eddie Alejandro Girón Carranza 1307419

GUATEMALA DE LA ASUNCIÓN, OCTUBRE 25 DE 2024

IPSec (Internet Protocol Security) es un conjunto de protocolos diseñado para asegurar las comunicaciones a nivel de red mediante la autenticación y cifrado de los paquetes IP. Es esencial para la creación de redes privadas virtuales (VPNs), permitiendo comunicaciones seguras a través de redes inseguras como Internet.

Existen dos modos principales en los que IPSec opera:

- **Modo Túnel:** Cifra y/o autentica todo el paquete IP, incluyendo encabezados y datos. Es ideal para conexiones entre gateways (por ejemplo, entre dos routers) o entre un gateway y un host.
- **Modo Transporte:** Sólo cifra y/o auténtica la carga útil del paquete IP, dejando intacto el encabezado original. Se utiliza principalmente para comunicaciones host a host.

Configuraciones básicas (túnel):

```
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key tunnel-mode address 10.0.12.1

crypto ipsec transform-set TUNNEL ah-md5-hmac
 mode tunnel

crypto ipsec profile TUNNEL_PROFILE
 set transform-set TUNNEL

interface Tunnel100
 ip address 100.0.12.2 255.255.255.0
 tunnel source 10.0.12.2
 tunnel destination 10.0.12.1
 tunnel protection ipsec profile TUNNEL_PROFILE
```

Configuraciones básicas (transporte):

```
crypto ipsec transform-set TUNNEL ah-md5-hmac
 mode transport

crypto ipsec profile TUNNEL_PROFILE
 set transform-set TUNNEL
```

```
interface Tunnel100
 ip address 100.0.12.1 255.255.255.0
 tunnel source 10.0.12.1
 tunnel mode gre
 tunnel destination 10.0.12.2
 tunnel protection ipsec profile TUNNEL_PROFILE
```

IPsec es una herramienta clave para la seguridad en redes, especialmente cuando hablamos de VPNs. Básicamente, es un conjunto de estándares abiertos que protegen las comunicaciones en Internet. Se apoya en cuatro puntos clave: confidencialidad (con cifrados como DES y AES para que los datos no se vean), integridad (con algoritmos como MD5 o SHA para que los datos no se modifiquen), autenticación (verificando que los que se comunican son quienes dicen ser, usando claves o certificados), y el intercambio seguro de claves con el protocolo Diffie-Hellman.

IPsec utiliza dos protocolos para encapsular datos. Uno es el Authentication Header, que asegura la integridad y autenticación, pero no cifra los datos. El otro, más utilizado, es el Encapsulation Security Payload (ESP), el cuál ofrece un paquete completo de seguridad: confidencialidad, integridad y autenticación. Además, IPsec tiene dos modos de operación: modo transporte (para asegurar comunicaciones dentro de una red) y modo túnel (para VPNs a través de Internet).

Para establecer una conexión IPsec, hay dos pasos. Primero, se crea un túnel seguro para negociar los parámetros de seguridad. Luego se establece el túnel IPsec que transporta los datos de manera segura. Este túnel se activa automáticamente cuando hay "tráfico interesante" y, si no se usa en 24 horas, se pone en modo inactivo, pero puede reactivarse rápido cuando sea necesario.