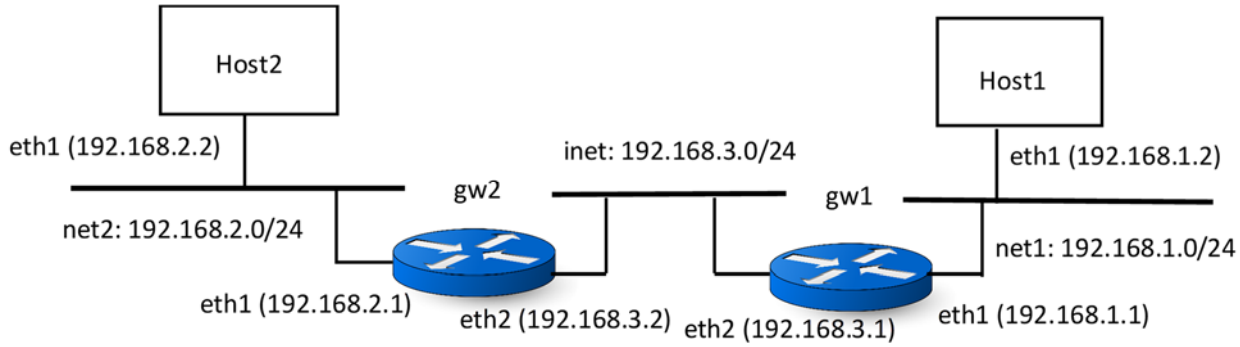
Seguridad en Redes

Práctica 3.5. IPsec

Preparación del entorno

Vamos a usar cuatro MVs (`gw1`, `gw2`, `host1` y `host2`) y tres redes internas (`inet`, `net1` y `net2`):



Importa una MV, haz tres clonaciones enlazadas y añade uno o dos interfaces de red a cada MV, según sea necesario, conectados a la red correspondiente.

Configura `gw1`:

```
sudo ifconfig eth1 192.168.1.1/24 up
sudo ifconfig eth2 192.168.3.1/24 up
sudo route add –net 192.168.2.0/24 gw 192.168.3.2
sudo sysctl -w net.ipv4.ip_forward=1
sudo apt-get update
sudo apt-get install ssh strongswan wireshark
```

Configura `gw2`:

```
sudo ifconfig eth1 192.168.2.1/24 up
sudo ifconfig eth2 192.168.3.2/24 up
sudo route add –net 192.168.1.0/24 gw 192.168.3.1
sudo sysctl -w net.ipv4.ip_forward=1
sudo apt-get update
sudo apt-get install ssh strongswan
```

Configura `Host1`:

```
sudo ifconfig eth1 192.168.1.2/24 up
sudo route add default gw 192.168.1.1
```

Configura `Host2`:

```
sudo ifconfig eth1 192.168.2.2/24 up
sudo route add default gw 192.168.2.1
```

strongSwan

strongSwan (https://www.strongswan.org) proporciona una implementación de los protocolos IKEv1 e IKEv2 (demonio `charon`) y usa NETKEY, que es la pila IPsec nativa de Linux. En NETKEY, la infraestructura XFRM (*transform*) permite configurar transformaciones en los paquetes IP para, por ejemplo, cifrarlos y/o autenticarlos con ESP, o también para comprimirlos.

Consulta la página de manual del comando `ipsec`, que ofrece toda la funcionalidad de strongSwan. Revisa la configuración (`/etc/ipsec.conf`).

Conexión IPsec de sitio a sitio con clave secreta

Configura la clave secreta, añadiendo al final del fichero `/etc/ipsec.secrets` de `gw1` la siguiente línea:

```
: PSK "Clave secreta muy segura"
```

Haz lo mismo en `gw2`:

```
: PSK "Clave secreta muy segura"
```

Normalmente, se usaría una clave generada aleatoriamente. Para ello, en lugar de una cadena, se puede indicar una secuencia de dígitos hexadecimales (comenzando con `0x`) o datos binarios codificados en Base64 (comenzando con `0s`).

En la configuración, `gw2` será el extremo izquierdo y `gw1`, el derecho. Eso permite tener la misma configuración en ambos extremos de la VPN. Sin embargo, la documentación de strongSwan sugiere denominar izquierdo al extremo local y derecho al remoto (aprovechando que, en inglés, comienzan por la misma letra).

Configura la VPN, añadiendo al fichero `/etc/ipsec.conf` de ambos extremos las siguientes líneas:

```
conn secret
      left=192.168.3.2
      leftsubnet=192.168.2.0/24
      leftauth=psk
      right=192.168.3.1
      rightsubnet=192.168.1.0/24
      rightauth=psk
      auto=add
```

Nota: Añadir la línea **`charondebug="ike4"`** en el **`config setup`** si se va a hacer la parte opcional.

Con `auto=start`, la conexión VPN se iniciaría automáticamente, lo cual es necesario si se pretende que la conexión sea permanente.

Reinicia el servicio en ambos extremos:

```
$ sudo ipsec restart
```

Inicia Wireshark para que escuche en todos los interfaces de `gw1`.
Inicia la conexión VPN en `gw1`:

```
$ sudo ipsec up secret
```

Revisa el fichero de registro `/var/log/daemon.log`.

Observa los detalles de la conexión con:

```
$ sudo ipsec status
$ sudo ipsec statusall
```

Observar las políticas y asociaciones de seguridad con:

```
$ sudo ip xfrm policy
$ sudo ip xfrm state
```

- **Entrega:**
  - Copia los registros del fichero `/var/log/daemon.log` de `gw1` relacionados con la conexión ipsec establecida.
  - Copia los detalles de la conexión (`sudo ipsec status`)
  - Copia las asociaciones de seguridad en `gw1` (`sudo ip xfrm state`). Explica cuántas asociaciones de seguridad hay por conexión ipsec y qué contiene cada SA.
  - Copia las políticas de seguridad de esa conexión en `gw1` (`sudo ip xfrm policy`). ¿Cuántas políticas de seguridad hay? ¿Para qué tipo de paquetes (según a dónde van dirigidos)? ¿Qué acción crees que está aplicando ipsec sobre esos paquetes (*protect, bypass o discard*)?

Analiza los paquetes ISAKMP capturados por Wireshark.

- **Entrega:**
  - ¿Cuántos mensajes de este tipo se intercambian? ¿Qué versión de IKE se está utilizando? ¿Cómo lo sabes?
  - ¿Sobre qué protocolo de la capa de transporte van estos mensajes? ¿Y por qué puerto?

- Explica qué se hace en el primer par de mensajes intercambiados. ¿Qué algoritmo de cifrado han acordado usar las dos partes? ¿Cuál es el tamaño de la clave? ¿Cuál es el algoritmo de autenticación que se va a utilizar? ¿Y la función generadora de números pseudo-aleatorios (PRF)? ¿Y qué grupo DH?
- ¿Qué intercambian las dos partes en el segundo par de mensajes? ¿Cuál es el objetivo de este intercambio? ¿Puede un atacante ver los valores intercambiados?

OPCIONAL

1. Analiza detenidamente el primer mensaje ISAKMP.

   ➢ **Entrega:** Especifica los distintos conjuntos de algoritmo de cifrado, tamaño de clave, algoritmo de autenticación, PRF y grupo DH que `gw1` ofrece a `gw2` a elegir para generar la SA.

2. Descifra el par de mensajes ISAKMP cifrados de IKEv2.

   ➢ **Entrega:**
   - Especifica los pasos que has tenido que realizar para conseguir descifrar estos mensajes
   - Haz una captura de pantalla de la ventana de wireshark en la que se vea la clave precompartida que se usa para hacer la autenticación de las partes (una vez descifrado el paquete).

Comprueba la conexión VPN haciendo un ping de host1 a host2. Analiza los paquetes ESP capturados por Wireshark.

Configura Wireshark para que descifre los paquetes ESP y compruebe su autenticidad. Para ello, en las preferencias del protocolo ESP (Edit → Preferences → Protocols → ESP), activa todas las casillas y añade los parámetros de las asociaciones de seguridad (`ip xfrm state`).

➢ **Entrega:**
- Copia una captura de Wireshark seleccionando un paquete ESP descifrado y con sus campos a la vista.
- ¿Se usan las mismas claves y el mismo SPI para los dos sentidos de la comunicación (ICM Request e ICMP Response)?
- Describe el encapsulado de ESP en modo túnel.

Para cerrar la conexión ipsec hacer:

```
$ sudo ipsec down secret
```

Conexión IPsec de sitio a sitio con certificados autofirmados

Crea una clave RSA y un certificado autofirmado en gw1:

```
$ sudo sh -c "ipsec pki --gen > /etc/ipsec.d/private/gw1-key.der"
$ sudo sh -c "ipsec pki --self --in /etc/ipsec.d/private/gw1-key.der --dn "CN=gw1" > /etc/ipsec.d/certs/gw1-cert.der"
```

Haz lo mismo en gw2:

```
$ sudo sh -c "ipsec pki --gen > /etc/ipsec.d/private/gw2-key.der"
$ sudo sh -c "ipsec pki --self --in /etc/ipsec.d/private/gw2-key.der --dn "CN=gw2" > /etc/ipsec.d/certs/gw2-cert.der"
```

Dado que son certificados autofirmados, deben estar accesibles localmente, ya que no se confiará en ningún certificado de este tipo intercambiado por la red. Copia el certificado de gw2 en gw1:

```
$ sudo scp usuario@192.168.3.2:/etc/ipsec.d/certs/gw2-cert.der /etc/ipsec.d/certs/
```

Haz lo mismo en gw2:

```
$ sudo scp usuario@192.168.3.1:/etc/ipsec.d/certs/gw1-cert.der /etc/ipsec.d/certs/
```

Configura las claves privadas, añadiendo al final del fichero `/etc/ipsec.secrets` de gw1 la siguiente línea:

```
: RSA gw1-key.der
```

Haz lo mismo en gw2:

```
: RSA gw2-key.der
```

Configura la VPN, añadiendo al fichero `/etc/ipsec.conf` de ambos extremos las siguientes líneas:

```
conn sscert
      left=192.168.3.2
      leftsubnet=192.168.2.0/24
      leftcert=gw2-cert.der
      leftid="CN=gw2"
      right=192.168.3.1
      rightsubnet=192.168.1.0/24
```

```
        rightcert=gw1-cert.der
        rightid="CN=gw1"
        auto=add
```

Reinicia el servicio en ambos extremos:

```
$ sudo ipsec restart
```

Inicia Wireshark para que escuche en todos los interfaces de `gw1`.

Inicia la conexión VPN en uno de los extremos:

```
$ sudo ipsec up sscert
```

Revisa el fichero de registro `/var/log/daemon.log`.

Observa los detalles de la conexión con:

```
$ sudo ipsec status
$ sudo ipsec statusall
```

Observa las políticas y asociaciones de seguridad con:

```
$ sudo ip xfrm policy
$ sudo ip xfrm state
```

Analiza los paquetes ISAKMP capturados por Wireshark.

- **Entrega:** Copia lo que devuelve por pantalla la orden `sudo ipsec statusall`. ¿En qué difiere este túnel en su establecimiento con respect al establecido con clave secreta compartida?