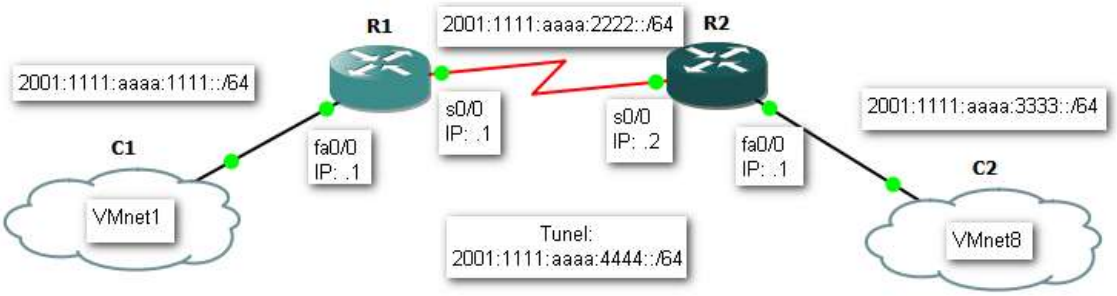
Configuración de un Túnel IPSec a través de IPv6

En esta práctica vamos a configurar una VPN (Túnel) IPSec sobre una red IPv6. Para ello usaremos GNS3 y dos routers modelo Cisco 3725 con la IOS "c3725-adventerprisek9-mz.124-15.T5.bin".

La topología es la siguiente:



En la que los hosts de los extremos estarán simulados con dos máquinas virtuales Windows XP y conectadas a GNS3 mediante dos nubes, una conectada a VMnet1 y la otra a VMnet8.

Empezaremos con la configuración básica de las interfaces físicas de R1 (DCE para el enlace serie):

```
R1# conf t

R1(config)# ipv6 unicast-routing

R1(config)# int fa 0/0

R1(config-if)# ipv6 enable

R1(config-if)# ipv6 address 2001:1111:aaaa:1111::1/64

R1(config-if)# no shut

R1(config-if)# int s0/0

R1(config-if)# ipv6 enable

R1(config-if)# ipv6 address 2001:1111:aaaa:2222::1/64

R1(config-if)# clock rate 64000

R1(config-if)# no shut
```

Y hacemos lo mismo con R2:

```
R2# conf t

R2(config)# ipv6 unicast-routing
```

```
R2(config)# int fa 0/0

R2(config-if)# ipv6 enable

R2(config-if)# ipv6 address 2001:1111:aaaa:333::1/64

R2(config-if)# no shut

R2(config-if)# int s0/0

R2(config-if)# ipv6 enable

R2(config-if)# ipv6 address 2001:1111:aaaa:2222::2/64

R2(config-if)# no shut
```

Pasamos ahora a configurar el túnel IPSec. Empezamos por R1, en el que configuraremos una política IKE y una clave precompartida. Podemos configurar múltiples políticas con diferentes prioridades y los dos extremos del túnel se pondrán de acuerdo en la que van a elegir. En este caso sólo crearemos una política que será la misma en los dos extremos:

`R1(config)# crypto isakmp policy 1` (empezamos la configuración de una política IKE con prioridad 1)

`R1(config-isakmp-policy)# authentication pre-share` (establecemos como modo de autenticación una clave precompartida)

`R1(config-isakmp-policy)# hash md5` (establecemos md5 como algoritmo de hash para garantizar la integridad)

`R1(config-isakmp-policy)# group 1` (especificamos el identificador de grupo de Diffie-Hellman en la política IKE)

`R1(config-isakmp-policy)# encryption 3des` (especificamos 3DES como algoritmo de cifrado)

`R1(config-isakmp-policy)# lifetime 86400` (especificamos el tiempo de vida en segundos para la Asociación de Seguridad, SA, es opcional)

`R1(config-isakmp-policy)# exit`

`R1(config)# crypto isakmp key 0 cisco address ipv6 2001:1111:aaaa:2222::2/128` (definimos la que será la clave precompartida, “cisco”, en texto plano, “0”, y la IP del que será el otro extremo del túnel en formato IPv6)

`R1(config)# crypto keyring ANILLO` (definimos el nombre del Keyring que se usará durante la autenticación)

`R1(config-keyring)# pre-shared-key address ipv6 2001:1111:aaaa:2222::2/128 key cisco` (definimos la clave precompartida a usar durante la autenticación IKE)

```
R1(config-keyring)# exit
```

```
R1(config)# crypto ipsec transform-set TRANSFORMADA esp-3des
```
(definimos un transform-set, es decir, una combinación de protocolos y algoritmos que sea aceptable por routers IPSec)

```
R1(cfg-crypto-trans)# crypto ipsec profile PERFIL
```
(define los parámetros que se van a usar para el cifrado IPSec entre los dos routers)

```
R1(ipsec-profile)# set transform-set TRANSFORMADA
```
(especifica el transform-set que se puede usar)

```
R1(ipsec-profile)# exit
```

```
R1(config)# interface tunnel 0
```
(empezamos la configuración de la interfaz virtual "tunnel 0")

```
R1(config-if)# ipv6 address 2001:1111:aaaa:4444::1/64
```

```
R1(config-if)# ipv6 enable
```

```
R1(config-if)# tunnel source 2001:1111:aaaa:2222::1
```
(definimos el origen del túnel, en algunas IOS también podemos poner "tunnel source serial 0/0")

```
R1(config-if)# tunnel destination 2001:1111:aaaa:2222::2
```
(definimos el destino del túnel)

```
R1(config-if)# tunnel mode ipsec ipv6
```
(establecemos el modo de encapsulamiento para la interfaz tunnel 0)

```
R1(config-if)# tunnel protection ipsec profile PERFIL
```
(asociamos la interfaz tunnel 0 con el perfil creado anteriormente)

```
R1(config-if)# exit
```

```
R1(config)# ipv6 route 2001:1111:aaaa:3333::/64 tunnel 0
```
(configuramos una ruta estática de forma que todo el tráfico que vaya a la red local de la derecha pase por el túnel)

Ahora vamos a realizar la configuración de R2.

```
R2(config)# crypto isakmp policy 1
```
(empezamos la configuración de una política IKE con prioridad 1)

```
R2(config-isakmp-policy)# authentication pre-share
```
(establecemos como modo de autenticación una clave precompartida)

```
R2(config-isakmp-policy)# hash md5
```
(establecemos md5 como algoritmo de hash para garantizar la integridad)

`R2(config-isakmp-policy)# group 1` (especificamos el identificador de grupo de Diffie-Hellman en la política IKE)

`R2(config-isakmp-policy)# encryption 3des` (especificamos 3DES como algoritmo de cifrado)

`R2(config-isakmp-policy)# lifetime 86400` (especificamos el tiempo de vida en segundos para la Asociación de Seguridad, SA, es opcional)

```
R2(config-isakmp-policy)# exit
```

`R2(config)# crypto isakmp key 0 cisco address ipv6 2001:1111:aaaa:2222::1/128` (definimos la que será la clave precompartida, "cisco", en texto plano, "0", y la IP del que será el otro extremo del túnel en formato IPv6)

`R2(config)# crypto keyring ANILLO` (definimos el nombre del Keyring que se usará durante la autenticación)

`R2(config-keyring)# pre-shared-key address ipv6 2001:1111:aaaa:2222::1/128 key cisco` (definimos la clave precompartida a usar durante la autenticación IKE)

```
R2(config-keyring)# exit
```

`R2(config)# crypto ipsec transform-set TRANSFORMADA esp-3des` (definimos un transform-set, es decir, una combinación de protocolos y algoritmos que sea aceptable por routers IPSec)

`R2(cfg-crypto-trans)# crypto ipsec profile PERFIL` (define los parámetros que se van a usar para el cifrado IPSec entre los dos routers)

`R2(ipsec-profile)# set transform-set TRANSFORMADA` (especifica el transform-set que se puede usar)

```
R2(ipsec-profile)# exit
```

`R2(config)# interface tunnel 0` (empezamos la configuración de la interfaz virtual "tunnel 0")

```
R2(config-if)# ipv6 address 2001:1111:aaaa:4444::2/64
```

```
R2(config-if)# ipv6 enable
```

`R2(config-if)# tunnel source 2001:1111:aaaa:2222::2` (definimos el origen del túnel, en algunas IOS también podemos poner "tunnel source serial 0/0")

`R2(config-if)# tunnel destination 2001:1111:aaaa:2222::1` (definimos el destino del túnel)

`R2(config-if)# tunnel mode ipsec ipv6` (establecemos el modo de encapsulamiento para la interfaz tunnel 0)

`R2(config-if)# tunnel protection ipsec profile PERFIL` (asociamos la interfaz tunnel 0 con el perfil creado anteriormente)

`R2(config-if)# exit`

`R2(config)# ipv6 route 2001:1111:aaaa:1111::/64 tunnel 0` (configuramos una ruta estática de forma que todo el tráfico que vaya a la red local de la izquierda pase por el túnel)

El siguiente paso será arrancar las dos máquinas virtuales, que pueden ser Windows XP y configurarlas con direcciones IPv6 dentro del segmento correspondiente (la autoconfiguración funciona sin problemas). Desde una de ellas debemos poder hacer ping a la otra y si capturamos el tráfico, veremos que va cifrado.

5	15.350000	2001:1111:aaaa:2222::2	2001:1111:aaaa:2222::1	ESP	ESP (SPI=0xad6a3680)
6	15.378000	2001:1111:aaaa:2222::1	2001:1111:aaaa:2222::2	ESP	ESP (SPI=0xffff9e08)
7	15.405000	2001:1111:aaaa:2222::2	2001:1111:aaaa:2222::1	ESP	ESP (SPI=0xad6a3680)
8	15.412000	2001:1111:aaaa:2222::1	2001:1111:aaaa:2222::2	ESP	ESP (SPI=0xffff9e08)
9	15.415000	2001:1111:aaaa:2222::2	2001:1111:aaaa:2222::1	ESP	ESP (SPI=0xad6a3680)
10	15.418000	2001:1111:aaaa:2222::1	2001:1111:aaaa:2222::2	ESP	ESP (SPI=0xffff9e08)
11	15.422000	2001:1111:aaaa:2222::2	2001:1111:aaaa:2222::1	ESP	ESP (SPI=0xad6a3680)
12	15.424000	2001:1111:aaaa:2222::1	2001:1111:aaaa:2222::2	ESP	ESP (SPI=0xffff9e08)
13	15.428000	2001:1111:aaaa:2222::2	2001:1111:aaaa:2222::1	ESP	ESP (SPI=0xad6a3680)
14	15.455000	2001:1111:aaaa:2222::1	2001:1111:aaaa:2222::2	ESP	ESP (SPI=0xffff9e08)
15	19.557000	N/A	N/A	CDP	Device ID: R2 Port ID: Serial0/0