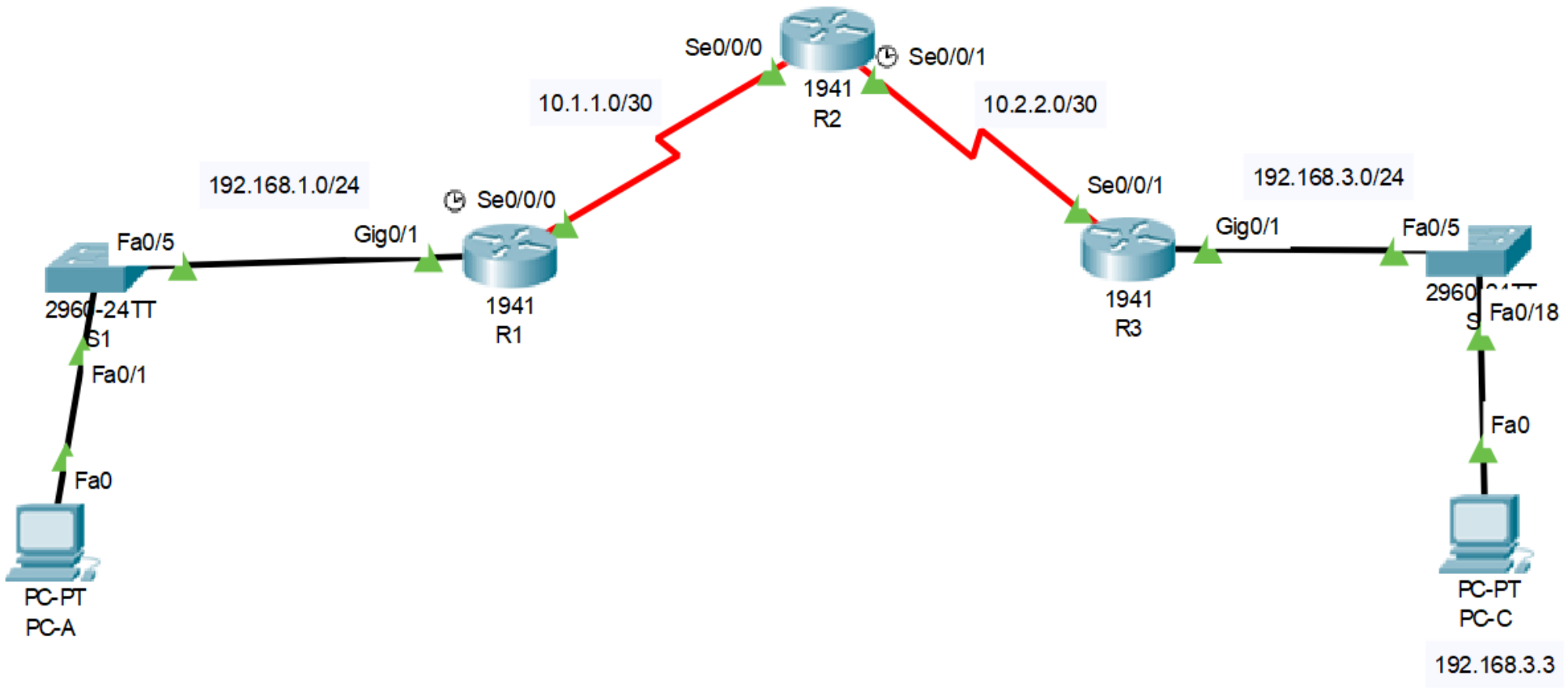
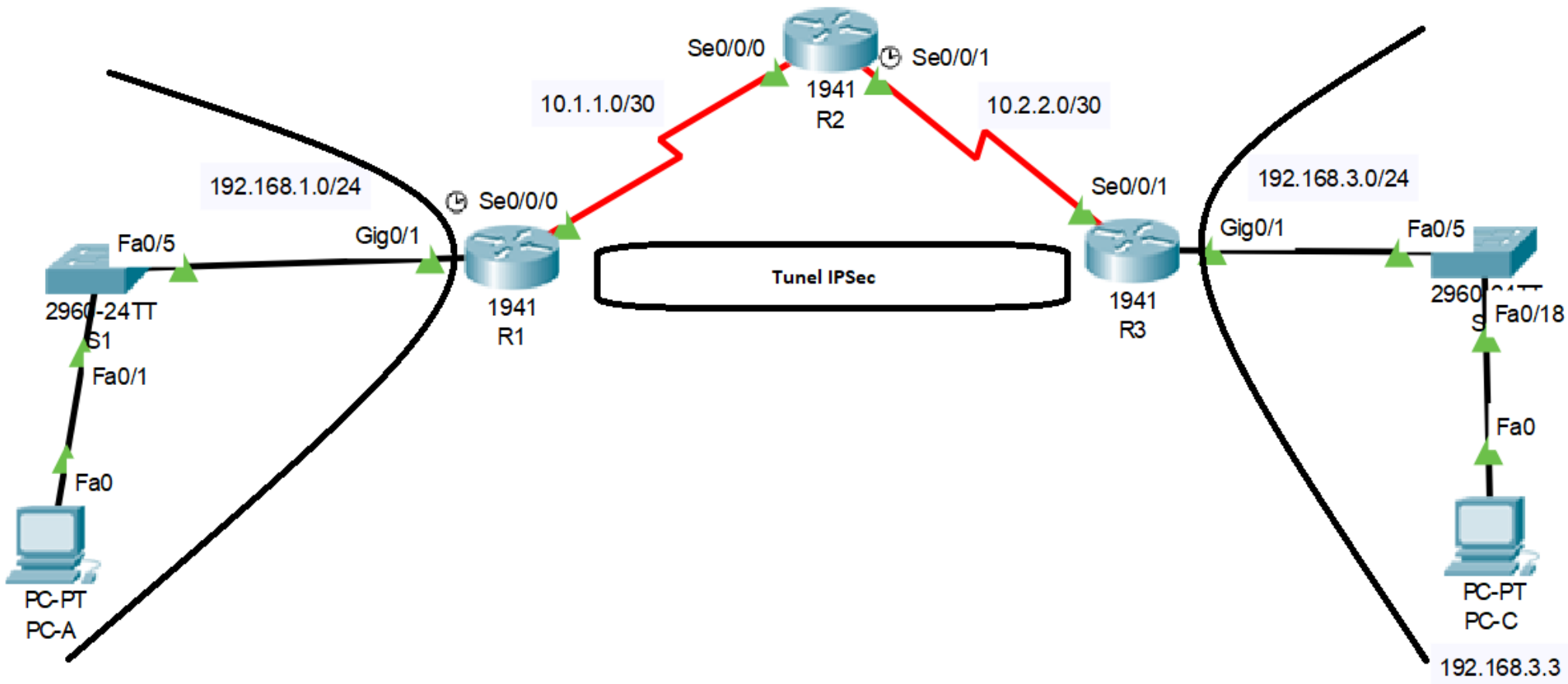
Lab 11 VPN utilizando la CLI




Se0/0/0
Se0/0/1
1941
R2
10.1.1.0/30
10.2.2.0/30
192.168.1.0/24
Se0/0/0
Se0/0/1
192.168.3.0/24
Fa0/5
Gig0/1
Gig0/1
Fa0/5
Tunel IPSec
1941
R1
1941
R3
2960-24TT
S1
Fa0/1
Fa0/18
Fa0
Fa0
PC-PT
PC-A
PC-PT
PC-C
192.168.3.3

Definiciones

VPN “Virtual Private Network “

VPN site to site, es realizada utilizando IPSec (capa3) y requiere lograr

- Confidencialidad
- Integridad
- Autenticación

Definiciones

- IPSec “Internet Protocol Security”, conjunto de protocolos cuya función es asegurar las comunicaciones sobre el protocolo de internet.
- IKE “Internet Key exchange”, utilizado para crear asociaciones de seguridad en el protocolo IPSec.
- ISAKMP “Internet Security Association and Key Management Protocol”, es un protocolo criptográfico, que constituye la base del protocolo IKE.

IKE ISAKMP Fase 1

Utilizado para que los routers se comuniquen directamente entre ellos.

No se envía DATA de los usuarios.

Intercambio de información de control.

Para que la fase 1 este completa ambos routers deben coincidir en:

- Algoritmo de Hash
- Algoritmo de encripción
- DH group
- Método de autenticación
- Lifetime

IKE ISAKMP Fase 2

Debe ser exitosa la fase 1.

Se envía la DATA de los usuarios.

Deben coincidir las variables de:

- Confidencialidad
- Integridad
- Autenticación

AH vs ESP

Para la fase 2 es necesario decidirse entre dos protocolos

- AH Authentication Header

Servicio de autenticación e integridad pero no encripción, no se puede utilizar con NAT.

- Encapsulation Security Payload

Servicio de CIA, si se puede utilizar en NAT.

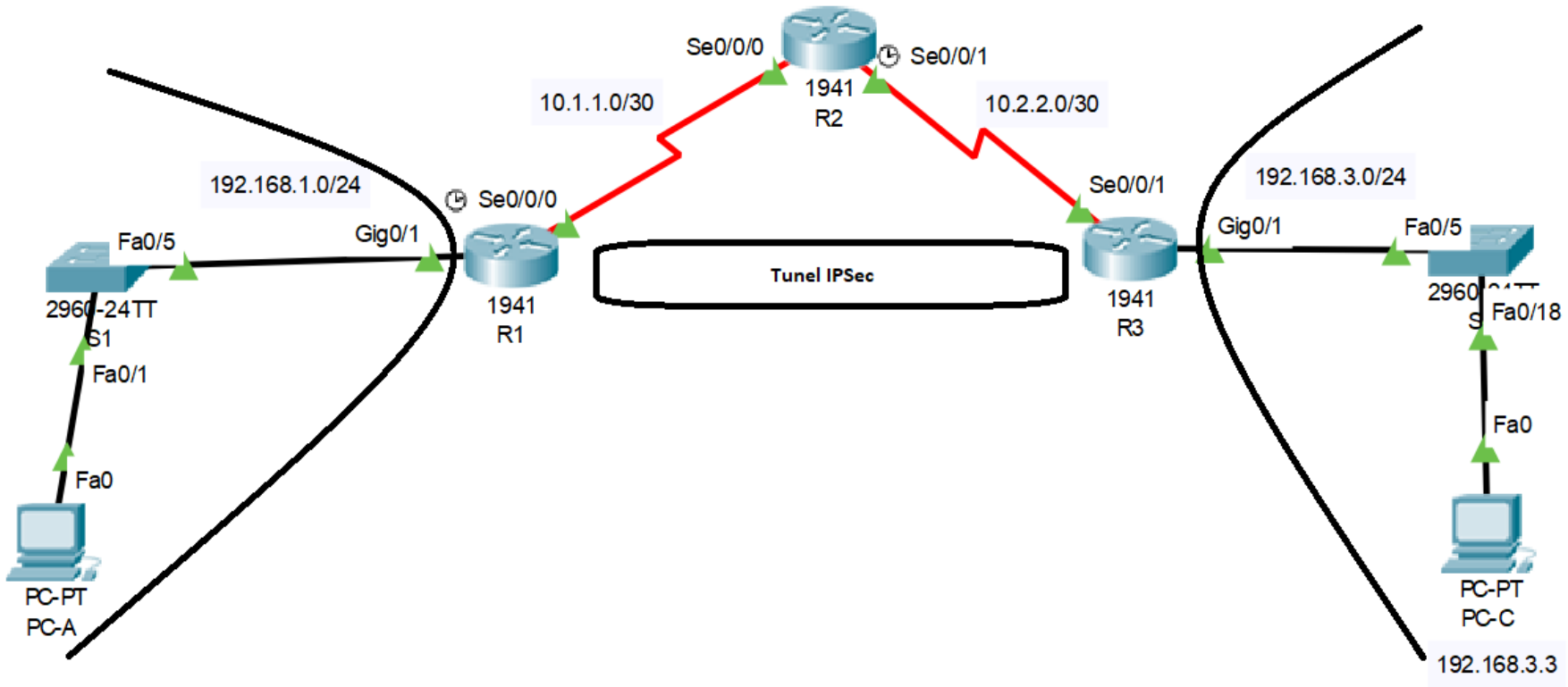
CIA

Confidencialidad
DES
3DES
AES
diffie hellman
RSA

Integridad
MD5
SHA1
SHA2

Autenticación
PSK
RSA

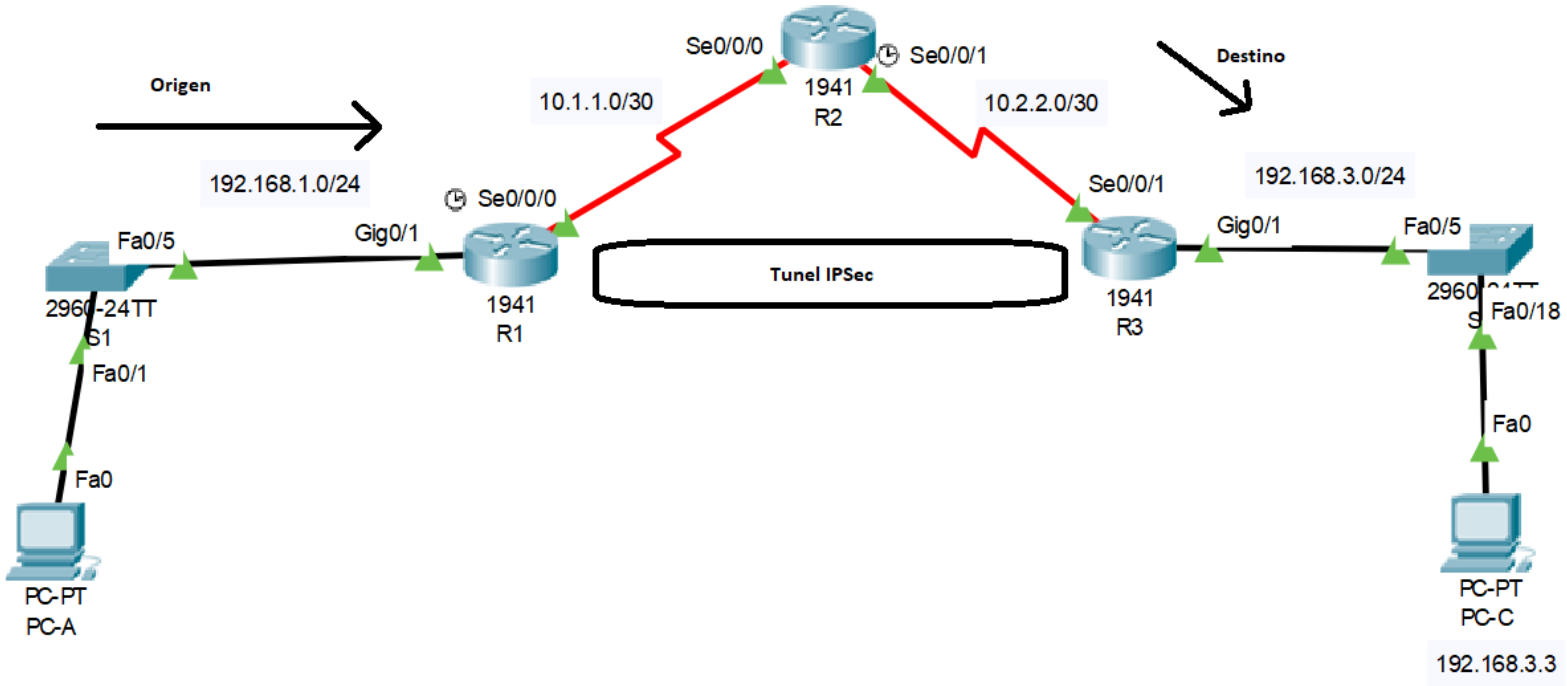
- R1(config)# **license boot module c1900 technology-package securityk9**



IKE ISAKMP Fase 1

Identificar tráfico interesante

- **R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255**



IKE ISAKMP Fase 1

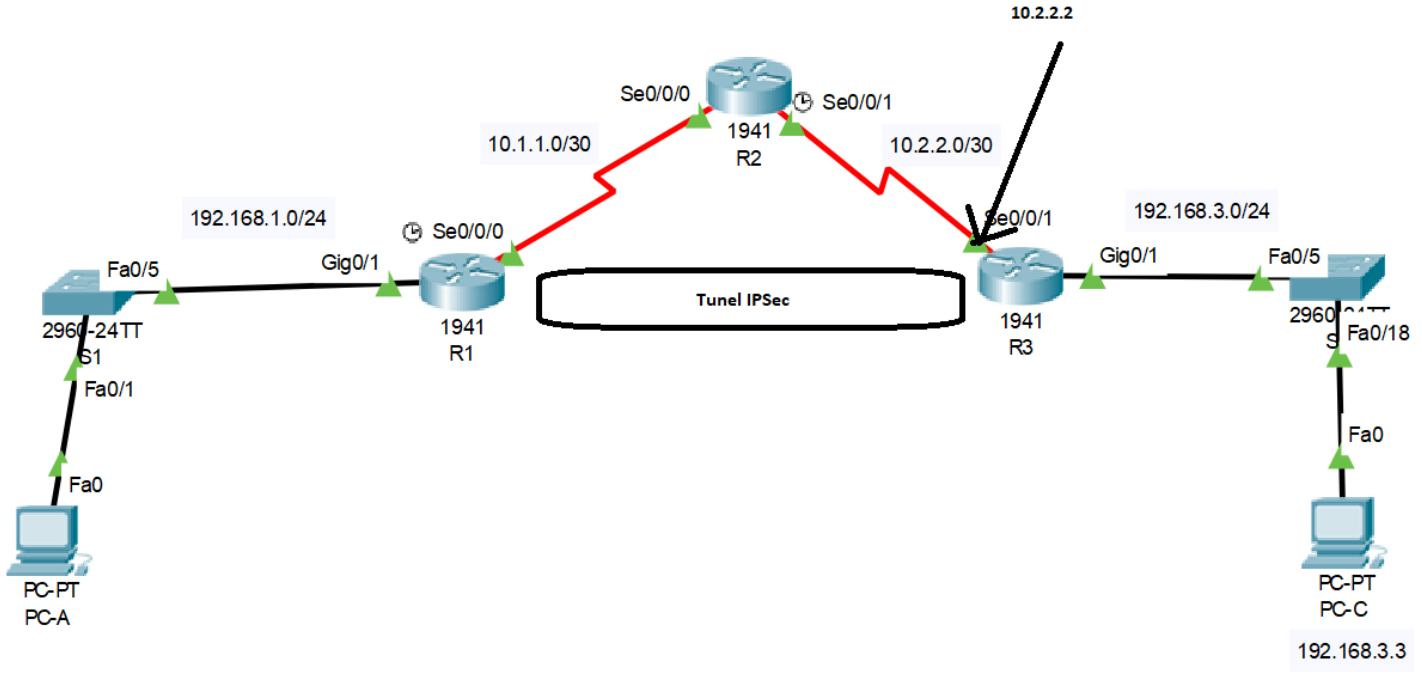
Configurar política de IKE ISAKMP Fase 1

- **R1(config)# crypto isakmp policy 10**
- **R1(config-isakmp)# encryption aes 256**
- **R1(config-isakmp)# authentication pre-share**
- **R1(config-isakmp)# group 5**
- **R1(config-isakmp)# exit**

IKE ISAKMP Fase 1

Asociar la pre-share con el gateway de la VPN

- **R1(config)# crypto isakmp key vpnpa55 address 10.2.2.2**



IKE ISAKMP Fase 2

Configurar los parámetros de trato para la DATA de los usuarios

“Transform Set”

- **R1(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac**

IKE ISAKMP Fase 2

Configurar un crypto-map que enlaza todos los parámetros

- **R1(config)# crypto map VPN-MAP 10 ipsec-isakmp**
- **R1(config-crypto-map)# description VPN connection to R3**
- **R1(config-crypto-map)# set peer 10.2.2.2**
- **R1(config-crypto-map)# set transform-set VPN-SET**
- **R1(config-crypto-map)# match address 110**
- **R1(config-crypto-map)# exit**

IKE ISAKMP Fase 2

Aplicar el crypto map a la interfaz

- **R1(config)# interface s0/0/0**
- **R1(config-if)# crypto map VPN-MAP**

Configuración de R3

Se debe hacer una configuración espejo en R3

Verificar funcionamiento

Realizar un ping entre redes

R1#show crypto ipsec sa