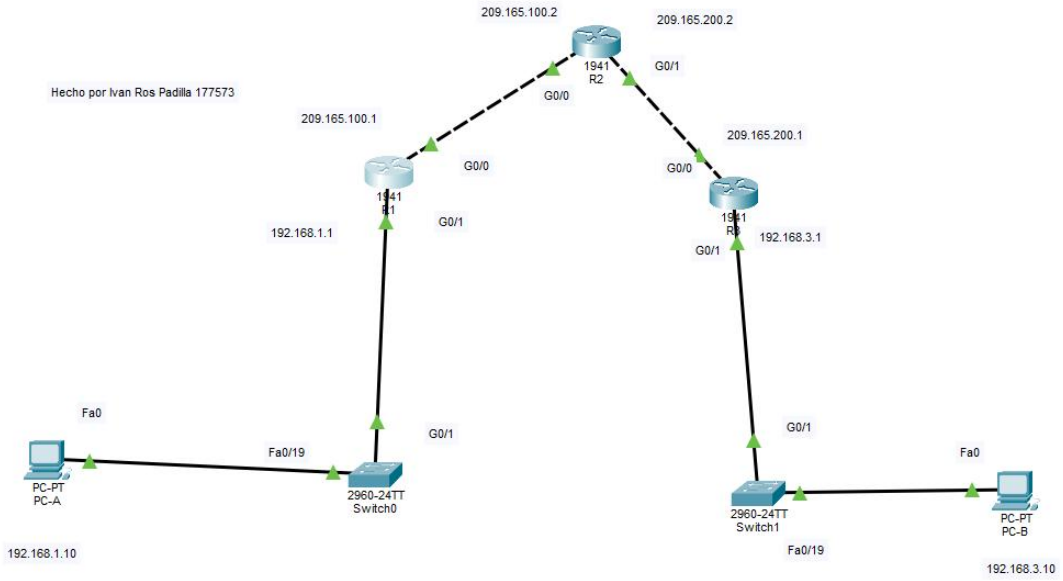
15-2-2026

Tarea 6 Túnel IPSec

Ivan Ros Padilla
UNIVERSIDAD POLITECNICA DE SAN LUIS POTOSI

Topología



1) Configuración Inicial

R1

En el router R1 se realizó la configuración básica asignando direcciones IP a las interfaces LAN y WAN, habilitándolas con el comando no shutdown y estableciendo una ruta por defecto hacia el router intermedio (R2). Este paso garantiza la conectividad inicial necesaria para que el tráfico pueda salir hacia la red externa y eventualmente establecer el túnel VPN con el router remoto.

```
Router>
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#interface g0/0
R1(config-if)# ip address 209.165.100.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)#
R1(config-if)#interface g0/0
R1(config-if)#interface g0/0
R1(config-if)#interface g0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)#ip route 0.0.0.0 0.0.0.0 209.165.100.2
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

R3

En el router R3 se realizó la configuración básica asignando direcciones IP a las interfaces LAN y WAN, habilitándolas y configurando una ruta por defecto hacia el router intermedio (R2). Este paso permitió garantizar la conectividad hacia la red externa y preparar el equipo para establecer comunicación con el router R1 a través de la red pública.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R3
R3(config)#interface g0/0
R3(config-if)# ip address 209.165.200.1 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)#interface g0/1
R3(config-if)# ip address 192.168.3.1 255.255.255.0
R3(config-if)# no shutdown
R3(config-if)#ip route 0.0.0.0 0.0.0.0 209.165.200.2
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
```

2) Licencia de seguridad habilitada

R1

Se verificó que el paquete de seguridad estuviera activo para permitir el uso de funciones criptográficas como ISAKMP e IPSec. La activación de la licencia es fundamental, ya que sin ella no es posible utilizar los comandos necesarios para la implementación del túnel VPN.

```
R1#show license all
License Store: Primary License Storage
StoreIndex: 0   Feature: ipbasek9                       Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium

License Store: Evaluation License Storage
StoreIndex: 0   Feature: securityk9                     Version: 1.0
        License Type: Evaluation
        License State: Active, Not in Use, EULA accepted
            Evaluation total period: 208 weeks 2 days
            Evaluation period left: 208 weeks 2 days
            Period used: 0  minute  0  second
        License Count: Non-Counted
        License Priority: None
StoreIndex: 1   Feature: datak9                         Version: 1.0
        License Type:
        License State: Active, Not in Use, EULA accepted
            Evaluation total period: 208 weeks 2 days
            Evaluation period left: 208 weeks 2 days
            Period used: 0  minute  0  second
        License Count: Non-Counted
        License Priority: None

R1#
```

R3

Se verificó que la licencia de seguridad estuviera activa para permitir la ejecución de comandos relacionados con criptografía e IPSec. Esta habilitación es indispensable para poder establecer túneles VPN y utilizar los mecanismos de cifrado y autenticación necesarios.

```
show license all
License Store: Primary License Storage
StoreIndex: 0   Feature: ipbasek9                          Version: 1.0
        License Type: Permanent
        License State: Active, In Use
        License Count: Non-Counted
        License Priority: Medium

License Store: Evaluation License Storage
StoreIndex: 0   Feature: securityk9                        Version: 1.0
        License Type: Evaluation
        License State: Active, Not in Use, EULA accepted
            Evaluation total period: 208 weeks 2 days
            Evaluation period left: 208 weeks 2 days
            Period used: 0  minute  0  second
        License Count: Non-Counted
        License Priority: None
StoreIndex: 1   Feature: datak9                            Version: 1.0
        License Type:
        License State: Active, Not in Use, EULA accepted
            Evaluation total period: 208 weeks 2 days
            Evaluation period left: 208 weeks 2 days
            Period used: 0  minute  0  second
        License Count: Non-Counted
        License Priority: None

R3#
```

3) Implementación de ACLs

R1

Se creó una lista de acceso extendida que define el “tráfico interesante”, es decir, el tráfico que será cifrado por el túnel IPSec. En este caso, se permitió el tráfico entre la red local 192.168.1.0/24 y la red remota 192.168.3.0/24. Esta ACL es esencial porque le indica al router qué tráfico debe protegerse mediante el proceso de cifrado.

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

R3

Se configuró una lista de acceso extendida que define el tráfico interesante desde la perspectiva de R3. En este caso, se permitió el tráfico entre la red local 192.168.3.0/24 y la red remota 192.168.1.0/24. Esta ACL es inversa a la configurada en R1, ya que cada router debe identificar el tráfico que sale desde su propia red local hacia la red remota para que pueda ser cifrado.

```
R3(config)#access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#
```

4) Phase 01: ISAKMP policy

R1

Se configuró la política ISAKMP especificando los parámetros de negociación para el establecimiento del canal seguro inicial. Se definieron el algoritmo de cifrado (AES), el algoritmo de hash (SHA), el método de autenticación mediante clave pre-compartida, el grupo Diffie-Hellman 2 y el tiempo de vida de la sesión. Además, se configuró la clave compartida asociada a la dirección IP pública del router R3. Esta fase permite establecer un canal seguro para negociar la protección de datos.

```
R1(config)#crypto is
R1(config)#crypto isakmp po
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#en
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#au
R1(config-isakmp)#authentication pre
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#gr
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#cry
R1(config)#crypto is
R1(config)#crypto isakmp key secretkey ad
R1(config)#crypto isakmp key secretkey address 209.165.200.1
```

R3

Se configuró la política ISAKMP utilizando los mismos parámetros definidos en R1: cifrado AES, hash SHA, autenticación mediante clave pre-compartida, grupo Diffie-Hellman 2 y tiempo de vida de la sesión. Además, se estableció la misma clave pre-compartida apuntando a la dirección IP pública de R1. Esta coincidencia de parámetros es fundamental para que la negociación inicial del túnel se realice correctamente.

```
R3(config)#cry
R3(config)#crypto is
R3(config)#crypto isakmp po
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#en
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#aut
R3(config-isakmp)#authentication pr
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#gro
R3(config-isakmp)#group 5
R3(config-isakmp)#exit
```

5) Phase 02: IPSec transform-set

R1

Se creó el transform-set IPSec donde se definieron los algoritmos que se utilizarán para cifrar y autenticar el tráfico de datos (ESP con AES y SHA). Esta fase es la encargada de proteger el tráfico real que viajará entre ambas redes a través del túnel.

```
R1(config)#cry
R1(config)#crypto ip
R1(config)#crypto ipsec tra
R1(config)#crypto ipsec transform-set R1-R3 esp-ae
R1(config)#crypto ipsec transform-set R1-R3 esp-aes 256 es
R1(config)#crypto ipsec transform-set R1-R3 esp-aes 256 esp-
sha-hmac
R1(config)#crypto ipsec transform-set R1-R3 esp-aes 256 esp-
sha-hmac
```

R3

Se creó el transform-set IPSec especificando los algoritmos de cifrado y autenticación que protegerán el tráfico de datos. Esta fase es la encargada de aplicar la seguridad al tráfico real que circula entre las dos redes privadas a través del túnel.

```
R3(config)#cry
R3(config)#crypto is
R3(config)#crypto isakmp po
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#en
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#aut
R3(config-isakmp)#authentication pr
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#gro
R3(config-isakmp)#group 5
R3(config-isakmp)#exit
R3(config)#cry
R3(config)#crypto isa
R3(config)#crypto isakmp key secretkey ad
R3(config)#crypto isakmp key secretkey address 209.165.100.1
```

6) Crear mapa criptográfico

R1

Se configuró un crypto map que vincula la dirección del peer remoto (R3), el transform-set definido y la ACL del tráfico interesante. El crypto map funciona como un contenedor que une todos los parámetros necesarios para que el túnel IPSec pueda establecerse correctamente.

```
R1(config)#cry
R1(config)#crypto map IPS
R1(config)#crypto map IPSEC-MAP 10 ips
R1(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#set
R1(config-crypto-map)#set pe
R1(config-crypto-map)#set peer 209.165.200.1
R1(config-crypto-map)#set
R1(config-crypto-map)#set pf
R1(config-crypto-map)#set pfs gr
R1(config-crypto-map)#set pfs grou
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set sec
R1(config-crypto-map)#set security-association life
R1(config-crypto-map)#set security-association lifetime seco
R1(config-crypto-map)#set security-association lifetime
seconds 86400
```

R3

Se configuró un crypto map asociando la dirección IP del peer remoto (R1), el transform-set previamente creado y la ACL del tráfico interesante. Este mapa criptográfico integra todos los elementos necesarios para establecer el túnel IPSec de manera estructurada.

```
R3(config)#crypto map IPSEC-MAP 10 ipse
R3(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
```

7) Aplicar mapa criptográfico

R1

Finalmente, el crypto map se aplicó a la interfaz WAN del router R1. Este paso es crucial, ya que es el que activa el proceso de cifrado en la interfaz que conecta hacia la red externa. A partir de este momento, cuando se detecta tráfico interesante, el router inicia automáticamente la negociación del túnel IPSec con el router R3.

```
R1(config)#cry
R1(config)#crypto map IPS
R1(config)#crypto map IPSEC-MAP 10 ips
R1(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
R1(config-crypto-map)#set
R1(config-crypto-map)#set pe
R1(config-crypto-map)#set peer 209.165.200.1
R1(config-crypto-map)#set
R1(config-crypto-map)#set pf
R1(config-crypto-map)#set pfs gr
R1(config-crypto-map)#set pfs grou
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set sec
R1(config-crypto-map)#set security-association life
R1(config-crypto-map)#set security-association lifetime seco
R1(config-crypto-map)#set security-association lifetime
seconds 86400
R1(config-crypto-map)#set
R1(config-crypto-map)#set tr
R1(config-crypto-map)#set transform-set R1-R3
R1(config-crypto-map)#ma
R1(config-crypto-map)#match ad
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
```

R3

Finalmente, el crypto map se aplicó a la interfaz WAN del router R3. Con esta acción se activa el proceso de cifrado en la interfaz que conecta hacia la red pública. Una vez generado tráfico interesante, el router inicia automáticamente la negociación del túnel IPSec con R1, estableciendo así la comunicación segura entre ambas redes.

```
R3(config-crypto-map)#set
R3(config-crypto-map)#set pe
R3(config-crypto-map)#set peer 209.165.100.1
R3(config-crypto-map)#set pfs
R3(config-crypto-map)#set pfs group5
R3(config-crypto-map)#set sec
R3(config-crypto-map)#set security-association lifetime seco
R3(config-crypto-map)#set security-association lifetime
seconds 86400
R3(config-crypto-map)#set
R3(config-crypto-map)#set tr
R3(config-crypto-map)#set transform-set R3-R1
R3(config-crypto-map)#mat
R3(config-crypto-map)#match ad
R3(config-crypto-map)#match address 100
R3(config-crypto-map)#exit
```