IMPLEMENTACION IPSEC VPN

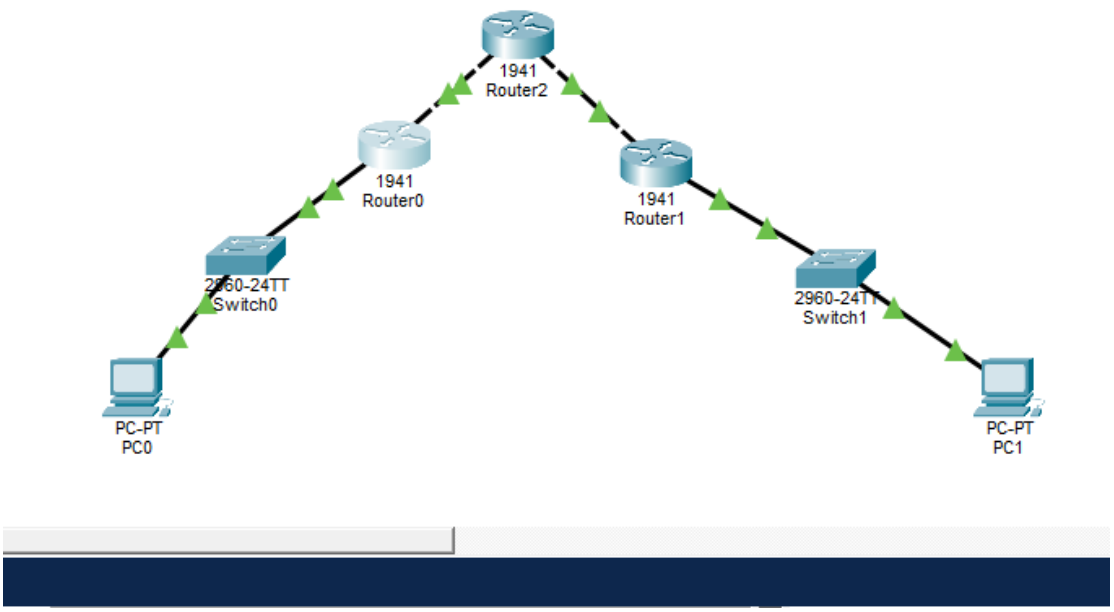
SEGURIDAD INFORMATICA ACTIVIDAD 6

LUIS EDUARDO AZNAR CUEVAS 179880

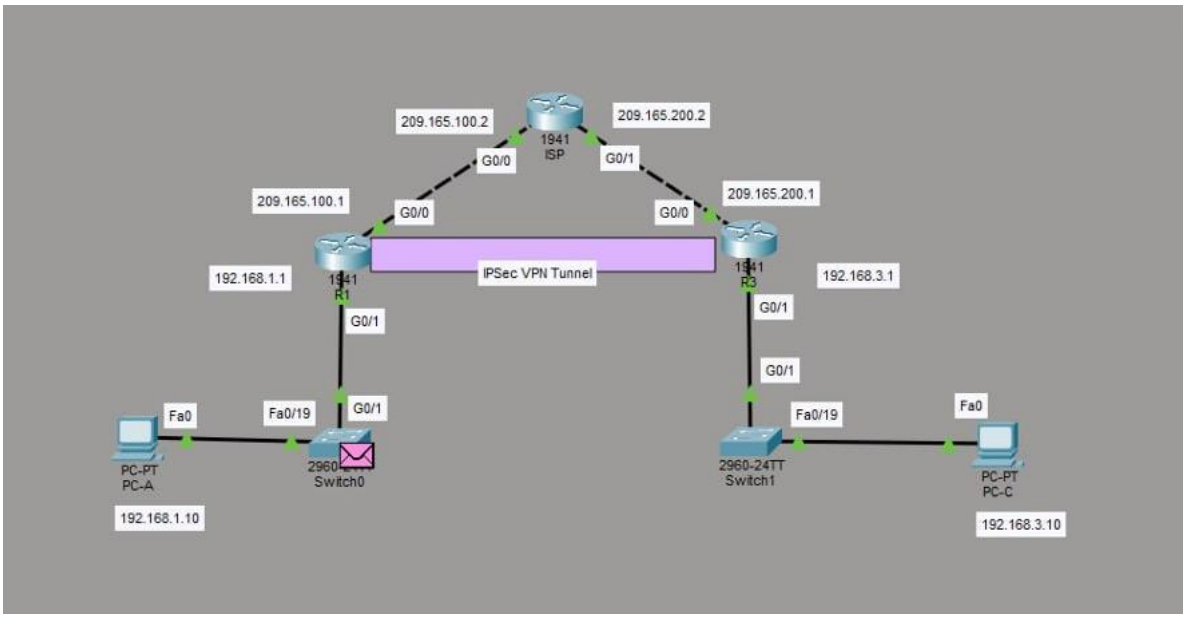
Introduccion

A través de esta práctica se configurarán dispositivos Cisco para establecer un túnel seguro sitio a sitio, aplicando conceptos fundamentales de ciberseguridad como criptografía simétrica, autenticación mediante claves pre-compartidas, políticas ISAKMP/IKE y listas de acceso para la definición del tráfico interesante. Esta actividad permitirá comprender el funcionamiento práctico de los servicios de seguridad en redes, reforzando los conocimientos teóricos sobre protección de datos en tránsito y gestión de comunicaciones seguras en infraestructuras empresariales.

1) Configuración inicial de equipo
2) Activar paquete de seguridad (licencia de seguridad habilitada)
3) Implementación de ACLS
4) Phase 01: ISAKMP POLICY
5) Phase 02: Ipsec transform set
6) Crear el mapa criptográfico
7) Aplicar el mapa criptográfico



Se configuraron las redes de los routers, de 1 a 3 con sus respectivas conexiones a cada uno de ellos, utilizando comandos como CONFIGURE TERMINAL y IP ADD para poder configurar cada router con su respectiva IP, estas siendo de esta manera:




```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname r1
r1(config)#int g0/0
r1(config-if)#ip add 209.165.100.1 255.255.255.0
r1(config-if)#no shutdown

r1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
int g0/1
r1(config-if)#ip add 192.168.1.1 255.255.255.0
r1(config-if)#no shutdown

r1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
exit
r1(config)#
```

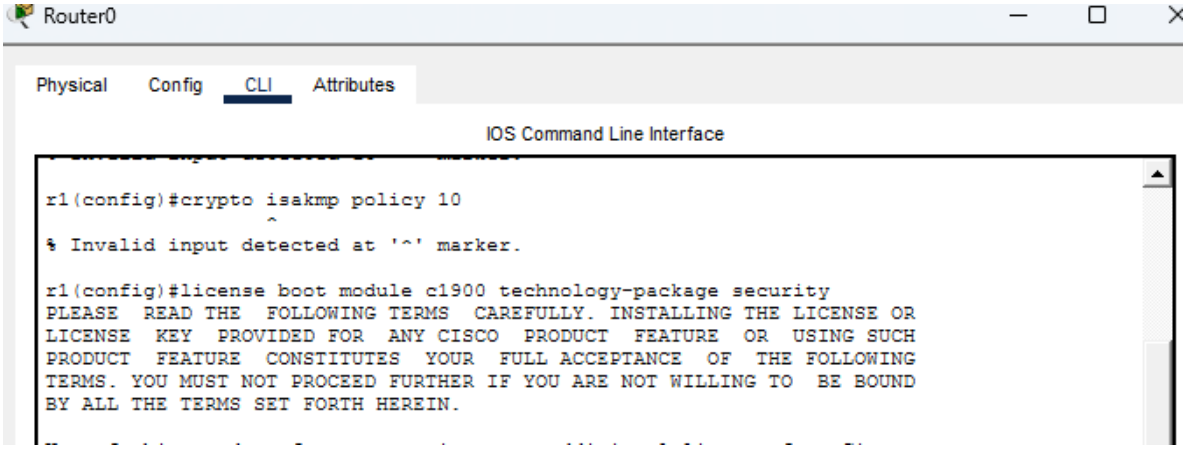
```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname r3
r3(config)#int g0/0
r3(config-if)#ip add 209.165.200.1 255.255.255.0
r3(config-if)#no shutdown

r3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
int g0/1
r3(config-if)#ip add 192.168.3.1 255.255.255.0
r3(config-if)#no shutdown

r3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
exit
r3(config)#
```

```
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname isp
isp(config)#int g0/0
isp(config-if)#ip add 209.165.100.2 255.255.255.0
isp(config-if)#no shutdown

isp(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
int g0/1
isp(config-if)#ip add 209.165.200.2 255.255.255.0
isp(config-if)#no shutdown

isp(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
exit
isp(config)#
```

Políticas de Seguridad ISAKMP

ISAKMP o Internet Security Association and Key Management Protocol es un protocolo que autentica los dispositivos y establece un canal seguro, esto corresponde a la FASE 1 de IKE, donde se crea el canal seguro antes de crear el túnel.

Para poder utilizar las políticas ISAKMP se tenía que bootear una licencia en Packet Tracer, la C1900 y loadear de nuevo los comandos para poder hacer uso de esta política.



Al terminar de loadear esta licencia, se utilizó la POLITICA 10 para poder configurar los parámetros de seguridad que se usaran para establecer los canales seguros.

Se utilizaron los comandos de #ENCRYPTION AES 256 Y AUTHENTICATION PRE-SHARE para el cifrado y la autenticación respectivamente. Esto inicia la fase 1 de la configuración de la ipsec, define las reglas de seguridad y permite establecer un canal seguro entre los routers antes de cifrar el tráfico.

```
r1>en
r1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
r1(config)#crypto isakmp policy 10
r1(config-isakmp)#encryption pre-sha
                             ^
% Invalid input detected at '^' marker.

r1(config-isakmp)#encryption aes 256
r1(config-isakmp)#encryption pre
                             ^
% Invalid input detected at '^' marker.

r1(config-isakmp)#encryption pr
                             ^
% Invalid input detected at '^' marker.

r1(config-isakmp)#authentication pre-share
r1(config-isakmp)#group 5
r1(config-isakmp)#exit
r1(config)#crypto isakmp key secretkey address 209.165.200.1
r1(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
r1(config)#crypto ipsec transform-set r1->r3 esp-aes 256 esp-sha-hmac
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)#
```

Esto se realiza en ambos routers, el router 1 y en el router 3 para poder configurar el tunel entre estos dos.

Conclusión

La implementación de una VPN IPsec en Cisco Packet Tracer permitió comprender de manera práctica cómo se establecen comunicaciones seguras entre redes remotas a través de una infraestructura pública. Mediante la configuración de políticas ISAKMP/IKE, claves pre compartidas, transform sets y listas de acceso para definir el tráfico interesante, se aplicaron conceptos fundamentales de ciberseguridad relacionados con confidencialidad, integridad y autenticación de la información.