IMPLEMENTACIÓN IPSEC VPN

Actividad 06

CNO V – Seguridad Informática

Parcial 1: Fundamentos del Hacking Ético

Mtro. Servando López Contreras

Omar Karim Alonso Castillo 179033

Universidad Politécnica de San Luis Potosí

Contenido

Introducción

La protección de la información en entornos de red es un aspecto fundamental dentro del estudio de la seguridad informática. En particular, cuando los datos deben atravesar infraestructuras públicas como Internet, resulta indispensable implementar mecanismos que aseguren su confidencialidad e integridad. Una de las soluciones más utilizadas para este propósito son las Redes Privadas Virtuales (VPN), que permiten establecer canales seguros de comunicación entre diferentes sedes o usuarios.

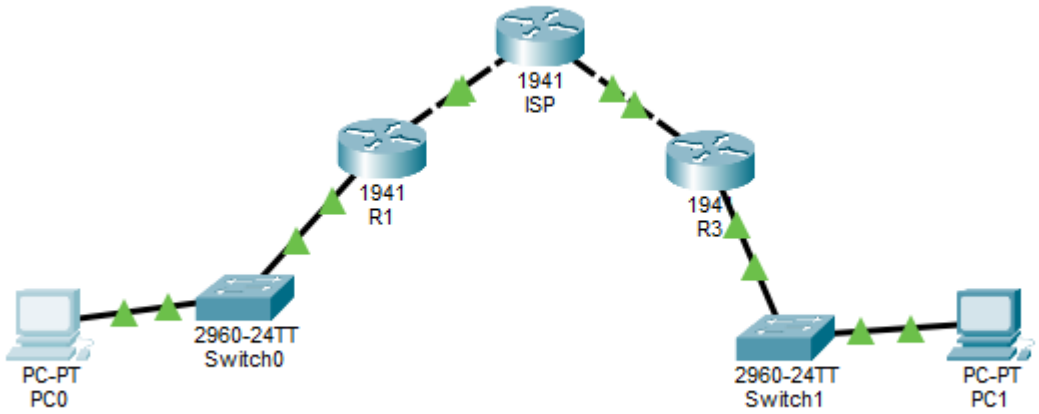
Dentro de las tecnologías disponibles, IPsec (Internet Protocol Security) se ha consolidado como un estándar ampliamente adoptado, ya que ofrece funciones de cifrado y autenticación directamente en la capa de red.

Objetivo

El propósito de esta práctica es comprender y aplicar los conceptos fundamentales de seguridad en redes mediante la implementación de una VPN IPsec sitio a sitio en el simulador Packet Tracer. A través de la configuración de routers Cisco, se busca establecer un túnel seguro que permita la comunicación entre dos redes locales a través de un proveedor de servicios simulado, garantizando la protección de la información mediante técnicas de cifrado y autenticación.

- De manera específica, los objetivos de la actividad son:
- Configurar el direccionamiento IP en los dispositivos de la topología (routers, switches y PCs).
- Establecer rutas estáticas que aseguren la conectividad extremo a extremo entre las redes.
- Implementar un túnel VPN IPsec con parámetros de seguridad robustos, incluyendo cifrado AES-256.
- Verificar el funcionamiento del túnel mediante pruebas de conectividad entre las LANs.
- Confirmar que el tráfico intercambiado entre las redes viaja de forma cifrada y protegido contra posibles interceptaciones

1. Configuración Inicial



Router 1 (R1)

```
Router>EN
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int g0/1
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no shut

R1(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
int g0/0
R1(config-if)#ip add 209.165.100.1 255.255.255.0
R1(config-if)#no shut

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
exit
R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.100.2
R1(config)#
```

Router 3 (R3)

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R3
R3(config)#int g0/1
R3(config-if)#ip add 192.168.3.1 255.255.255.0
R3(config-if)#no shut

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
int g0/0
R3(config-if)#ip add 209.165.200.1 255.255.255.0
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
exit
R3(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.2
R3(config)#
```

ISP

```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname ISP
ISP(config)#int g0/1
ISP(config-if)#ip add 209.165.200.2 255.255.255.0
ISP(config-if)#no shut

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
int g0/0
ISP(config-if)#ip add 209.165.100.2 255.255.255.0
ISP(config-if)#no shut

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
exit
ISP(config)#
```

2. Licencia de seguridad habilitada

En routers Cisco modernos (como los 1941), se necesita el conjunto de funciones de seguridad para usar IPSec.

Comando: license boot module c1900 technology-package securityk9

Se debe guardar la configuración (write) y reiniciar el router para que se active.

EJEMPLO CON R1 (se hizo lo mismo en los demás routers):

```
R1>en
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#license boot module c1900 technology-package securityk9
PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires  an additional license from Cisco,
together with an additional  payment.  You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the  product,  including  during the 60 day  evaluation  period,  is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day  evaluation  period,  your  use of the  product  feature will be
governed  solely by the Cisco  end user license agreement (link above),
together  with any supplements  relating to such product  feature.  The
above  applies  even if the evaluation  license  is  not  automatically
terminated  and you do  not receive any notice of the expiration of the
evaluation  period.  It is your  responsibility  to  determine when the
evaluation  period is complete and you are required to make  payment to
Cisco for your use of the product feature beyond the evaluation period.

Your  acceptance  of  this agreement  for the software  features on one
product  shall be deemed  your  acceptance  with  respect  to all  such
software  on all Cisco  products  you purchase  which includes the same
software.  (The foregoing  notwithstanding, you must purchase a license
for each software  feature you use past the 60 days evaluation  period,
so  that  if you enable a software  feature on  1000  devices, you must
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? [yes/no]: yes
```

```
R1#write
Building configuration...
[OK]
R1#
```

3. Implementación de ACLs

Se debe definir qué tráfico debe ser cifrado. En este caso, el tráfico que va de la red local de R1 (192.168.1.0/24$) a la de R3 (192.168.3.0/24$).

ROUTER 1 (R1)

```
R1>en
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
R1(config)#
```

```
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)#
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#crypto isakm
R1(config)#crypto isakmp  ke
R1(config)#crypto isakmp  key secre
R1(config)#crypto isakmp  key secret
R1(config)#crypto isakmp  key secretkey address 209.165.200.1
R1(config)#crypto ipsec trans
R1(config)#crypto ipsec transform-set  R1-R3 esp
R1(config)#crypto ipsec transform-set  R1-R3 esp-aes 256 esp-sha-hmac
R1(config)#crypto map IPSEC-MAP 10 ipsec- isakmp
                                  ^
% Invalid input detected at '^' marker.

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 peer 209.165.200.1
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 sec
R1(config-crypto-map)#set security-association lifetime seconds 86400
R1(config-crypto-map)#set tra
R1(config-crypto-map)#set transform-set R1-R3
R1(config-crypto-map)#match add
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
R1(config)#int g0/0
R1(config-if)#cry
R1(config-if)#crypto map ips
R1(config-if)#crypto map IPSEC-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#exit
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)#
```

ROUTER 3 (R3)

```
R3>en
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#
```

```
R3>
R3>en
R3#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#do wr
Building configuration...
[OK]
R3(config)#crypto ipsec tra
R3(config)#crypto ipsec transform-set R3-R1 esp-aes 256 esp-sha-hmac
R3(config)#cr
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.
R3(config-crypto-map)#set peer 209.165.100.1
R3(config-crypto-map)#set pfs group5
R3(config-crypto-map)#set sec
R3(config-crypto-map)#set security-association lifetim
R3(config-crypto-map)#set security-association lifetime se
R3(config-crypto-map)#set security-association lifetime seconds 86400
R3(config-crypto-map)#set trans
R3(config-crypto-map)#set transform-set R3-R1
R3(config-crypto-map)#match add
R3(config-crypto-map)#match address 100
R3(config-crypto-map)#exit
R3(config)#int g0/0
R3(config-if)#cry
R3(config-if)#crypto map IPSEC-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R3(config-if)#exit
R3(config)#acces
R3(config)#access-list 100 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

Aquí se define cómo los routers se autenticarán y negociarán la seguridad inicial.

El objetivo de esta etapa es crear un "canal seguro" inicial donde los routers puedan negociar cómo protegerán el tráfico final.

- **crypto isakmp policy 10**: Crea una política de negociación. El número '10' es la prioridad; si existen varias, el router intentará usar la más baja primero.
- **encryption aes 256**: Define el estándar de cifrado AES con una llave de 256 bits, proporcionando un nivel de seguridad robusto contra ataques de fuerza bruta.
- **authentication pre-share**: Indica que los routers se identificarán mediante una contraseña secreta previamente acordada.
- **group 5**: Establece el uso del algoritmo Diffie-Hellman (DH) Grupo 5 para el intercambio de llaves, asegurando que las claves de cifrado no se envíen por la red.

Autenticación de Extremo a Extremo

- **crypto isakmp key secretkey address 209.165.200.1**: Aquí se define la "palabra de paso" (secretkey) y se vincula específicamente a la IP pública del peer remoto (R3). Sin esta coincidencia exacta, el túnel jamás se levantará.

R1

```
R1(config)#crypto isakmp  key secretkey address 209.165.200.1
R1(config)#crypto ipsec trans
R1(config)#crypto ipsec transform-set  R1-R3 esp
R1(config)#crypto ipsec transform-set  R1-R3 esp-aes 256 esp-sha-hmac
R1(config)#crypto map IPSEC-MAP 10 ipsec- isakmp
                                        ^
% Invalid input detected at '^' marker.

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 peer 209.165.200.1
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 sec
R1(config-crypto-map)#set security-association lifetime seconds 86400
R1(config-crypto-map)#set tra
R1(config-crypto-map)#set transform-set R1-R3
R1(config-crypto-map)#match add
R1(config-crypto-map)#match address 100
R1(config-crypto-map)#exit
R1(config)#int g0/0
R1(config-if)#cry
R1(config-if)#crypto map ips
R1(config-if)#crypto map IPSEC-MAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R1(config-if)#exit
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)#cry
R1(config)#crypto isak
R1(config)#crypto isakmp pol
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#encr
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#authent
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 5
R1(config-isakmp)#exit
R1(config)#cryp
R1(config)#crypto isakmp key sec
```

R3

```
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#encryp
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#gro
R3(config-isakmp)#group 5
R3(config-isakmp)#exit
R3(config)#crypt
R3(config)#crypto isakmp key secretkey address 209.165.100.1
R3(config)#
```

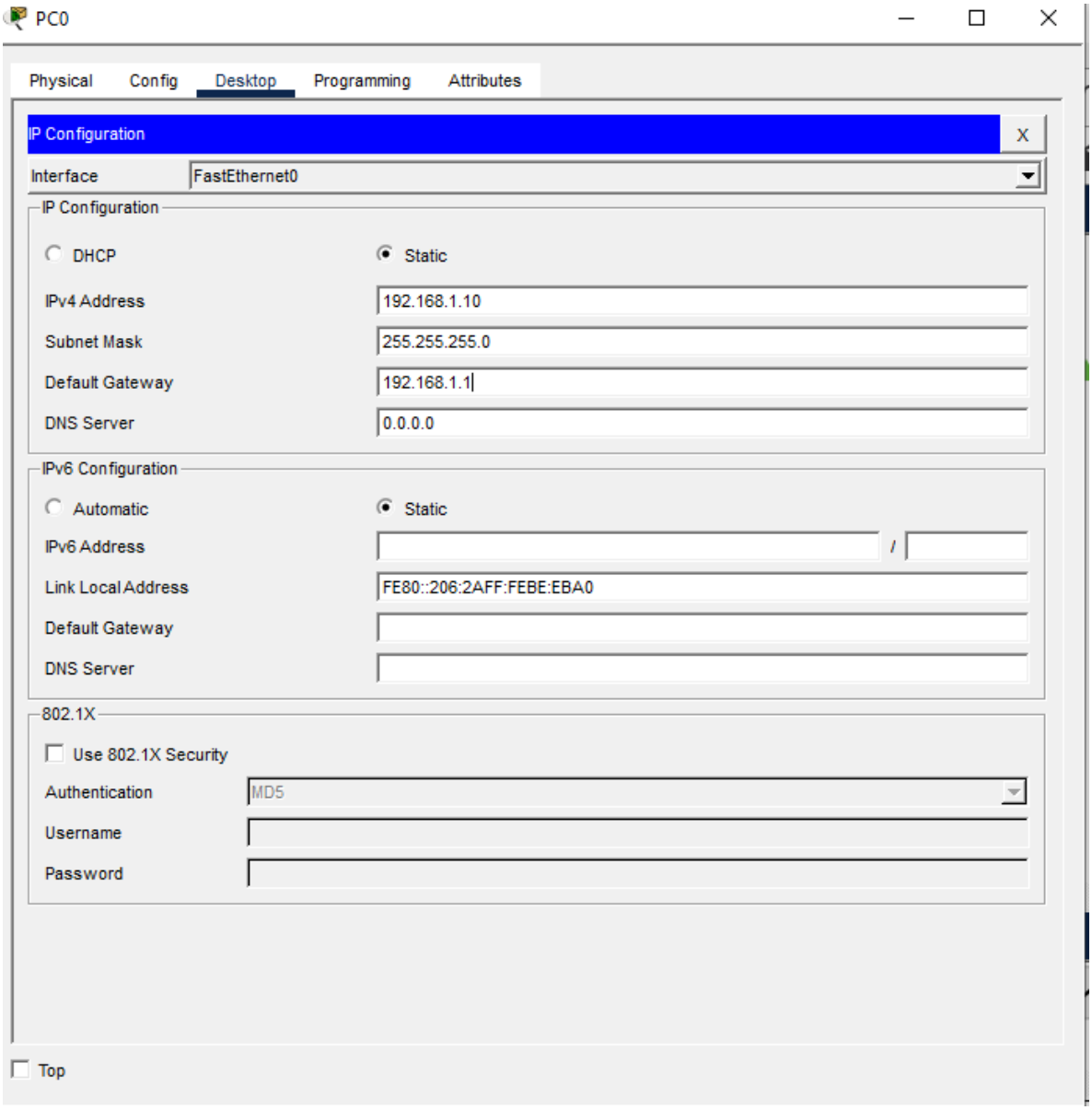
5 Phase 02: IPSec transform-set

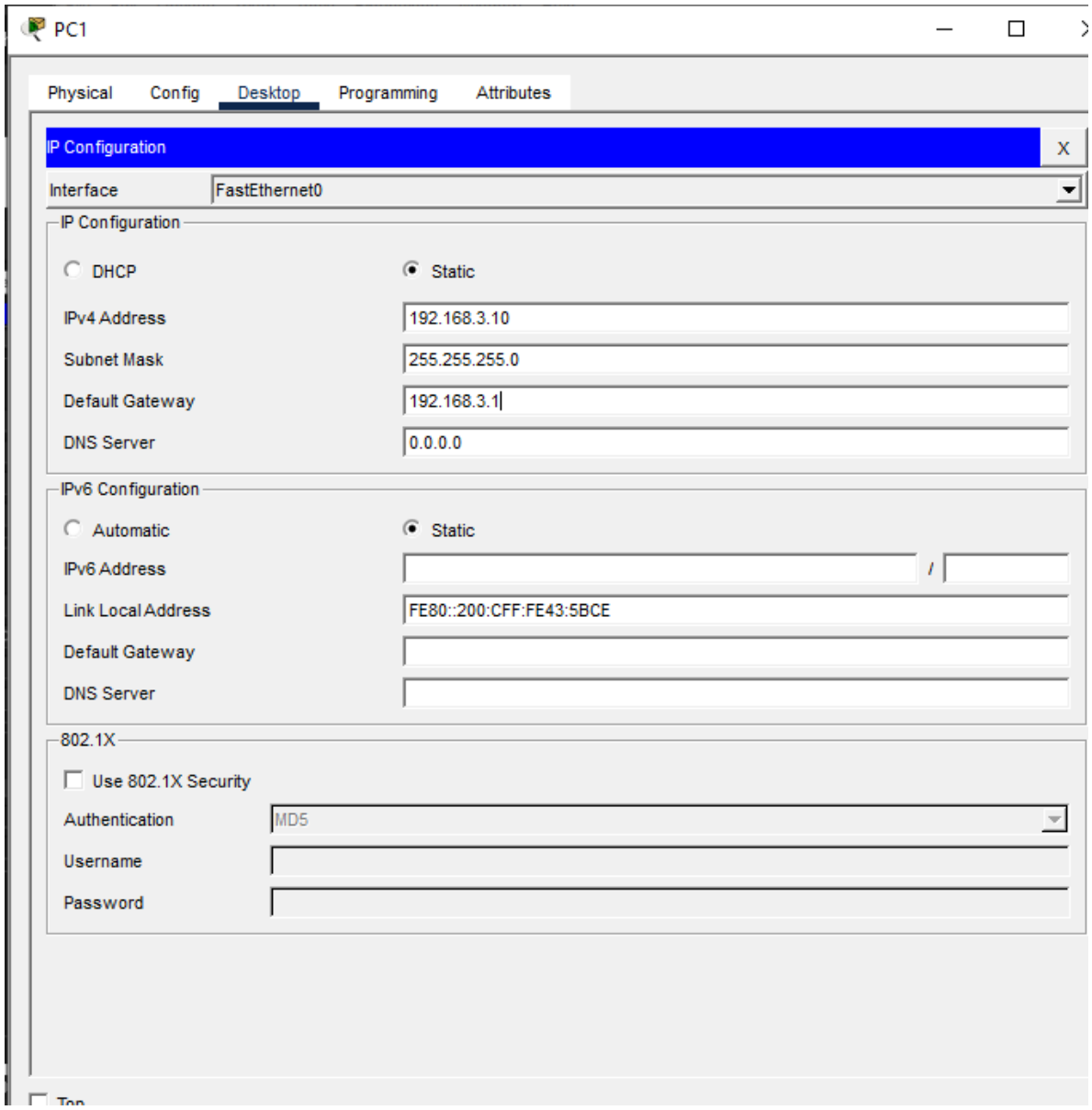
Mientras que la Fase 1 establece el "túnel de gestión", la **Fase 2** define cómo se protegerán los datos reales del usuario que atraviesan la red pública. Aquí se acuerdan los algoritmos de cifrado y hash específicos para el tráfico de datos.

- **crypto ipsec transform-set R1-R3 esp-aes 256 esp-sha-hmac**

- **Propósito:** Este comando crea una "combinación de seguridad".
- **esp-aes 256**: Utiliza el protocolo *Encapsulating Security Payload* (ESP) para cifrar el paquete completo. Se elige AES de 256 bits por ser el estándar de oro en seguridad actual.
- **esp-sha-hmac**: Aplica un código de autenticación de mensajes (HMAC) basado en SHA para asegurar que los datos no hayan sido alterados durante el tránsito (integridad).

Configuración IP




PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.3.10
Subnet Mask
255.255.255.0
Default Gateway
192.168.3.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
/
Link Local Address
FE80::200:CFF:FE43:5BCE
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

PING

```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.1.10: bytes=32 time<1ms TTL=126
Reply from 192.168.1.10: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

6 Crear el mapa criptografico

El **Crypto Map** es el componente de software que amalgama todas las piezas anteriores: quién es el vecino, qué tráfico cifrar y qué métodos de seguridad usar. Es el "manual de instrucciones" que el router consulta antes de enviar un paquete.

- **crypto map IPSEC-MAP 10 ipsec-isakmp**
  - Inicia la creación del mapa llamado "IPSEC-MAP". El número 10 permite tener múltiples secuencias para diferentes sucursales.
- **set peer 209.165.200.1**
  - Define la dirección IP pública del router remoto (R3). Es el destino final del túnel.
- **set pfs group5**
  - Activa *Perfect Forward Secrecy* (PFS). Esto obliga al router a generar una clave nueva y única para cada sesión, de modo que si una clave es comprometida, el resto de las comunicaciones pasadas y futuras permanezcan seguras.
- **set security-association lifetime seconds 86400**
  - Establece que la asociación de seguridad expire cada 24 horas. Esto fuerza una re-negociación periódica de las llaves para frustrar intentos de criptoanálisis a largo plazo.
- **set transform-set R1-R3**
  - Vincula el conjunto de cifrado definido en el paso anterior (Fase 2) a este mapa específico.
- **match address 100**
  - Hace referencia a una Lista de Control de Acceso (ACL). Solo el tráfico que coincida con las reglas de la ACL 100 será procesado por la VPN.

7 Aplicar el mapa criptografico

Tener el mapa creado no sirve de nada si no se le indica al router en qué puerto físico debe actuar. Este es el paso final donde la política de seguridad se vuelve operativa.

- **interface g0/0**
  - Entra en la configuración de la interfaz física que está conectada hacia el exterior (Internet/WAN).
- **crypto map IPSEC-MAP**
  - **Propósito:** Activa el motor de cifrado en esta interfaz. A partir de este momento, cada paquete que intente salir por g0/0 será comparado con la ACL del mapa; si coincide, se cifra y se encapsula antes de salir al mundo exterior.

Conclusión

El aprendizaje principal de esta configuración radica en la comprensión de la modularidad de la seguridad. Dividir el proceso en Fase 1 (Control) y Fase 2 (Datos) enseña que una comunicación robusta no nace de un solo paso, sino de una negociación jerárquica. Primero se establece un entorno de confianza mutua y, solo después de asegurar esa "conversación", se permite que el tráfico privado del usuario toque la red pública.

Por otro lado, este despliegue refuerza la importancia de la precisión técnica y la simetría. En el mundo de la criptografía aplicada, el más mínimo error en un algoritmo de hash o en un grupo Diffie-Hellman resulta en un fallo total de conectividad. Esto nos enseña que la seguridad informática es una disciplina de exactitud, donde el éxito no es solo que un paquete llegue a su destino, sino que lo haga de forma invisible e inalterable para cualquier observador externo.

Finalmente, el uso de herramientas de diagnóstico como show crypto ipsec sa transforma nuestra visión de la red: pasamos de buscar una simple conexión a validar la integridad de los datos. El aprendizaje real se consolida al entender que somos capaces de crear un "túnel privado" dentro del caos de Internet, garantizando que la confidencialidad sea una constante y no una variable en la comunicación empresarial.