UNIVERSIDAD ANDINA DEL CUSCO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TEMA

"REDES PRIVADAS VIRTUALES (VPN) BASADAS EN IPSEC"

DOCENTE

Mgt. Ing. Ediwn Carrasco Poblete

ALUMNOS

Almanza Cuno, Gonzalo Jair

Condori Contretas, Mike Maraco

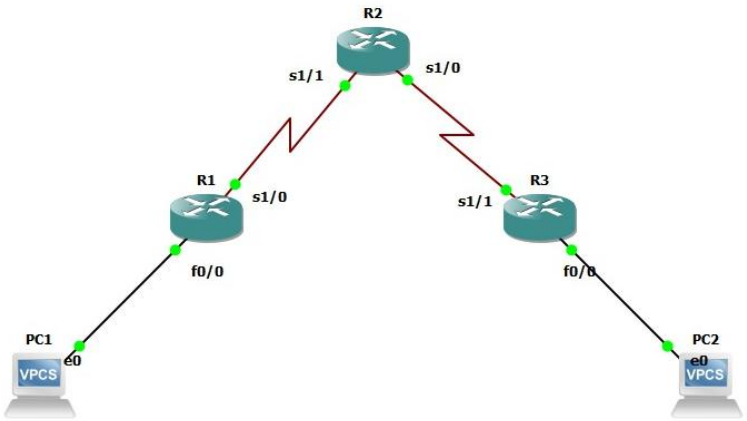
Ninantay Halanoca, Jesus Sergio

Villena Rojas, Oscar Phool

CUSCO – PERÚ

2023

1. Diseño de la topologia de la red



2. Configuración de equipos terminales

A. Configuracion de PC1

```
PC1> ip 192.168.1.10/24 gateway 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.10 255.255.255.0 gateway 192.168.1.1
```

```
PC1> ping 192.168.1.1
84 bytes from 192.168.1.1 icmp_seq=1 ttl=255 time=15.314 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=255 time=15.417 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=255 time=15.219 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=255 time=15.764 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=255 time=15.215 ms
```

B. Configuracion de PC2

```
PC2> ip 192.168.2.10/24 gateway 192.168.2.1
Checking for duplicate address...
PC1 : 192.168.2.10 255.255.255.0 gateway 192.168.2.1
```

```
PC2> ping 192.168.2.1
84 bytes from 192.168.2.1 icmp_seq=1 ttl=255 time=15.346 ms
84 bytes from 192.168.2.1 icmp_seq=2 ttl=255 time=15.082 ms
84 bytes from 192.168.2.1 icmp_seq=3 ttl=255 time=15.176 ms
84 bytes from 192.168.2.1 icmp_seq=4 ttl=255 time=15.128 ms
84 bytes from 192.168.2.1 icmp_seq=5 ttl=255 time=14.938 ms
```

3. Configuración de enrutadores

a) Configuración del enrutador R1

```
 changed state to down
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 1/0
R1(config-if)#ip address 20.0.0.1 255.0.0.0
R1(config-if)#clock rate 64000
R1(config-if)#encapsulation ppp
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
*Mar  1 00:01:51.579: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:01:52.579: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config)#
*Mar  1 00:01:53.223: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
R1(config)#
*Mar  1 00:02:10.431: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up
```

b) Configuración del enrutador R2

```
R2#
R2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface serial1/1
R2(config-if)#ip address 20.0.0.2 255.0.0.0
R2(config-if)#encapsulation ppp
R2(config-if)#clock rate 64000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#interface serial1/0
R2(config-if)#ip address 30.0.0.1 255.0.0.0
R2(config-if)#encapsulation ppp
R2(config-if)#clock rate 64000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*Mar  1 00:01:55.527: %LINK-3-UPDOWN: Interface Serial1/1, changed state to up
*Mar  1 00:01:55.963: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up
```

c) Configuración del enrutador R3

PC1 | PC2 | R1 | R2 | R3

```
 changed state to down
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#interface serial1/1
R3(config-if)#ip address 30.0.0.2 255.0.0.0
R3(config-if)#encapsulation ppp
R3(config-if)#clock rate 64000
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface fastethernet 0/0
R3(config-if)#ip address 192.168.2.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
*Mar  1 00:01:58.459: %LINK-3-UPDOWN: Interface Serial1/1, changed state to up
R3(config-if)#exit
R3(config)#
*Mar  1 00:01:59.495: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/1, changed state to up
R3(config)#
*Mar  1 00:02:00.263: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:02:01.263: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

4. Configuración de la VPN

a) Configuración del enrutador R1

PC1 PC2 R1

```
*Mar  1 00:00:06.483: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to up
*Mar  1 00:00:06.855: %LINK-5-CHANGED: Interface Serial1/1, changed state to adm
inistratively down
*Mar  1 00:00:06.883: %LINK-5-CHANGED: Interface Serial1/2, changed state to adm
inistratively down
*Mar  1 00:00:06.887: %LINK-5-CHANGED: Interface Serial1/3, changed state to adm
inistratively down
*Mar  1 00:00:08.343: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0,
 changed state to up
R1#
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#crypto isakmp enable
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#hash md5
R1(config-isakmp)#encryption des
R1(config-isakmp)#group 2
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#exit
R1(config)#crypto isakmp key security address 30.0.0.2 255.0.0.0
A pre-shared key for address mask 30.0.0.2 255.0.0.0 already exists!

R1(config)#crypto ipsec transform-set hoset esp-des esp-md5-hmac
R1(cfg-crypto-trans)#exit
R1(config)#$ 101 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
R1(config)#crypto map r1map 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 30.0.0.2
R1(config-crypto-map)#set transform-set hoset
R1(config-crypto-map)#match address 101
R1(config-crypto-map)#exit
R1(config)#interface Serial 1/0
R1(config-if)#crypto map r1map
R1(config-if)#exit
R1(config)#
```

b) Configuración del enrutador R3

```
R3(config)#crypto isakmp enable
R3(config)#crypto isakmp policy 10
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#hash md5
R3(config-isakmp)#encryption des
R3(config-isakmp)#group 2
R3(config-isakmp)#lifetime 3600
R3(config-isakmp)#exit
R3(config)#crypto isakmp key security address 20.0.0.1 255.0.0.0
R3(config)#crypto ipsec transform-set r3set esp-des esp-md5-hmac
R3(cfg-crypto-trans)#exit
R3(config)#$ 101 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#crypto map r3map 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 20.0.0.1
R3(config-crypto-map)#set transform-set r3set
R3(config-crypto-map)#match address 101
R3(config-crypto-map)#exit
R3(config)#interface serial 1/1
R3(config-if)#crypto map r3map
R3(config-if)#exit
*Mar  1 00:02:50.179: %CRYPTO-6-ISAKMP ON OFF: ISAKMP is ON
```

5. Configuración del enrutamiento

a) **Cofiguración del router R1**

```
R1(config)#ip route 0.0.0.0 0.0.0.0 20.0.0.2
```

b) **Cofiguración del router R**

```
R3(config)#ip route 0.0.0.0 0.0.0.0 30.0.0.1
```

6. Habilitar la depuracion para IPSEC e ISAKMP

a) **Configuración del enrutador R1**

```
R1#debug crypto ipsec
Crypto IPSEC debugging is on
R1#debug crypto isakmp
Crypto ISAKMP debugging is on
R1#
*Mar  1 00:04:32.143: IPSEC(sa_request): ,
  (key eng. msg.) OUTBOUND local= 20.0.0.1, remote= 30.0.0.2,
```

b) **Configuración del enrutador R3**

```
R3#debug crypto ipsec
Crypto IPSEC debugging is on
R3#debug crypto isakmp
*Mar  1 00:03:48.171: %SYS-5-CONFIG_I: Configured from console by console
R3#debug crypto isakmp
Crypto ISAKMP debugging is on
R3#
```

7. Pruebas de conectividad

a) **Prueba desde PC1**

```
PC1> ping 192.168.2.10
192.168.2.10 icmp_seq=1 timeout
192.168.2.10 icmp_seq=2 timeout
84 bytes from 192.168.2.10 icmp_seq=3 ttl=62 time=90.463 ms
84 bytes from 192.168.2.10 icmp_seq=4 ttl=62 time=90.954 ms

84 bytes from 192.168.2.10 icmp_seq=5 ttl=62 time=91.355 ms
```

c) **Prueba desde PC2**

```
PC2> ping 192.168.1.10
192.168.1.10 icmp_seq=1 timeout
192.168.1.10 icmp_seq=2 timeout
84 bytes from 192.168.1.10 icmp_seq=3 ttl=62 time=91.852 ms
84 bytes from 192.168.1.10 icmp_seq=4 ttl=62 time=90.262 ms
84 bytes from 192.168.1.10 icmp_seq=5 ttl=62 time=90.860 ms
```

8. Diagnostico VPN

a) En el enrutador R1

```
R1#
R1#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               3600 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
R1#
```

b) En el enrutador R2

```
R3#
R3#show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               3600 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume limit
R3#
```