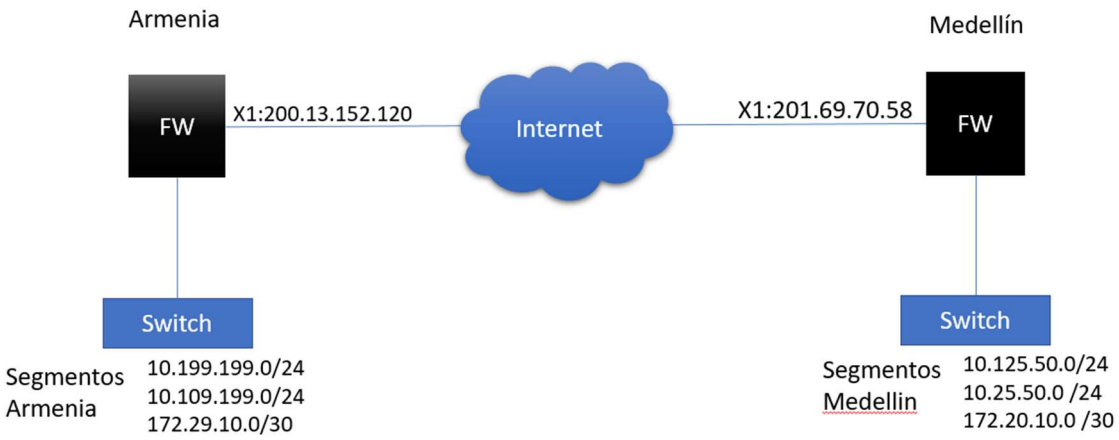
Proceso de aprovisionamiento de VPNs usando CLI en Sonicwall

Esquema Ejemplo:



Proceso:

1- Crear Address Objects
2- Crear Address Groups
3- Crear la VPN
- Dirección IP del otro extremo (IP Valida)
- IKE IDs (Local, Remoto, Si es aplicable)
- Red local, Red remota (en caso de Site to Site)
- Parámetros de cifrado (AES 256, SHA1... timeout, etc.)
- Asociar a la interface 1
- Crear rutas (en caso de Tunnel Interface)

En el firewall de Medellin

1. Crear Address Objects

Creación de Address Objects correspondiente a la local

```
address-object ipv4 "Red Medellin 1" network 10.125.50.0 /24 zone LAN
address-object ipv4 "Red Medellin 2" network 10.25.50.0 /24 zone LAN
address-object ipv4 "Red Medellin 3" network 172.20.10.0 /30 zone LAN
```

Creación de Address Objects correspondiente a la red remota

```
address-object ipv4 "Red Armenia 1" network 10.199.199.0 /24 zone VPN
address-object ipv4 "Red Armenia 2" network 10.109.199.0 /24 zone VPN
address-object ipv4 "Red Armenia 3" network 172.29.10.0 /30 zone VPN
```

2. Creación de Address Groups

Creación de Redes locales y remotas

```
address-group ipv4 "Redes Armenia"
address-object ipv4 "Red Armenia 1"
address-object ipv4 "Red Armenia 2"
address-object ipv4 "Red Armenia 3"
end

address-group ipv4 "Redes Medellin"
address-object ipv4 "Red Medellin 1"
address-object ipv4 "Red Medellin 2"
address-object ipv4 "Red Medellin 3"
end
commit
```

3. Creación de la VPN hacia la red remota

Opción 1: Usando Tunnel Interface

(en este caso hemos usado IKE Versión 2 y Cifrado AES-GCM-256)

```
vpn policy tunnel-interface "VPN Armenia"
enable
gateway primary 201.69.70.58
auth-method shared-secret
shared-secret XXXXXX
ike-id local ipv4 5.5.5.7
ike-id peer ipv4 6.6.6.7
exit
proposal ike exchange ikev2
proposal ike encryption aes-256
proposal ike authentication sha-256
proposal ike dh-group 2
proposal ike lifetime 28800
proposal ipsec protocol esp
proposal ipsec encryption aes-gcm16-256
no proposal ipsec authentication
no proposal ipsec perfect-forward-secrecy
proposal ipsec lifetime 28800
No keepalive
bound-to interface X1
exit
commit

route-policy ipv4 interface "VPN Armenia" metric 20
name "Ruta Armenia"
interface "VPN Armenia"
source any
destination group "Redes Armenia"
service any
exit
```

```
commit
```

Opción 2: Usando Site to Site
(en este caso hemos usado Modo Main y Cifrado AES-256)

```
vpn policy site-to-site "VPN Armenia"
enable
gateway primary 201.69.70.58
auth-method shared-secret
shared-secret XXXXXX
ike-id local ipv4 5.5.5.7
ike-id peer ipv4 6.6.6.7
exit
network local group "Redes Medellin"
network remote destination-network group "Redes Armenia"
proposal ike exchange main
proposal ike encryption aes-256
proposal ike authentication sha-256
proposal ike dh-group 2
proposal ike lifetime 28800
proposal ipsec protocol esp
proposal ipsec encryption aes-256
proposal ipsec authentication sha-256
no proposal ipsec perfect-forward-secrecy
proposal ipsec lifetime 28800
No keepalive
bound-to interface X1
exit
commit
```

En el firewall de Armenia

1. Crear Address Objects

Creación de Address Objects correspondiente a la local

```
address-object ipv4 "Red Armenia 1" network 10.199.199.0 /24 zone LAN
address-object ipv4 "Red Armenia 2" network 10.109.199.0 /24 zone LAN
address-object ipv4 "Red Armenia 3" network 172.29.10.0 /30 zone LAN
```

Creación de Address Objects correspondiente a la red remota

```
address-object ipv4 "Red Medellin 1" network 10.125.50.0 /24 zone VPN
address-object ipv4 "Red Medellin 2" network 10.25.50.0 /24 zone VPN
address-object ipv4 "Red Medellin 3" network 172.20.10.0 /30 zone VPN
```

2. Creación de Address Groups

Creación de redes locales y remotas

```
address-group ipv4 "Redes Armenia"
address-object ipv4 "Red Armenia 1"
address-object ipv4 "Red Armenia 2"
address-object ipv4 "Red Armenia 3"
```

```
end

address-group ipv4 "Redes Medellin"
address-object ipv4 "Red Medellin 1"
address-object ipv4 "Red Medellin 2"
address-object ipv4 "Red Medellin 3"
end
commit
```

3. Creación de la VPN hacia la red remota

Opción 1: Usando Tunnel Interface
(en este caso hemos usado IKE Versión 2 y Cifrado AES-GCM-256)

```
vpn policy tunnel-interface "VPN Medellin"
enable
gateway primary 200.13.152.120
auth-method shared-secret
shared-secret XXXXXX
ike-id local ipv4 6.6.6.7
ike-id peer ipv4 5.5.5.7
exit
proposal ike exchange ikev2
proposal ike encryption aes-256
proposal ike authentication sha-256
proposal ike dh-group 2
proposal ike lifetime 28800
proposal ipsec protocol esp
proposal ipsec encryption aes-gcm16-256
no proposal ipsec authentication
no proposal ipsec perfect-forward-secrecy
proposal ipsec lifetime 28800
No keepalive
bound-to interface X1
exit
commit

route-policy ipv4 interface "VPN Medellin" metric 20
name "Ruta Medellin"
interface "VPN Medellin"
source any
destination group "Redes Medellin"
service any
exit
commit
```

Opción 2: Usando Site to Site
(en este caso hemos usado Modo Main y Cifrado AES-256)

```
vpn policy site-to-site "VPN Medellin"
enable
gateway primary 200.13.152.120
```

```
auth-method shared-secret
shared-secret XXXXXX
ike-id local ipv4 6.6.6.7
ike-id peer ipv4 5.5.5.7
exit
network local group "Redes Armenia"
network remote destination-network group "Redes Medellin"
proposal ike exchange main
proposal ike encryption aes-256
proposal ike authentication sha-256
proposal ike dh-group 2
proposal ike lifetime 28800
proposal ipsec protocol esp
proposal ipsec encryption aes-256
proposal ipsec authentication sha-256
no proposal ipsec perfect-forward-secrecy
proposal ipsec lifetime 28800
bound-to interface X1
exit
commit
```