

MODULO 24

Tuneles VPN

1. Tunelizacion SITE to SITE (MikroTik a MikroTik)

1.1. Cambiar el IDENTITY en ambos MikroTik para identificarlos por CLI o GUI

1.2. Establecer una conexión estática en ambos MikroTik

MT-Rusia-Server

MT-Bolivia-Cliente

Address List			
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> <div>Find</div> </div>			
Address	Network	Interface	
192.168.0.20/...	192.168.0.0	ether1	

Address List			
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> <div>Find</div> </div>			
Address	Network	Interface	
192.168.0.215...	192.168.0.0	ether1	

1.3. Configurar ruta de salida en ambos MikroTik

Route List			
<div> <div>Routes</div> <div>Nexthops</div> <div>Rules</div> <div>VRF</div> </div>			
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> </div>			
	Dst. Address	Gateway	
AS	0.0.0.0/0	192.168.0.1 reachable ether1	
DAC	192.168.0.0/24	ether1 reachable	

Route List			
<div> <div>Routes</div> <div>Nexthops</div> <div>Rules</div> <div>VRF</div> </div>			
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> </div>			
	Dst. Address	Gateway	
AS	0.0.0.0/0	192.168.0.1 reachable ether1	
DAC	192.168.0.0/24	ether1 reachable	

1.4. Configurar NAT de enmascaramiento en ambos MikroTik

Firewall				
<div> <div>Filter Rules</div> <div>NAT</div> <div>Mangle</div> <div>Raw</div> <div>Service Ports</div> </div>				
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> <div>🔄 Reset Counters</div> </div>				
#	Action	Chain	Out. Int...	Src. Address
0	mas...	srcnat	ether1	

Firewall				
<div> <div>Filter Rules</div> <div>NAT</div> <div>Mangle</div> <div>Raw</div> <div>Service Ports</div> </div>				
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> <div>🔄 Reset Counters</div> </div>				
#	Action	Chain	Out. Int...	Src. Address
0	mas...	srcnat	ether1	

1.5. Crear subred necesaria para las PC dentro de cada MikroTik

Address List			
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> <div>Find</div> </div>			
Address	Network	Interface	
172.16.20.1/24	172.16.20.0	ether2	
192.168.0.20/...	192.168.0.0	ether1	

Address List			
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> <div>Find</div> </div>			
Address	Network	Interface	
192.168.0.1/24	192.168.0.0	ether5	
192.168.0.215...	192.168.0.0	ether1	

1.6. Conectar las PC's virtuales a cada MikroTik con una conexión estática.

```

PC1> ip 172.16.20.15 /24 172.16.20.1
Checking for duplicate address...
PC1 : 172.16.20.15 255.255.255.0 gateway 172.16.20.1

PC2> ip 192.168.50.26 /24 192.168.50.1
Checking for duplicate address...
PC2 : 192.168.50.26 255.255.255.0 gateway 192.168.50.1
  
```

1.7. Verificar conexión en ambas PC's de ambos MikroTik

```
PC1> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=54 time=75.601 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=54 time=53.052 ms

PC2> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=54 time=66.433 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=54 time=57.929 ms
```

1.8. **MT-Rusia-Server** Paso a considerar.

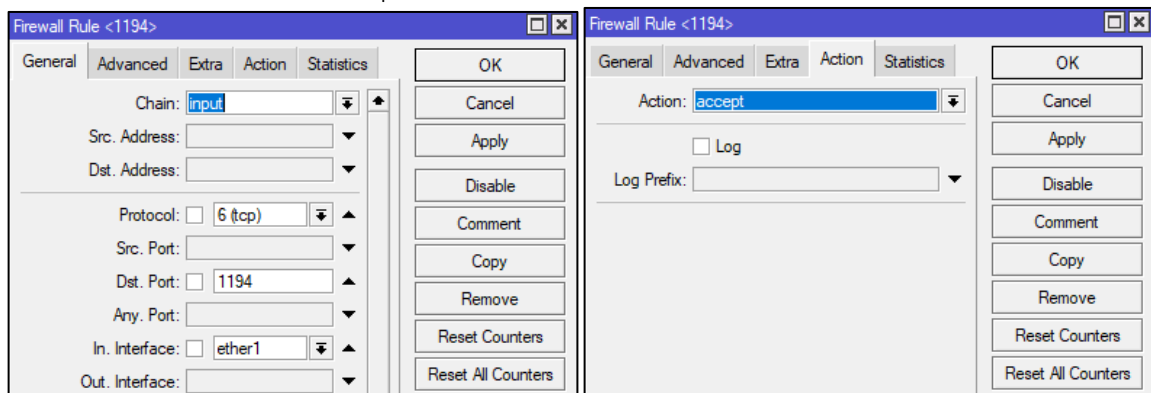
Si existen reglas de negado de trafico en MT, debemos abrir el puerto con el que trabaja OpenVPN

GENERAL

Chain: input
Protocol: 6(tcp)
Dst. Port: 1194
In. Interface: ether1

ACTION

Action: accept



1.9. **MT-Rusia-Server** Creación de certificados para trabajar con OpenVPN

En System -> Certificate, Vamos a crear 3 tipos de certificados.

- Certificado CA

GENERAL

Name: CA-TMP
Country: RU
Common Name: MT-Rusia-Server
Subject Alt. Name: IP
Key Size: 4096
Days Valid: 365

KEY USAGE

- ✓ crl sign
- ✓ Key cert. sign

- Certificado SERVER

GENERAL

Name: SERVER
Country: RU
Common Name: 192.168.0.20 (La IP donde se escucha las conexiones, ej ip publica)
Subject Alt. Name: IP
Key Size: 4096
Days Valid: 365

KEY USAGE

- ✓ digital signature
- ✓ key encipherment
- ✓ tls server

- Certificado CLIENTE

GENERAL

Name: CLIENTE
Country: BO
Common Name: MT-Bolivia-CLIENTE
Subject Alt. Name: IP
Key Size: 4096
Days Valid: 365

KEY USAGE

✓ tls client

Quedando de la siguiente forma

Certificates							
Certificates SCEP Servers SCEP RA Requests OTP CRL							
+ - Import Card Reinstall Card Verify Revoke Settings Find							
Name	Issuer	Common Name	Subject Alt. N...	Key Size	Days Valid	Ti	
CA-TMP		MT-Rusia-Ser...	unknown:::	4096	365		
CLIENTE		MT-Bolivia-Cli...	unknown:::	4096	365		
SERVER		192.168.0.20	unknown:::	4096	365		

1.10. **MT-Rusia-Server**, Ahora procedemos a firmar cada certificado

- Firmado del certificado CA (cli)

/certificate sing CA-TMP name-CA

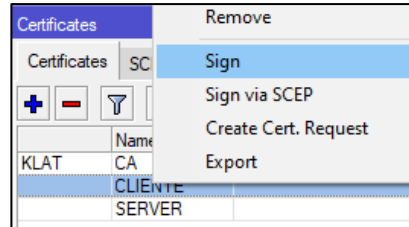
```
[admin@MT-Rusia-Server] > /certificate sign CA-TMP name=CA
progress: done
```

Esperamos hasta que termine el firmado del certificado

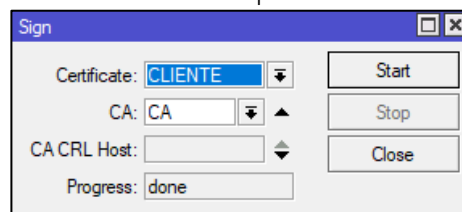
- Firmado del certificado de CLIENTE

En **system** -> **Certificantes**, vamos a firmar el certificado del cliente.

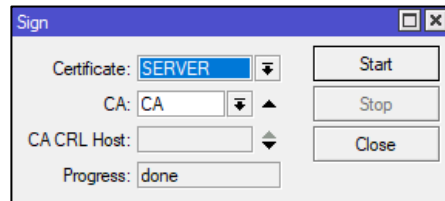
Clic derecho en el certificado a firmar seleccionar **Sign**



Seleccionamos el CA para realizar el firmado, damos **start** para iniciar



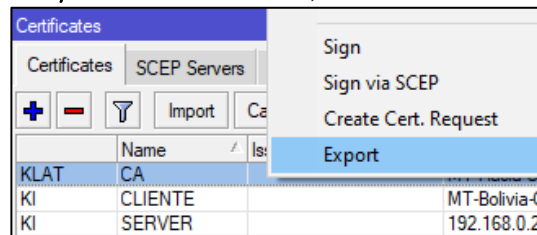
- Firmado del certificado SERVER



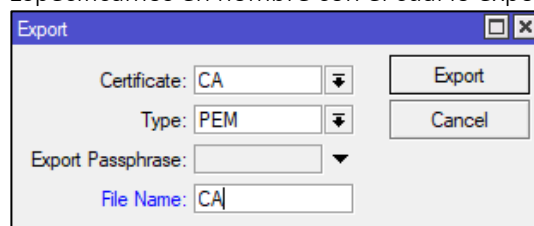
1.11. **MT-Rusia-Server**, Exportar los certificados a files, para instalarlos en el CLIENTE

- Exportar CA

En **system** -> **certificantes**, damos clic derecho en el objetivo y export.

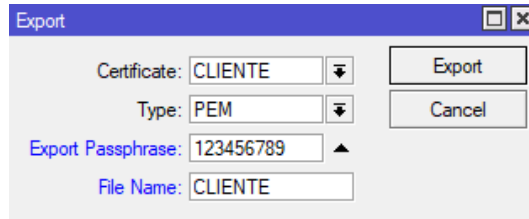


Especificamos en nombre con el cual lo exportaremos



- Exportar CLIENTE

Exportamos el CLIENTE, Especificamos el nombre y establecemos password.



Export

Certificate: CLIENTE

Type: PEM

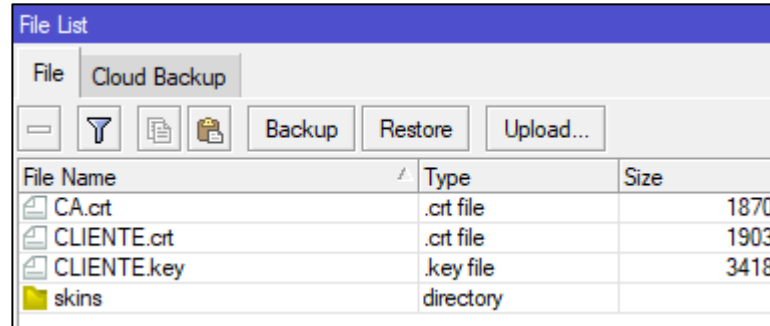
Export Passphrase: 123456789

File Name: CLIENTE

Export

Cancel

- En files debe quedar de la siguiente forma



File Name	Type	Size
CA.crt	.crt file	1870
CLIENTE.crt	.crt file	1903
CLIENTE.key	.key file	3418
skins	directory	

1.12. **MT-Rusia-Server**, Habilitar el Servidor OVPN

En PPP -> OVNP Server, habilitamos el servicio.

Status: Enable

Port: 1194

Mode: ip

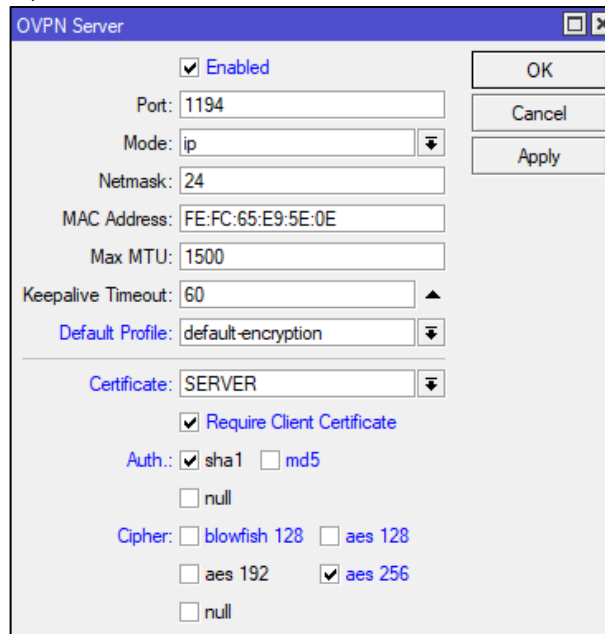
Default profile: default encryption

Certificate: SERVER

Require Client Certificate: Enable

Auth: sha1

Cipher: aes256



OVPN Server

☒ Enabled

Port: 1194

Mode: ip

Netmask: 24

MAC Address: FE:FC:65:E9:5E:0E

Max MTU: 1500

Keepalive Timeout: 60

Default Profile: default-encryption

Certificate: SERVER

☒ Require Client Certificate

Auth: ☒ sha1 ☐ md5

☐ null

Cipher: ☐ blowfish 128 ☐ aes 128

☐ aes 192 ☒ aes 256

☐ null

OK

Cancel

Apply

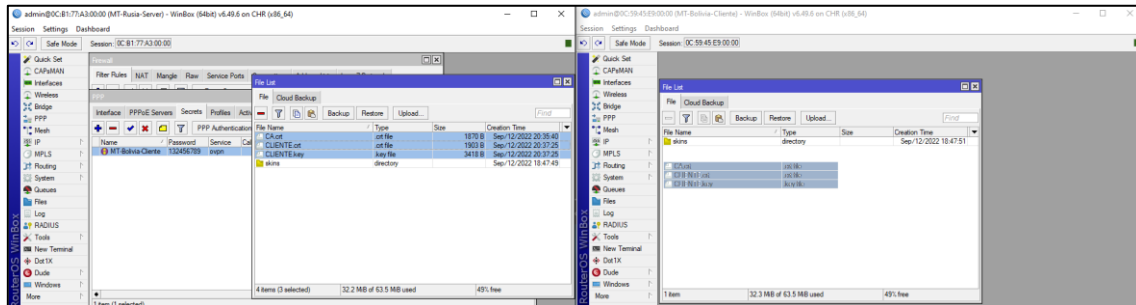
1.13. **MT-Rusia-Server**, Creación del perfil de conexión.

En PPP -> **Secret**, Vamos a crear el perfil de conexión.

Name: MT-Cliente-Bolivia
Password: 123456789
Service: ovpn
Profile: default encryption
Local Address: 10.10.10.1 (Red local del servidor)
Remote Address: 10.10.10.2 (IP proporcionada al cliente)

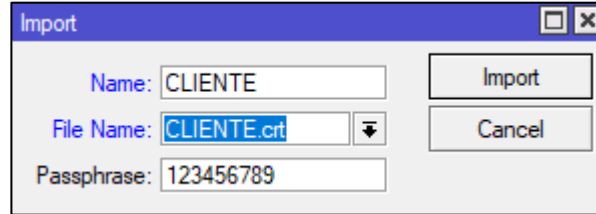
1.14. **MT-Bolivia-Cliente**, Importación de los certificados desde MT-Rusia-Server

Con la acción de arrastrar y soltar pasamos los certificados generados en MT-Rusia-SERVER a MT-Bolivia-Cliente.



- En **system** -> **Certificates**, importamos el certificado CA, especificado, el archivo y el password correspondiente.

- En **system** -> **Certificates**, importamos el certificado el CLIENTE.crt, especificado, el archivo y el password correspondiente.

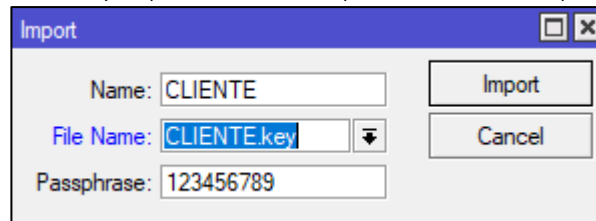


Import dialog box showing the following fields:

- Name: CLIENTE
- File Name: CLIENTE.crt
- Passphrase: 123456789

Buttons: Import, Cancel

- En **system** -> **Certificates**, importamos el certificado el CLIENTE.key, especificado, el archivo y el password correspondiente. Hasta que cambie el estado (T) a (KT)

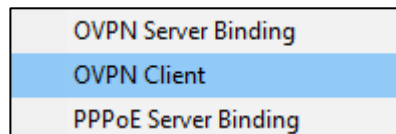


Import dialog box showing the following fields:

- Name: CLIENTE
- File Name: CLIENTE.key
- Passphrase: 123456789

Buttons: Import, Cancel

- 1.15. Establecemos la conexión del CLIENTE
En **Interfaces** -> Seleccionamos **OVPN Cliente**,

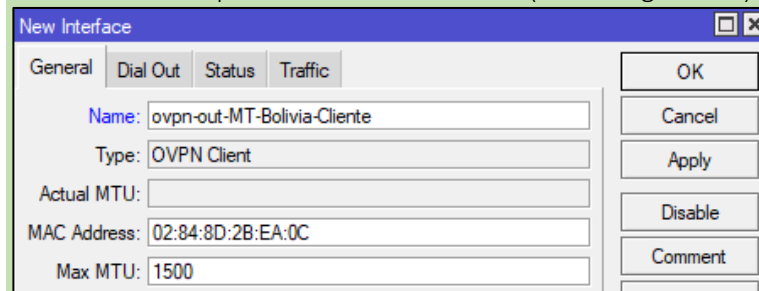


Menu showing the following options:

- OVPN Server Binding
- OVPN Client** (selected)
- PPPoE Server Binding

GENERAL

Name: ovpn-out-MT-Bolivia-Cliente (Nombre genérico)



New Interface dialog box showing the following fields:

- Name: ovpn-out-MT-Bolivia-Cliente
- Type: OVPN Client
- Actual MTU:
- MAC Address: 02:84:8D:2B:EA:0C
- Max MTU: 1500

Buttons: OK, Cancel, Apply, Disable, Comment

DIAL OUT

Connect To: 192.168.0.20 (IP pública de MT-RusiaServer)
 Port: 1194
 Mode: IP
 User: MT-Bolivia-Cliente
 Password: 123456789
 Profile: Default Profile
 Certificate: CLIENTE
 Auth: sha1
 Cipher: aes256

1.16. Verificación de conexión exitosa

MT-Bolivia-Cliente, En **log** podemos verificar el estado de conexión

#	Time	Buffer	Topics	Message
208	Sep/12/2022 21:25:11	memory	ovpn, info	ovpn-out-MT-Bolivia-Cliente: connecting...
209	Sep/12/2022 21:25:11	memory	system, info	device changed by admin
210	Sep/12/2022 21:25:12	memory	ovpn, info	ovpn-out-MT-Bolivia-Cliente: using encoding - AES-256-CBC/SHA1
211	Sep/12/2022 21:25:12	memory	ovpn, info	ovpn-out-MT-Bolivia-Cliente: connected

212 items

MT-Bolivia-Cliente, En **IP -> Addresses**, verificamos la creación de la nueva interface de conexión.

	Address	Network	Interface
D	10.10.10.2/24	10.10.10.0	ovpn-out-MT-B...
	192.168.0.215...	192.168.0.0	ether1
	192.168.50.1/...	192.168.50.0	ether5

MT-Rusia-Servidor, En **PPP -> Interface**, Podemos ver un cliente conectado

PPP

Interface	PPPoE Servers	Secrets	Profiles	Active Connections
+	-	✓	✗	📄
🔍	🔍	🔍	🔍	🔍
PPP Scanner	PPTP Server			
Name	Type			
DR <> <ovpn-MT-Bolivia-Cliente>	OVPN Server Binding			

1.17. Creación de rutas para Cliente y Servidor

- **MT-Bolivia-Cliente**, En IP -> **Route**, Vamos a conectar la ruta de conexión desde la PC cliente hasta la PC servidor.

Route <172.16.20.0/24>

General	Attributes
Dst. Address: 172.16.20.0/24	
Gateway: 10.10.10.1	reachable ovpn-out-MT-Bolivia-Cliente
Check Gateway:	
Type: unicast	
Distance: 1	
Scope: 30	
Target Scope: 10	
Routing Mark:	
Pref. Source:	

OK Cancel Apply Disable Comment Copy Remove

- **MT-Rusia-Servidor**, En IP -> **Route**, Vamos a conectar la ruta de conexión desde la PC servidor hasta la PC cliente.

Route <192.168.50.0/24>

General	Attributes
Dst. Address: 192.168.50.0/24	
Gateway: 10.10.10.2	reachable <ovpn-MT-Bolivia-Cliente>
Check Gateway:	
Type: unicast	
Distance: 1	
Scope: 30	
Target Scope: 10	
Routing Mark:	
Pref. Source:	

OK Cancel Apply Disable Comment Copy Remove

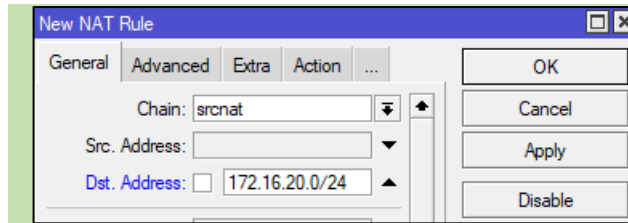
1.18. Creación de NAT en ambos Servidores

- **MT-Bolivia-Cliente**, En IP -> **Firewall** -> **NAT**, Creamos una regla NAT para llegar del cliente al servidor.

GENERAL

Chain: srcnat

Dst. Address: 172.16.20.0/24 (Red privada de MT-Rusia-Servidor)



New NAT Rule

General Advanced Extra Action ...

Chain: srcnat

Src. Address:

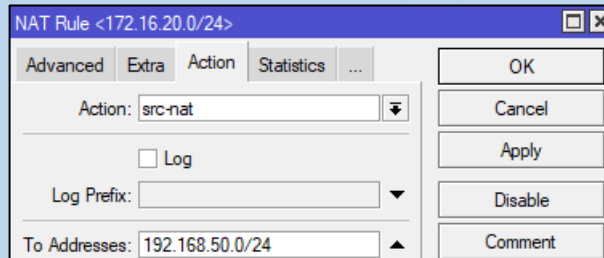
Dst. Address: 172.16.20.0/24

OK Cancel Apply Disable

ACTION

Action: src-nat

To Addresses: 192.168.50.0/24 (Red privada de MT-Bolivia-Cliente)



NAT Rule <172.16.20.0/24>

Advanced Extra Action Statistics ...

Action: src-nat

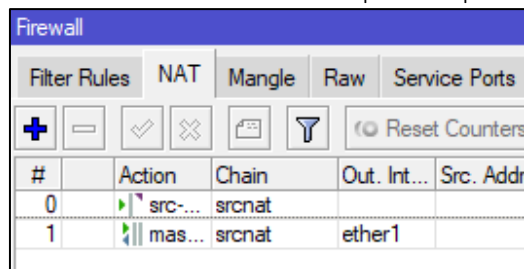
☐ Log

Log Prefix:

To Addresses: 192.168.50.0/24

OK Cancel Apply Disable Comment

Acomodamos el srcnat antes que masquerade para que funcione.



Firewall				
Filter Rules NAT Mangle Raw Service Ports				
#	Action	Chain	Out. Int...	Src. Addr
0	src-...	srcnat		
1	mas...	srcnat	ether1	

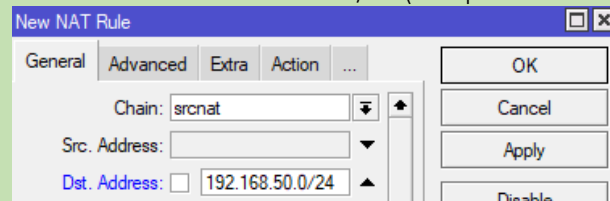
- MT-Rusia-Servidor,

En IP -> Firewall -> NAT, Creamos una regla NAT para llegar del cliente al servidor.

GENERAL

Chain: srcnat

Dst. Address: 192.168.50.0/24 (Red privada de MT-Bolivia-Cliente)



New NAT Rule

General Advanced Extra Action ...

Chain: srcnat

Src. Address:

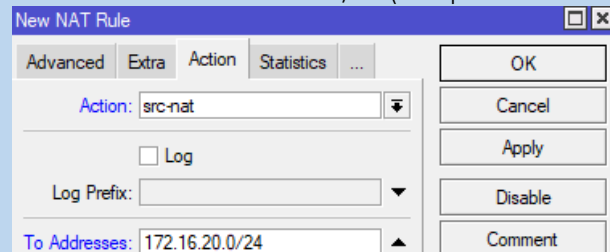
Dst. Address: 192.168.50.0/24

OK Cancel Apply Disable

ACTION

Action: src-nat

To Addresses: 172.16.20.0/24 (Red privada de MT-Rusia-Servidor)



New NAT Rule

Advanced Extra Action Statistics ...

Action: src-nat

☐ Log

Log Prefix:

To Addresses: 172.16.20.0/24

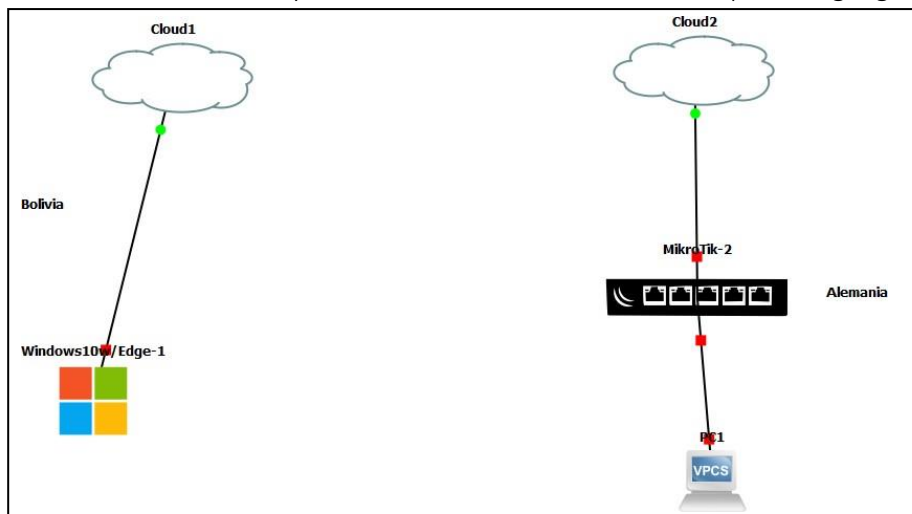
OK Cancel Apply Disable Comment

Acomodamos el srcnat antes que masquerade para que funcione.

Firewall				
Filter Rules NAT Mangle Raw Service Ports				
<div> <div>+</div> <div>-</div> <div>✓</div> <div>✗</div> <div>📄</div> <div>🔍</div> <div>🔄 Reset Counters</div> </div>				
#	Action	Chain	Out. Int...	Src. Addr
0	src-...	srcnat		
1	mas...	srcnat	ether1	

2. Configuraciones VPN PPTP bajo la siguiente topología

El cliente esta en Bolivia y el servidor VPN está en Alemania separados geográficamente.



2.1. Habilitar el servidor PPTP

El PPP -> PPTP Server, habilitamos el servidor VPN.

2.2. Crear el pozo de direcciones a asignar a cada conexión nueva (es como el DHCP)

En IP -> Pool, creamos un nuevo pozo indicando el rango de direcciones LAN que están completamente libres, que ningún dispositivo o usuario las esté usando.

2.3. Creación del perfil de conexión.

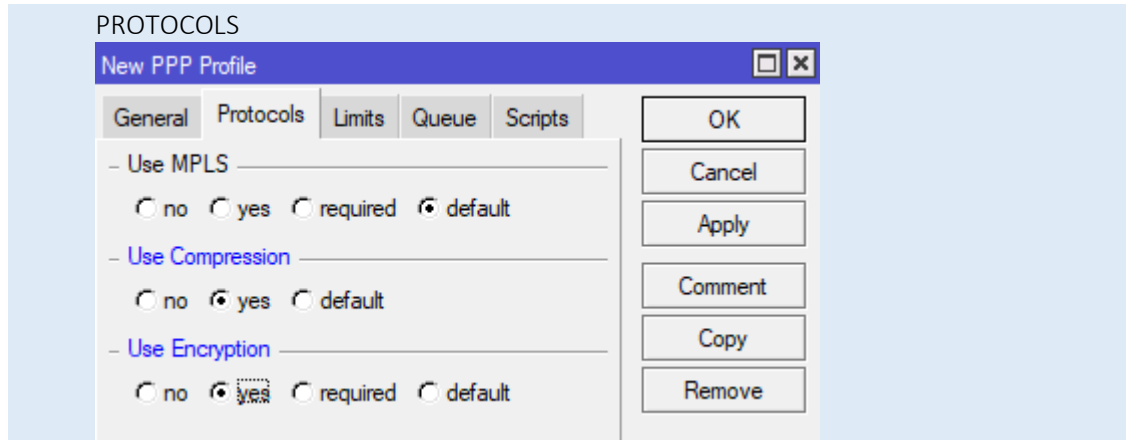
En PPP -> Profiles, vamos a crear un nuevo perfil de conexión.

GENERAL

Debemos proporcionar la misma dirección IP de la red LAN de nuestro MikroTik

En RemoteAddress ponemos el Pool de direcciones que creamos.

Dejamos todo lo demás por defecto.



2.4. Creación del cliente VPN

En PPP -> Secrets, creamos las credenciales para que un cliente pueda conectarse a nuestra VPN

Nombre:

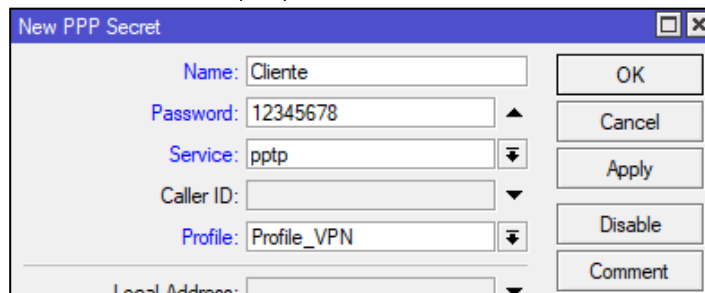
Ciente

Password:

12345678

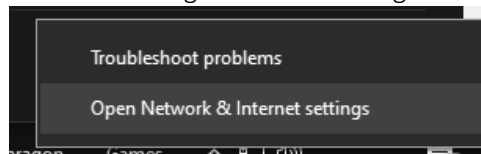
Service: pptp

Profile: ProfileVPN que ya creamos

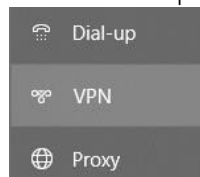


2.5. Pruebas de conexión desde un cliente hacia el MikroTik

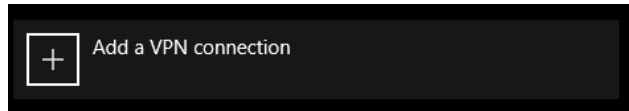
En Windows ingresamos a: Configuraciones de red e internet.



Buscamos la opción VPN

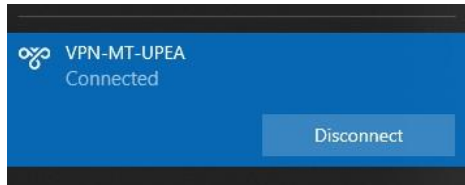
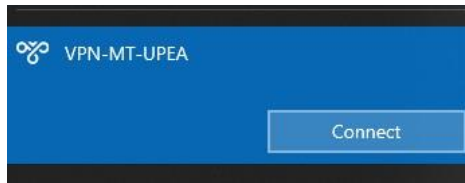


Agregamos una nueva conexión de tipo VPN



Luego de configurar la nueva conexión VPN, nos conectamos al nuevo VPN





```
Ethernet adapter Ethernet:

Connection-specific DNS Suffix  . : 
Link-local IPv6 Address . . . . . : fe80::c03:a1d5:ba92:a56f%14
IPv4 Address. . . . . : 192.168.254.2
Subnet Mask . . . . . : 255.255.255.248
Default Gateway . . . . . : 192.168.254.1

Ethernet adapter Ethernet 4:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . : 

PPP adapter VPN-MT-UPEA:

Connection-specific DNS Suffix  . : 
IPv4 Address. . . . . : 30.30.30.52
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 0.0.0.0
```

En interfaces de PPP del MT podemos ver que hay un cliente conectado a la VPN

PPP									
Interface		PPPoE Servers	Secrets	Profiles	Active Connections		L2TP Secrets		
+		-	✓	✗	📄	🔍			
		PPP Scanner		PPTP Server	SSTP Server	L2TP Server	OVPN Server	PPPoE Scan	Find
Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)		R	
DR <=> <pptp-Cliente>	PPTP Server Binding	1400			616 bps	320 bps		1	

2.6. Prueba de conectividad desde PC en Bolivia hacia la PC en Alemania

```
C:\Users\Leonel>ping 30.30.30.254

Pinging 30.30.30.254 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 30.30.30.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

2.7. Solución del error anterior En el MikroTik de Alemania

En IP -> Firewall -> NAT, creamos una regla de enmascaramiento por la interface LAN.

The image shows two side-by-side screenshots of the 'New NAT Rule' dialog in MikroTik WinBox. The left window is on the 'General' tab, showing 'Chain: srcnat' and 'Out. Interface: ether3'. The right window is on the 'Action' tab, showing 'Action: masquerade'.

Realizamos nuevamente la prueba

```
C:\Users\Leonel>ping 30.30.30.254

Pinging 30.30.30.254 with 32 bytes of data:
Reply from 30.30.30.254: bytes=32 time=5ms TTL=127
Reply from 30.30.30.254: bytes=32 time=5ms TTL=127
Reply from 30.30.30.254: bytes=32 time=3ms TTL=127
Reply from 30.30.30.254: bytes=32 time=3ms TTL=127

Ping statistics for 30.30.30.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 5ms, Average = 4ms
```