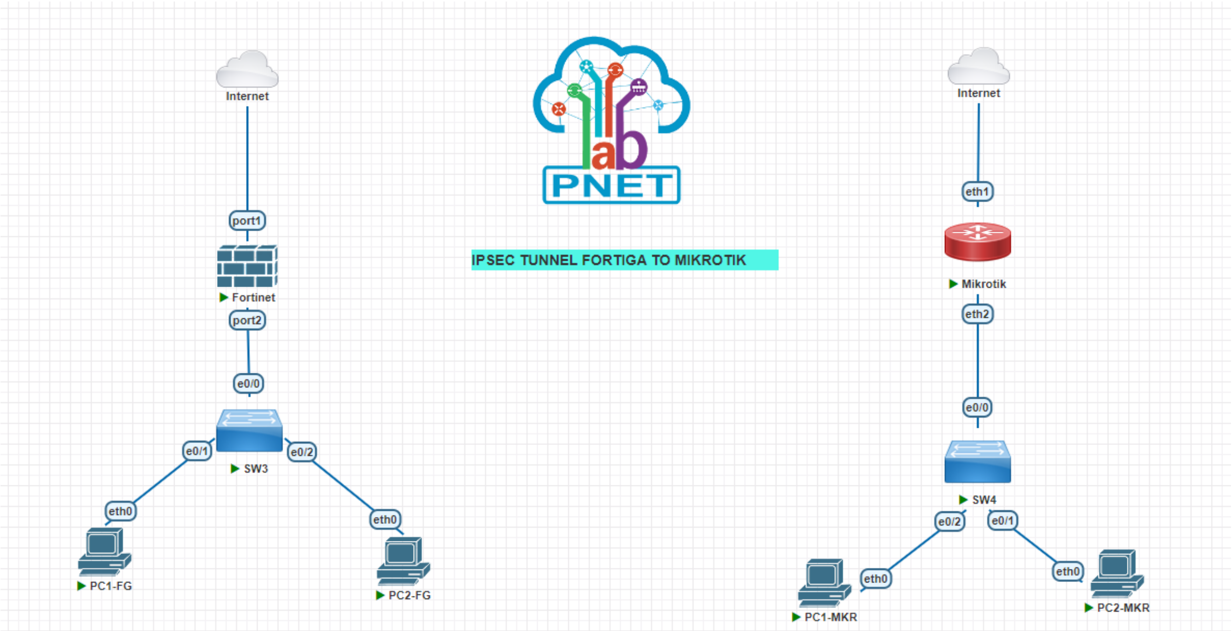
IPSec VPN between FortiGate and MikroTik

Topology



To set up an IPSec VPN between FortiGate and MikroTik with the given parameters, follow these detailed steps:

Summary :
IP WAN FG : 192.168.93.147/24
IP LAN FG : 10.10.10.0/24

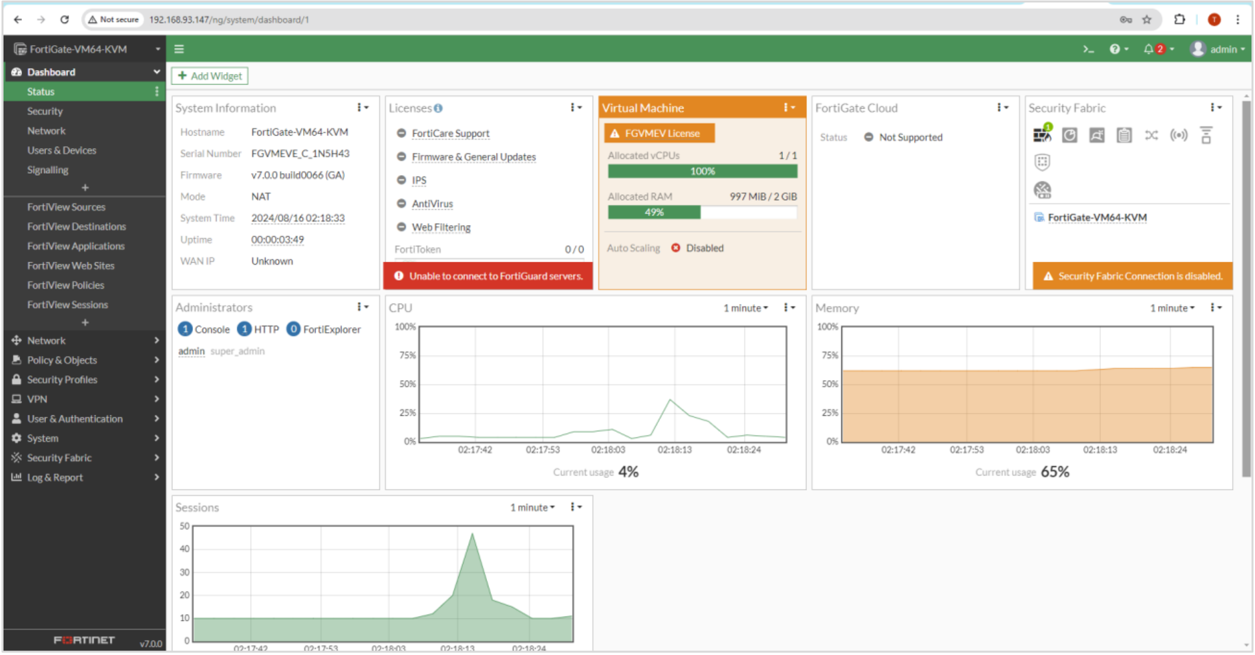
IP WAN MKR : 192.168.93.147/24
IP LAN MKR : 10.10.10.0/24

Configure FortiGate

Configure Phase 1

1. Log in to FortiGate:

- Access the FortiGate web interface via your browser.



Hostname	FortiGate-VM64-KVM
Serial Number	FGVMEVE_C_1N5H43
Firmware	v7.0.0 build0066 (GA)
Mode	NAT
System Time	2024/08/16 02:18:33
Uptime	00:00:03:49
WAN IP	Unknown

Unable to connect to FortiGuard servers.

Allocated vCPUs	1 / 1	100%
Allocated RAM	997 MiB / 2 GiB	49%
Auto Scaling	Disabled	

Status Not Supported

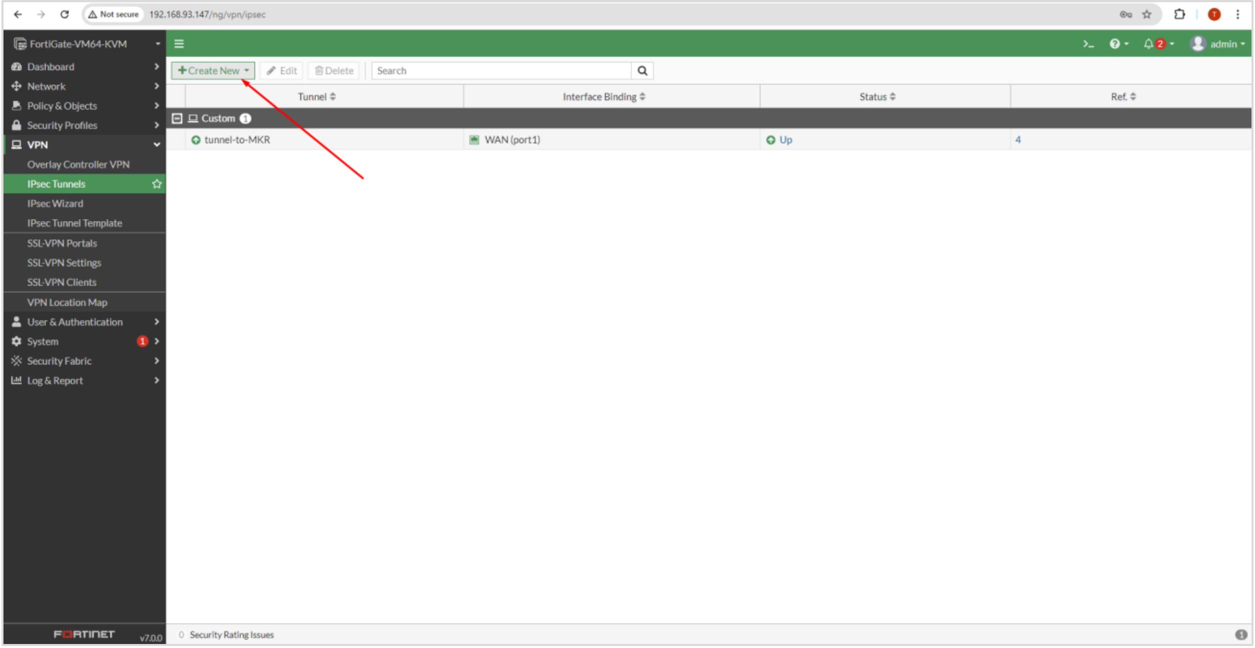
Security Fabric Connection is disabled.

Current usage 4%

Current usage 65%

2. Navigate to IPSec VPN Settings:

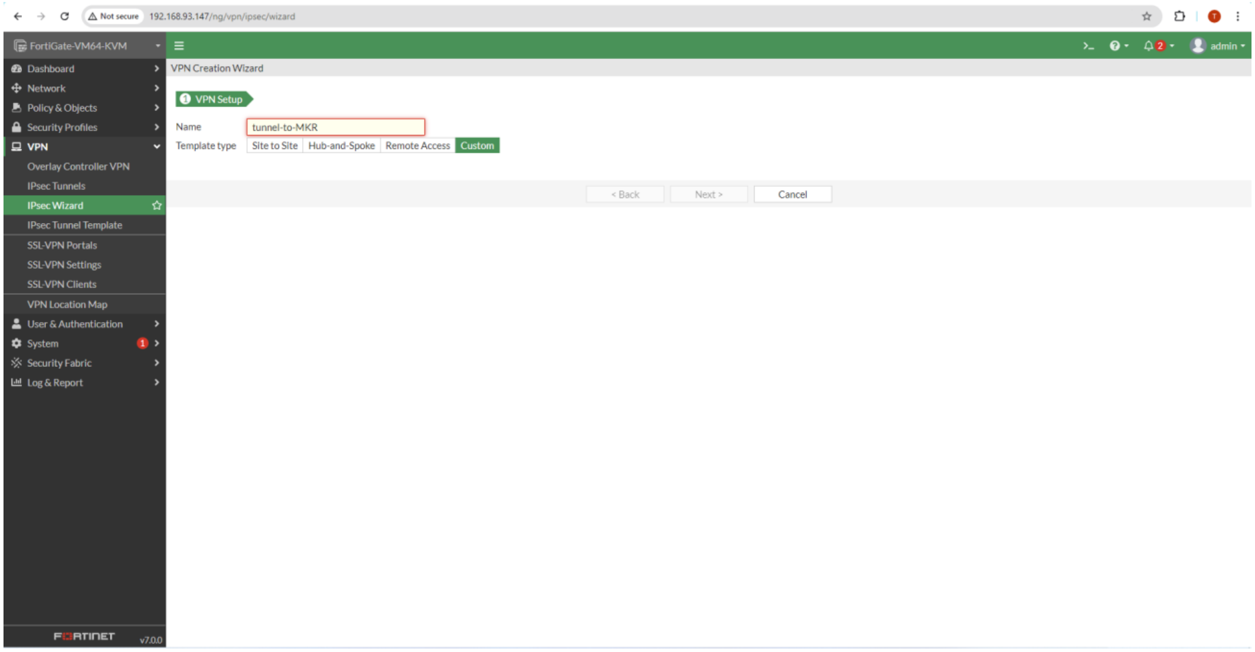
- Go to VPN > IPSec Tunnels > Create New.



Tunnel	Interface Binding	Status	Ref.
Custom 1			
tunnel-to-MKR	WAN (port1)	Up	4

3. Create a New Tunnel:

- Select Custom and name the tunnel (e.g., tunnel-to-MKR).

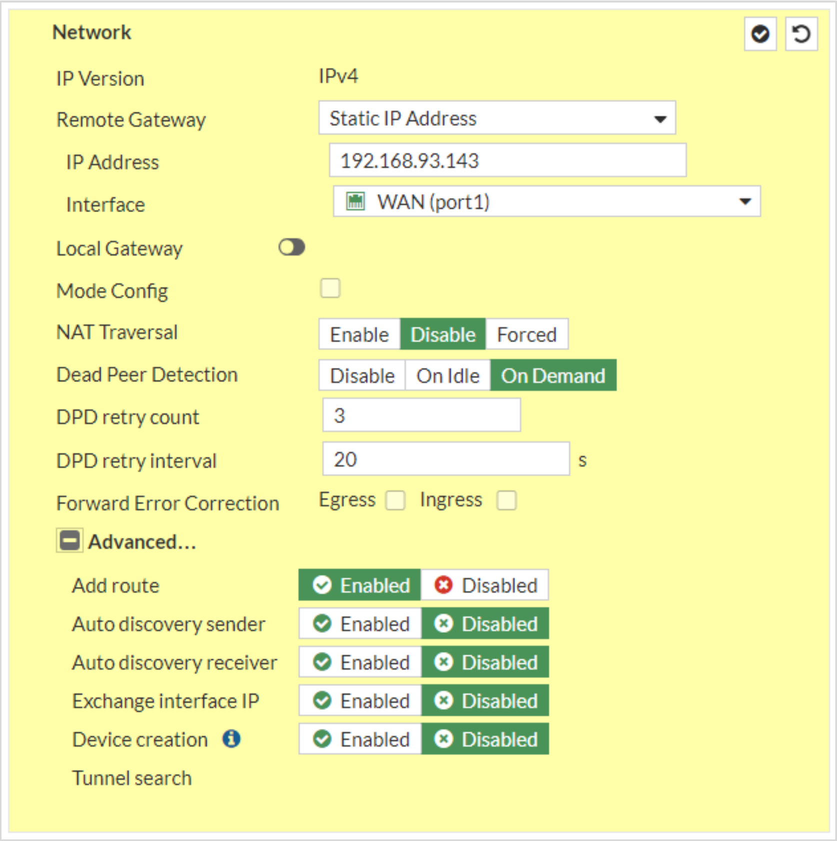


Name: tunnel-to-MKR

Template type: Custom

4. Configure Phase 1 Settings:

- Remote Gateway: Select Static IP Address
- IP Address: Enter 192.168.93.143 (MikroTik’s WAN IP)
- Interface: Choose the WAN interface connected to the internet.
- Authentication Method: Select Pre-shared Key
- Pre-shared Key: Enter adminadmin
- IPSec Version: Choose IKEv1
- Encryption: Select DES
- Authentication: Select SHA1
- DH Group: Choose 2
- Key Lifetime: Set to 86400



Network

IP Version: IPv4

Remote Gateway: Static IP Address

IP Address: 192.168.93.143

Interface: WAN (port1)

Local Gateway

Mode Config □

NAT Traversal: Enable [✓ Disable] Forced

Dead Peer Detection: Disable On Idle [✓ On Demand]

DPD retry count: 3

DPD retry interval: 20 s

Forward Error Correction: Egress □ Ingress □

Advanced...

Add route: [✓ Enabled] Disabled

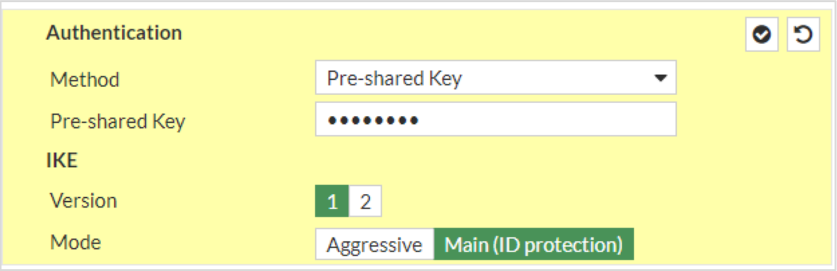
Auto discovery sender: Enabled [✓ Disabled]

Auto discovery receiver: Enabled [✓ Disabled]

Exchange interface IP: Enabled [✓ Disabled]

Device creation: Enabled [✓ Disabled]

Tunnel search



Authentication

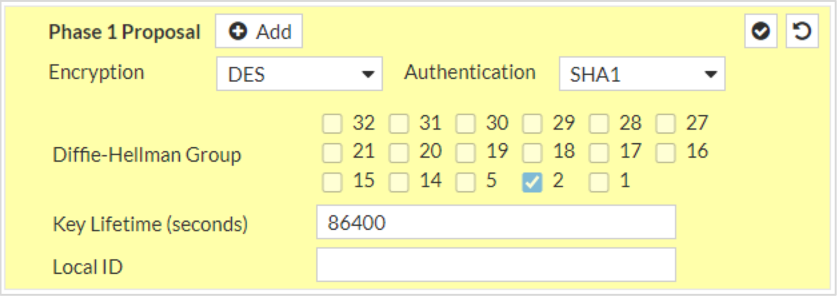
Method: Pre-shared Key

Pre-shared Key: ••••••••

IKE

Version: [✓ 1] 2

Mode: Aggressive [✓ Main (ID protection)]



Phase 1 Proposal

Encryption: DES Authentication: SHA1

Diffie-Hellman Group: □ 32 □ 31 □ 30 □ 29 □ 28 □ 27 □ 21 □ 20 □ 19 □ 18 □ 17 □ 16 □ 15 □ 14 □ 5 ☑ 2 □ 1

Key Lifetime (seconds): 86400

Local ID:

Configure Phase 2

1. Configure Phase 2 Settings:

- Local Subnet: Enter 10.10.10.0/24 (FortiGate’s LAN network)

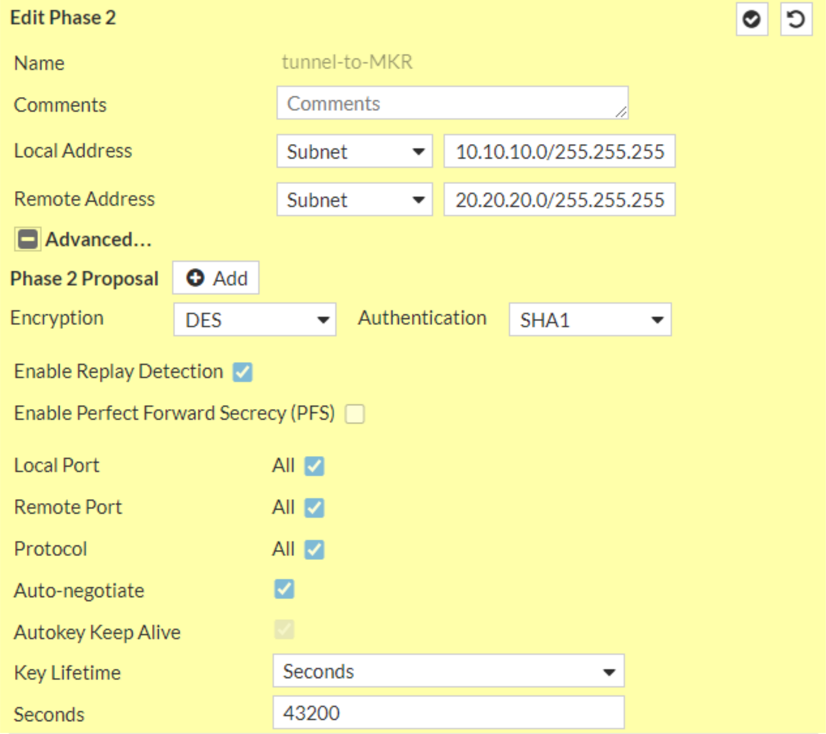
- Remote Subnet: Enter 20.20.20.0/24 (MikroTik’s LAN network)

- Encryption: Select DES

- Authentication: Select SHA1

- PFS: Select Disable

- Key Lifetime: Set to 43200



Edit Phase 2

Name	tunnel-to-MKR
Comments	Comments
Local Address	Subnet ▾ 10.10.10.0/255.255.255
Remote Address	Subnet ▾ 20.20.20.0/255.255.255

⊟ Advanced...

Phase 2 Proposal ⊕ Add

Encryption DES ▾ Authentication SHA1 ▾

Enable Replay Detection ☑

Enable Perfect Forward Secrecy (PFS) □

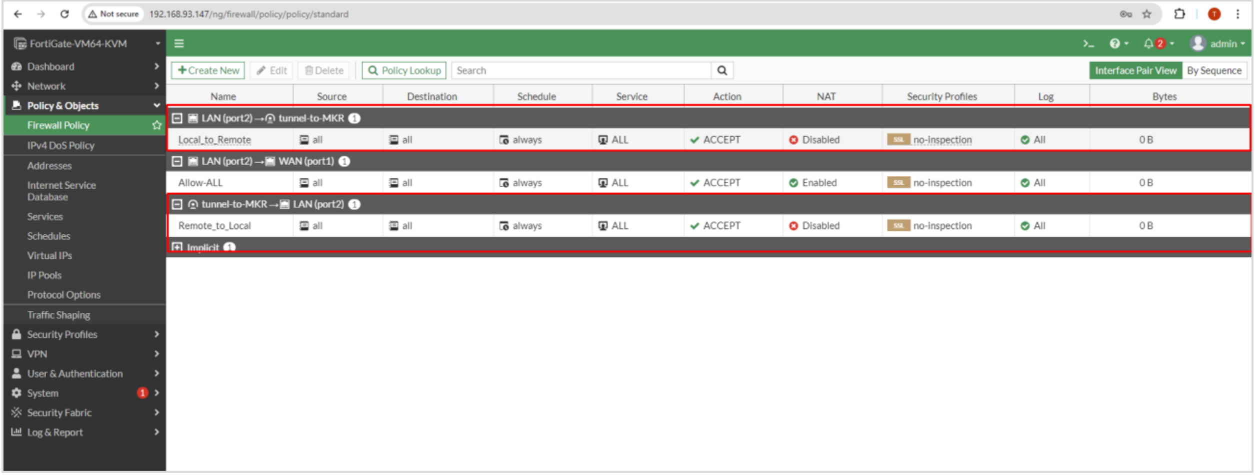
Local Port	All ☑
Remote Port	All ☑
Protocol	All ☑
Auto-negotiate	☑
Autokey Keep Alive	☑
Key Lifetime	Seconds ▾
Seconds	43200

2. Click OK to save.

Create Firewall Policy

1. Navigate to Policy Configuration, and must create reverse policy for this rules :

- Go to Policy & Objects > IPv4 Policy > Create New.



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
LAN (port2) → tunnel-to-MKR 1									
Local_to_Remote	all	all	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	All	0 B
LAN (port2) → WAN (port1) 1									
Allow-ALL	all	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	All	0 B
tunnel-to-MKR → LAN (port2) 1									
Remote_to_Local	all	all	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	All	0 B
Implicit 1									

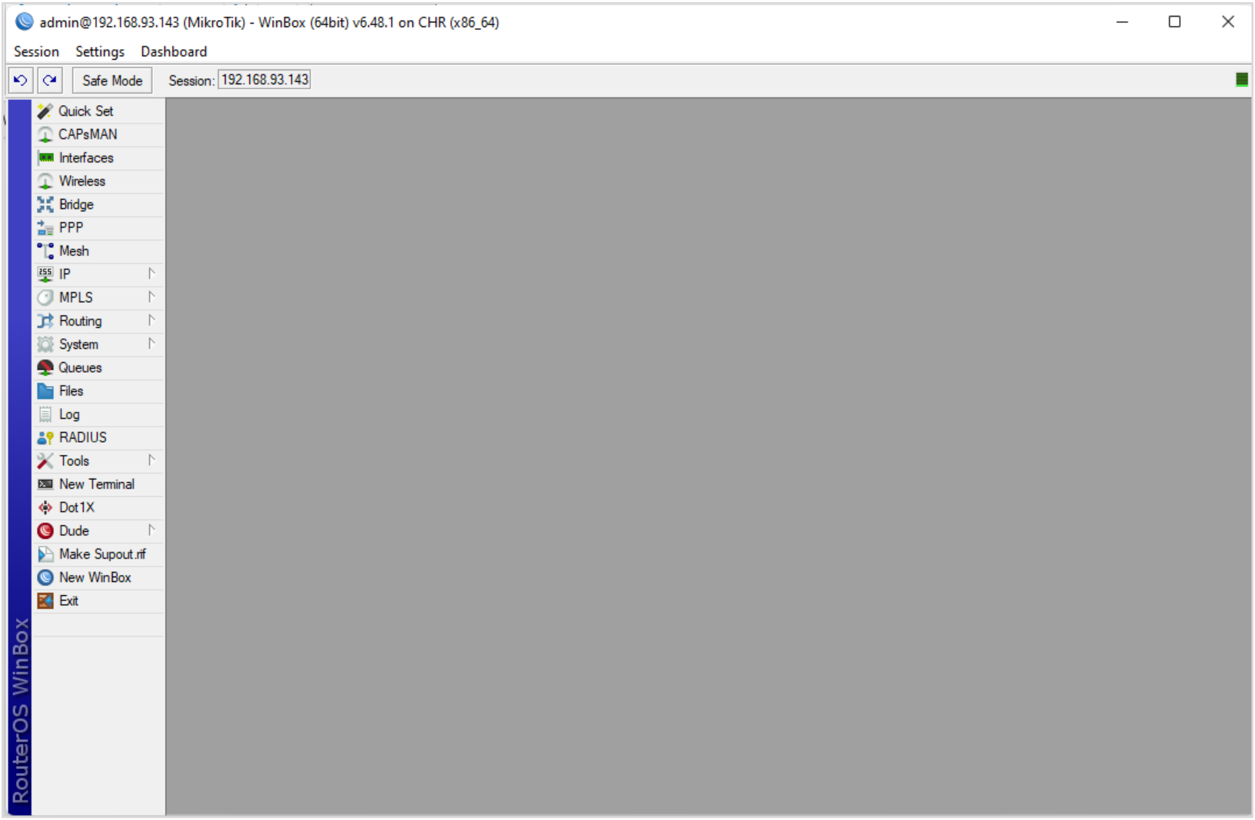
2. Click OK to save the policy.

Configure MikroTik

Configure Phase 1

1. Log in to MikroTik:

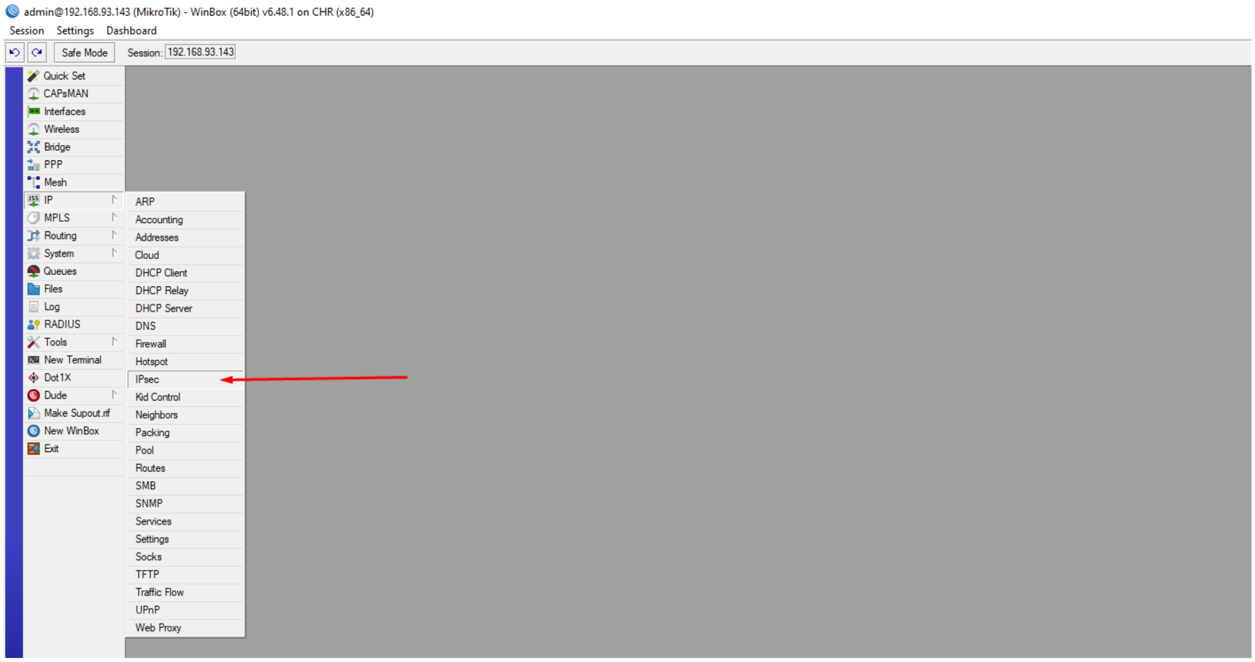
- Access MikroTik via Winbox



admin@192.168.93.143 (MikroTik) - WinBox (64bit) v6.48.1 on CHR (x86_64)

2. Navigate to IPSec Settings:

- Go to IP > IPSec.



3. Create a New Proposal:

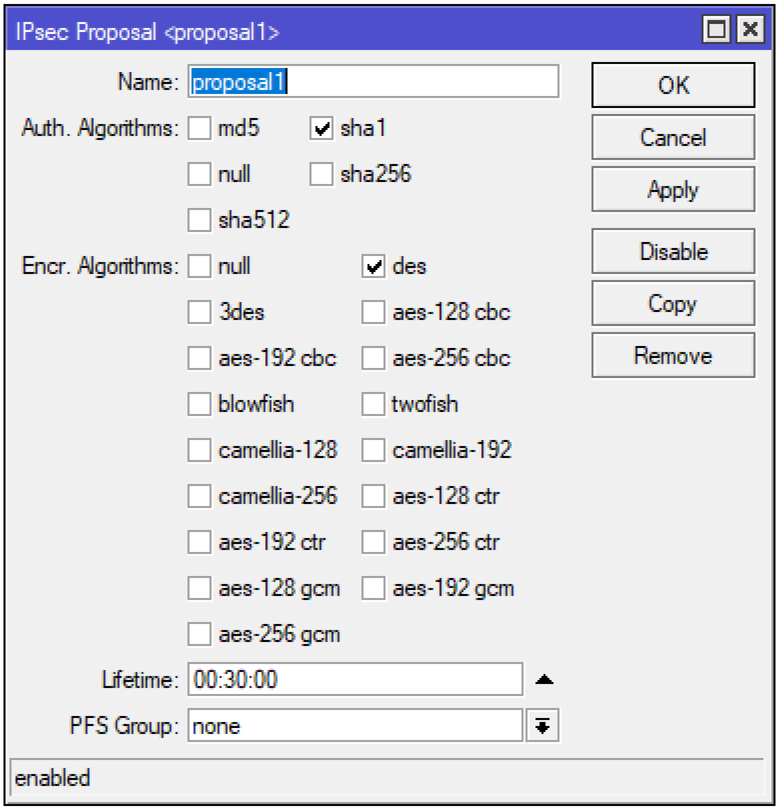
- Go to the Proposals tab and click + to add a new proposal.

- Name: **proposal1**

- Encryption Algorithms: Select “des”

- Hash Algorithms: Select “sha1”

- PFS Group: Choose none



IPsec Proposal <proposal1>

Name: proposal1

Auth. Algorithms: □ md5 ☑ sha1 □ null □ sha256 □ sha512

Encr. Algorithms: □ null ☑ des □ 3des □ aes-128 cbc □ aes-192 cbc □ aes-256 cbc □ blowfish □ twofish □ camellia-128 □ camellia-192 □ camellia-256 □ aes-128 ctr □ aes-192 ctr □ aes-256 ctr □ aes-128 gcm □ aes-192 gcm □ aes-256 gcm

Lifetime: 00:30:00

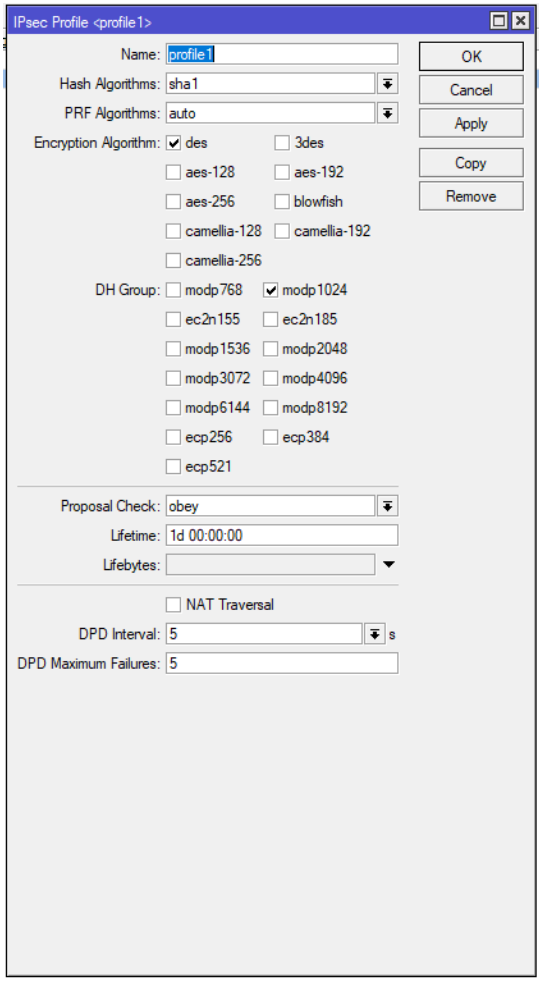
PFS Group: none

enabled

- Click apply and ok

4. Create a New Profile

  - Go to the profiles tab and click + to add a new profile
  - Enter name : profile1
  - Encryption Algoritm : des
  - DH Group : mod1024
  - Disable NAT Traversal (Uncheck)



IPsec Profile <profile1>

Name: profile1

Hash Algorithms: sha1

PRF Algorithms: auto

Encryption Algorithm: ☑ des ☐ 3des ☐ aes-128 ☐ aes-192 ☐ aes-256 ☐ blowfish ☐ camellia-128 ☐ camellia-192 ☐ camellia-256

DH Group: ☐ modp768 ☑ modp1024 ☐ ec2n155 ☐ ec2n185 ☐ modp1536 ☐ modp2048 ☐ modp3072 ☐ modp4096 ☐ modp6144 ☐ modp8192 ☐ ecp256 ☐ ecp384 ☐ ecp521

Proposal Check: obey

Lifetime: 1d 00:00:00

Lifebytes:

☐ NAT Traversal

DPD Interval: 5 s

DPD Maximum Failures: 5

- click apply and ok

5. Create a New Peer:

  - Go to the Peers tab and click + to add a new peer

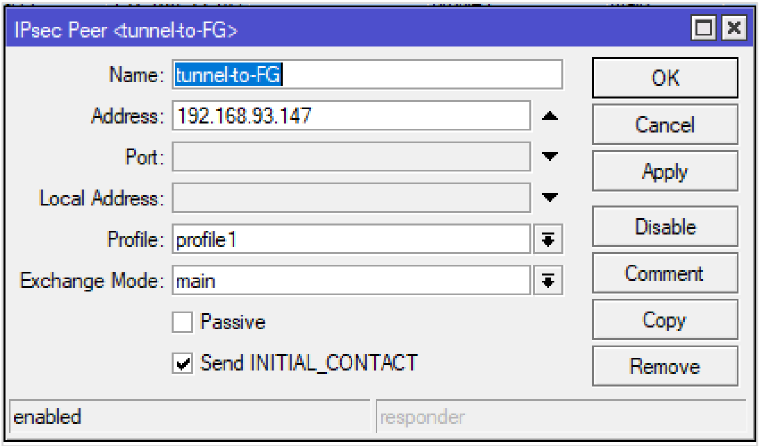
  - Enter name : **tunnel-to-FG**

  - Address: Enter 192.168.93.147 (FortiGate's WAN IP)

  - Port: skip

  - Select Profile : **profile1**

  - Select Exchange mode : **main**


IPsec Peer <tunnel-to-FG>

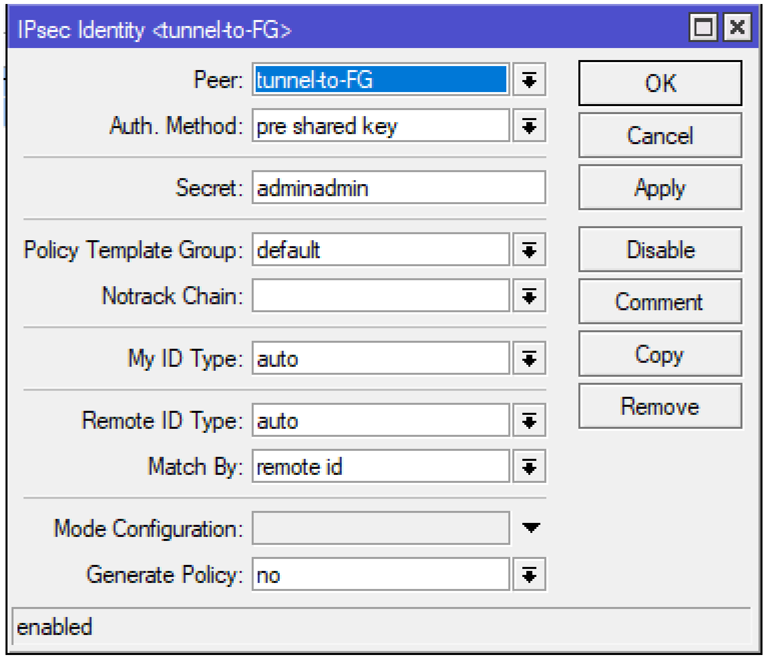
Name: tunnel-to-FG
Address: 192.168.93.147
Port:
Local Address:
Profile: profile1
Exchange Mode: main
☐ Passive
☑ Send INITIAL_CONTACT

enabled | responder

- Click Apply and OK.

6. Create a new Identity :

- Go to the identities tab and click + to add a new identity
- Select peer : tunnel-to-FGT
- For authod method select : preshared-key
- Enter key : adminadmin


IPsec Identity <tunnel-to-FG>

Peer: tunnel-to-FG
Auth. Method: pre shared key
Secret: adminadmin
Policy Template Group: default
Notrack Chain:
My ID Type: auto
Remote ID Type: auto
Match By: remote id
Mode Configuration:
Generate Policy: no

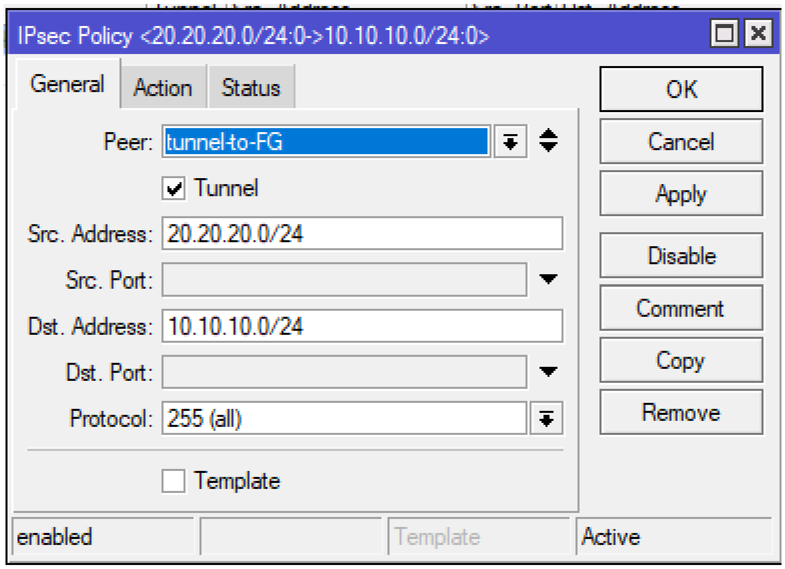
enabled

- Click apply and ok

Create IPSec Policy

1. Create a New Policy:

- Go to the Policies tab and click + to add a new policy
- Select peer : tunnel-to-FG
- Checklist “Tunnel”
- Src. Address: Enter 10.10.10.0/24
- Dst. Address: Enter 20.20.20.0/24



IPsec Policy <20.20.20.0/24:0->10.10.10.0/24:0>

Peer: tunnel-to-FG

☑ Tunnel

Src. Address: 20.20.20.0/24

Src. Port:

Dst. Address: 10.10.10.0/24

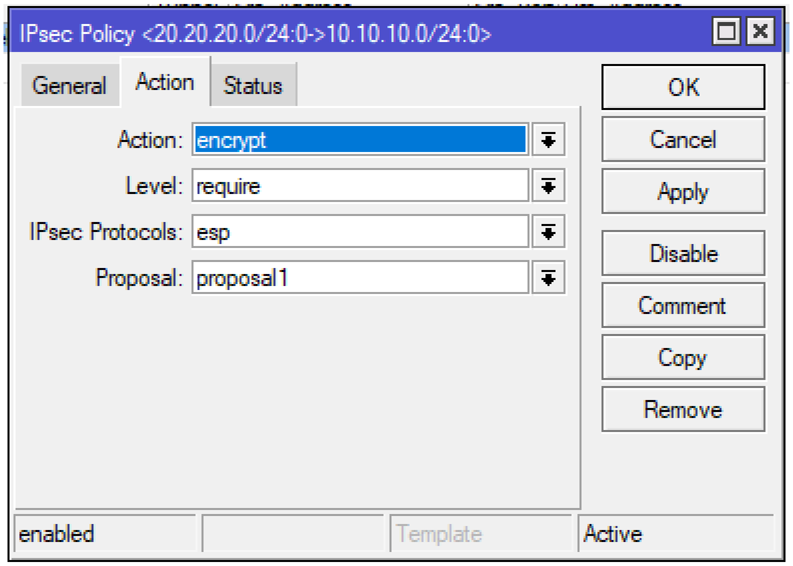
Dst. Port:

Protocol: 255 (all)

☐ Template

enabled | | Template | Active

- Action: Select encrypt
- IPSec Protocol: esp
- Proposal: Select **proposal1**



IPsec Policy <20.20.20.0/24:0->10.10.10.0/24:0>

Action: encrypt

Level: require

IPsec Protocols: esp

Proposal: proposal1

enabled

Active

- Click Apply and OK.

Configure IP FIREWALL NAT

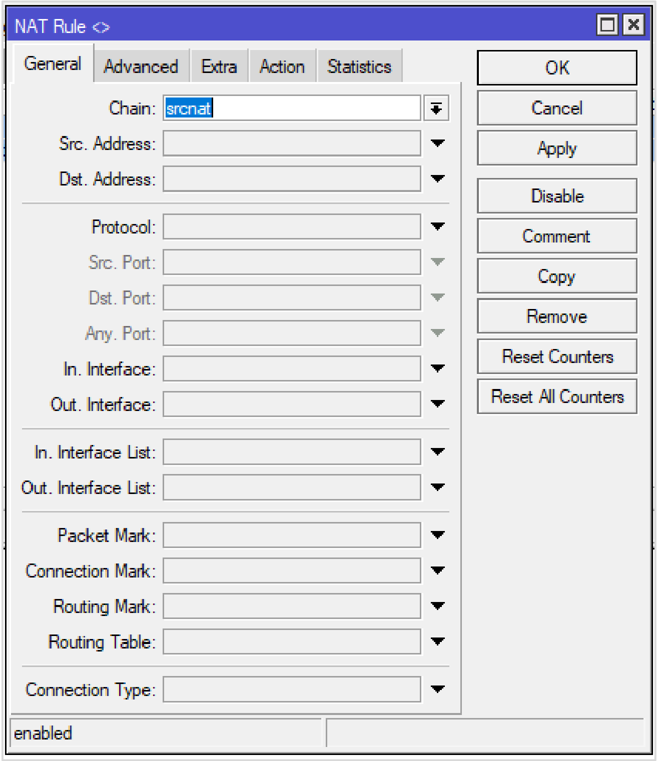
1. Create a NAT Rule to Allow VPN Traffic:

   - Go to IP > Firewall > NAT.

   - Click + to add a new NAT rule.

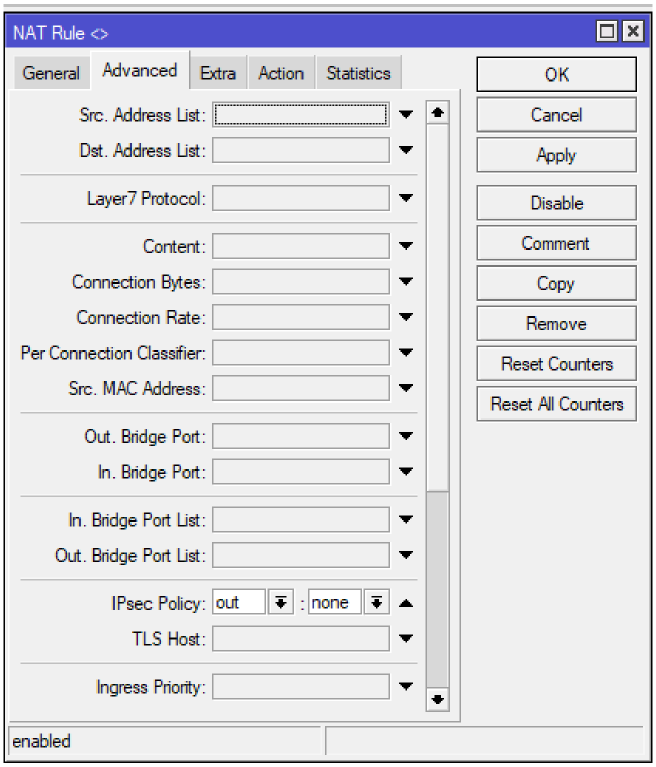
   - Chain: Select srcnat

   - in **Advanced** tab, in IPSec Policy Select “**out**”



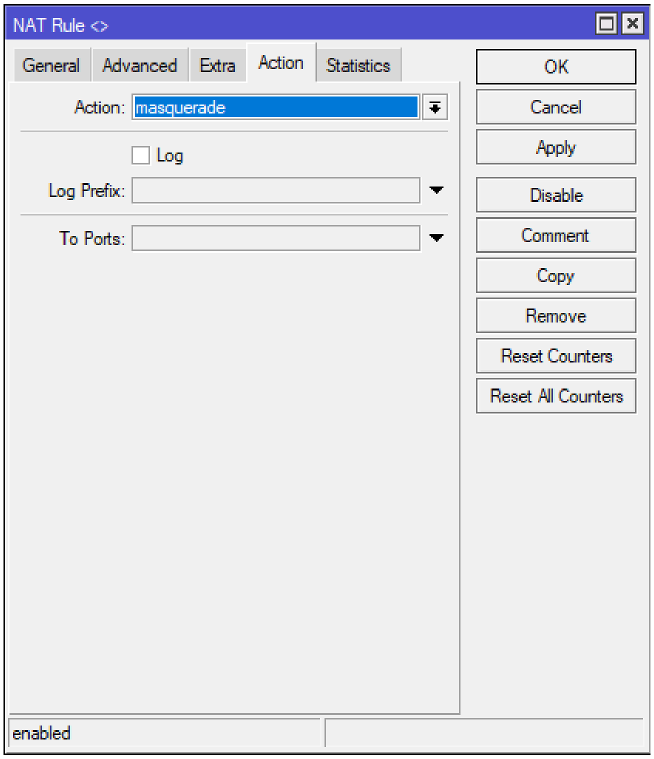
Chain: srcnat

enabled



IPsec Policy: out : none

enabled



Action: masquerade

□ Log

Log Prefix:

To Ports:

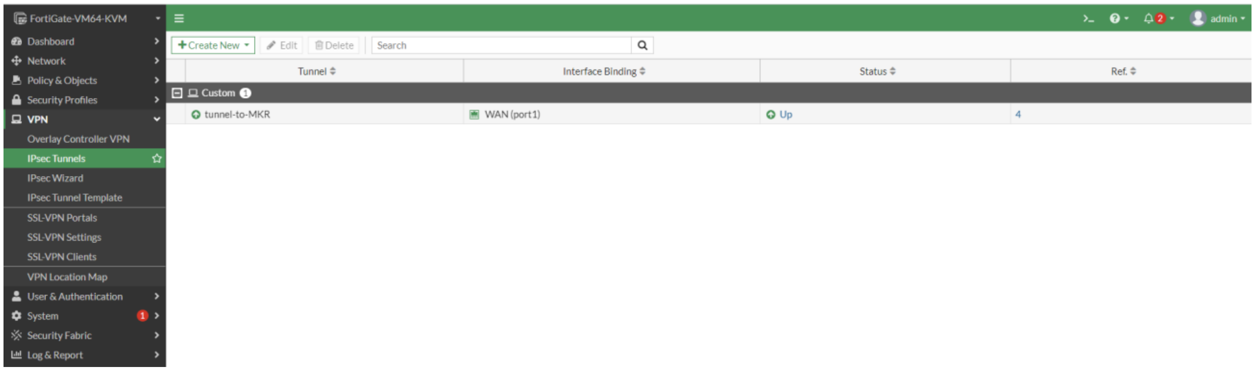
enabled

- Click Apply and OK.

3. Verification and Troubleshooting

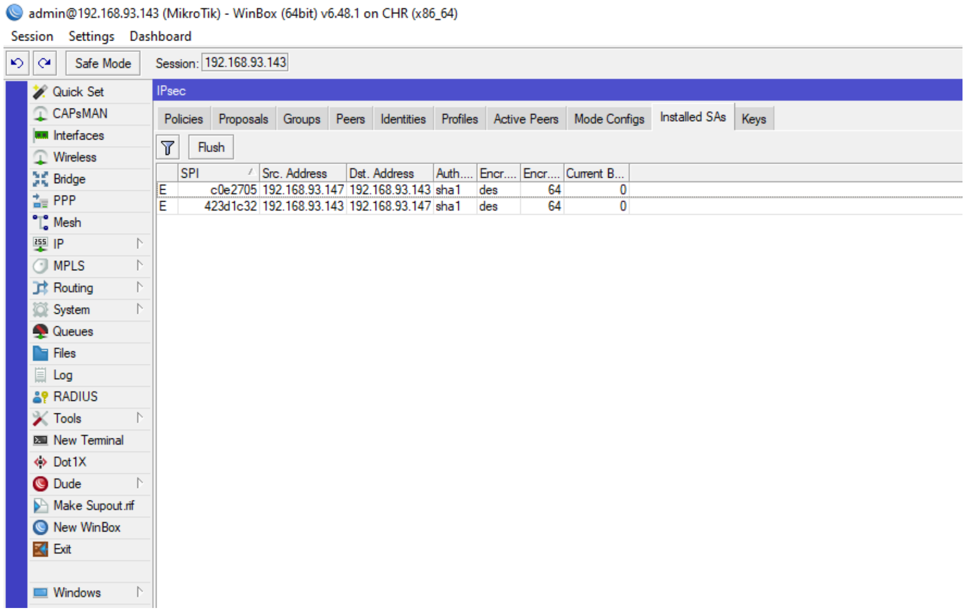
1. Verify VPN Status:

- On FortiGate: Go to VPN > IPSec Tunnels to check if the tunnel is active.



Tunnel	Interface Binding	Status	Ref.
Custom 1			
tunnel-to-MKR	WAN (port1)	Up	4

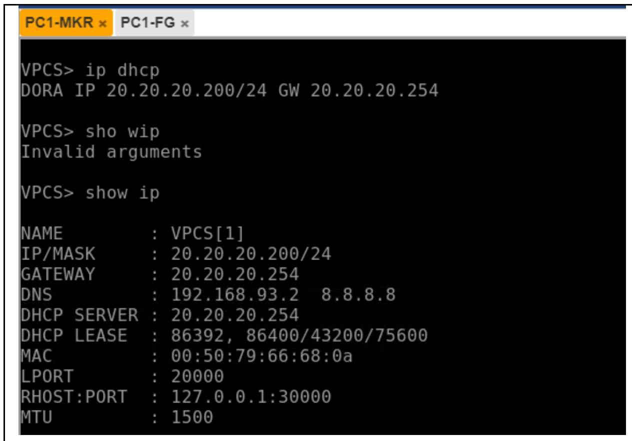
- On MikroTik: Go to IP > IPSec > Installed SAs to check the status.



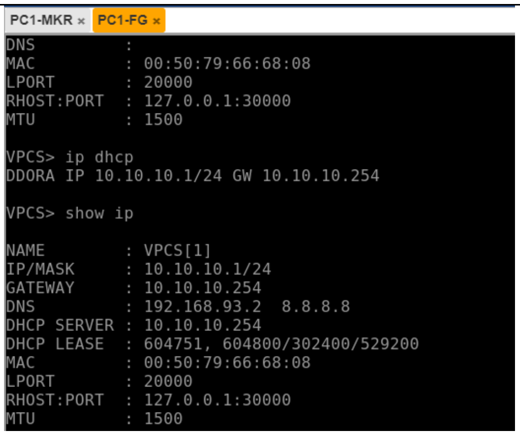
	SPI	Src. Address	Dst. Address	Auth....	Encr....	Encr....	Current B...
E	c0e2705	192.168.93.147	192.168.93.143	sha1	des	64	0
E	423d1c32	192.168.93.143	192.168.93.147	sha1	des	64	0

2. Test Connectivity:

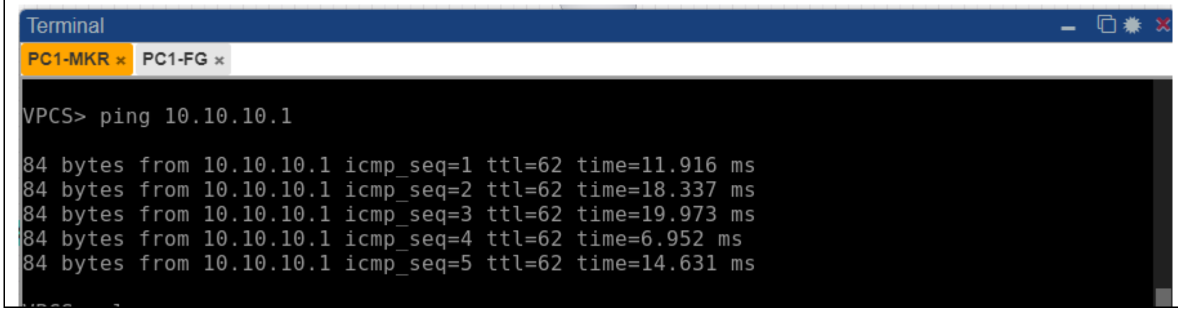
- Ping from MikroTik's LAN (20.20.20.200) to FortiGate's LAN (10.10.10.1)



```
VPCS> ip dhcp
DORA IP 20.20.20.200/24 GW 20.20.20.254

VPCS> sho wip
Invalid arguments

VPCS> show ip

NAME        : VPCS[1]
IP/MASK     : 20.20.20.200/24
GATEWAY     : 20.20.20.254
DNS         : 192.168.93.2  8.8.8.8
DHCP SERVER : 20.20.20.254
DHCP LEASE  : 86392, 86400/43200/75600
MAC         : 00:50:79:66:68:0a
LPORT       : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU         : 1500
```

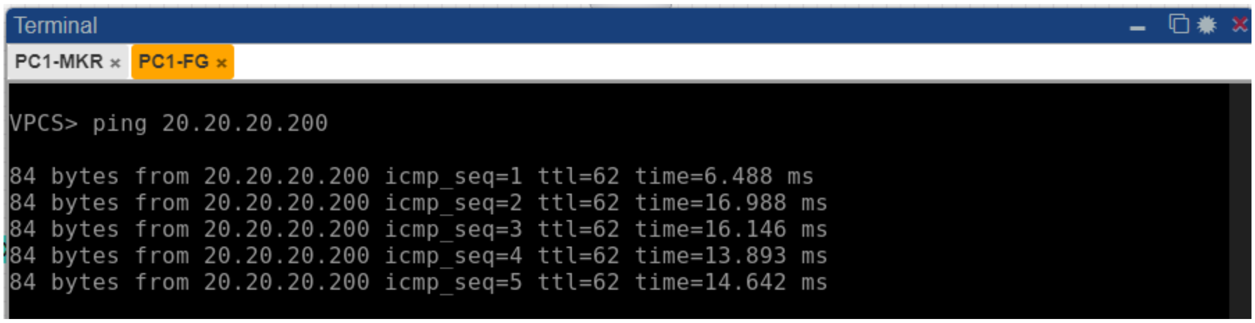


```
DNS         :
MAC         : 00:50:79:66:68:08
LPORT       : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU         : 1500

VPCS> ip dhcp
DDORA IP 10.10.10.1/24 GW 10.10.10.254

VPCS> show ip

NAME        : VPCS[1]
IP/MASK     : 10.10.10.1/24
GATEWAY     : 10.10.10.254
DNS         : 192.168.93.2  8.8.8.8
DHCP SERVER : 10.10.10.254
DHCP LEASE  : 604751, 604800/302400/529200
MAC         : 00:50:79:66:68:08
LPORT       : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU         : 1500
```



```
VPCS> ping 10.10.10.1

84 bytes from 10.10.10.1 icmp_seq=1 ttl=62 time=11.916 ms
84 bytes from 10.10.10.1 icmp_seq=2 ttl=62 time=18.337 ms
84 bytes from 10.10.10.1 icmp_seq=3 ttl=62 time=19.973 ms
84 bytes from 10.10.10.1 icmp_seq=4 ttl=62 time=6.952 ms
84 bytes from 10.10.10.1 icmp_seq=5 ttl=62 time=14.631 ms
```

- Ping from FortiGate’s LAN to Mikrotik’s LAN



```
VPCS> ping 20.20.20.200

84 bytes from 20.20.20.200 icmp_seq=1 ttl=62 time=6.488 ms
84 bytes from 20.20.20.200 icmp_seq=2 ttl=62 time=16.988 ms
84 bytes from 20.20.20.200 icmp_seq=3 ttl=62 time=16.146 ms
84 bytes from 20.20.20.200 icmp_seq=4 ttl=62 time=13.893 ms
84 bytes from 20.20.20.200 icmp_seq=5 ttl=62 time=14.642 ms
```

3. Troubleshooting:

- Check the logs on both FortiGate and MikroTik if the VPN is not functioning as expected.

- Ensure firewall and NAT rules are correctly configured to allow VPN traffic.

This setup will create a secure IPSec VPN tunnel between FortiGate and MikroTik, enabling communication between their respective LANs over the internet.