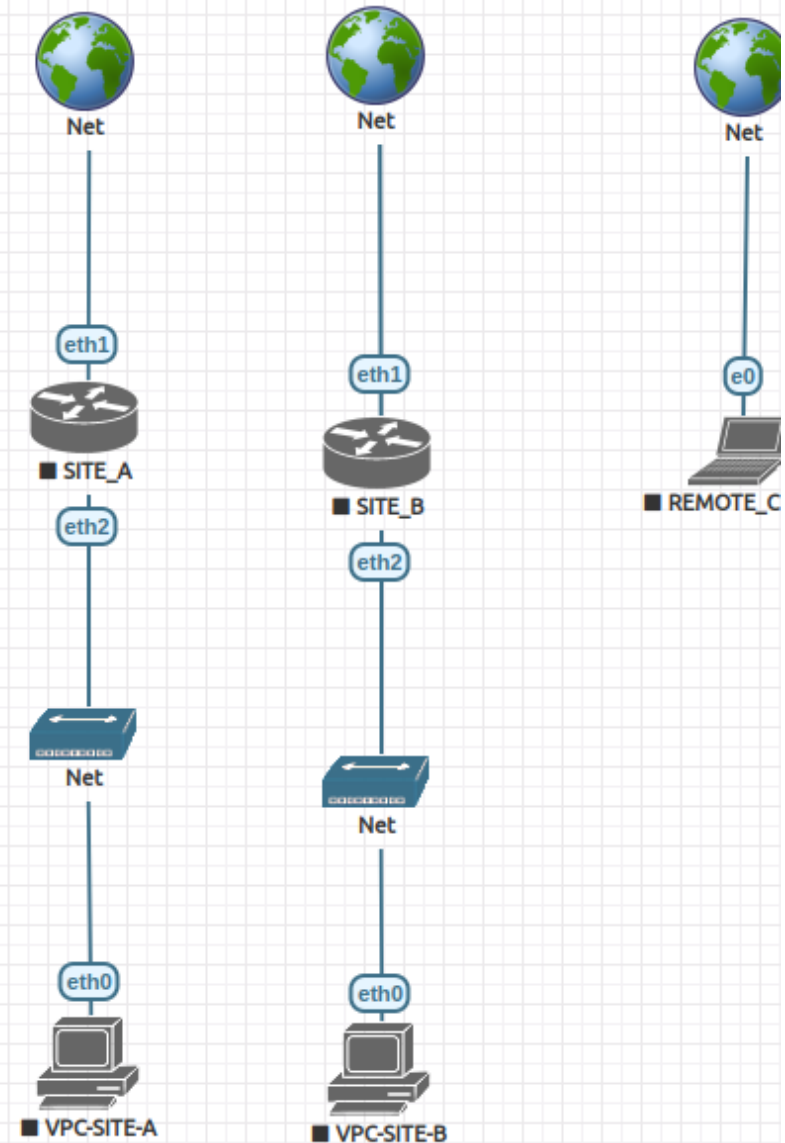


Laboratoare Retelistica

# Protocolul IPsec/L2TP site-to-site si client-to-site

# Topologie

- Aceasta topologie este asemanatoare cu cele precedente folosite in scenariile de VPN.
- Avem doua Site-uri si un client remote
- In cazul site-urilor vom folosi doar IPSec iar in cazul clientului va trebui sa folosim IPSec cu L2TP.



# Configurare Router SITE\_A

- Atat in cazul routerului SITE\_A cat si SITE\_B vom avea predefinita o retea LAN 192.168.1.0/24 respectiv 192.168.2.0/24 si regula de NAT activa.
- Pentru a incepe configurarea mergem in IP->IPsec in sectiunea profiles.
- Aici configuram zona criptografica a protocolului in functie de ce suporta si celalalt site (in cazul nostru nu exista probleme de compatibilitate asa ca putem bifa orice).

New IPsec Profile

Name:

Hash Algorithms:

PRF Algorithms:

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:

Lifetime:

Lifebytes:

☒ NAT Traversal

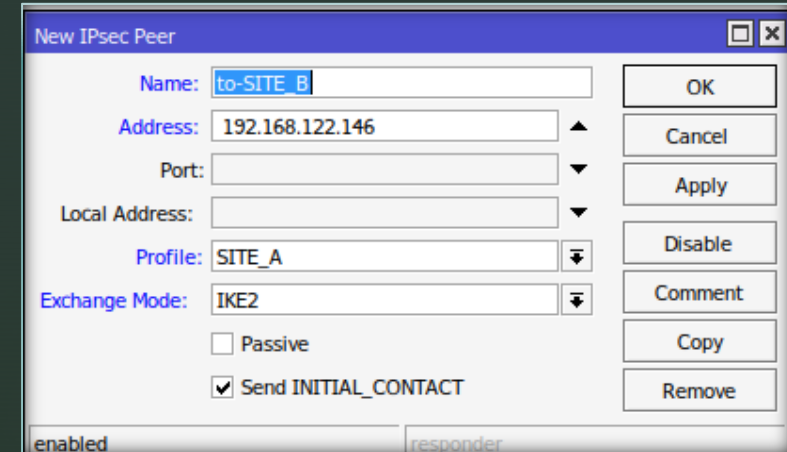
DPD Interval:  s

DPD Maximum Failures:

OK  
Cancel  
Apply  
Copy  
Remove

# Configurare Router SITE\_A

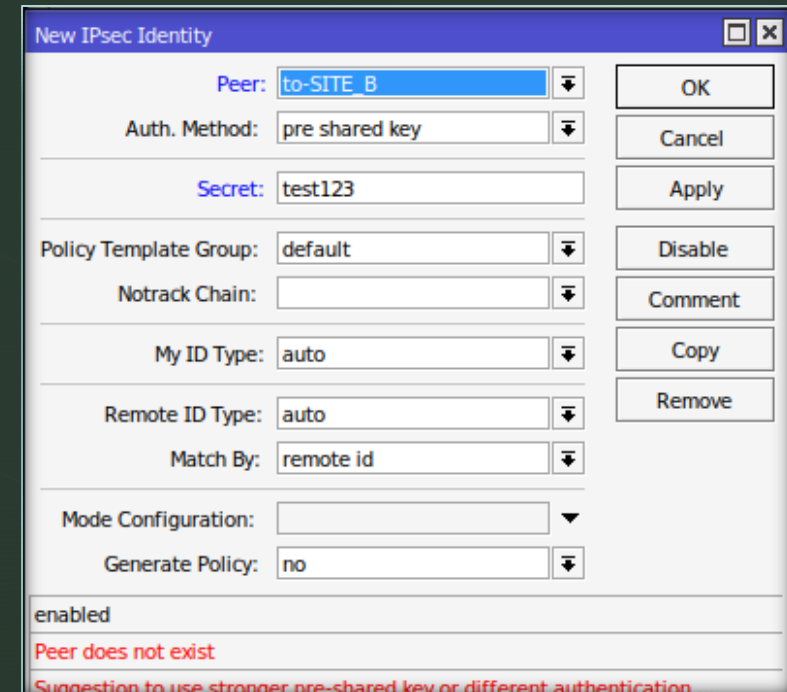
- Acum configuram peer-ul la care ne vom conecta (SITE\_B) in sectiunea Peers.
- Aici Intrducem adresa remote profilul facut si ca exchange mode setam IKE2 (versiunea 1 nu este recomandata).
- Apoi in sectiunea Identity facem o noua identitate si ca metoda de autentificare selectam pre shared key (recomand certificate sau alta metoda pentru productie).



The 'New IPsec Peer' window is used to configure a new peer. It includes fields for Name, Address, Port, Local Address, Profile, and Exchange Mode. The 'Name' field is set to 'to-SITE\_B', 'Address' is '192.168.122.146', 'Profile' is 'SITE\_A', and 'Exchange Mode' is 'IKE2'. There are checkboxes for 'Passive' and 'Send INITIAL\_CONTACT', with the latter being checked. On the right, there are buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove. At the bottom, there are status indicators for 'enabled' and 'responder'.

Name:	to-SITE_B
Address:	192.168.122.146
Port:	
Local Address:	
Profile:	SITE_A
Exchange Mode:	IKE2
<input type="checkbox"/> Passive	
<input checked="" type="checkbox"/> Send INITIAL_CONTACT	

enabled responder



The 'New IPsec Identity' window is used to configure a new identity. It includes fields for Peer, Auth. Method, Secret, Policy Template Group, Notrack Chain, My ID Type, Remote ID Type, Match By, Mode Configuration, and Generate Policy. The 'Peer' field is set to 'to-SITE\_B', 'Auth. Method' is 'pre shared key', 'Secret' is 'test123', 'Policy Template Group' is 'default', 'My ID Type' is 'auto', 'Remote ID Type' is 'auto', 'Match By' is 'remote id', and 'Generate Policy' is 'no'. On the right, there are buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove. At the bottom, there are status indicators for 'enabled', 'Peer does not exist', and a suggestion to use stronger pre-shared key or different authentication.

Peer:	to-SITE_B
Auth. Method:	pre shared key
Secret:	test123
Policy Template Group:	default
Notrack Chain:	
My ID Type:	auto
Remote ID Type:	auto
Match By:	remote id
Mode Configuration:	
Generate Policy:	no

enabled

Peer does not exist

Suggestion to use stronger pre-shared key or different authentication ...

## Configurare Router SITE\_A

- Configurare Proposal, aceste setari trebuie sa fie identice cu cele din profilul facut.
- Dupa care ultimul pas este sa facem o politica in sectiunea Policies.
- Aici selectam peerul facut la adresa sursa punem clasa noastra de LAN (SITE\_A) si la destinatie clasa la care vrem sa ajunge (SITE\_B).

The left screenshot shows the 'New IPsec Proposal' dialog. The 'Name' field is 'SITE\_A-proposal'. Under 'Auth. Algorithms', 'sha512' is selected. Under 'Encr. Algorithms', 'aes-256 cbc' is selected. 'Lifetime' is '00:30:00' and 'PFS Group' is 'modp8192'. The 'enabled' checkbox is checked.

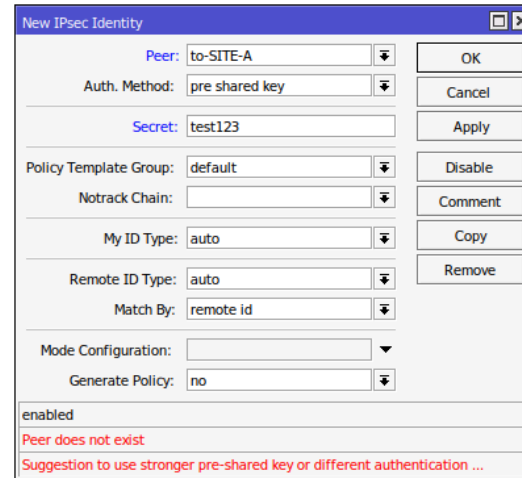
The right screenshot shows the 'IPsec Profile <SITE\_A>' dialog. The 'Name' field is 'SITE\_A'. 'Hash Algorithms' and 'PRF Algorithms' are both 'sha512'. Under 'Encryption Algorithm', 'aes-256' is selected. 'DH Group' is 'modp8192'. 'Proposal Check' is 'obey', 'Lifetime' is '1d 00:00:00', and 'Lifebytes' is empty. 'NAT Traversal' is checked. 'DPD Interval' is '120' and 'DPD Maximum Failures' is '5'. The 'enabled' checkbox is checked.

The 'New IPsec Policy' dialog has three tabs: 'General', 'Action', and 'Status'. The 'General' tab is active. 'Action' is 'encrypt', 'Level' is 'require', 'IPsec Protocols' is 'esp', and 'Proposal' is 'SITE\_A-proposal'. The 'enabled' checkbox is checked.

The 'General' tab of the IPsec Policy configuration is shown. 'Peer' is 'to-SITE\_B'. 'Tunnel' is checked. 'Src. Address' is '192.168.1.0/24' and 'Dst. Address' is '192.168.2.0/24'. 'Protocol' is '255 (all)'. The 'Template' checkbox is unchecked. The 'enabled' checkbox is checked.

## Configurare Router SITE\_B

- Configurarea protocolului trebuie sa fie identica pentru ca cele doua sa poata comunica, orice mismatch va duce la o eroare si refuzarea conexiunii.



New IPsec Identity

Peer: to-SITE-A

Auth. Method: pre shared key

Secret: test123

Policy Template Group: default

Notrack Chain:

My ID Type: auto

Remote ID Type: auto

Match By: remote id

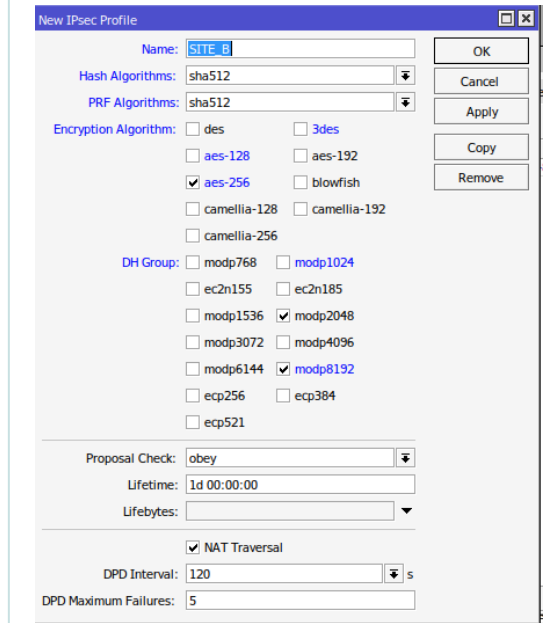
Mode Configuration:

Generate Policy: no

enabled

Peer does not exist

Suggestion to use stronger pre-shared key or different authentication ...



New IPsec Profile

Name: SITE\_B

Hash Algorithms: sha512

PRF Algorithms: sha512

Encryption Algorithms:

- ☐ des
- ☐ aes-128
- ☒ aes-256
- ☐ camellia-128
- ☐ camellia-256
- ☐ 3des
- ☐ aes-192
- ☐ blowfish
- ☐ camellia-192

DH Group:

- ☐ modp768
- ☐ ec2n155
- ☐ modp1536
- ☐ modp3072
- ☐ modp6144
- ☐ ec2n185
- ☒ modp2048
- ☐ modp4096
- ☒ modp8192
- ☐ ec384
- ☐ ecp521

Proposal Check: obey

Lifetime: 1d 00:00:00

Lifeytes:

☒ NAT Traversal

DPD Interval: 120 s

DPD Maximum Failures: 5

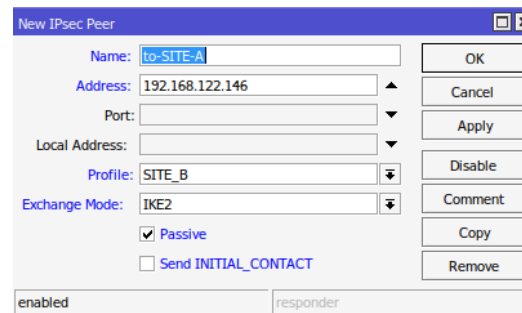
OK

Cancel

Apply

Copy

Remove



New IPsec Peer

Name: to-SITE-A

Address: 192.168.122.146

Port:

Local Address:

Profile: SITE\_B

Exchange Mode: IKE2

☒ Passive

☐ Send INITIAL\_CONTACT

enabled

responder

OK

Cancel

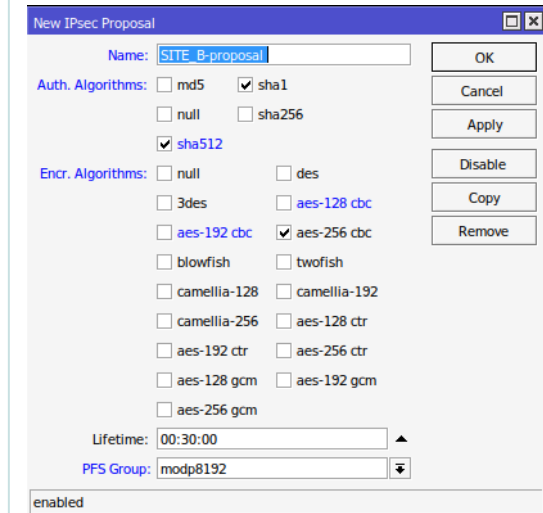
Apply

Disable

Comment

Copy

Remove



New IPsec Proposal

Name: SITE\_B-proposal

Auth. Algorithms:

- ☐ md5
- ☒ sha1
- ☐ null
- ☐ sha256
- ☒ sha512

Encr. Algorithms:

- ☐ null
- ☐ 3des
- ☐ aes-192 cbc
- ☐ blowfish
- ☐ camellia-128
- ☐ camellia-256
- ☐ aes-192 ctr
- ☐ aes-128 gcm
- ☐ aes-256 gcm
- ☐ des
- ☐ aes-128 cbc
- ☒ aes-256 cbc
- ☐ twofish
- ☐ camellia-192
- ☐ aes-128 ctr
- ☐ aes-256 ctr
- ☐ aes-192 gcm

Lifetime: 00:30:00

PFS Group: modp8192

enabled

OK

Cancel

Apply

Disable

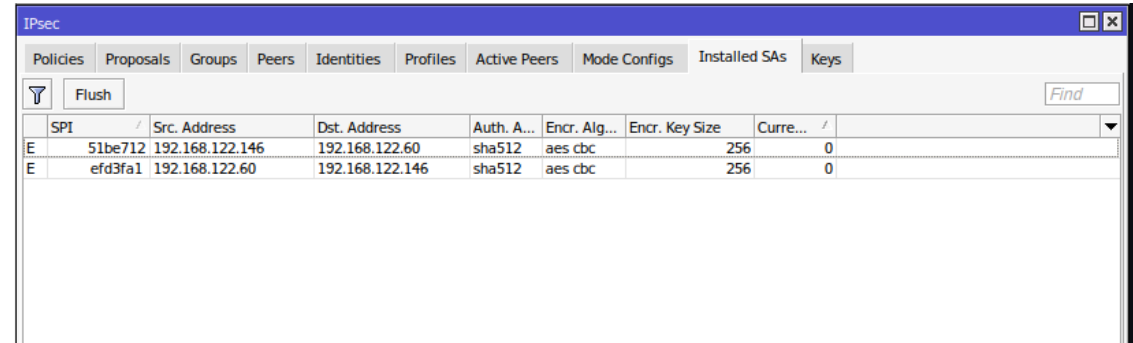
Copy

Remove



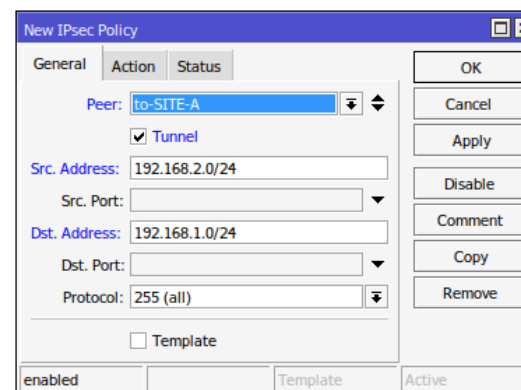
## Configurare Router SITE\_B

- La Policy la fel ca in cazul SITE\_A trebuie sa configuram sursa si destinatia care vor fi puse invers fata de SITE\_A si la "Action" setata politica.
- Acum putem verifica faptul ca avem conexiune uitandu-ne in tabul "Installed SAs"



The screenshot shows the 'IPsec' configuration window with the 'Installed SAs' tab selected. It displays a table of installed Security Associations (SAs) with columns for SPI, Src. Address, Dst. Address, Auth. A..., Encr. Alg..., Encr. Key Size, and Curre... (Current state). There are two entries, both marked with an 'E' in the first column.

	SPI	Src. Address	Dst. Address	Auth. A...	Encr. Alg...	Encr. Key Size	Curre...
E	51be712	192.168.122.146	192.168.122.60	sha512	aes cbc	256	0
E	efd3fa1	192.168.122.60	192.168.122.146	sha512	aes cbc	256	0



The screenshot shows the 'New IPsec Policy' dialog box with the 'General' tab selected. The 'Peer' is set to 'to-SITE-A', 'Tunnel' is checked, 'Src. Address' is '192.168.2.0/24', 'Dst. Address' is '192.168.1.0/24', and 'Protocol' is '255 (all)'. The 'Template' checkbox is unchecked. The 'enabled' checkbox is checked, and the 'Active' checkbox is also checked.

General Action Status

Peer: to-SITE-A

☒ Tunnel

Src. Address: 192.168.2.0/24

Src. Port:

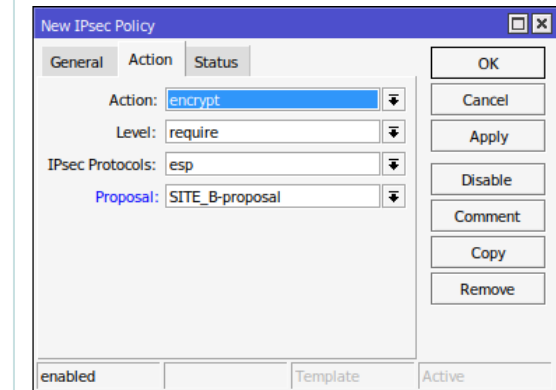
Dst. Address: 192.168.1.0/24

Dst. Port:

Protocol: 255 (all)

☐ Template

enabled ☒ Template ☒ Active



The screenshot shows the 'New IPsec Policy' dialog box with the 'Action' tab selected. The 'Action' is set to 'encrypt', 'Level' is 'require', 'IPsec Protocols' is 'esp', and 'Proposal' is 'SITE\_B-proposal'. The 'enabled' checkbox is checked, and the 'Active' checkbox is also checked.

General Action Status

Action: encrypt

Level: require

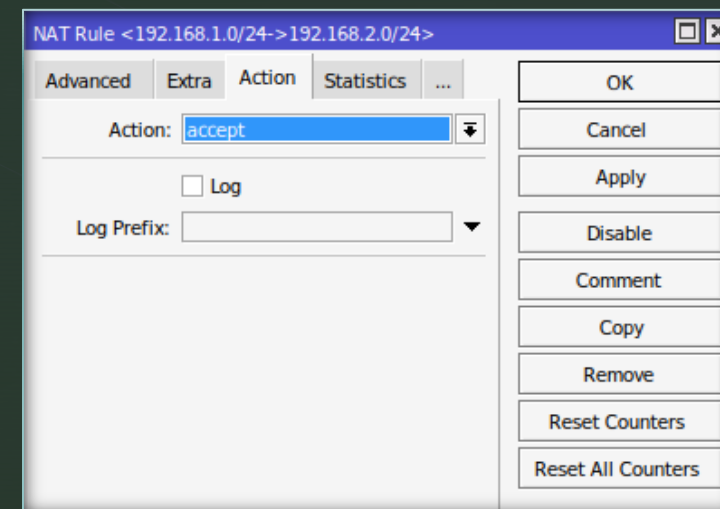
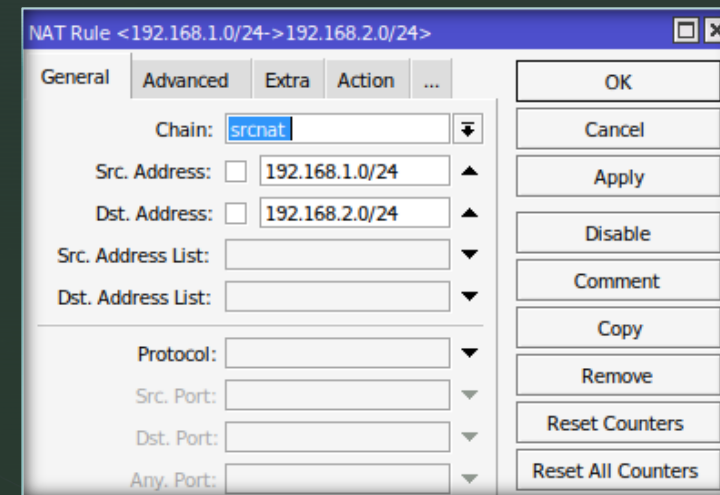
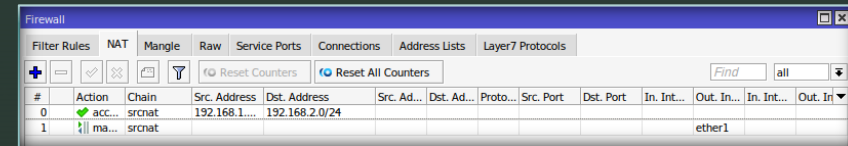
IPsec Protocols: esp

Proposal: SITE\_B-proposal

enabled ☒ Template ☒ Active

# Configurare Firewall

- Atat pe SITE\_A cat si pe SITE\_B trebuie sa facem reguli noi de NAT pentru a permite accesul in retele remote.
- Folosind chain-ul srcnat setam la adresa sursa reteaua lan iar la destinatie reteaua remote (ex pentru SITE\_A SRC: 192.168.1.0/24 si DST: 192.168.2.0/24) iar la "Action" setam accept.
- Dupa care ridicam regula la prima regula de NAT.





# Testare site-to-site

```
VPC-SITE-A
VPCS> show ip
NAME       : VPCS[1]
IP/MASK    : 192.168.1.254/24
GATEWAY    : 192.168.1.1
DNS        : 192.168.122.1
DHCP SERVER : 192.168.1.1
DHCP LEASE  : 574, 600/300/525
MAC        : 00:50:79:66:68:02
LPORT      : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU        : 1500

VPCS> ping 192.168.2.254

84 bytes from 192.168.2.254 icmp_seq=1 ttl=62 time=4.534 ms
84 bytes from 192.168.2.254 icmp_seq=2 ttl=62 time=2.299 ms
^C
VPCS> █

VPC-SITE-B
VPCS> show ip
NAME       : VPCS[1]
IP/MASK    : 192.168.2.254/24
GATEWAY    : 192.168.2.1
DNS        : 192.168.122.1
DHCP SERVER : 192.168.2.1
DHCP LEASE  : 589, 600/300/525
MAC        : 00:50:79:66:68:04
LPORT      : 20000
RHOST:PORT  : 127.0.0.1:30000
MTU        : 1500

VPCS> ping 192.168.1.254

84 bytes from 192.168.1.254 icmp_seq=1 ttl=62 time=2.184 ms
84 bytes from 192.168.1.254 icmp_seq=2 ttl=62 time=1.950 ms
^C
VPCS> █
```

# Configurare site-to-client (IPsec/L2TP)

- Pentru aceasta configurare va trebui sa activam si sa configuram serverul de L2TP din PPP apasand pe butonul L2TP Server.
- Trebuie sa il setam ca enabled
- Use IPsec setat pe required
- Si un shared IPsec secret.
- In tabul Secrets facem utilizatorul.
- Aici ii setam numele, parola
- Servicul sa fie l2tp, adresa locala este adresa interfetei LAN iar cea remote o stabilim din subnetul LAN-ului.

The screenshot shows the 'L2TP Server' configuration window with the 'L2TPv3' tab selected. The 'General' section has the 'Enabled' checkbox checked. Below it, 'Max MTU' and 'Max MRU' are both set to 1450. 'MRRU' is empty. 'Keepalive Timeout' is set to 30. 'Default Profile' is 'default-encryption'. 'Max Sessions' is empty. Under 'Authentication', 'mschap2', 'mschap1', 'chap', and 'pap' are all checked. In the 'Use IPsec' section, 'required' is selected. The 'IPsec Secret' is set to 'test123'. 'Caller ID Type' is set to 'ip address'. At the bottom, 'One Session Per Host' and 'Allow Fast Path' are unchecked.

The screenshot shows the 'New PPP Secret' configuration window. 'Name' is 'test'. 'Password' is 'Passowrd123'. 'Service' is 'l2tp'. 'Caller ID' is empty. 'Profile' is 'default'. 'Local Address' is '192.168.2.1'. 'Remote Address' is '192.168.2.10'. 'Remote IPv6 Prefix' is empty. 'Routes' and 'IPv6 Routes' are empty. 'Limit Bytes In' and 'Limit Bytes Out' are empty. 'Last Logged Out', 'Last Caller ID', and 'Last Disconnect Reason' are empty. At the bottom, the status is 'enabled'.

# Configurare site-to-client (IPsec/L2TP)

- Acum putem adauga un server binding in tabul Interface apasand pe butonul "+" si alegand L2TP Server Binding.
- Acum putem configura un client bazat pe ubuntu.
- In gateway putem ip-ul extern al routerului.
- La user si parola putem cele setate in router.
- Apoi dam click pe IPsec Settings pentru a activa serviciul si a pune cheia.

Name:

Type:

Actual MTU:

User:

Buttons: Cancel, Apply, Disable, Comment, Copy, Remove, Torch, Reset Traffic Counters

VPN 1 VPN

Cancel Apply

Details Identity IPv4 IPv6

Name:

General

Gateway:

User Authentication

Type:

User name:

Password:

☒ Show password

NT Domain:

☐ Use L2TP ephemeral source port

IPsec Settings... PPP Settings...

L2TP IPsec Options

☒ Enable IPsec tunnel to L2TP host

Machine Authentication

Type:

Pre-shared key:

☐ Show password

> Advanced

Cancel OK

# Testare conexiune

```
user@ubuntu22-desktop: ~  
^C  
--- 192.168.1.1 ping statistics ---  
5 packets transmitted, 0 received, 100% packet loss, time 4100ms  
  
user@ubuntu22-desktop:~$ ^C  
user@ubuntu22-desktop:~$ ping 192.168.1.1  
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.  
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63 time=2.15 ms  
64 bytes from 192.168.1.1: icmp_seq=2 ttl=63 time=2.23 ms  
64 bytes from 192.168.1.1: icmp_seq=3 ttl=63 time=1.44 ms  
^C  
--- 192.168.1.1 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2003ms  
rtt min/avg/max/mdev = 1.438/1.937/2.226/0.354 ms  
user@ubuntu22-desktop:~$ ping 192.168.2.1  
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.  
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=0.880 ms  
64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=0.754 ms  
64 bytes from 192.168.2.1: icmp_seq=3 ttl=64 time=0.895 ms  
^C  
--- 192.168.2.1 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2054ms  
rtt min/avg/max/mdev = 0.754/0.843/0.895/0.063 ms  
user@ubuntu22-desktop:~$
```