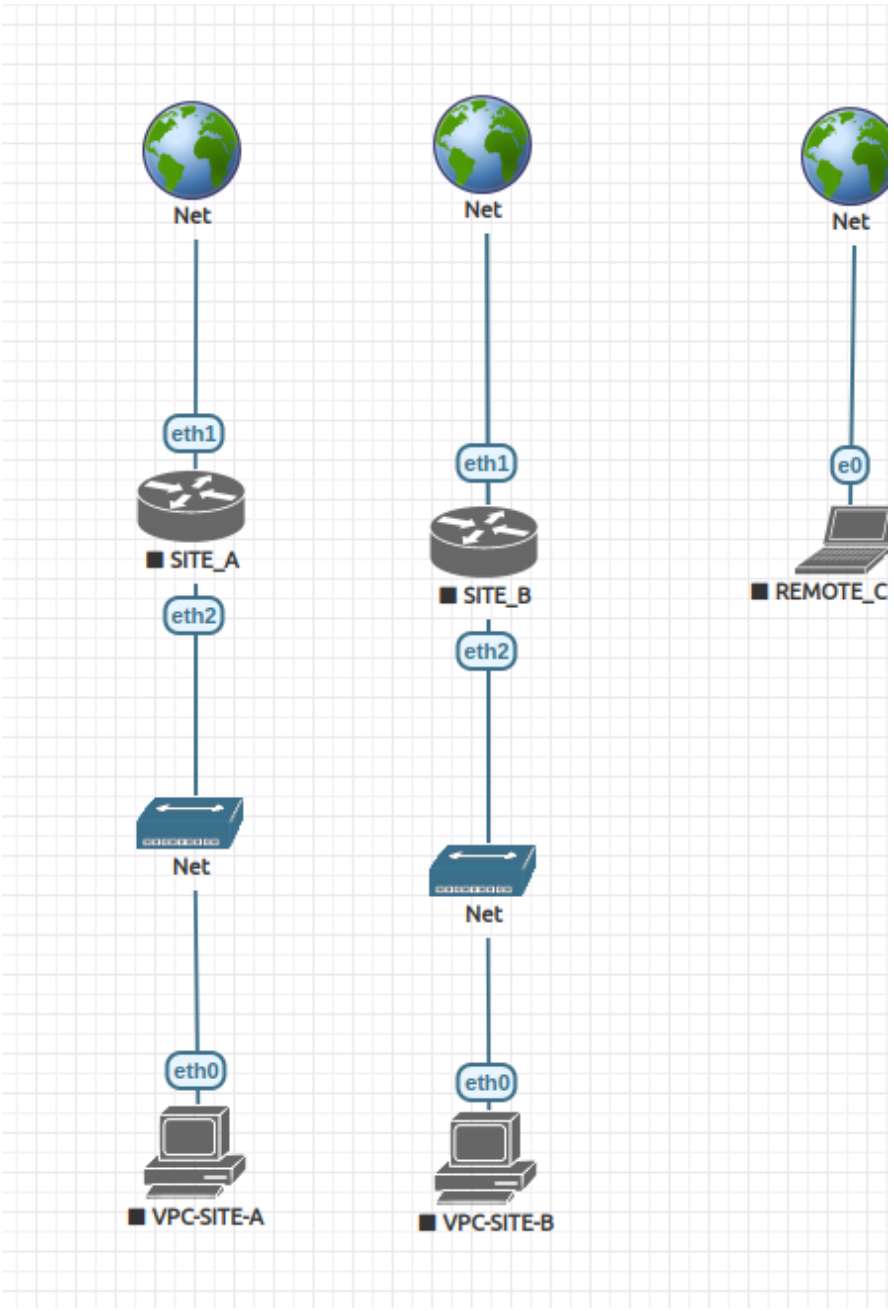
Laboratoare Retelistica

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

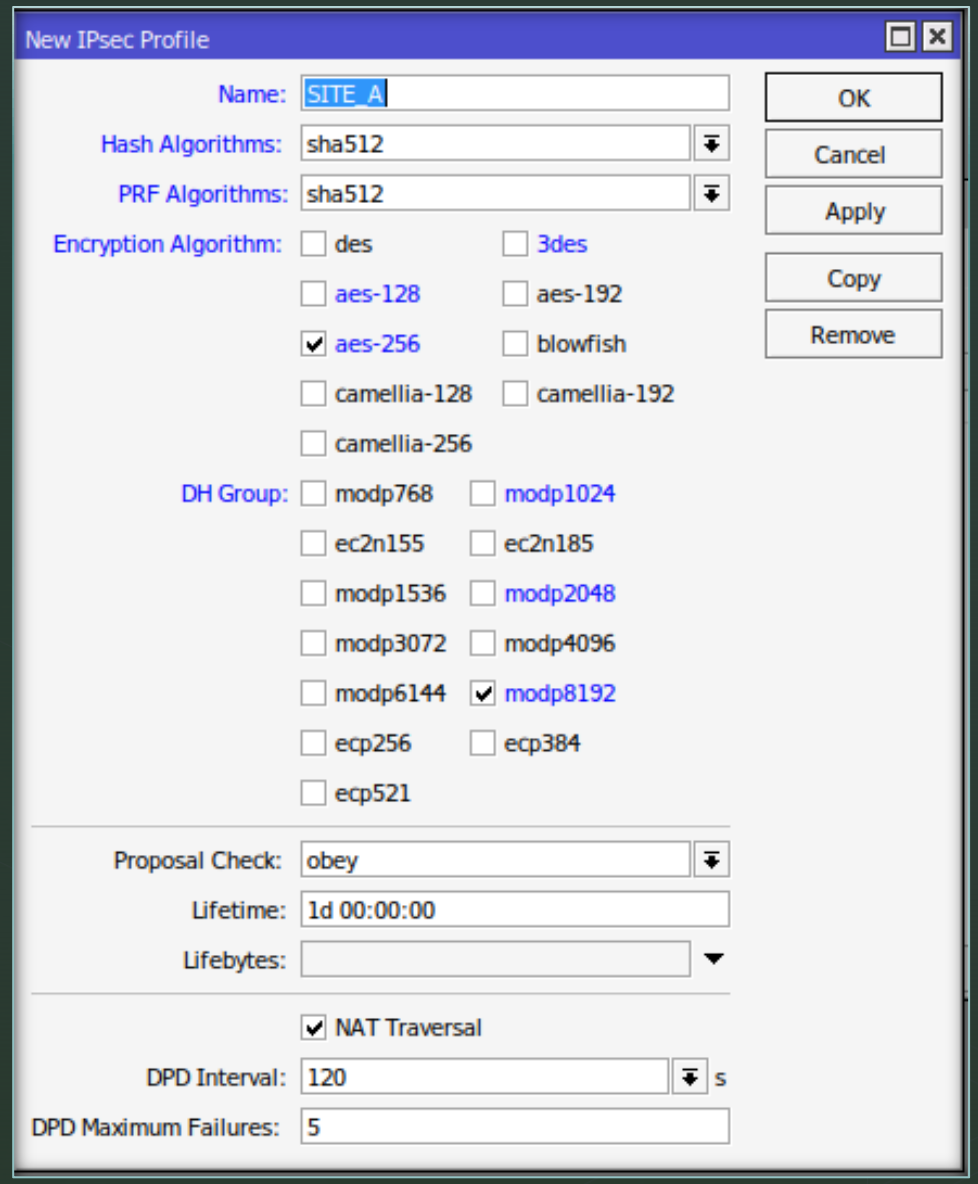
Topologie

- 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.



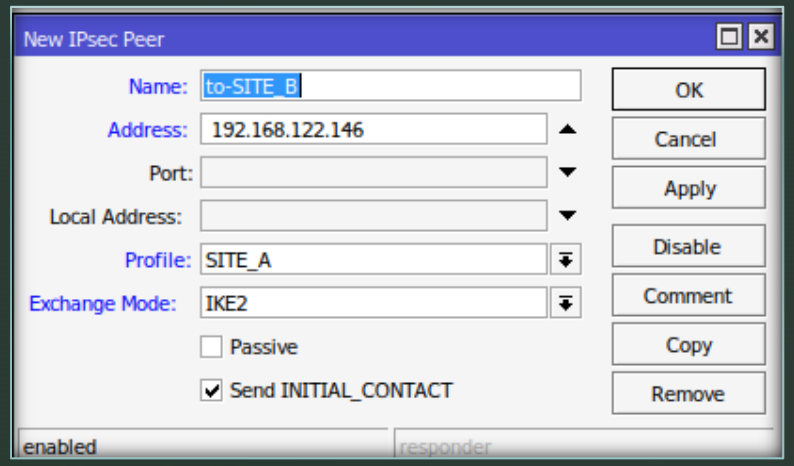
Configurare Router SITE_A

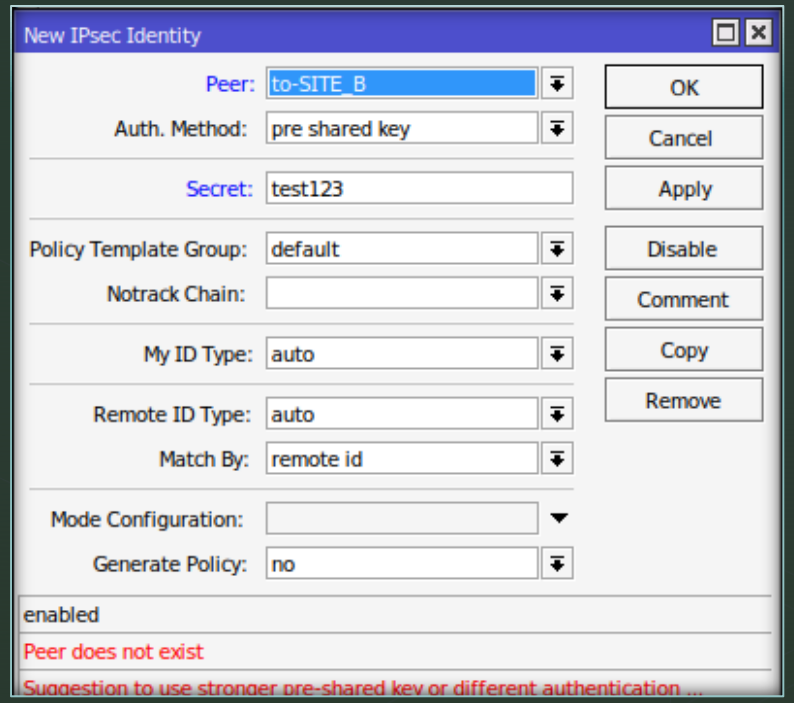
- Atat in cazul routerului SITE_A cat si SITE_B vom avea predefinita o retea LAN 192.168.1.0/24 respectiv 192.168.2.0/24 si regula de NAT activa.
- Pentru a incepe configurarea mergem in IP->IPsec in sectiunea profiles.
- Aici configuram zona criptografica a protocoluli in functie de ce suporta si celalat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



Configurare Router SITE_A

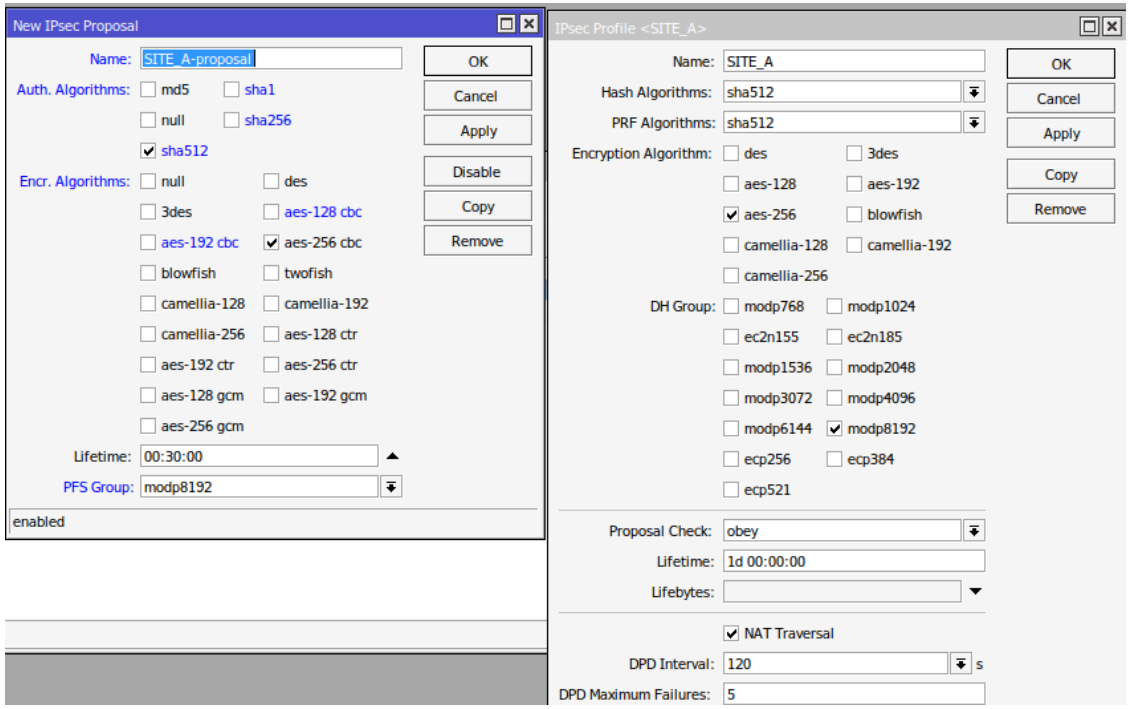
- Acum configuram peer-ul la care ne vom conecta (SITE_B) in sectiunea Peers.
- Aici Intrducem adresa remote profilul facut si ca exchange mode setam IKE2 (versiunea 1 nu este recomandata).
- Apoi in sectiunea Identity facem o noua identitate si ca metoda de autentificare selectam pre shared key (recomand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

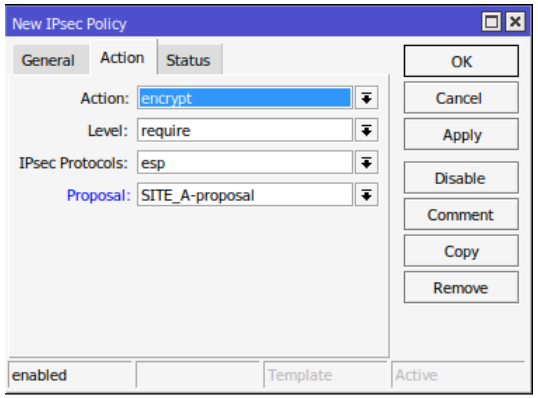


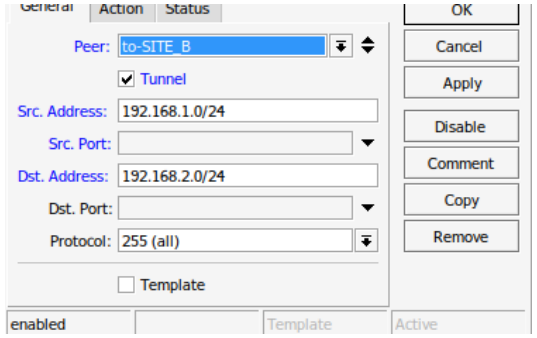


Configurare Router SITE_A

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

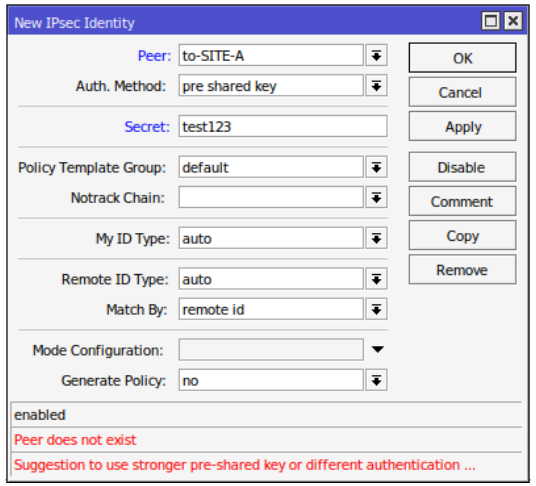


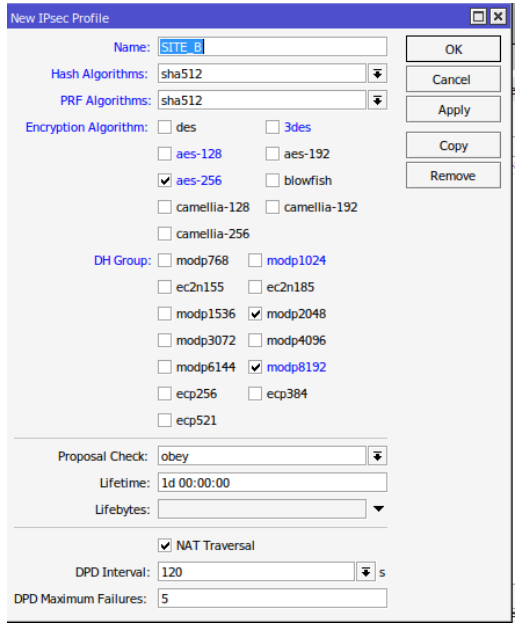


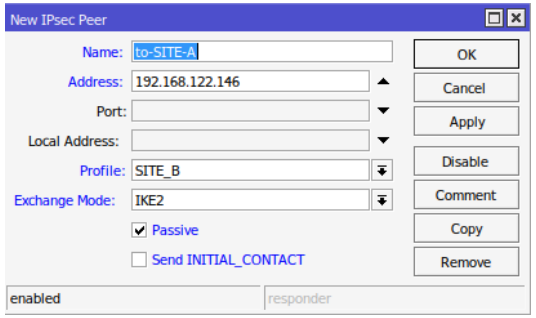


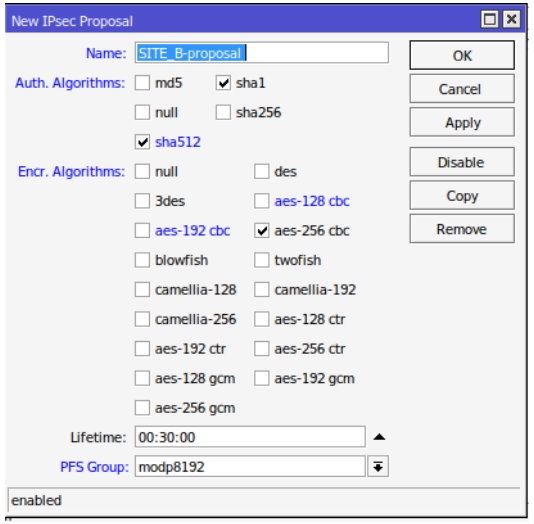
Configurare Router SITE_B

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



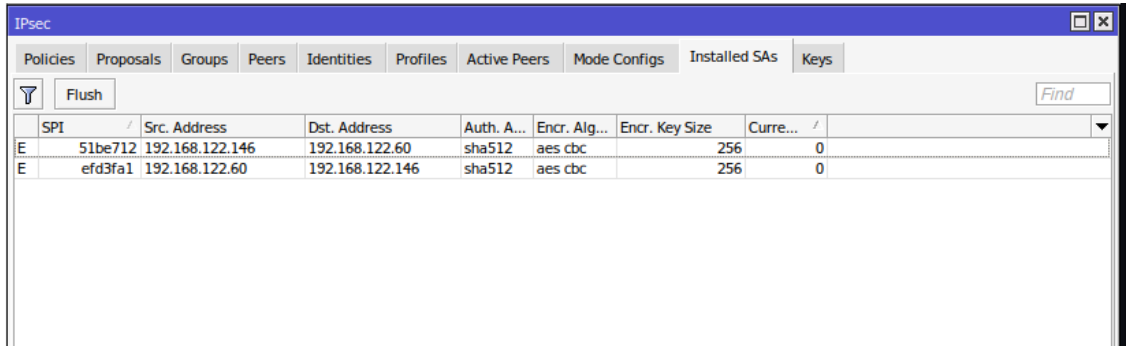


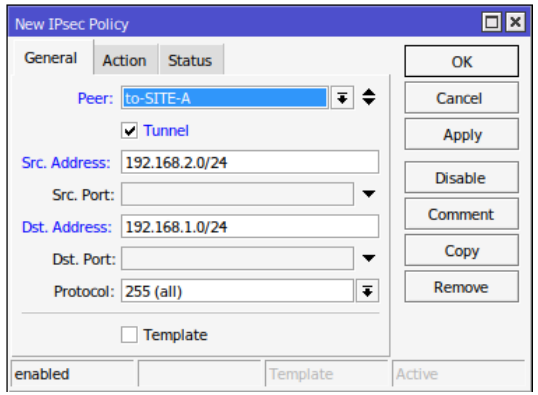


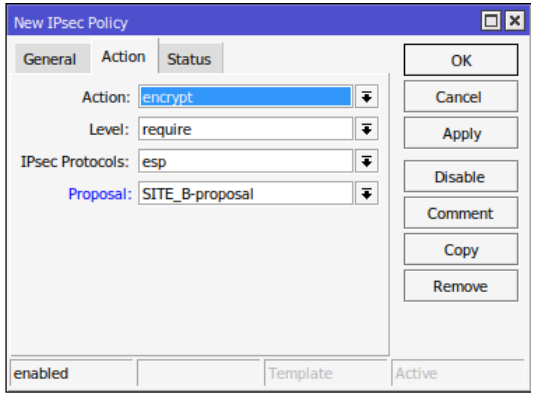


Configurare Router SITE_B

- 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"

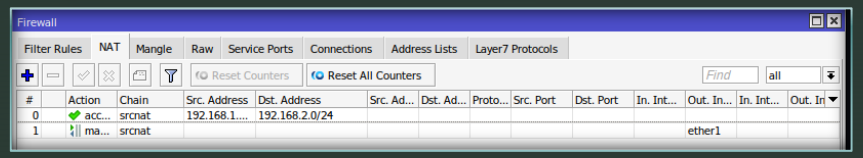


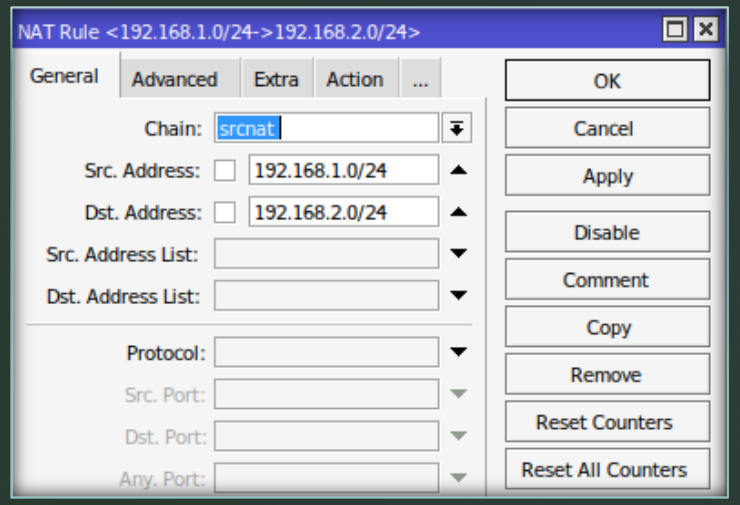


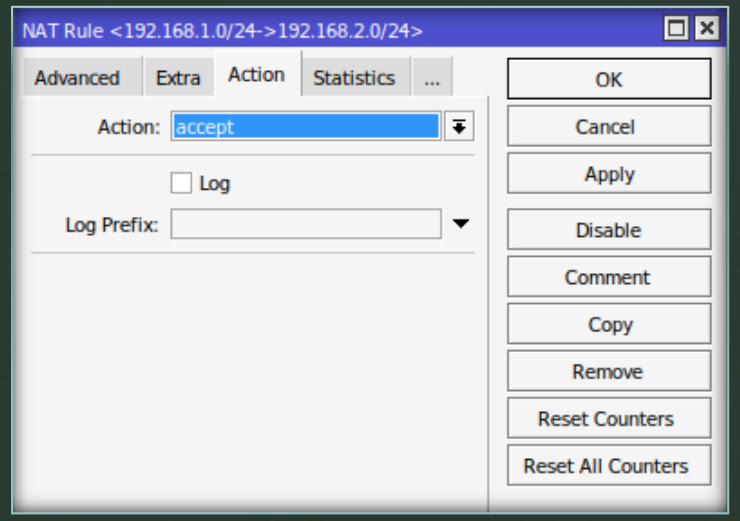


Configurare Firewall

- 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 scrnat 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

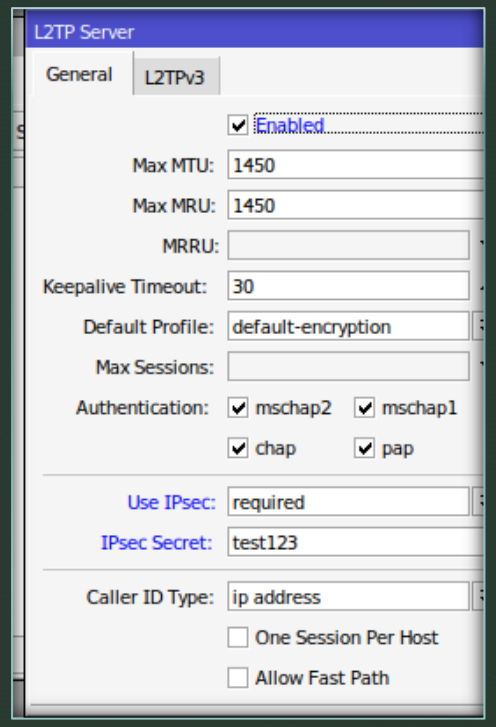
```
VPCS> show ip

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>
```

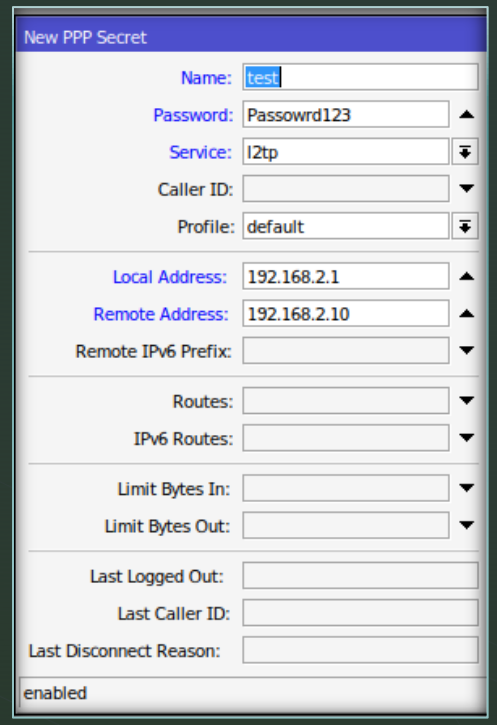
VPC-SITE-B

```
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)

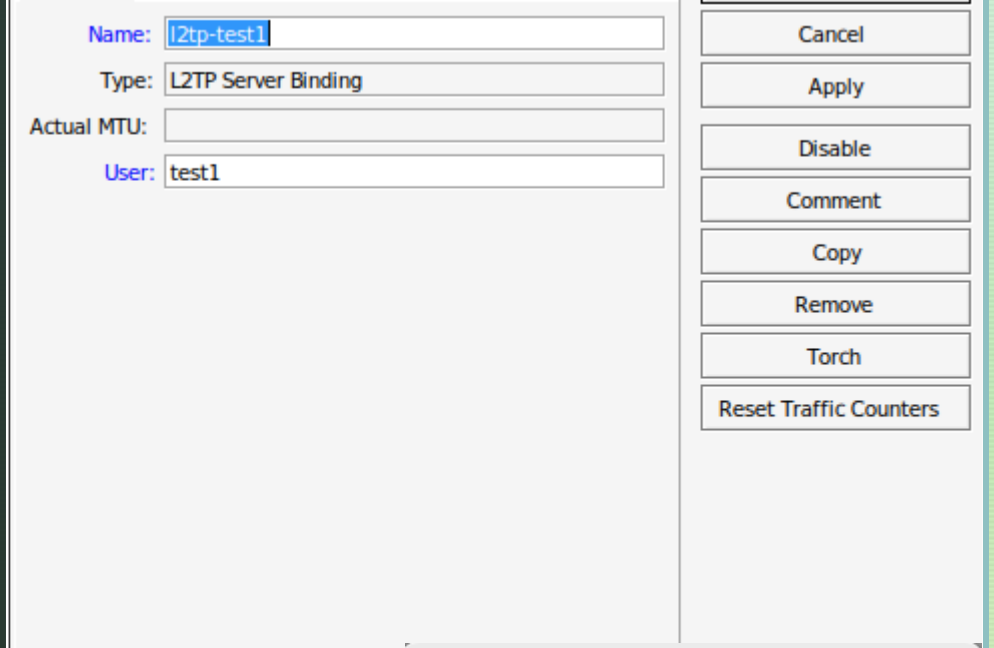
- Pentru aceasta configurare va trebui sa activam si sa configuram serverul de L2TP din PPP apasand pe butonul L2TP Server.
- Trebuie sa il setam ca enabled
- Use IPsec setat pe required
- Si un shared IPsec secret.
- In tabul Secrets facem utilizatorul.
- Aici ii setam numele, parola
- Servicul sa fie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

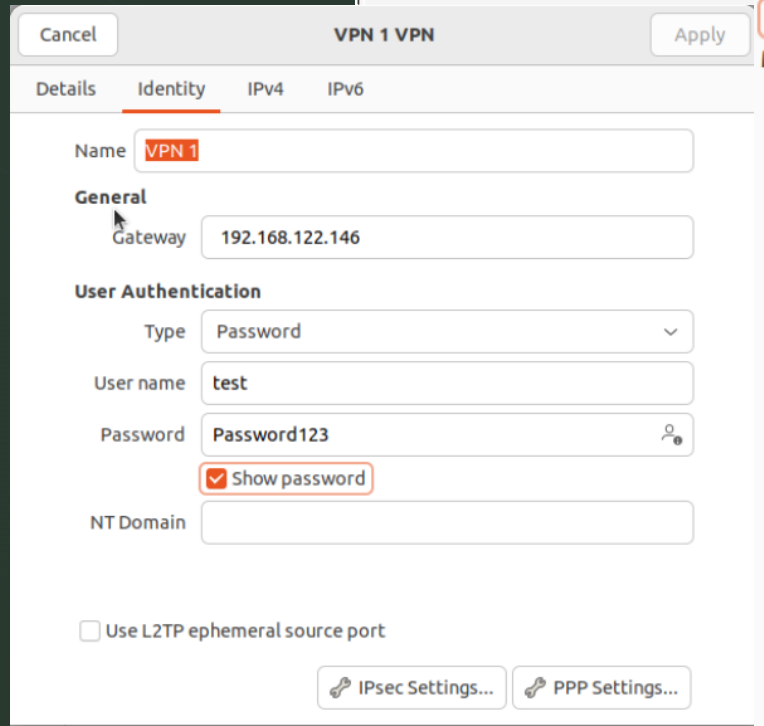


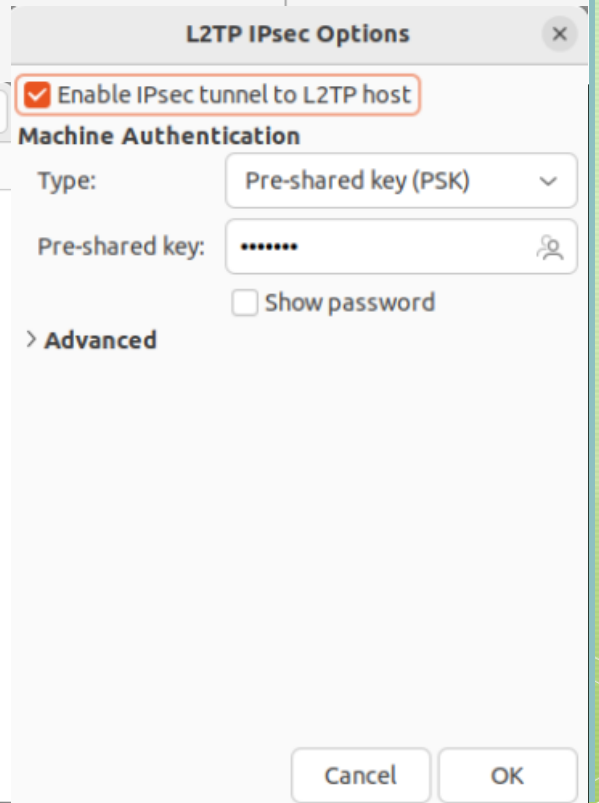


Configurare site-to-client (IPsec/L2TP)

- Acum putem adauga un server binding in tabul Interface apasand pe buntonul "+" 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 servicul si a pune cheia.







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:~$
```