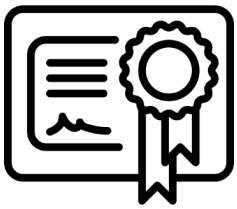
IPSEC IKE2 SITE 2 SITE – ROUTING BASE



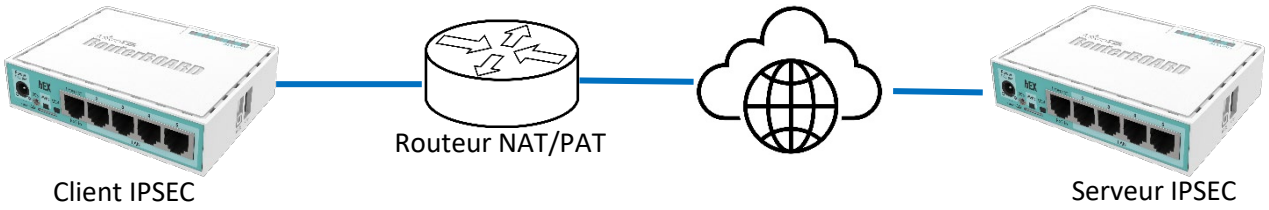
Cette documentation traite de la configuration à mettre en place sur des routeurs Mikrotik afin de créer une connexion IPSec site à site. Celle-ci est exploitée en route-based, on appelle ici « Serveur » le master IPSec, et le « Client » le peer IPSec.

Lien utile : https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/security-ipsec-vpn-overview.html

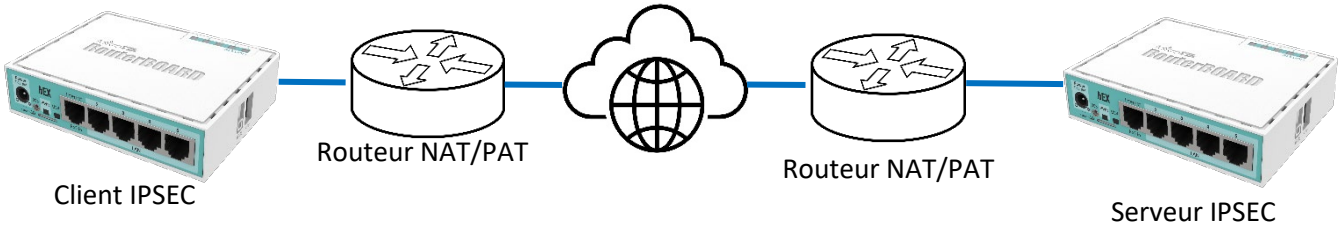
Révision : v2.2

Plusieurs topologies :

- Client(s) derrière du NAT/PAT, et serveur avec IP publique



- Client(s) derrière du NAT/PAT et serveur derrière du NAT/PAT



----------DEBUT DE LA CONFIGURATION IPSEC----------

1 - CONFIGURATION PRÉALABLE

On considère que le serveur et le client ont une configuration par défaut, et qu'ils ont obtenu une adresse IP (statique ou DHCP) sur leur interface WAN, ils effectuent du NAT/PAT pour tout le trafic à destination d'Internet.

Le firewall du serveur doit contenir ces règles pour autoriser la trafic entrant IPSEC :

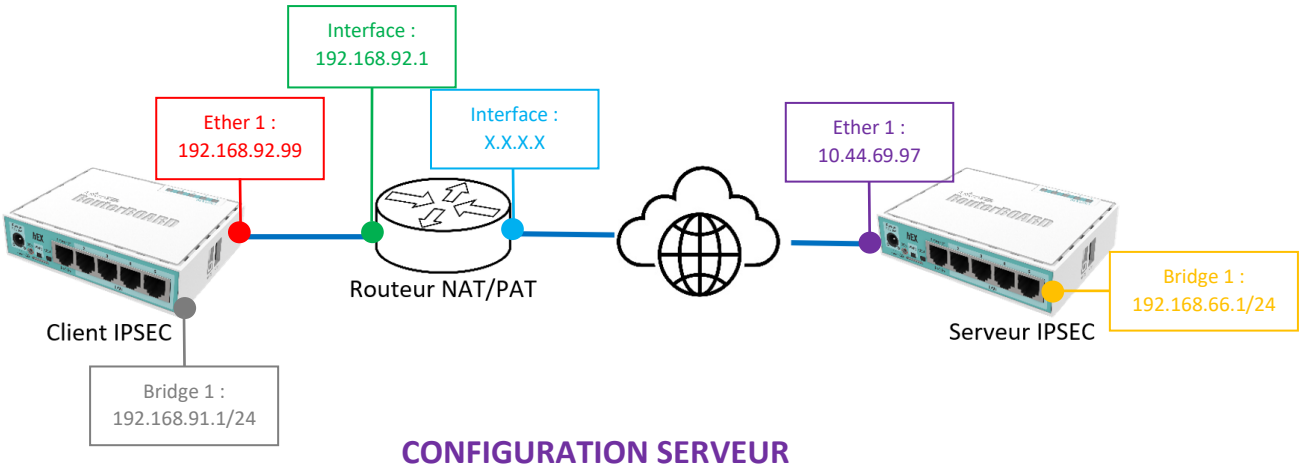
*/ip/firewall/filter add place-before=[find where comment~"defconf: drop all not coming from LAN"] protocol=udp dst-port=500,4500 dst-address=**a.a.a.a** action=accept chain=input comment="Allow UDP 500,4500 IPSec for **a.a.a.a**"*

*/ip/firewall/filter add place-before=[find where comment~"defconf: drop all not coming from LAN"] protocol=ipsec-esp dst-address=**a.a.a.a** action=accept chain=input comment="Allow IPSec-esp for **a.a.a.a**"*

/ip/firewall/filter add place-before=[find where comment~"defconf: drop all not coming from LAN"] protocol=4 dst-address=10.0.88.1 action=accept chain=input comment="Allow ipsec through IpIp tunnel"

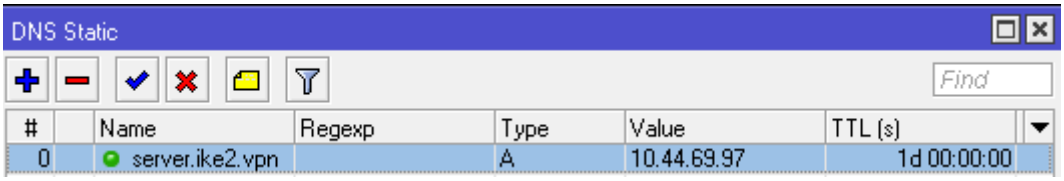
Remplacer **a.a.a.a** par l'IP WAN du routeur, dans le cas où l'IP est obtenue par DHCP, s'assurer qu'elle ne changera pas (bail ou configuration IP statique).

Première typologie : Client(s) derrière du NAT/PAT, et serveur avec IP publique (supposée publique dans l'exemple)



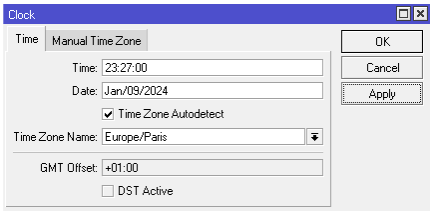
CONFIGURATION SERVEUR

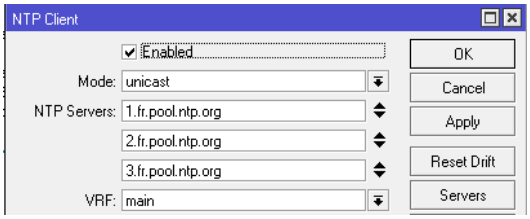
2 - Création du nom DNS du serveur, utiliser une entrée statique ou un service DNS publique.



/ip/dns/static/add name="server.ike2.vpn" address=10.44.69.97

3 - Time zone et NTP

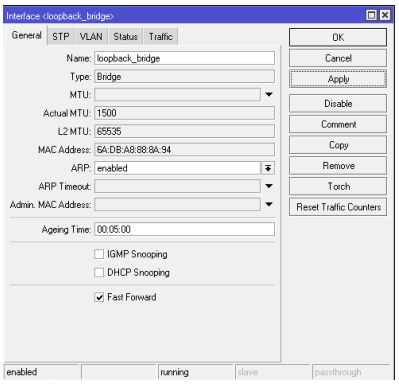




/system/clock/set time-zone-name=Europe/Paris

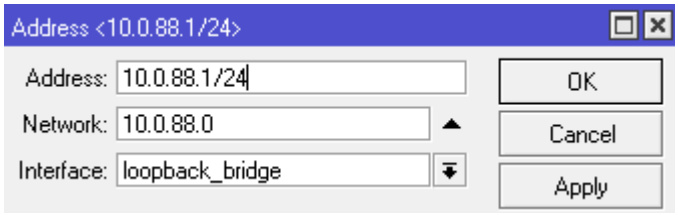
/system/ntp/client/set enabled=yes servers=1.fr.pool.ntp.org,2.fr.pool.ntp.org,3.fr.pool.ntp.org

4 - Création d'un bridge loopback



/interface/bridge add name=bridge-loopback

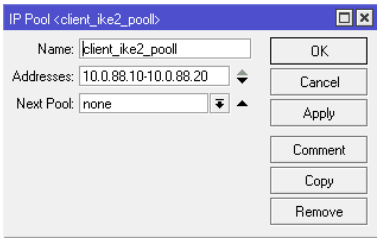
5 - Assignation d'une adresse IP (master IPSEC) à la la loopback



/ip/address/add address=10.0.88.1/24 interface=bridge-loopback network=10.0.88.0

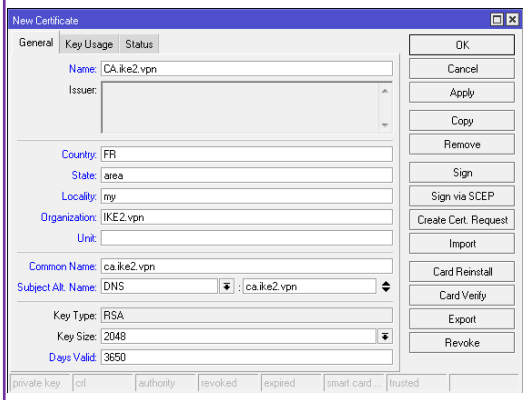
6 - Création d'un pool d'adresses IP pour les clients IPSEC

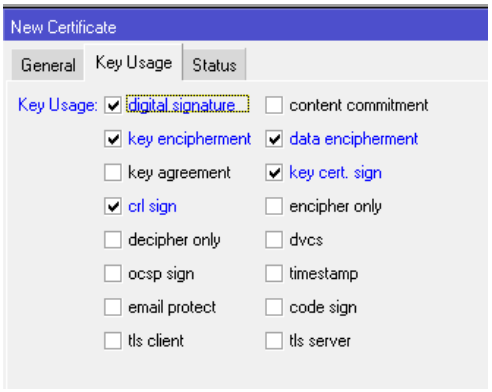
Etape optionnelle car non utile dans cette configuration



/ip/pool/add name=client_ike2_pooll ranges=10.0.88.10-10.0.88.20

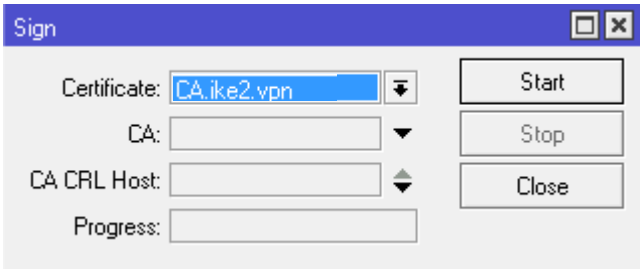
7 - Génération du certificat CA (si non existant)





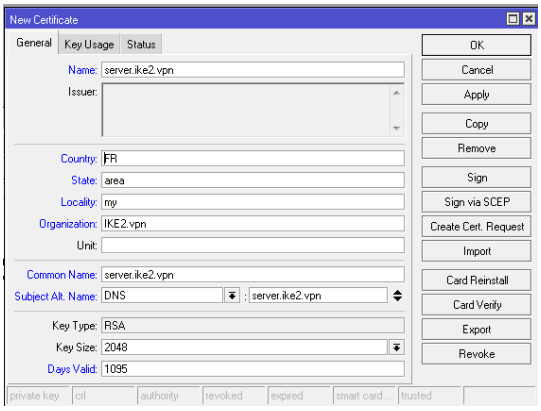
/certificate/add name=CA.ike2.vpn country=FR state=area locality=my organization=IKE2.vpn common-name=ca.ike2.vpn subject-alt-name=DNS:ca.ike2.vpn days-valid=3650 key-usage=digital-signature,key-encipherment,data-encipherment,key-cert-sign,crl-sign

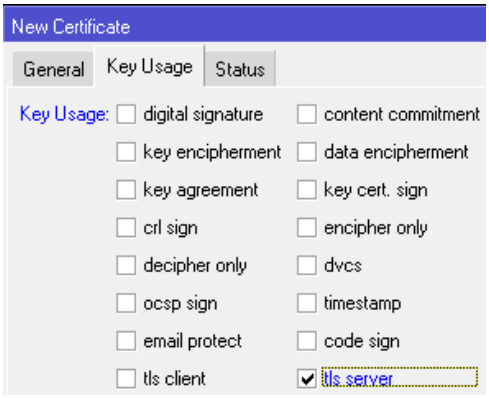
8 - Auto-signature du CA



/certificate/sign CA.ike2.vpn

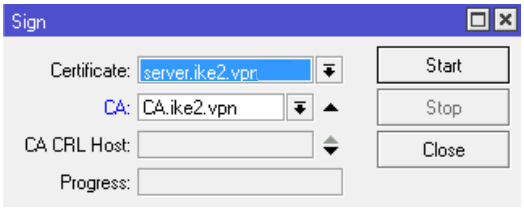
9 - Génération du certificat serveur IPSEC





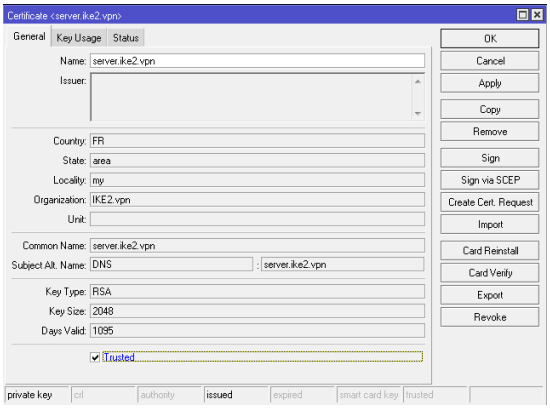
/certificate/add name=server.ike2.vpn country=FR state=area locality=my organization=IKE2.vpn common-name=server.ike2.vpn subject-alt-name=DNS:server.ike2.vpn days-valid=1095 key-usage=tls-server

10 - Signature du certificat serveur par le CA



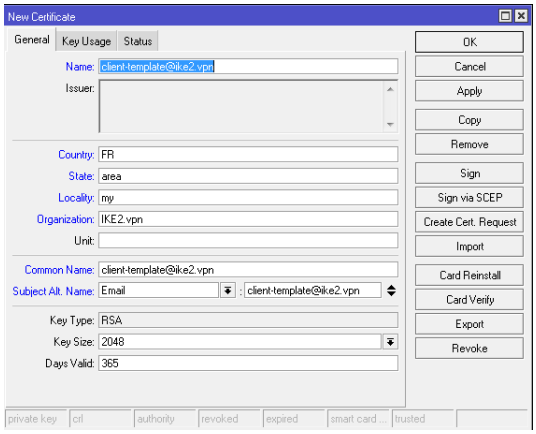
/certificate/sign server.ike2.vpn ca=CA.ike2.vpn

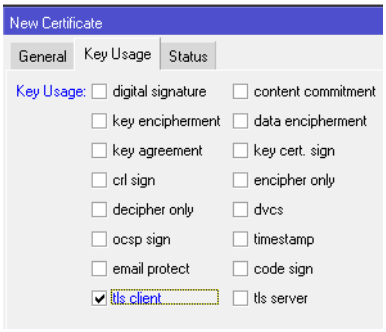
11 - Certificat serveur 'trusted'



/certificate/set server.ike2.vpn trusted=yes

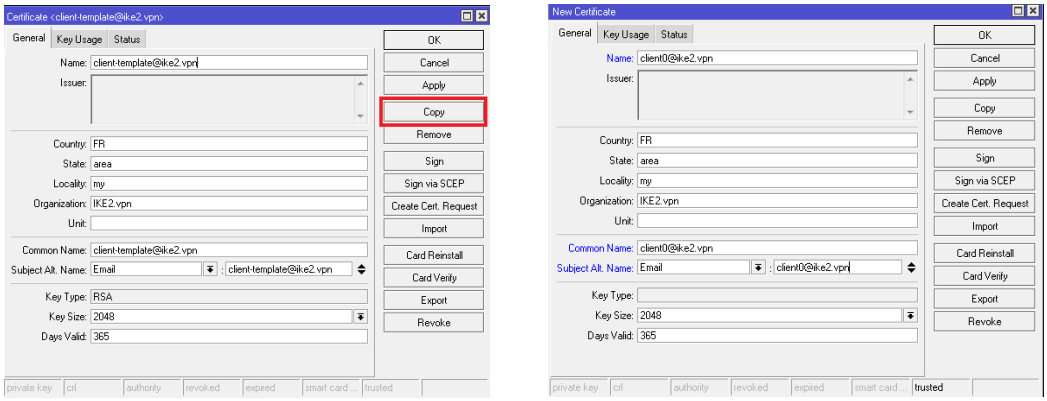
12 - Création d'une template de certificat client





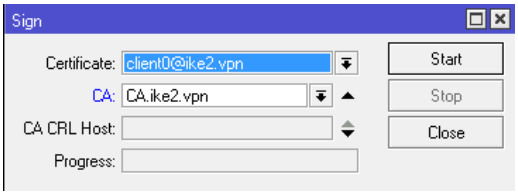
/certificate/add name=client-template@ike2.vpn country=FR state=area locality=my organization=IKE2.vpn common-name=client-template@ike2.vpn subject-alt-name=email:client-template@ike2.vpn key-usage=tls-client

13 - Génération d'un certificat client à partir de la template



/certificate/add copy-from=client-template@ike2.vpn name=client0@ike2.vpn common-name=client0@ike2.vpn subject-alt-name=email:client0@ike2.vpn

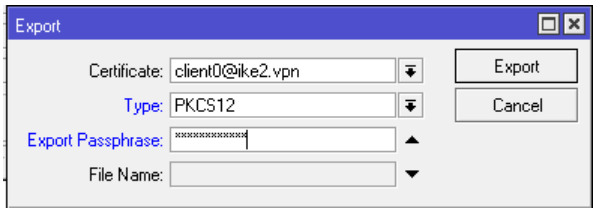
14 - Signature du certificat client par l'autorité de certification (CA)



/certificate/sign client0@ike2.vpn ca=CA.ike2.vpn

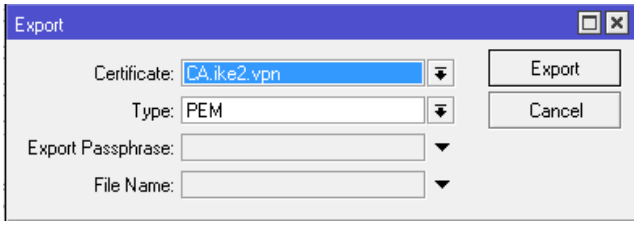
15 - Exportation du certificat client

Si passage par ligne de commande, la ligne est automatiquement effacée après exécution pour ne pas conserver le mot de passe visible dans le terminal



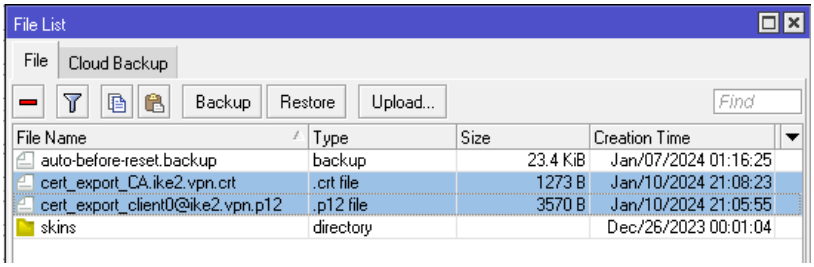
/certificate/export-certificate client0@ike2.vpn type=pkcs12 export-passphrase=password

16 - Exportation du CA

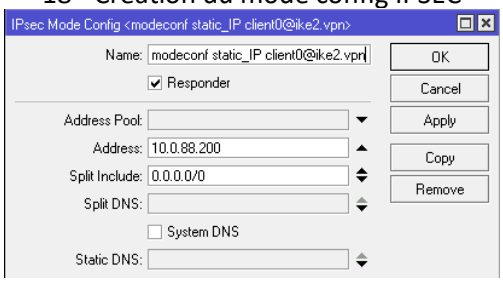


/certificate/export-certificate CA.ike2.vpn type=pem

17 - Exporter les certificats sur la machine en effectuant un "drad and drop" depuis l'onglet 'Files'

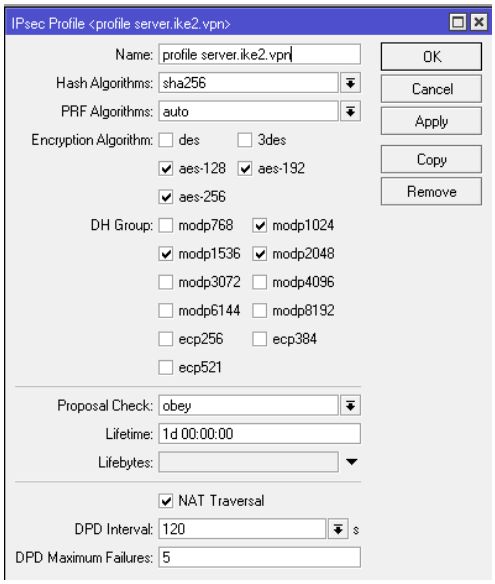


18 - Création du mode config IPSEC



/ip/ipsec/mode-config/add name=modeconf_static-IP_client0@ike2.vpn address=10.0.88.200 split-include=0.0.0.0/0

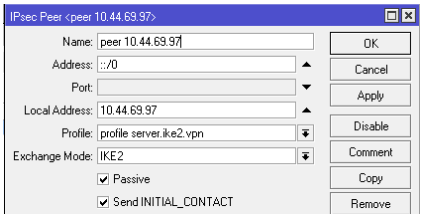
19 - Création d'un peer profile



/ip/ipsec/profile/add name="profile server.ike2.vpn" hash-algorithm=sha256 prf-algorithm=auto enc-algorithm=aes-128,aes-192,aes-256 dh-group=modp1024,modp1536,modp2048 proposal-check=obey nat-traversal=yes

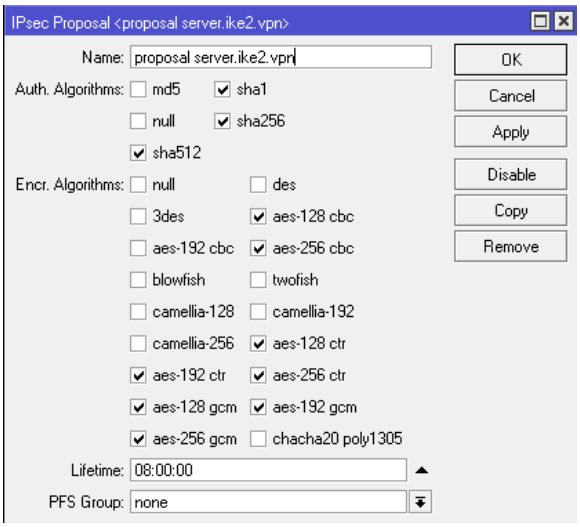
20 - Création d'un peer IPSEC

Accepte toutes les connexions à destination de l'IP de l'interface WAN du routeur



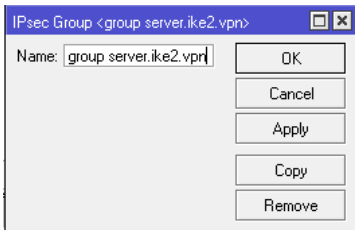
/ip/ipsec/peer/add name="peer 10.44.69.97" address=::/0 local-address=10.44.69.97 profile="profile server.ike2.vpn" exchange-mode=ike2 passive=yes send-initial-contact=yes

21 - Création d'un IPSEC proposal



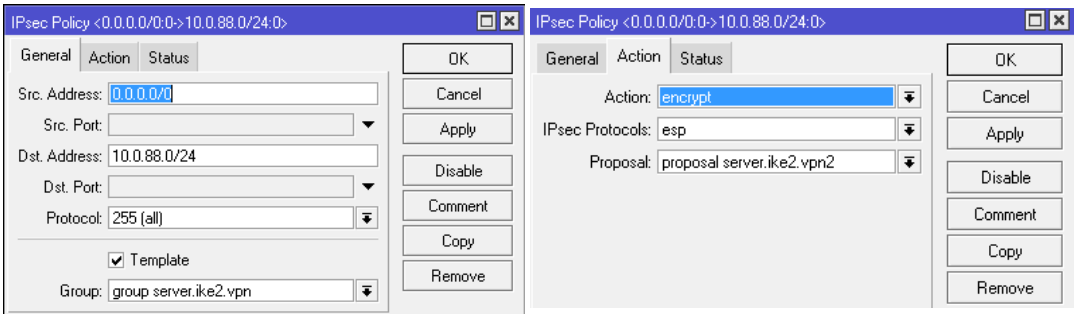
/ip/ipsec/proposal/add name="proposal server.ike2.vpn" auth-algorithms=sha1,sha256,sha512 enc-algorithms=aes-128-cbc,aes-256-cbc,aes-128-ctr,aes-192-ctr,aes-256-ctr,aes-128-gcm,aes-192-gcm,aes-256-gcm lifetime=08:00:00 pfs-group=none

22 - Création d'un groupe IPSEC policy



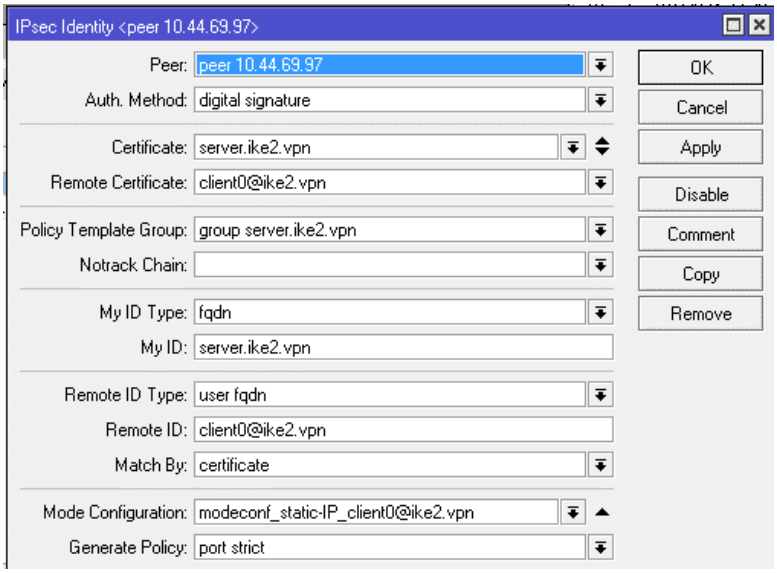
/ip/ipsec/policy/group/add name="group server.ike2.vpn"

23 - Création d'une template de policy



/ip/ipsec/policy/add src-address=::/0 dst-address=10.0.88.0/24 protocol=all template=yes group="group server.ike2.vpn" action=encrypt ipsec-protocols=esp proposal="proposal server.ike2.vpn"

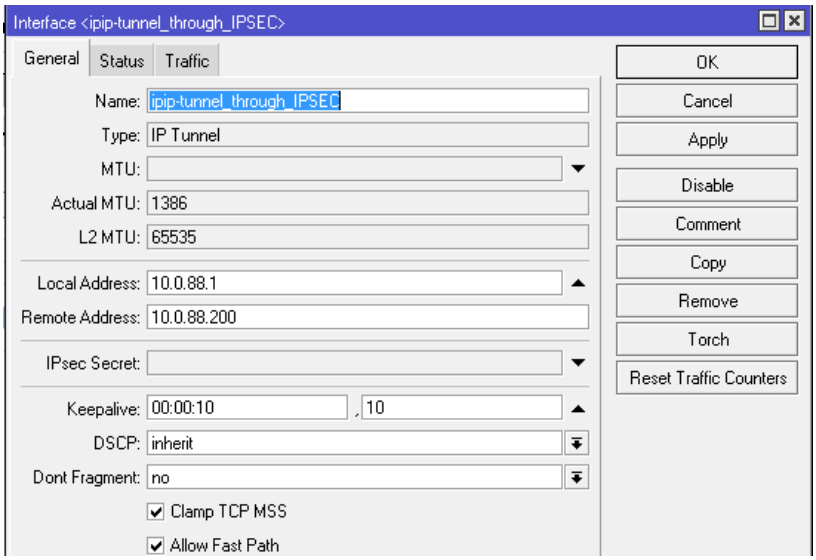
24 - Création d'un identité cliente



/ip/ipsec/identity/add peer="peer 10.44.69.97" auth-method=digital-signature certificate=server.ike2.vpn remote-certificate=client0@ike2.vpn policy-template-group="group server.ike2.vpn" my-id=fqdn:server.ike2.vpn remote-id=user-fqdn:client0@ike2.vpn match-by=certificate mode-config=modeconf_static-IP_client0@ike2.vpn generate-policy=port-strict

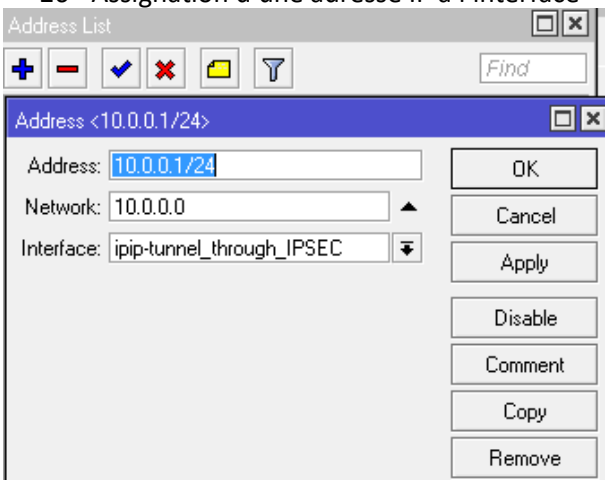
Attention : il a été remarqué dans certains cas qu'il est nécessaire de passer le champ "My ID type" en "auto"

25 - Création d'un tunnel IP-IP afin d'identifier le VPN IPSEC sur une interface



/interface/ipip/add name=ipip-tunnel_through_IPSEC local-address=10.0.88.1 remote-address=10.0.88.200

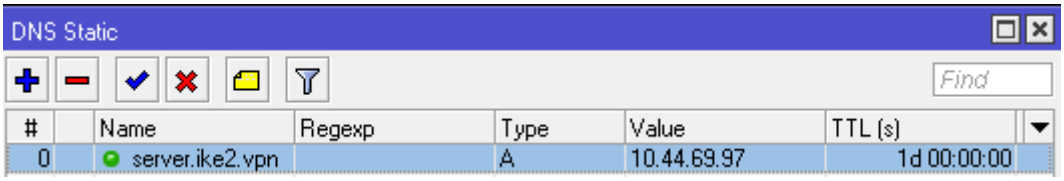
26 - Assignation d'une adresse IP à l'interface



/ip/address/add address=10.0.0.1/24 network=10.0.0.0 interface=ipip-tunnel_through_IPSEC

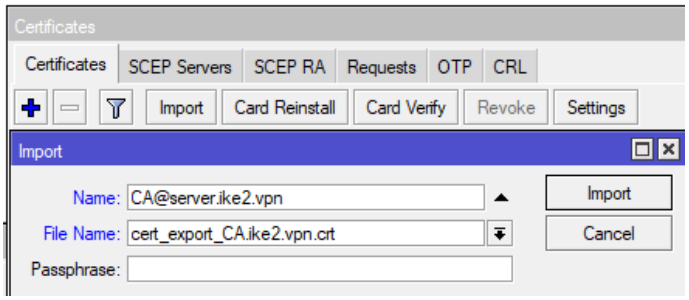
CONFIGURATION CLIENT

27 - Création du nom DNS du serveur, utiliser une entrée statique ou un service DNS publique.



/ip/dns/static/add name="server.ike2.vpn" address=10.44.69.97

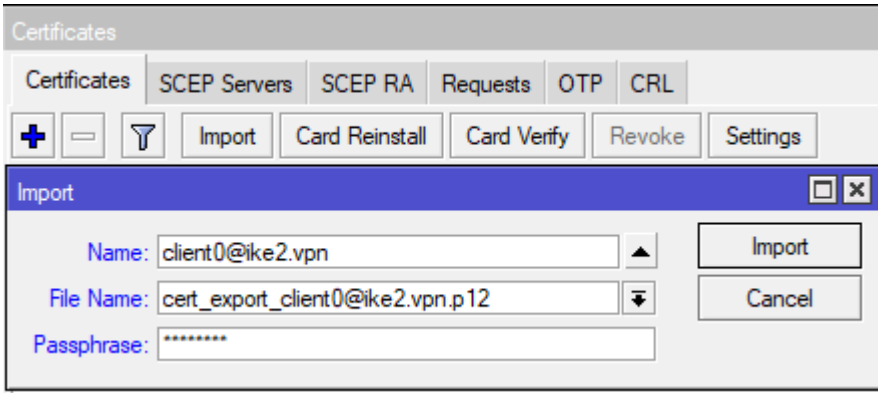
28 - Importation du CA



/certificate/import name=CA@server.ike2.vpn file-name=cert_export_CA.ike2.vpn.crt

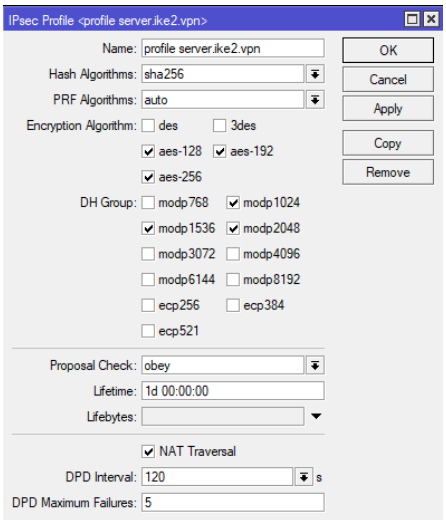
29 - Importation du certificat client, "drag and drop" les fichiers au préalable dans l'onglet 'Files'

Si passage par ligne de commande, la ligne est automatiquement effacée après exécution pour ne pas conserver le mot de passe visible dans le terminal



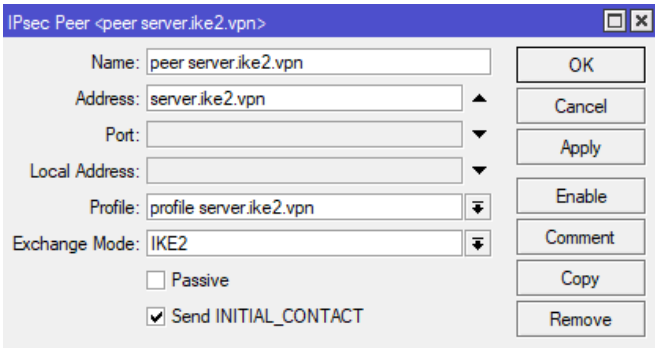
/certificate/import name=client0@ilke2.vpn file-name=cert_export_client0@ike2.vpn.p12 passphrase=password

30 - Création d'un peer profile



/ip/ipsec/profile/add name="profile server.ike2.vpn" hash-algorithm=sha256 prf-algorithm=auto enc-algorithm=aes-128,aes-192,aes-256 dh-group=modp1024,modp1536,modp2048 proposal-check=obey nat-traversal=yes

31 - Ajout d'un peer IPSEC

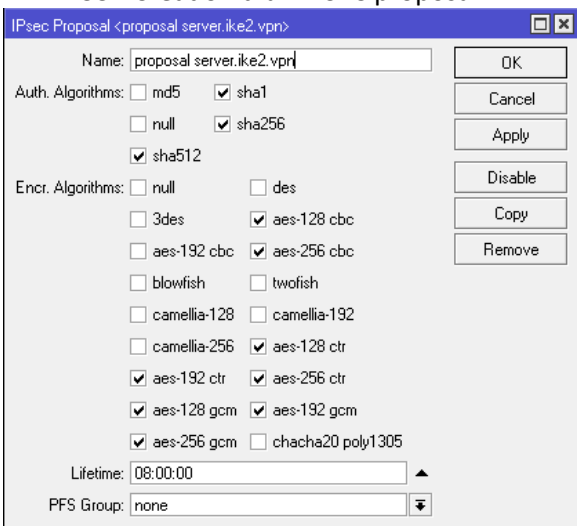


/ip/ipsec/peer/add name="peer server.ike2.vpn" address=server.ike2.vpn profile="profile server.ike2.vpn" exchange-mode=ike2 send-initial-contact=yes

32 - Création d'un groupe IPSEC policy

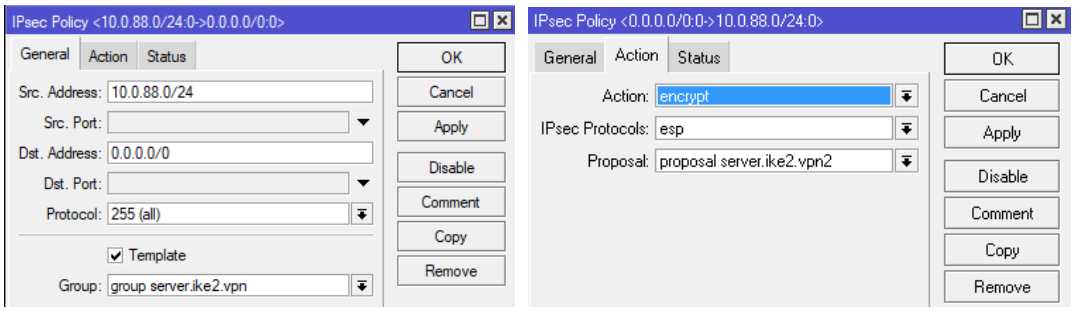
/ip/ipsec/policy/group/add name="group server.ike2.vpn"

33 - Création d'un IPSEC proposal



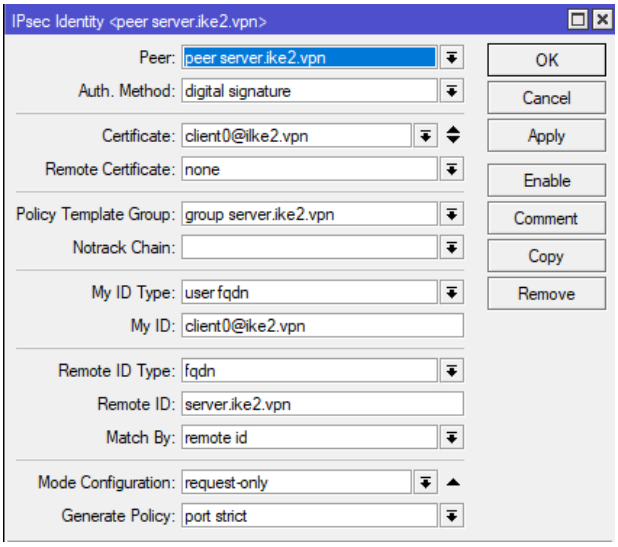
/ip/ipsec/proposal/add name="proposal server.ike2.vpn" auth-algorithms=sha1,sha256,sha512 enc-algorithms=aes-128-cbc,aes-256-cbc,aes-128-ctr,aes-192-ctr,aes-256-ctr,aes-128-gcm,aes-192-gcm,aes-256-gcm lifetime=08:00:00 pfs-group=none

34 - Création d'une template de policy



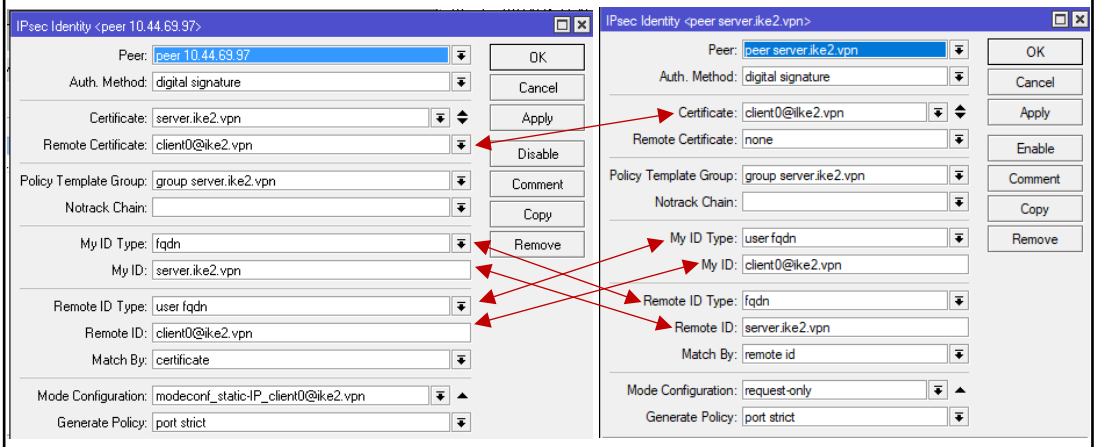
/ip/ipsec/policy/add src-address=10.0.88.0/24 dst-address=::/0 protocol=all template=yes group="group server.ike2.vpn" action=encrypt ipsec-protocols=esp proposal="proposal server.ike2.vpn"

35 - Création de l'identité cliente



/ip/ipsec/identity/add peer="peer server.ike2.vpn" auth-method=digital-signature certificate=client0@ilke2.vpn remote-certificate=none policy-template-group="group server.ike2.vpn" my-id=user-fqdn:client0@ike2.vpn remote-id=fqdn:server.ike2.vpn match-by=remote-id mode-config=request-only generate-policy=port-strict

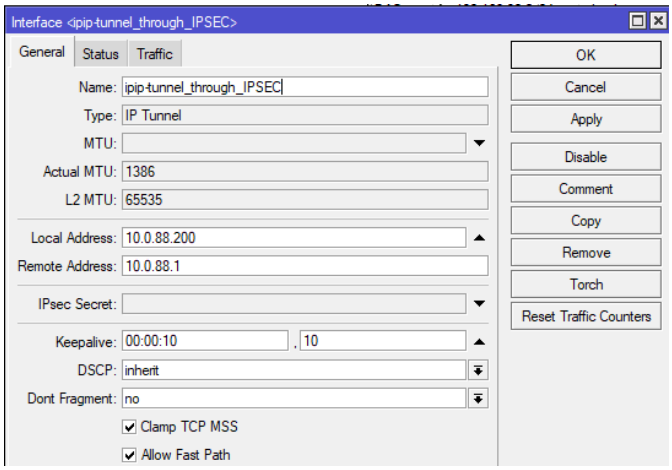
36 - Vérification croisée entre l'identité créée sur le serveur et sur le client



SERVEUR CLIENT

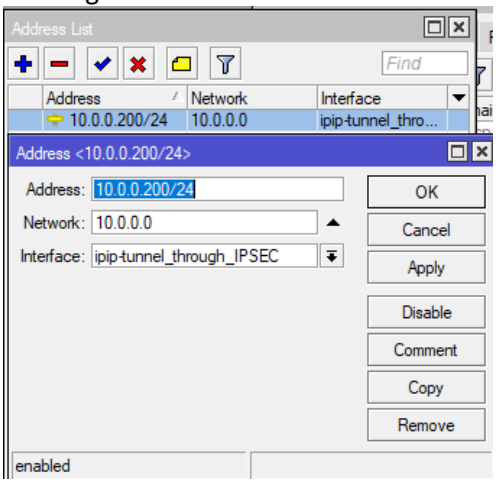
Attention : il a été remarqué dans certains cas qu'il est nécessaire de passer, sur le serveur, le champ "My ID type" en "auto"

37 - Création d'un tunnel IP-IP afin d'identifier le VPN IPSEC sur une interface



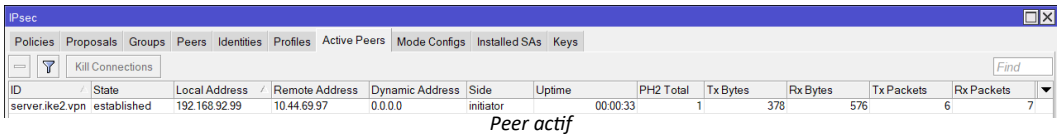
/interface/ipip/add name=ipip-tunnel_through_IPSEC local-address=10.0.88.200 remote-address=10.0.88.1

38 - Assignation d'une adresse IP à l'interface

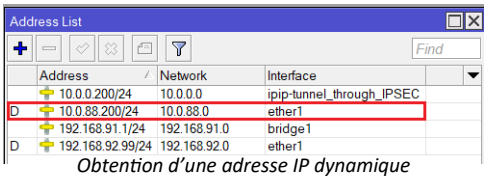


/ip/address/add address=10.0.0.200/24 network=10.0.0.0 interface=ipip-tunnel_through_IPSEC

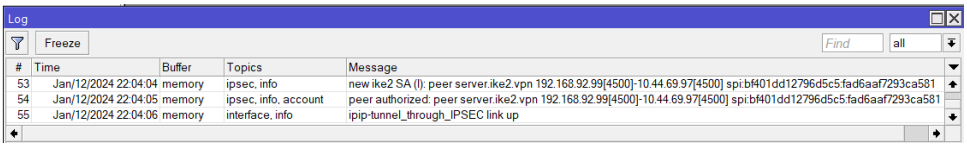
39 - Vérification de l'établissement de la liaison IPSEC



Peer actif

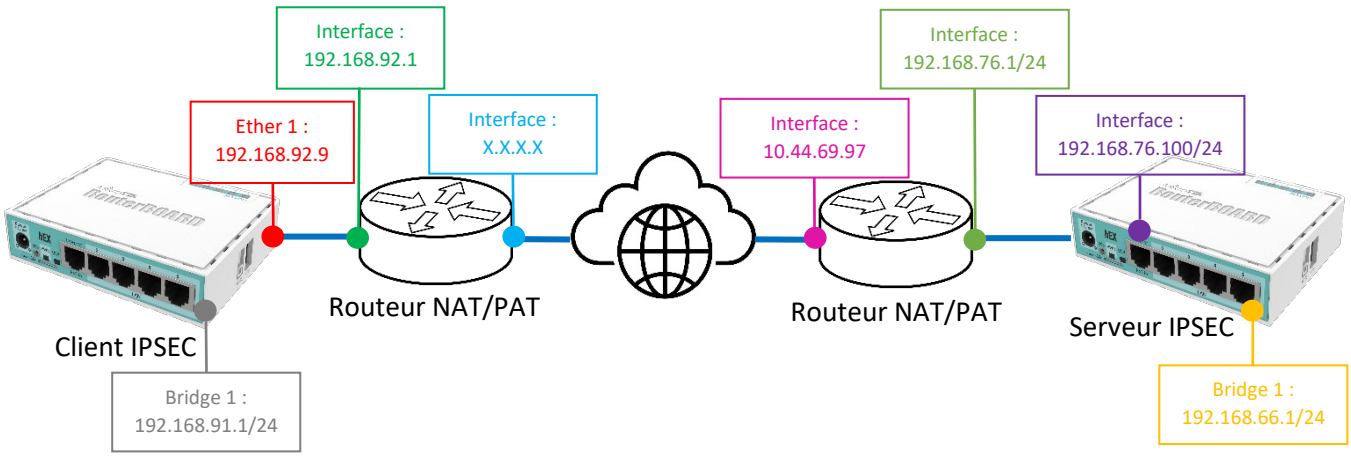


Obtention d'une adresse IP dynamique



Peer actif, tunnel ipip monté

Deuxième typologie : Client et serveur derrière des routeurs NAT/PAT

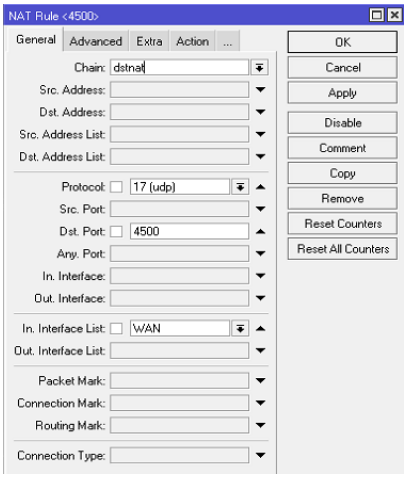


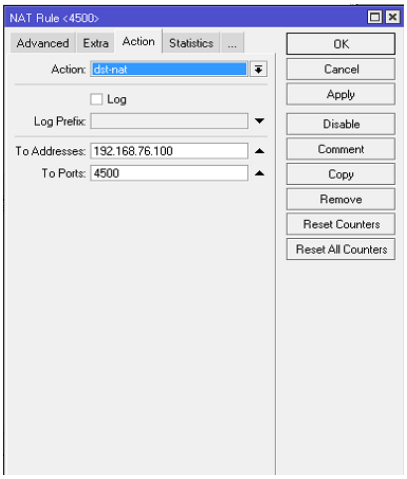
Dans cette typologie, la configuration consiste à modifier celle mise en place dans le cas de la première typologie.

NB : Il est nécessaire de pouvoir faire du dst-nat (redirection de port) sur le routeur NAT/PAT en amont du serveur IPSEC. Il n'est pas forcément nécessaire que ce routeur soit un Mikrotik. Une box Internet fournie par un FAI a la capacité de supporter cette configuration

40 - Configuration du dest-nat

La configuration est montrée ici sur un routeur Mikrotik, mais peut être appliquée sur tout type de routeur.



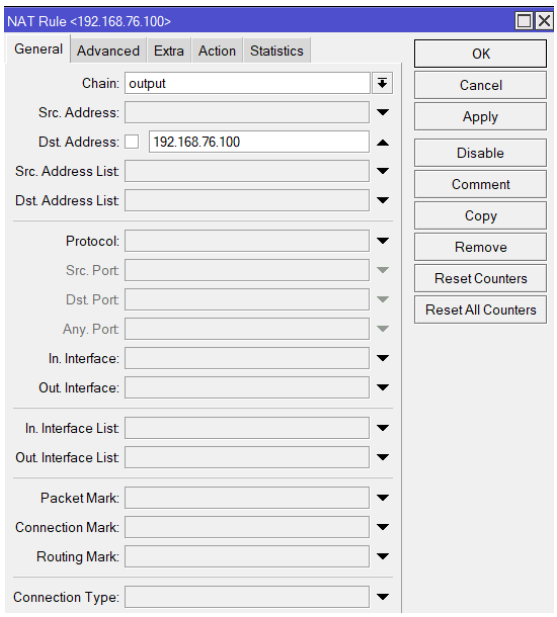


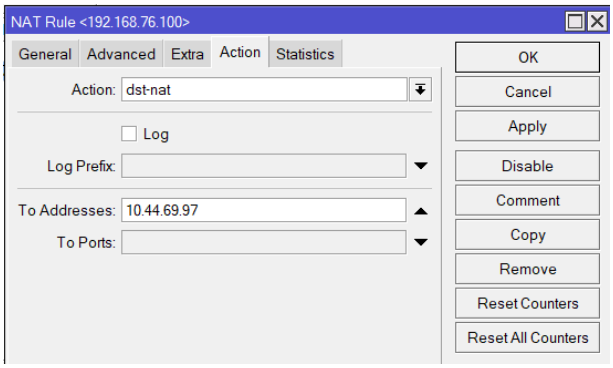
/ip/firewall/nat/add chain=dstnat protocol=udp dst-port=4500 in-interface-list=WAN action=dst-nat to-addresses=192.168.76.100 to-ports=4500

Pour le reste de la configuration, répéter les mêmes étapes que pour la première section **mais** appliquer ces modifications :

- A toutes les étapes nécessaires, associer le nom DNS du serveur VPN à l'adresse IP de son interface WAN (ici : 192.168.76.100)
- A l'étape 20, remplacer l'IP 10.44.69.97 par 192.168.76.100 (IP de l'interface WAN du serveur IPSEC)
- A l'étape 24, utiliser le peer "peer 192.168.76.100" précédemment créé
- Suivre les étapes ci-dessous

41 – Dest-NAT en sortie du routeur client





/ip/firewall/nat/add chain=output dst-address=192.168.76.100 action=dst-nat to-addresses=10.44.69.98

Vérifier à présent que la connexion est établie.

----------FIN DE LA CONFIGURATION IPSEC----------

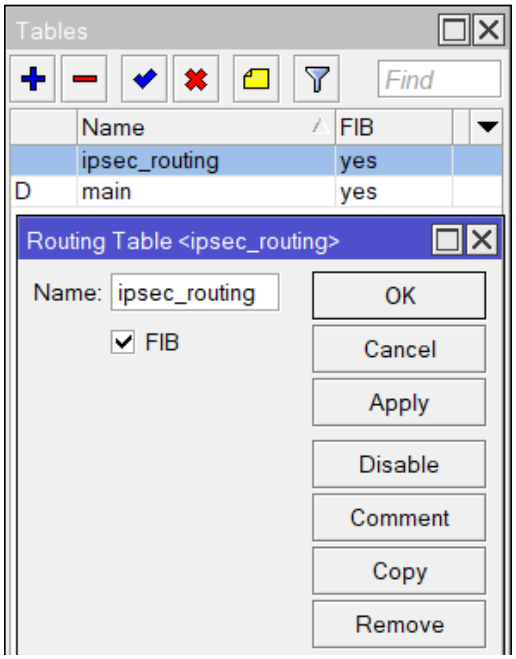
A partir de là, il est possible de créer une route statique pour joindre le réseau du serveur à travers le lien IPSC en utilisant le tunnel ipip.
Il est également possible de mettre en place du routage dynamique sur cette interface.

Dans le cas où l'on veut rediriger tout le trafic dans le lien IPSEC, il y a deux possibilités :

- VRF : assigner le bridge et le lien IPSEC à une VRF, créer la route par défaut dans la table de routage de la VRF (solution non traitée ici).
- Routing rule : créer une table de routage sous un nom différent que celle par défaut, y placer des routes, créer des règles de routage associées qui sélectionnent la table de routage précédemment créée.

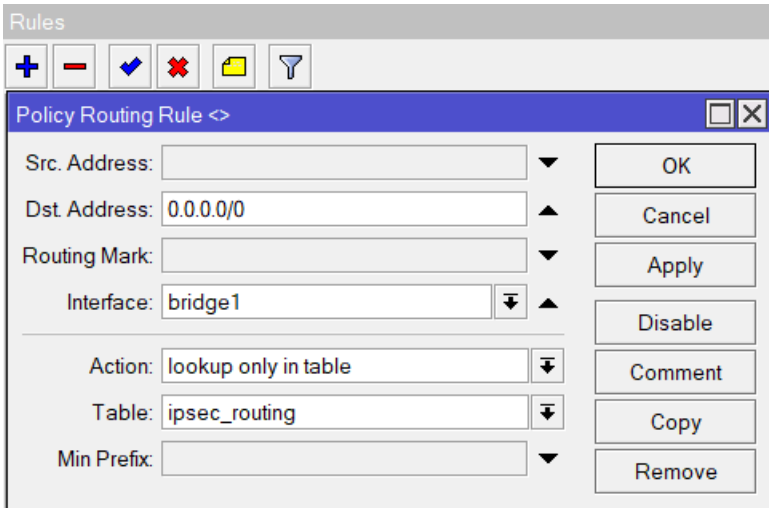
----------DEBUT DE LA CONFIGURATION DE ROUTAGE----------

42 – Création d'une nouvelle table de routage



/routing/table/add name=ipsec_routing fib

43 – Ajout d'une règle de routage

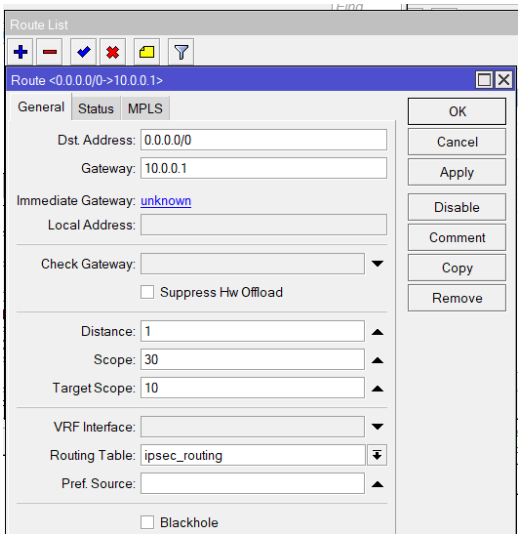


/routing/rule/add dst-address=0.0.0.0/0 interface=bridge action=lookup-only-in-table table=ipsec_routing

44 – Ajout d'une route par défaut

dst-address=0.0.0.0/0 ==> route par défaut
gateway=10.0.0.1 ==> interface du tunnel ipip côté serveur IPSEC

routing-table=ipsec_routing ==> table de routage précédemment créée



/ip/route/add dst-address=0.0.0.0/0 gateway=10.0.0.1 distance=1 scope=30 target-scope=10 routing-table=ipsec_routing

A présent, tout le trafic arrivant du LAN du client IPSEC est transféré dans le lien IPSEC via le tunnel ipip. Le serveur IPSEC se charge ensuite du routage.

----------FIN DE LA CONFIGURATION DE ROUTAGE----------