GIGACLOUD

Тунель IPSec VPN між роутерами в E-CLoud і S-CLoud 2.0

Посібник користувача послугою

версія 1.1 5_2021

03022, Україна, м. Київ,
вул. Васильківська, 37-В

+38 (044) 233-71-70
sales@gigacloud.ua

www.gigacloud.ua

Зміст

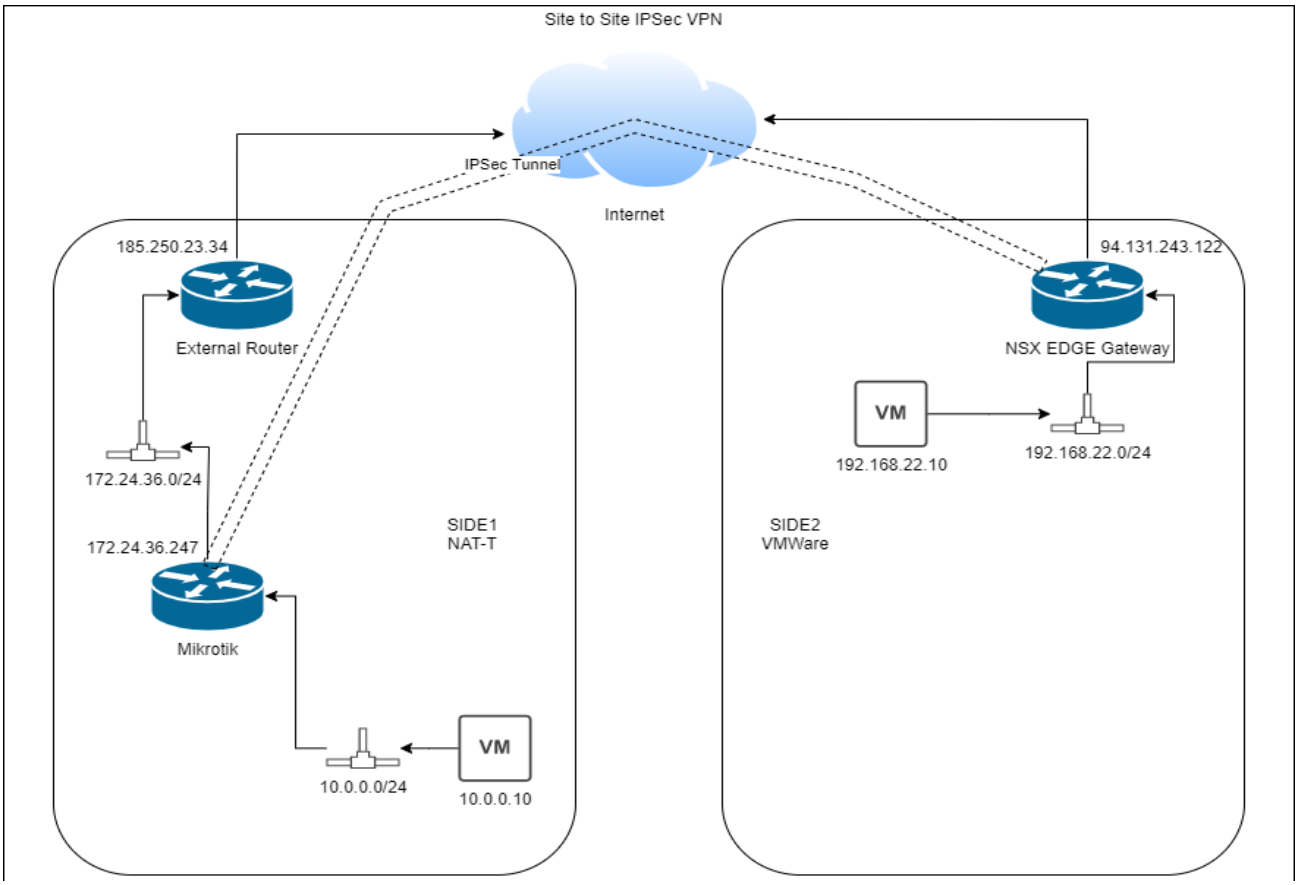
Терміни та визначення 3
Тунель IPSec VPN між проектами у різних хмарах GigaCloud 4
Налаштування програмного роутера MikroTik у хмарі OpenStack 5
Налаштування NSX EDGE Gateway в хмарі VMWare 11
Перевірка працездатності тунелю IPSec VPN 13

Терміни та визначення

VPN	Virtual Private Network – позначення технологій для створення приватної віртуальної мережі, що забезпечують захищене з'єднання між її вузлами з використанням «на нижчому рівні» транспортних протоколів публічних, загальнодоступних мереж Інтернет
IPsec	IP Security – набір протоколів для забезпечення захисту даних під час передачі засобами IP (аутентифікація, перевірка цілісності, шифрування IP-пакетів)
Хмара, хмарна інфраструктура	Модель надання доступу через канали зв'язку до розподілених обчислювальних ресурсів, віртуальних мереж і систем зберігання даних, із можливістю гнучкої зміни конфігурації та масштабування за запитом
OpenStack	Комплекс проектів вільного програмного забезпечення (**ПЗ**) із відкритим вихідним кодом (за моделлю Open Source), призначений для побудови приватних або публічних обчислювальних хмар і хмарних сховищ, поєднаних мережами
Project (Проект)	Віртуальна інфраструктура в межах хмари, обмежена квотами користувача на ресурси
IaaS (Публічна хмара)	Пул ресурсів провайдера з доступом через Інтернет, що розподіляється між Клієнтами (згідно їх замовленої квоти на умовах оренди) з метою: ▪ створення віртуальних серверів і сховищ; ▪ поєднання їх мережами між собою та з Інтернетом; ▪ розгортання на них операційних систем із клієнтськими застосунками
vCloud Director	Платформа управління **VMWare**, що дозволяє створювати ізольовані віртуальні інфраструктури та керувати доступами до них
Платформа NSX	Платформа віртуалізації мережі у **хмарі E-Cloud**, що відтворює мережеву інфраструктуру програмними засобами
Edge Gateway (Віртуальний роутер)	Рішення від компанії VMWare, що дозволяє налаштувати мережеві сервіси (NAT, VPN, Firewall, DHCP та ін.) у хмарі E-Cloud

Тунель IPSec VPN між проектами у різних хмарах GigaCloud

Приклад організації **тунелю IPSec VPN** між маршрутизаторами (роутерами) **MikroTik** у проекті S-Cloud 2.0 (OpenStack) та **NSX EDGE Gateway в хмарі E-Cloud (VMWare)** наведено нижче:



Віртуальні сервери та інфраструктура кожного з проектів знаходяться «за NAT». На кожному боці IPSec-тунелю (Side «A» хмари S-Cloud 2.0 та Side «B» хмари E-Cloud) існує своя приватна локальна мережа інфраструктури проекту, підключена до власного роутера:

- 10.0.0.0/24 **для Side «A»**, де програмний роутер **MikroTik знаходиться «за NAT-T»**;
- 192.168.22.0/24 **для Side «B»**, де роутер **EDGE безпосередньо використовує публічну (так звану «білу») IP-адресу для виходу до Інтернету**.

Увага! Для встановлення VPN-з'єднання потрібно забезпечити ряд обов'язкових вимог (одночасно на обох боках тунелю).

Найперше, **має бути забезпечена мережева доступність між роутерами**, за протоколами:

- UDP, port 500 (for IKE, to manage encryption keys);
- UDP, port 4500 (for IPSec NAT-Traversal mode);
- ESP, value 50 (for IPSec);
- AH, value 51 (for IPSec).

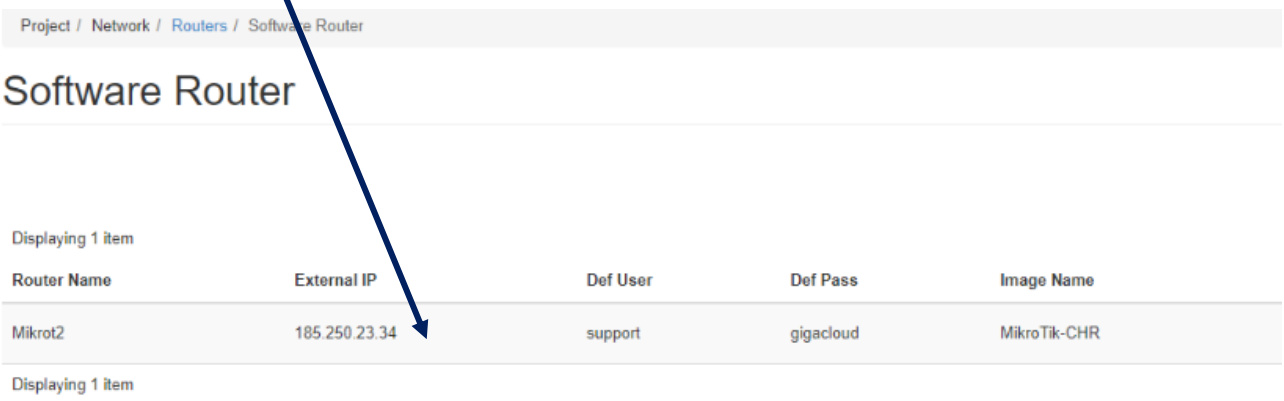
По-друге, **правила файєрволов не повинні блокувати мережевий трафік** між маршрутизаторами (роутерами) та приватними підмережами.

Наступне, **приватні локальні мережі, що будуть поєднані засобами IPSec – мають бути різними** (також, жодна з них не може бути частиною (підмережею) другої мережі).

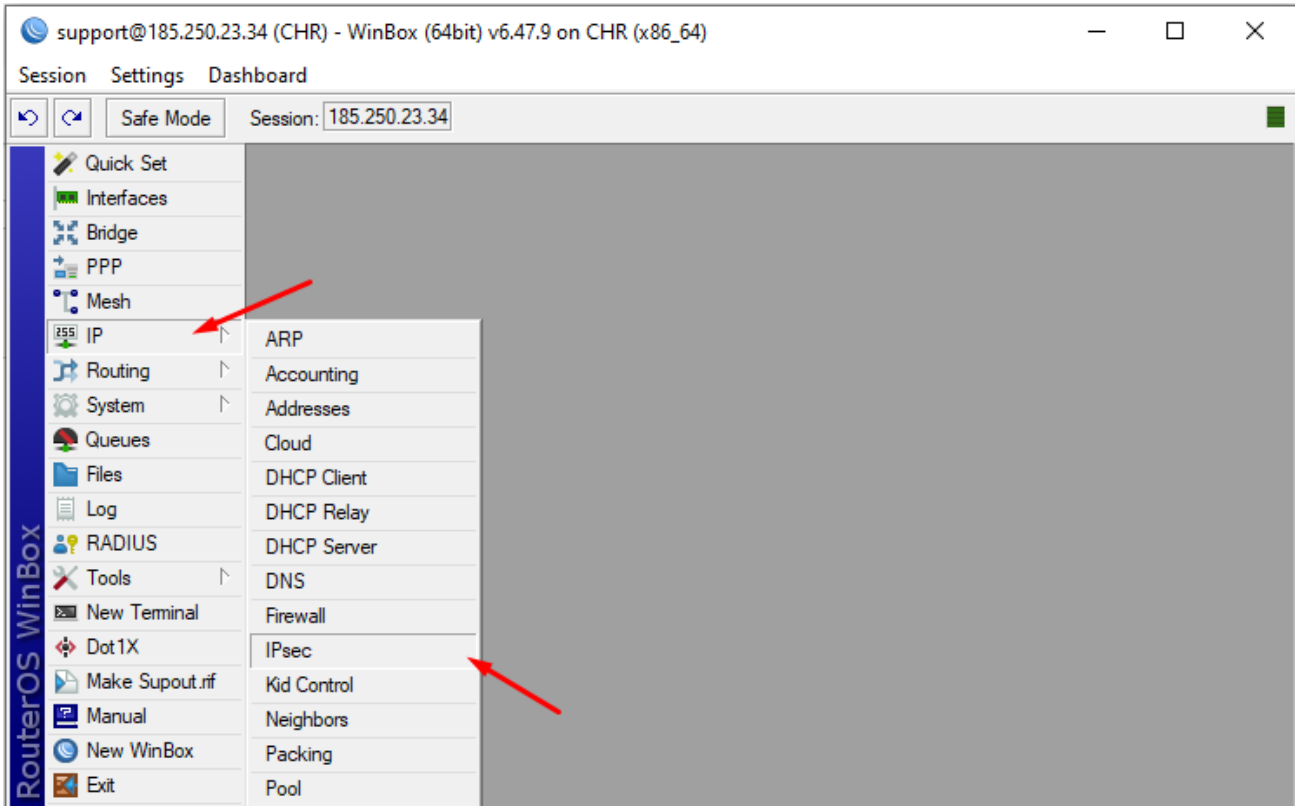
Налаштування програмного роутера MikroTik у хмарі OpenStack

Для налаштувань програмного роутера MikroTik вашого проекту в хмарі S-Cloud 2.0, користуйтесь фірмовою програмною утилітою **Winbox** https://mikrotik.com/download.

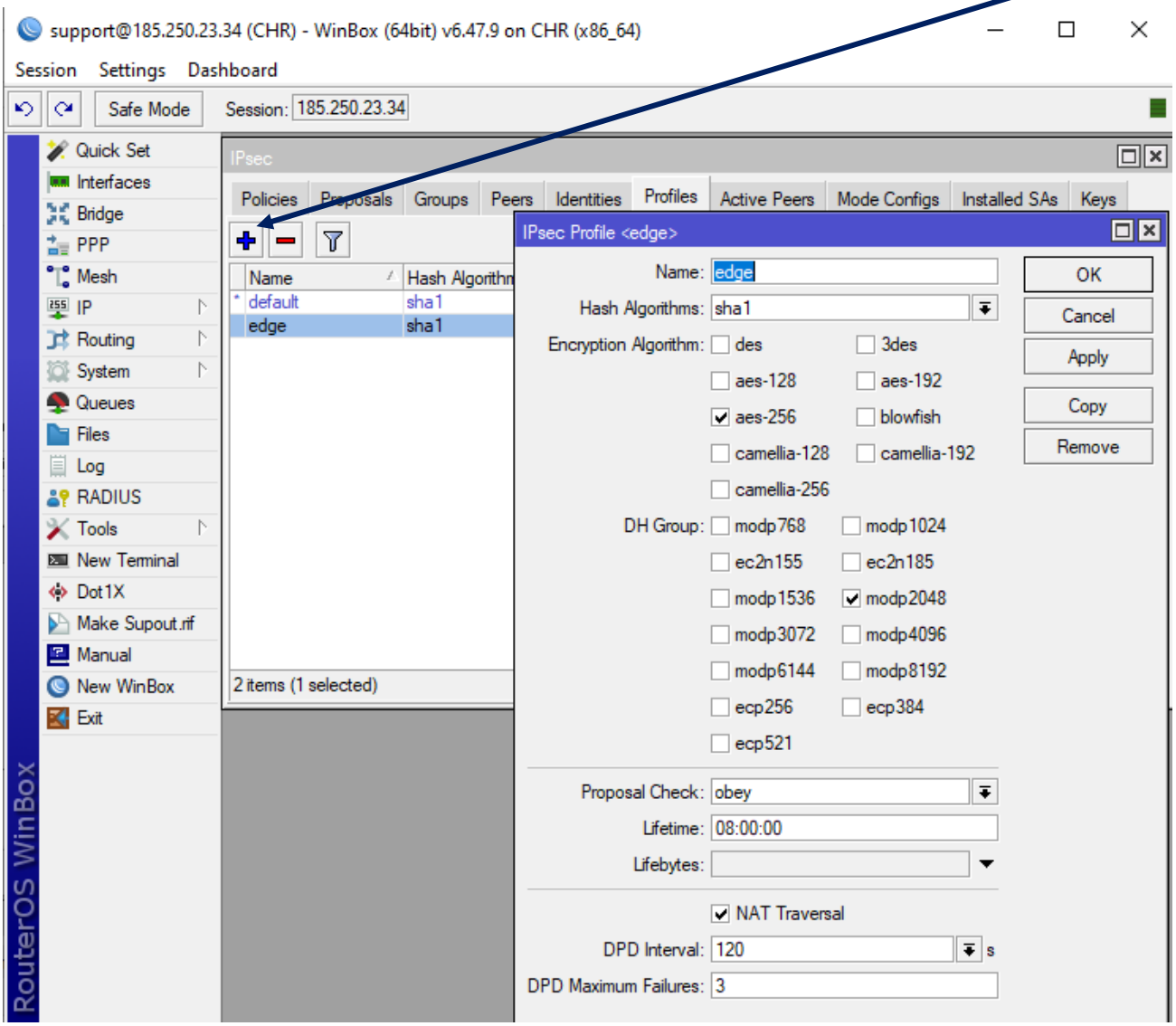
Увага! Під час авторизації у програмі **Winbox** (поля «**Connect to/Login/Password**»), використовуйте відповідні значення параметрів у полі вкладки «**Project –> Network –> Routers –> Software Router**» (див. стор. 7 Посібника користувача програмного роутера MikroTik у хмарі S-CLoud 2.0):



Виконайте послідовність налаштувань у розділі меню **«IP –> IPsec»** утиліти **Winbox:**



Додайте новий профіль натисканням на позначку «**+**» вкладки «**Profiles**» в екранному вікні «**IPsec**» (у наведеному нижче прикладі новому **IPsec Profile** призначено назву «**edge**»):



Увага! Надзвичайно важливо, щоб параметри шифрування SHA та AES співпадали на обох боках безпечного IPSec VPN тунелю.

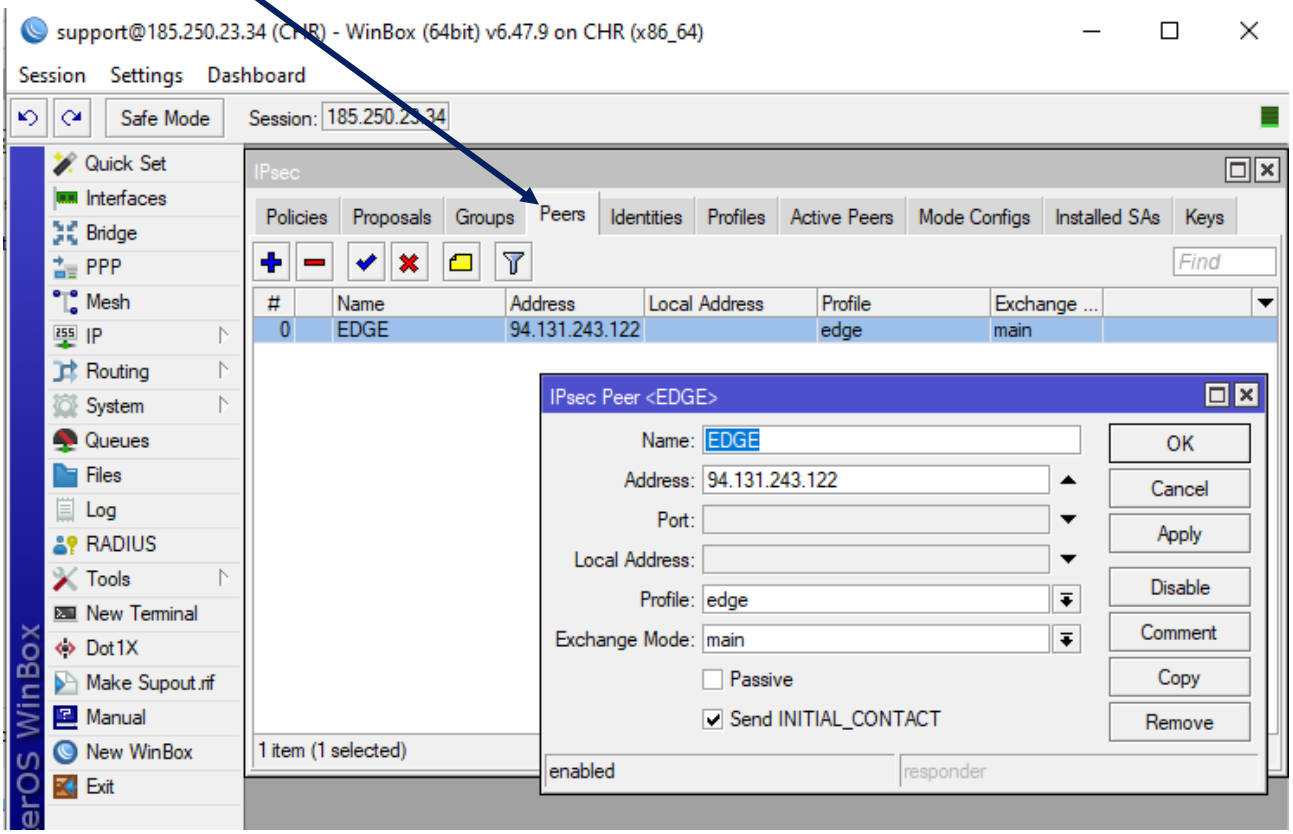
Значення інших параметрів у наведеному прикладі:

- **modp2048** для роутера MikroTik – відповідає **DH Group 14** для роутера EDGE;
- час існування тунелю **Lifetime** – дорівнює 8 годинам.

Важливо мати на увазі: технології IPSec використовують протоколи мережевого рівня, **не зумісні з механізмом трансляції IP-адрес NAT**. Вирішенням проблеми є технологія **NAT-T** (**NAT Traversal** – розширення в IKE та частина IKEv2), тобто додаткова **інкапсуляція пакетів IPSec в UDP** пакети, які коректно обробляються NAT.

Увага! Обов'язково встановіть позначку ☑ у полі «NAT Traversal» екранної форми «IPsec Profile» (оскільки [роутер MikroTik знаходиться «за NAT»](#)).

Додайте новий вузол **Peer** (для з'єднання «точка–точка») натисканням на позначку «**+**» вкладки «**Peers**»:

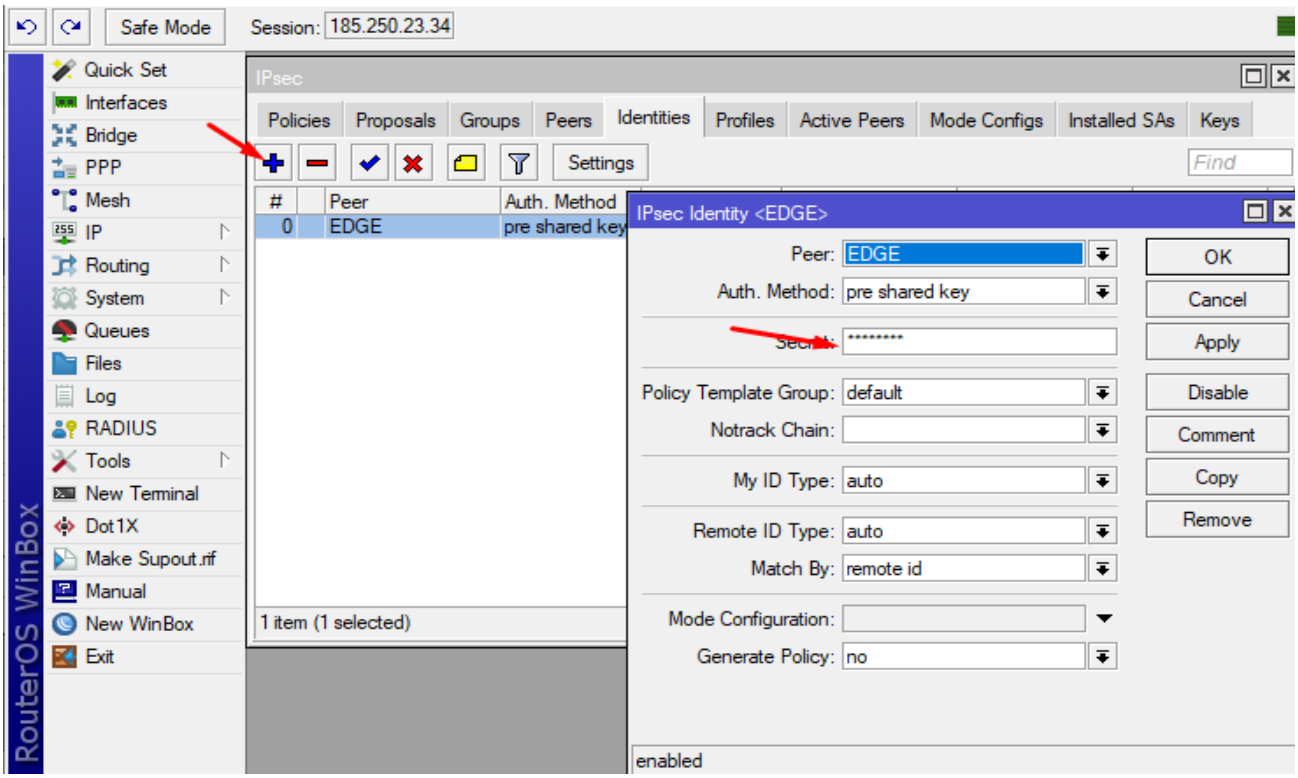


Заповніть поля форми «**IPsec Peer**» або оберіть необхідні значення з переліку:

- **Name** – найменування (у наведеному прикладі новому вузлу IPsec Peer призначено назву «**EDGE**»);
- **Address** – публічна (зовнішня, так звана «біла») IP-адреса віддаленого **Peer** (роутера EDGE вашого проекта у хмарі E-Cloud);
- **Profile** – створений попередньо профіль «**edge**»;
- **Exchange mode** – оберіть «**main**» для використання IKEv1.

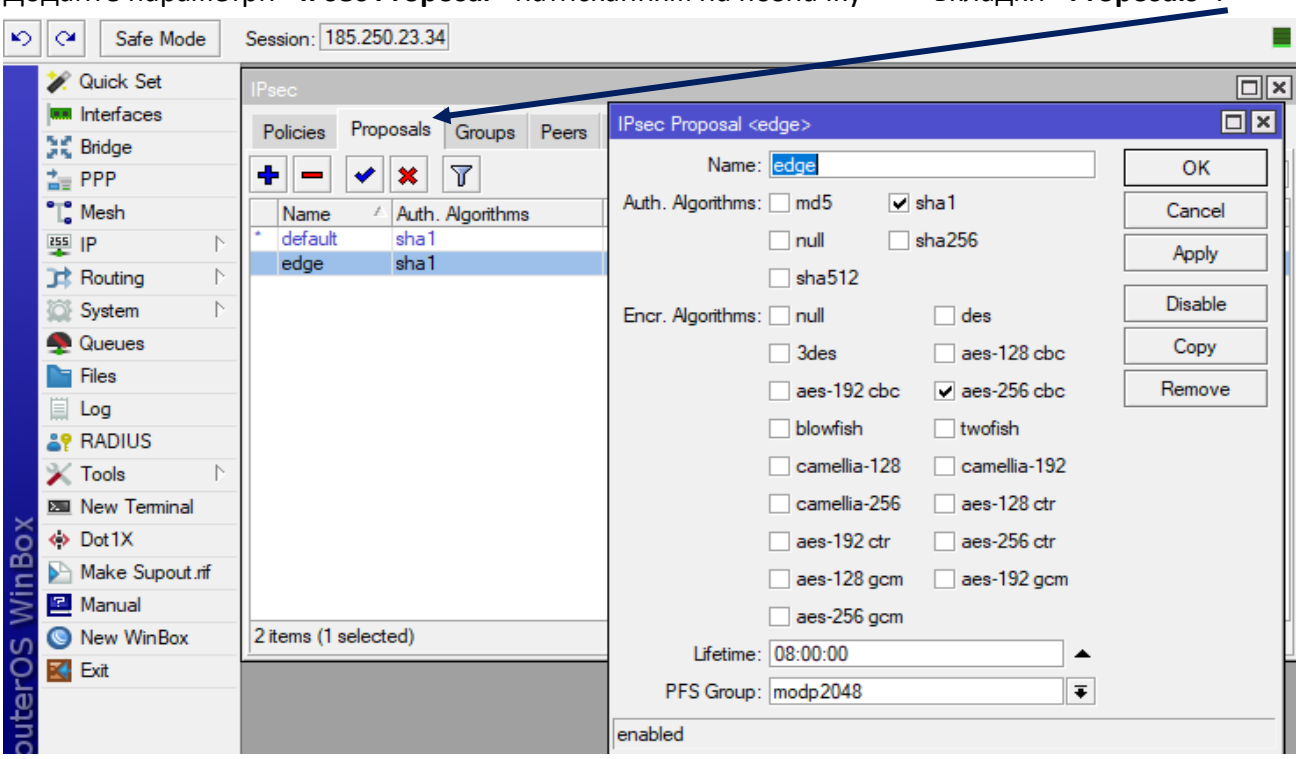
Додайте параметри ідентифікації натисканням на позначку «**+**» вкладки «**Identities**».

Заповніть обов’язкові поля форми «**IPsec Identity**» або оберіть необхідні значення з переліку:



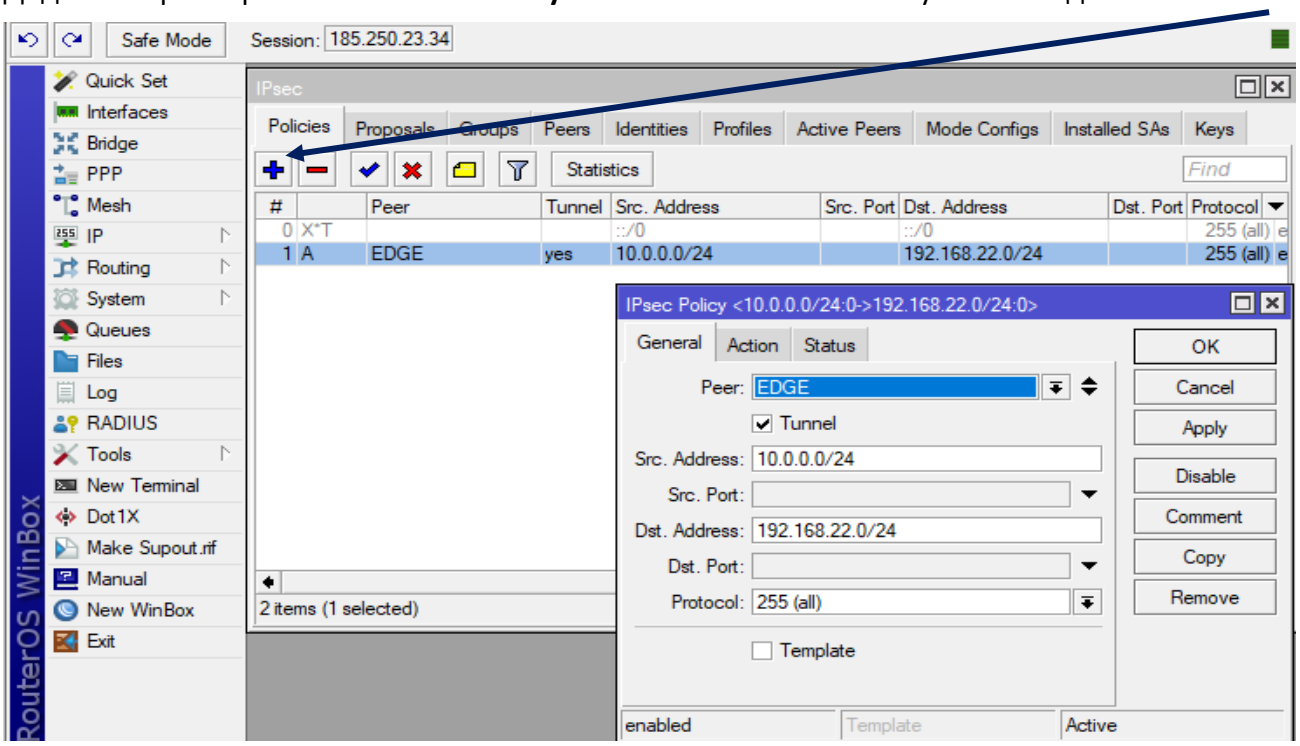
Встановіть значення ключа Pre Shared Key (відповідно до значення на іншому боці тунелю).

Додайте параметри «**IPsec Proposal**» натисканням на позначку «**+**» вкладки «**Proposals**»:



Параметри AES, SHA, Modp (DH Group) мають відповідати параметрам на іншому боці тунелю).

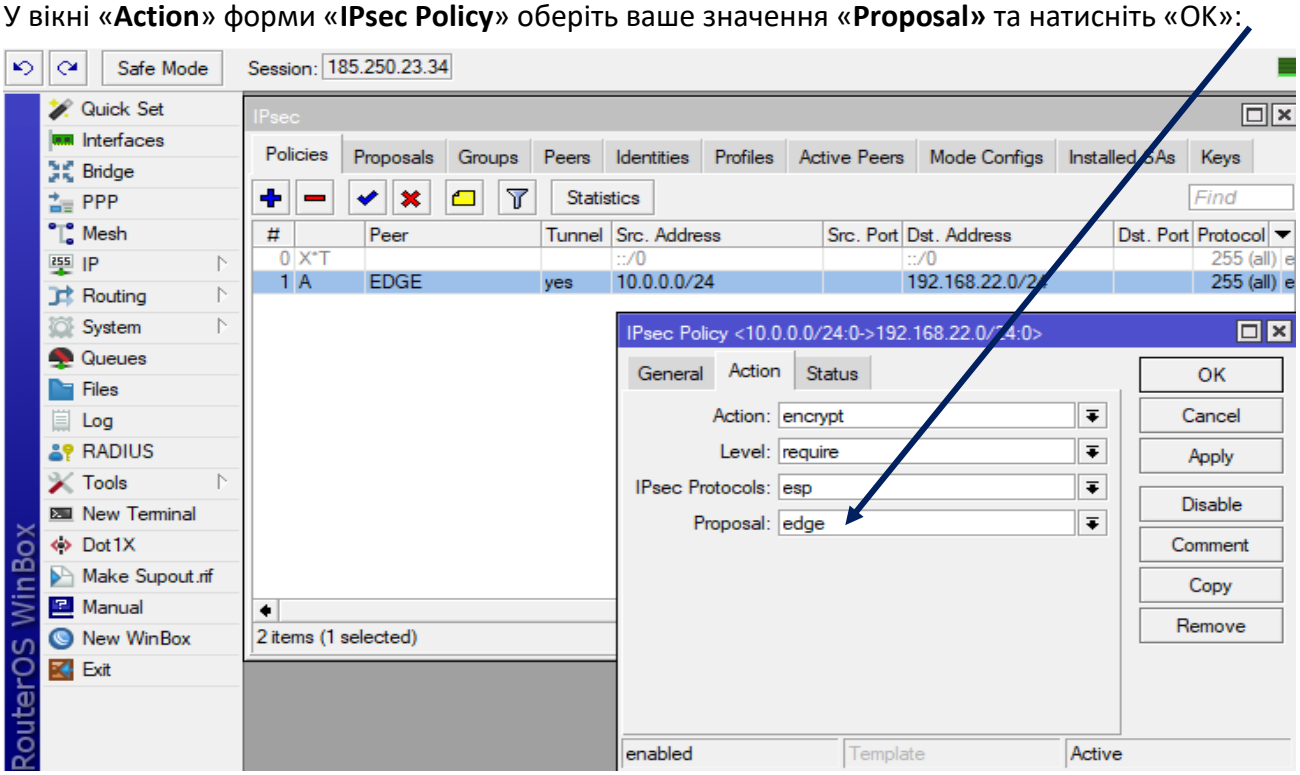
Додайте параметри політик «**IPsec Policy**» натисканням на позначку «**+**» вкладки «**Policies**»:



Заповніть поля вікна «**General**» форми «**IPsec Policy**» або оберіть необхідні значення з переліку:

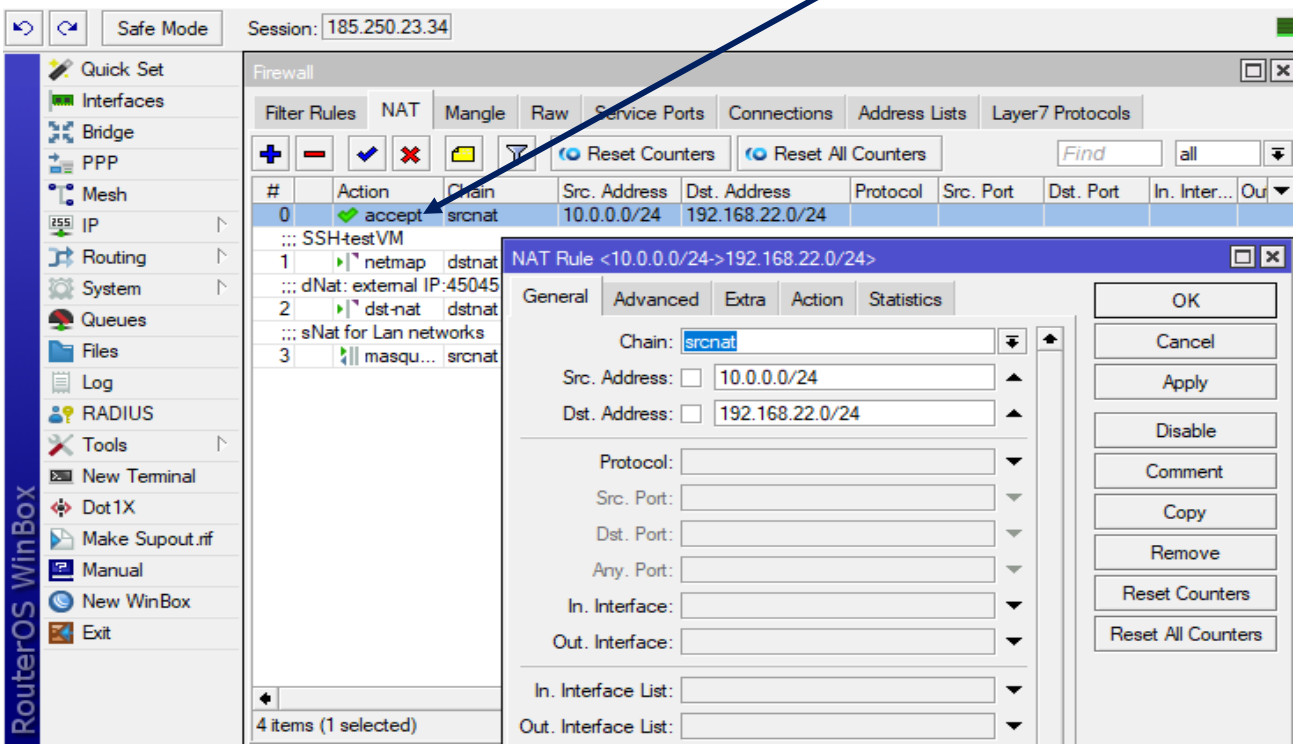
- **Peer** – раніше створений вузол для з'єднання «точка–точка» (у даному випадку «EDGE»);
- **Tunnel** – встановіть позначку ☑;
- **Src. Address** – локальна мережа «за роутером MikroTik» (Side «A»);
- **Dst. Address** – локальна мережа «за роутером EDGE» (Side «B»).

У вікні «**Action**» форми «**IPsec Policy**» оберіть ваше значення «**Proposal»** та натисніть «OK»:

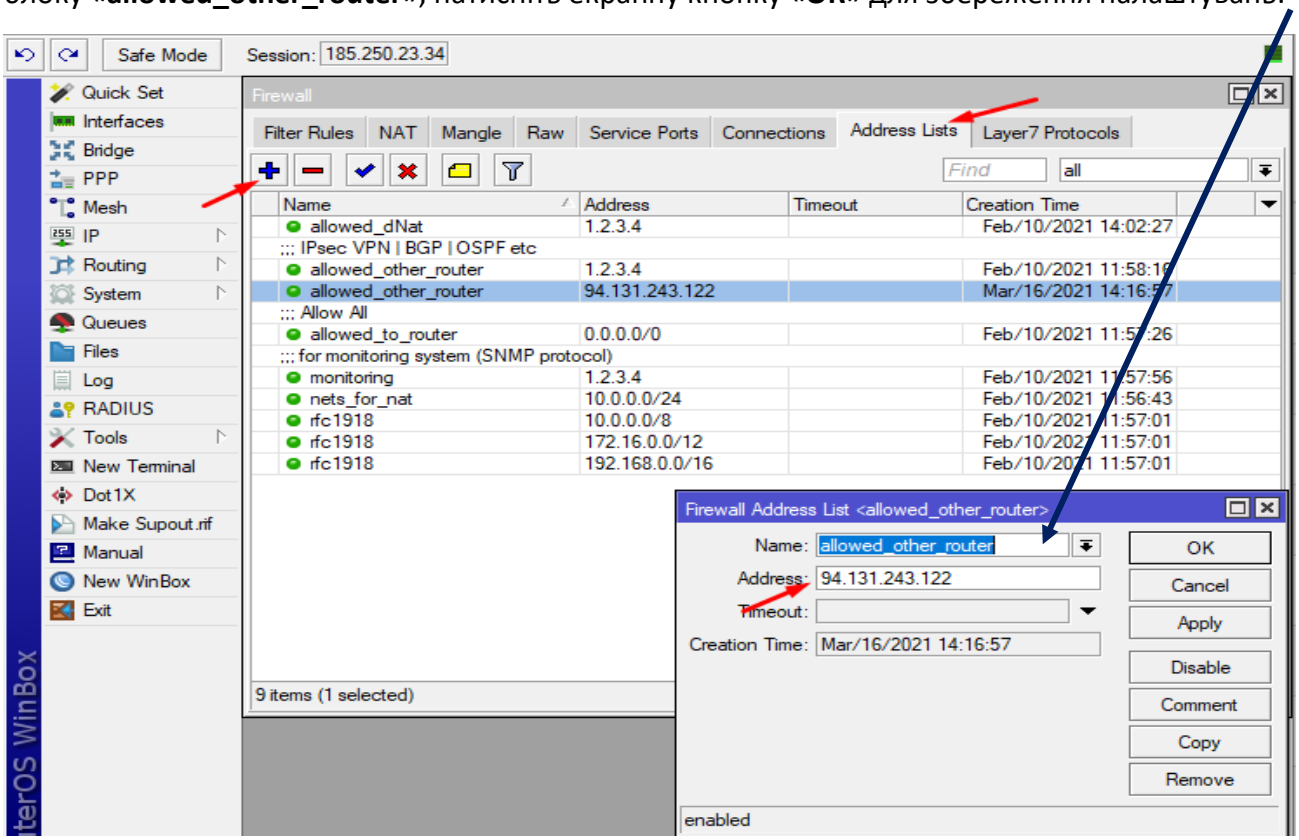


У розділі меню утиліти «**IP –> Firewall**» оберіть вкладку «**NAT**» і натисніть на позначку «**+**».

У вікні «**NAT Rule**» додайте «**srcnat** правило» трансляції адрес із внутрішньої локальної мережі до віддаленої, встановіть для нового правила дію «**accept**»:

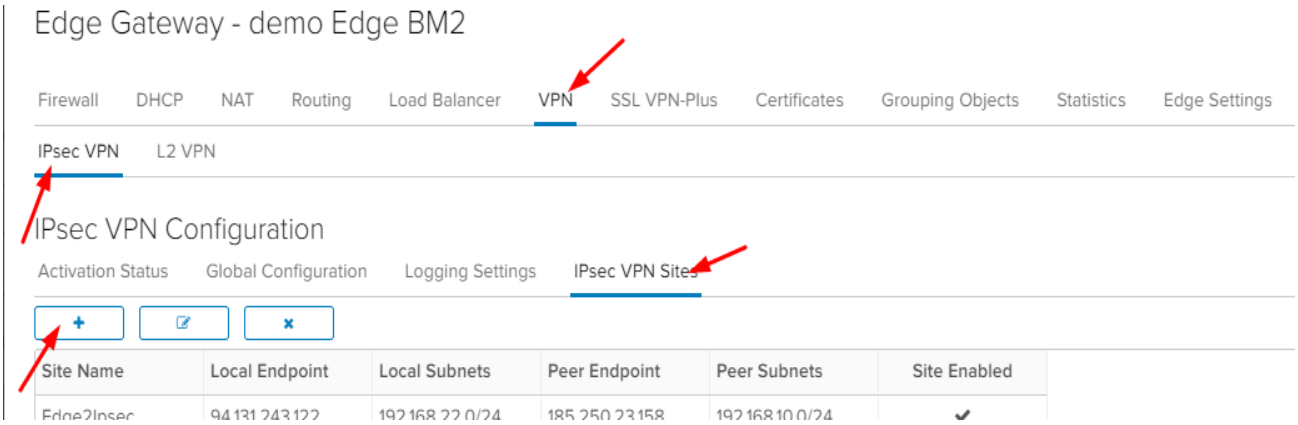


Натисніть позначку «**+**» вкладки «**Address Lists**» і **додайте публічну IP-адресу роутера EDGE** до блоку «**allowed_other_router**», натисніть екранну кнопку «**OK**» для збереження налаштувань:



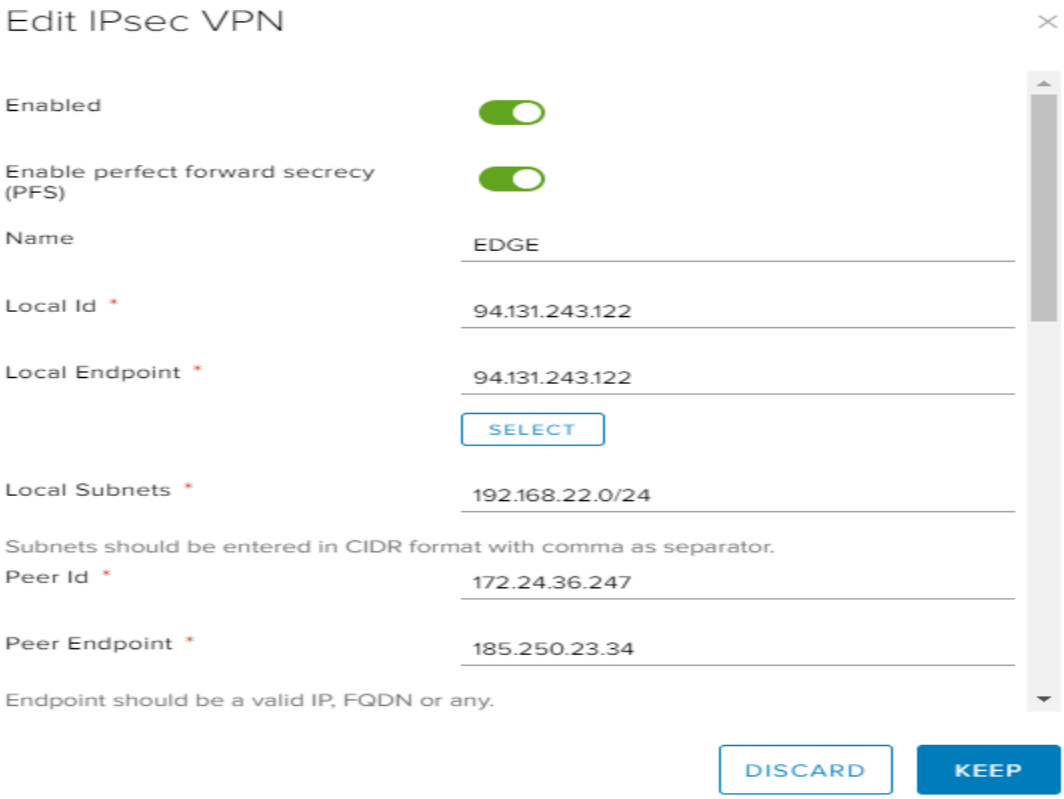
Налаштування NSX EDGE Gateway в хмарі VMWare

Створіть **нове IPSec VPN підключення для роутера «EDGE»**, натиснувши позначку «**+**» вкладки «**IPSec VPN Sites**» у відповідному розділі «**vCloud Director**»:



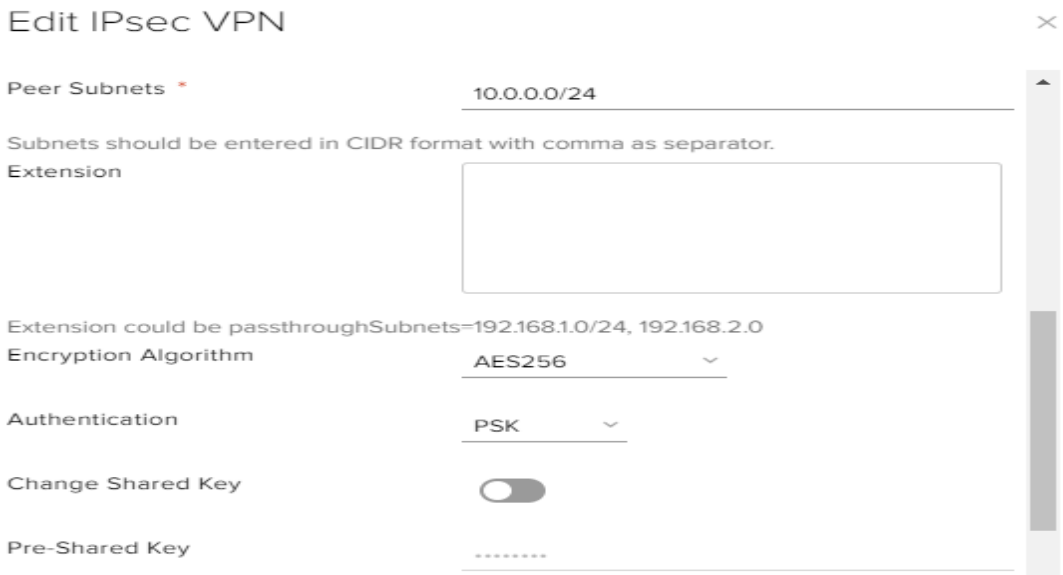
Заповніть поля екранної форми «**Edit IPsec VPN**» і встановіть належні значення екранних «вимикачів»:

- **Name** – найменування з'єднання (у наведеному прикладі – «EDGE»);
- **Enable PFS** – встановіть стан «активовано» для відновлення тунелю у випадку розриву або «зависання» з'єднання;
- **Local ID**, **Local Endpoint** – публічна (зовнішня, так звана «біла») IP-адреса роутера EDGE;
- **Local Subnets** – локальна мережа «за роутером EDGE» (у хмарі E-Cloud);
- **Peer ID** – приватна (внутрішня, так звана «сіра») IP-адреса роутера Mikrotik за NAT-T;
- **Peer Endpoint** – публічна IP-адреса **зовнішнього роутера проекту в хмарі S-Cloud 2.0** з безпосереднім виходом до Інтернет (використовується першою фазою IPSec Connect):

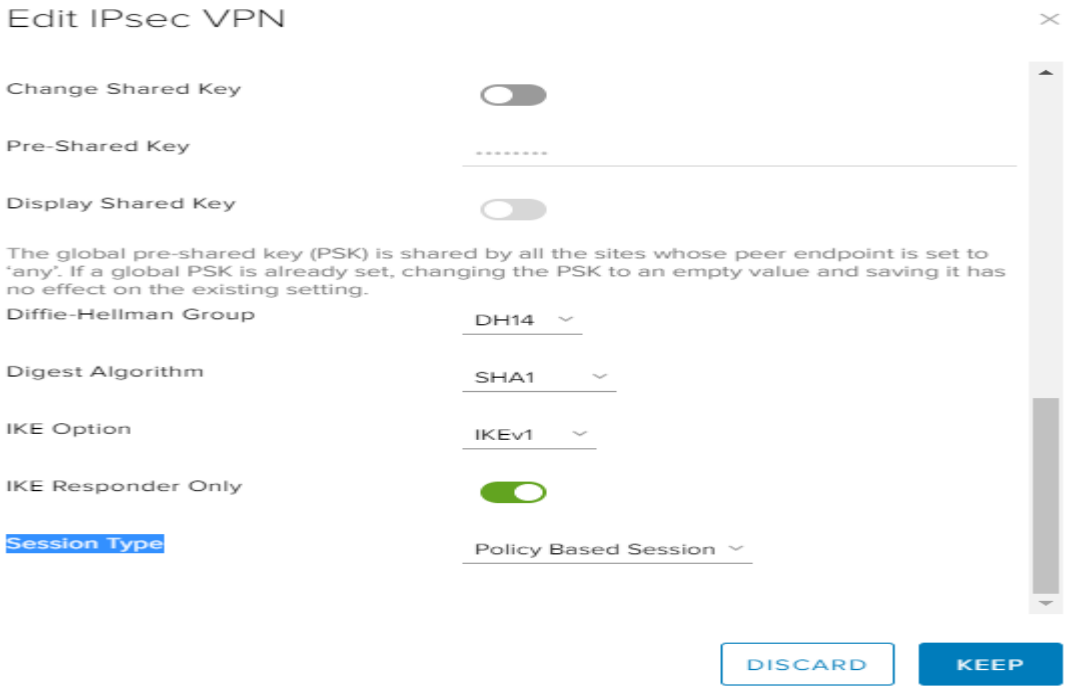


Далі, встановіть значення у наступних полях екранної форми «**Edit IPsec VPN**» (продовження):

- **Peer Subnets** – локальна мережа «за роутером MikroTik» (у хмарі S-Cloud);
- **Encryption Algorithm** – відповідно до налаштувань MikroTik на іншому боці тунелю;
- **Authentication** – оберіть PSK (Pre Shared Key);
- **Pre-Shared Key** – відповідно до налаштувань MikroTik на іншому боці тунелю;



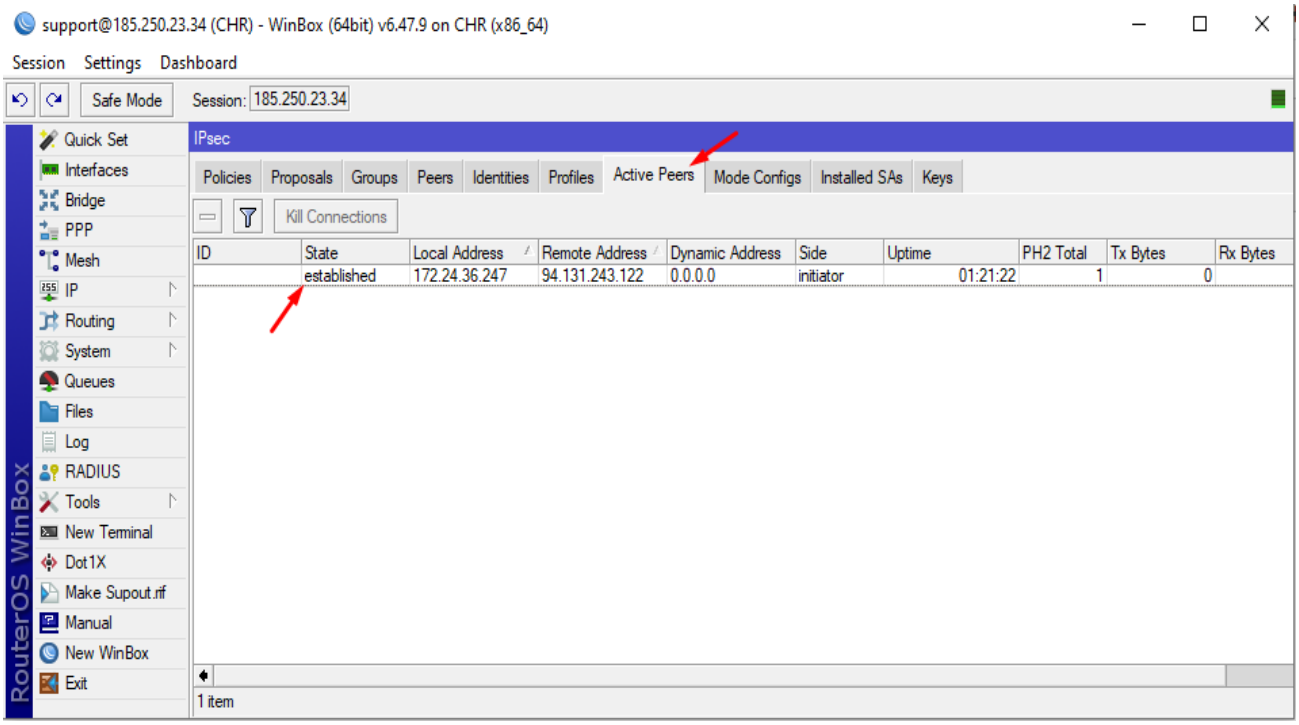
- **Diffie-Hellman Group** – значення **DH14** відповідає Modp2048 в налаштуваннях Mikrotik;
- **Digest Algorithm** – відповідно до налаштувань MikroTik на іншому боці тунелю;
- **IKE Option** – відповідно параметру Exchange mode "**main**" на MikroTik
- **IKE Responder Only** – встановіть «**активовано**» для переведення EDGE в Passive Mode (**для надходження запиту з'єднання від роутера MikroTik, розміщеного «за NAT-T»**);
- **Session Type** – встановіть значення «**Policy Based Session**».



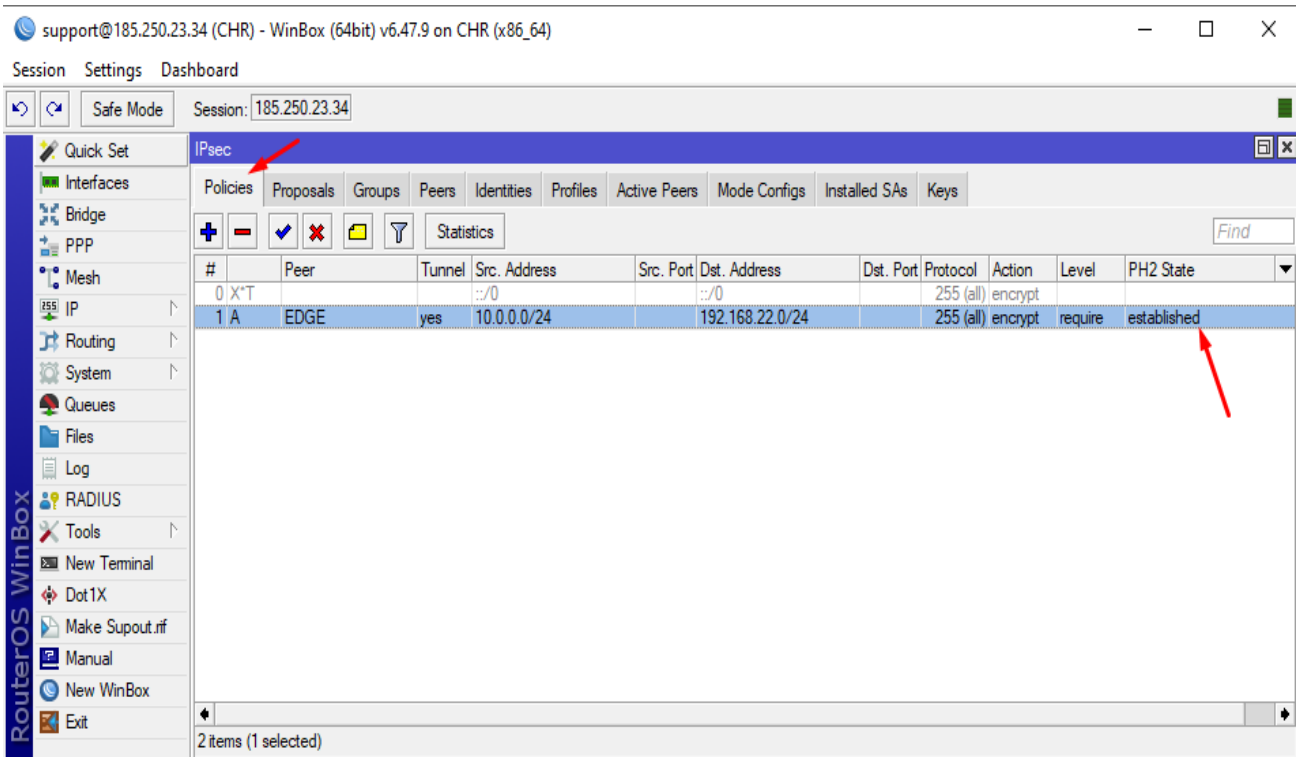
Сбережіть налаштування роутера EDGE натисканням екранної кнопки «KEEP».

Перевірка працездатності тунелю IPSec VPN

Пересвідчіться, що у вкладці «**Active Peers**» (розділу меню **«IP –> IPsec»** утиліти **Winbox**) стан активності вузлів **Peers** відображено подібно наведеному нижче:



Пересвідчіться, що у вкладці «**Policies**» стан фази з'єднання **PH2 State** відображено подібно наведеному нижче, тобто тунель **IPsec VPN** створено успішно:



На завершення, **перевірте мережеву зв'язність між двома ВМ** (що знаходяться у локальних приватних мережах **«за роутерами» проектів у різних хмарах**) та взаємну доступність за їх приватними (так званими «сірими») IP адресами:

root@test-convert: ~

```
root@test-convert:~# ifconfig
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.10  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 fe80::f816:3eff:fe4c:4954  prefixlen 64  scopeid 0x20<link>
        ether fa:16:3e:4c:49:54  txqueuelen 1000  (Ethernet)
        RX packets 75286  bytes 99112412 (99.1 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 49710  bytes 4065784 (4.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 304  bytes 26914 (26.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 304  bytes 26914 (26.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@test-convert:~# ping 192.168.22.10
PING 192.168.22.10 (192.168.22.10) 56(84) bytes of data.
64 bytes from 192.168.22.10: icmp_seq=1 ttl=62 time=1.86 ms
64 bytes from 192.168.22.10: icmp_seq=2 ttl=62 time=1.81 ms
64 bytes from 192.168.22.10: icmp_seq=3 ttl=62 time=2.02 ms
64 bytes from 192.168.22.10: icmp_seq=4 ttl=62 time=2.29 ms
^C
--- 192.168.22.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.811/1.996/2.291/0.191 ms
root@test-convert:~#
```

Це підтверджує працездатність створеної вами IPSec VPN, що поєднує локальні мережі проектів у різних хмарах провайдера GigaCloud.