



LAB WEEK 8:

Firewall – VPN Site to Site – MikroTik

NGUYEN CONG LUC

nguyencongluc.82@gmail.com

[Luc Nguyen | LinkedIn](#)

0329206845

MỤC LỤC

MỤC TIÊU	3
<i>Phần 1. Chuẩn bị hạ tầng</i>	4
1.1 Chuẩn bị cấu hình Hardware cho MikroTik	4
1.2 Cài đặt MikroTik	5
<i>Phần 2. Cấu hình chi tiết trong MikroTik</i>	8
2.1 Cấu hình IP	8
2.2 Bảo mật MikroTik	9
2.2.1 Đổi lại mật khẩu mặc định nếu đang để đơn giản.....	10
2.2.2 Tắt dịch vụ không cần thiết	10
2.2.3 Cài đặt để SSH vào MikroTik	11
2.2.4 Bảo mật nâng cao (Firewall) – Tùy chọn chỉ thêm khi cần..	13
<i>Phần 3. Cấu hình Client Server & check lưu lượng gửi đi</i>	14
3.1 Cấu hình IP tại Client	14
3.2 Kiểm tra kết nối	15
3.2.1 Ping từ Client Site 1 đến Gateway MikroTik 1 và Net	15
3.2.2 Ping từ Client Site 1 đến Gateway MikroTik 2	15
3.2.3 Ping từ Client Site 1 đến Client Site	15
<i>Phần 4. Cấu hình VPN IPsec</i>	16
4.1 Cấu hình tại 2 Site MikroTik	16
4.2 Kiểm tra kết quả	18
<i>Phần 5. Cấu hình để truy cập MikroTik qua WinBox hoặc WebFig</i>	19
5.1 Truy cập qua WinBox	19
5.2 Truy cập qua WebFig	20

MỤC TIÊU

Lab Week 8: VPN Site-to-Site

Chuẩn bị:

- 4 VM trên Proxmox:
 - 2 VM Router:
 - MikroTik Site 1 (2 NIC: 1 WAN, 1 LAN).
 - MikroTik Site 2 (2 NIC: 1 WAN, 1 LAN).
 - 2 VM Client:
 - Ubuntu Server Site 1 (1 NIC).
 - Ubuntu Server Site 2 (1 NIC).
- NIC: Network Interface Card.

Mục tiêu:

- Cấu hình VPN Site-to-Site (IPsec) để:
 1. Ping thành công từ Client Site 1 sang Client Site 2.
 2. Đảm bảo lưu lượng được mã hóa qua đường:
Client Site 1 → MikroTik Site 1 → MikroTik Site 2 → Client Site 2.

Lưu ý:

- MikroTik dễ bị tấn công bruteforce khi khởi động, cần:
 - Cấu hình SSH an toàn.
 - Tăng cường bảo mật (tắt dịch vụ không cần thiết, đổi port mặc định nếu cần).

- Client Site 1:

IP: vmbr1 10.0.1.2/24, Gateway: 10.0.1.1

- MikroTik Site 1:

vmbr0 (WAN): 45.122.223.81/25, Gateway: 45.122.223.1

vmbr1 (LAN): 10.0.1.1/24

- MikroTik Site 2:

vmbr0 (WAN): 45.122.223.85/25, Gateway: 45.122.223.1

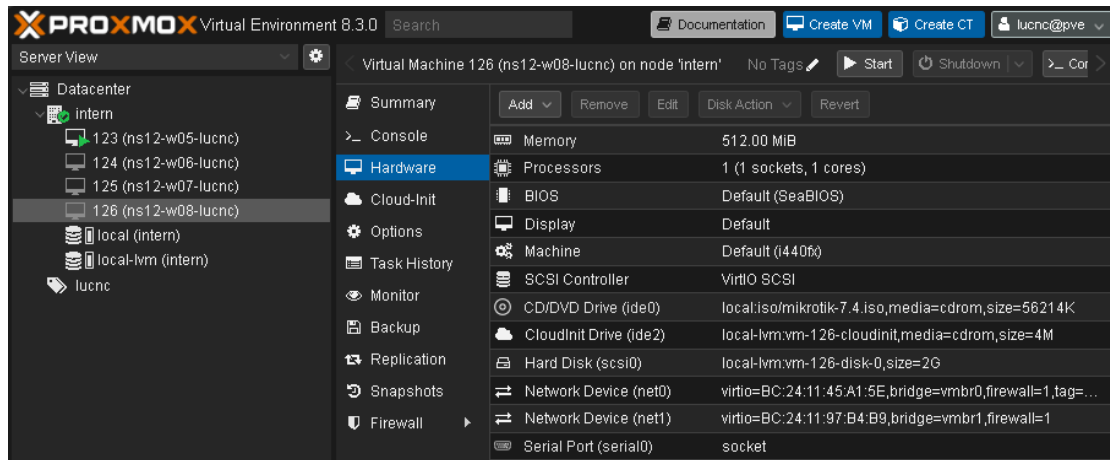
vmbr1 (LAN): 10.0.2.1/24

- Client Site 2:

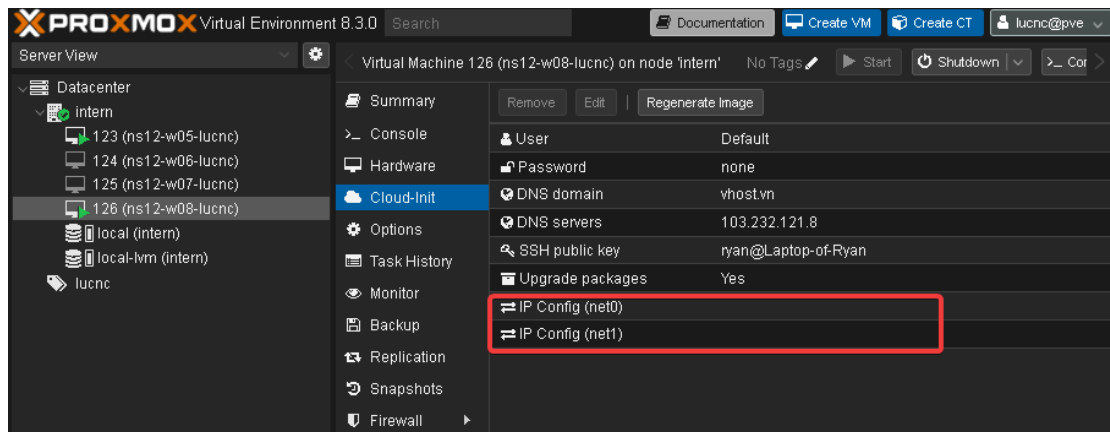
IP: vmbr1 10.0.2.2/24, Gateway: 10.0.2.1

Phần 1. Chuẩn bị hạ tầng

1.1 Chuẩn bị cấu hình Hardware cho MikroTik



- Đặt Memory tối thiểu 512MB
- Đặt CPU: 1 socket, 1cores
- Hard Disk: 2G (Type: scsi0)
- IP WAN: 45.122.223.81/
- IP LAN: 10.0.1.1/
- CD/DVD: Iso Mikrotik
- Tạm thời không set IP WAN cho router để không lộ IP ra Net giảm thiểu bị tấn công trong quá trình cài đặt



1.2 Cài đặt MikroTik

- Trong màn hình boot, thực hiện nhấn i để install, và nhấn tiếp y để cài đặt, cuối cùng nhất enter để reboot

```

Welcome to MikroTik Router Software installation

Move around menu using 'p' and 'n' or arrow keys, select with 'spacebar'.
Select all with 'a', minimum with 'm'. Press 'i' to install locally or 'q' to
cancel and reboot.

[X] system

system (depends on nothing):
Main package with most of services and drivers
-
```

```

Move around menu using 'p' and 'n' or arrow keys, select with 'spacebar'.
Select all with 'a', minimum with 'm'. Press 'i' to install locally or 'q' to
cancel and reboot.

[X] system

system (depends on nothing):
Main package with most of services and drivers

Warning: all data on the disk '/dev/sda' will be erased!
Continue? [y/n]:_
```

```

system (depends on nothing):
Main package with most of services and drivers

Warning: all data on the disk '/dev/sda' will be erased!
Continue? [y/n]:y

Creating partitions...+(2013 MB)...

Formatting 'RouterOS' 100%
Formatting 'RouterOS Boot' 100%

Software installed.
Press ENTER to reboot

```

- Sau khi reboot, đổi device trong Boot Order, đẩy scsi0 lên trên cùng:



- Giao diện chính của MikroTik, login với user admin, password: không có (Nhấn enter)

```

MikroTik 7.4 (stable)
MikroTik Login: admin
Password:

MMM      MMM      KKK      TTTTTTTTTT      KKK
MMMM     MMMM     KKK      TTTTTTTTTT      KKK
MMM MMMM MMM III  KKK KKK RRRRRR  000000  TTT  III  KKK KKK
MMM MM  MMM III  KKKKKK  RRR RRR  000 000  TTT  III  KKKKKK
MMM     MMM III  KKK KKK RRRRRR  000 000  TTT  III  KKK KKK
MMM     MMM III  KKK KKK RRR RRR  000000  TTT  III  KKK KKK

MikroTik RouterOS 7.4 (c) 1999-2022      https://www.mikrotik.com/

Do you want to see the software license? [Y/n]: _

```

- MikroTik sẽ tự động yêu cầu đổi password, nhập password thật phức tạp

```
MikroTik RouterOS 7.4 (c) 1999-2022      https://www.mikrotik.com/

Do you want to see the software license? [Y/n]: n

ROUTER HAS NO SOFTWARE KEY
-----
You have 23h48m to configure the router to be remotely accessible,
and to enter the key by pasting it in a Telnet window or in Winbox.
Turn off the device to stop the timer.
See www.mikrotik.com/key for more details.

Current installation "software ID": JAUG-HGCP
Please press "Enter" to continue!

Change your password

new password> *****
repeat new password> *****

Password changed
[admin@MikroTik] >
```

Phần 2. Cấu hình chi tiết trong MikroTik

2.1 Cấu hình IP

- Cấu hình IP

/ip address/add address=45.122.223.81/25 interface=ether1

```
[admin@MikroTik] > /ip address/add address=45.122.223.81/25 interface=ether1
```

/ip address/add address=10.0.1.1/24 interface=ether2

```
[admin@MikroTik] > /ip address/add address=10.0.1.1/24 interface=ether2
```

- Cấu hình Gateway:

/ip route/add gateway=45.122.223.1

```
[admin@MikroTik] > /ip route/add gateway=45.122.223.1
```

- Ping ra net và MikroTik Site 2 để kiểm tra:

```
[admin@MikroTik] > ping 8.8.8.8
```

SEQ	HOST	SIZE	TTL	TIME	STATUS
0	8.8.8.8	56	119	29ms113us	
1	8.8.8.8	56	119	35ms512us	

sent=2 received=2 packet-loss=0% min-rtt=29ms113us avg-rtt=32ms312us max-rtt=35ms512us


```
[admin@MikroTik] > ping 45.122.223.85
```

SEQ	HOST	SIZE	TTL	TIME	STATUS
0	45.122.223.85	56	64	800us	
1	45.122.223.85	56	64	826us	

sent=2 received=2 packet-loss=0% min-rtt=800us avg-rtt=813us max-rtt=826us

- Cấu hình NAT (Masquerade) để tất cả IP LAN đều ra WAN:

/ip firewall nat/add chain=srcnat out-interface=ether1 action=masquerade

```
[admin@MikroTik] > /ip firewall/nat/add chain=srcnat out-interface=ether1 action=masquerade
```

- Lệnh kiểm tra: /ping 8.8.8.8 src-address=10.0.1.1

```
[admin@MikroTik] > /ping 8.8.8.8 src-address=10.0.1.1
```

SEQ	HOST	SIZE	TTL	TIME	STATUS
0	8.8.8.8	56	119	30ms9us	
1	8.8.8.8	56	119	29ms791us	

sent=2 received=2 packet-loss=0% min-rtt=29ms791us avg-rtt=29ms900us max-rtt=30ms9us

- Set đường đi mạng cho MikroTik, cho phép router biết cách gửi lưu lượng đến mạng 10.0.2.0/24 (mạng đích) thông qua gateway 45.122.223.85. Từ đó sẽ ping được client site 2

/ip route/add dst-address=10.0.2.0/24 gateway=45.122.223.85

```
[admin@MikroTik] > /ip route/add dst-address=10.0.2.0/24 gateway=45.122.223.85
```

*Làm ngược lại bên Site2

2.2 Bảo mật MikroTik

- Lý do: Khi MikroTik kết nối Internet, các dịch vụ mặc định có thể bị khai thác ngay khi có IP. Firewall trước đảm bảo chỉ IPsec được phép, sau đó mới gán IP và kiểm tra. Hình dưới là quá trình bruteforce của attacker vào các service của MikroTik

```
[admin@MikroTik] >
02:14:05 echo: system,error,critical login failure for user root from 59.93.232.124 via telnet
[admin@MikroTik] >
02:14:12 echo: system,error,critical login failure for user admin from 59.93.232.124 via telnet
[admin@MikroTik] >
02:14:19 echo: system,error,critical login failure for user root from 59.93.232.124 via telnet
[admin@MikroTik] >
[admin@MikroTik] >
02:14:26 echo: system,error,critical login failure for user root from 59.93.232.124 via telnet
[admin@MikroTik] >
[admin@MikroTik] >
02:14:30 echo: system,error,critical login failure for user support from 134.209.151.132 via ssh
[admin@MikroTik] >
02:14:31 echo: system,error,critical login failure for user admin from 134.209.151.132 via ssh
[admin@MikroTik] >
02:14:32 echo: system,error,critical login failure for user user from 134.209.151.132 via ssh
02:14:33 echo: system,error,critical login failure for user root from 59.93.232.124 via telnet
[admin@MikroTik] >
02:14:34 echo: system,error,critical login failure for user root from 134.209.151.132 via ssh
[admin@MikroTik] >
02:14:35 echo: system,error,critical login failure for user ubnt from 134.209.151.132 via ssh
[admin@MikroTik] >
02:14:39 echo: system,error,critical login failure for user root from 59.93.232.124 via telnet
[admin@MikroTik] >
02:14:46 echo: system,error,critical login failure for user root from 59.93.232.124 via telnet
[admin@MikroTik] >
02:14:54 echo: system,error,critical login failure for user guest from 59.93.232.124 via telnet
[admin@MikroTik] >
02:14:55 echo: system,error,critical login failure for user 0 from 88.214.25.16 via ssh
02:14:55 echo: system,error,critical login failure for user root from 88.214.25.16 via ssh
02:14:56 echo: system,error,critical login failure for user admin from 88.214.25.16 via ssh
[admin@MikroTik] >
02:14:57 echo: system,error,critical login failure for user ubnt from 88.214.25.16 via ssh
02:14:57 echo: system,error,critical login failure for user uucp from 88.214.25.16 via ssh
02:14:57 echo: system,error,critical login failure for user admin from 88.214.25.16 via ssh
[admin@MikroTik] >
02:15:01 echo: system,error,critical login failure for user bin from 59.93.232.124 via telnet
[admin@MikroTik] >
02:15:08 echo: system,error,critical login failure for user adm from 88.214.25.16 via ssh
02:15:08 echo: system,error,critical login failure for user telecomadmin from 59.93.232.124 via telnet
02:15:08 echo: system,error,critical login failure for user adm from 88.214.25.16 via ssh
[admin@MikroTik] >
02:15:10 echo: system,error,critical login failure for user admin from 88.214.25.16 via ssh
02:15:10 echo: system,error,critical login failure for user NONE from 88.214.25.16 via ssh
[admin@MikroTik] >
02:15:12 echo: system,error,critical login failure for user user from 88.214.25.16 via ssh
[admin@MikroTik] >
02:15:14 echo: system,error,critical login failure for user root from 59.93.232.124 via telnet
02:15:15 echo: system,error,critical login failure for user ubnt from 88.214.25.16 via ssh
[admin@MikroTik] >
02:15:15 echo: system,error,critical login failure for user root from 88.214.25.16 via ssh
```

2.2.1 Đổi lại mật khẩu mặc định nếu đang để đơn giản

/user/ set 0 name=admin password="Adm!nMikr0t!k2025"

2.2.2 Tắt dịch vụ không cần thiết

- MikroTik mặc định bật một số dịch vụ như Telnet, FTP, WWW, API,.... Nếu không sử dụng, hãy tắt chúng để giảm nguy cơ bị tấn công từ bên ngoài:

Dùng lệnh: /ip service/disable telnet,www,api,api-ssl

Và kiểm tra với lệnh: /ip service/print

```
[admin@MikroTik] > /ip service/disable telnet,www,api,api-ssl
[admin@MikroTik] > /ip service/print
Flags: X, I - INVALID
Columns: NAME, PORT, CERTIFICATE, VRF
#  NAME      PORT  CERTIFICATE  VRF
0  X telnet    23      none         main
1  ftp        21      none         main
2  X www       80      none         main
3  ssh        22      none         main
4  www-ssl    443     none         main
5  X api       8728    none         main
6  winbox     8291    none         main
7  X api-ssl   8729    none         main
```

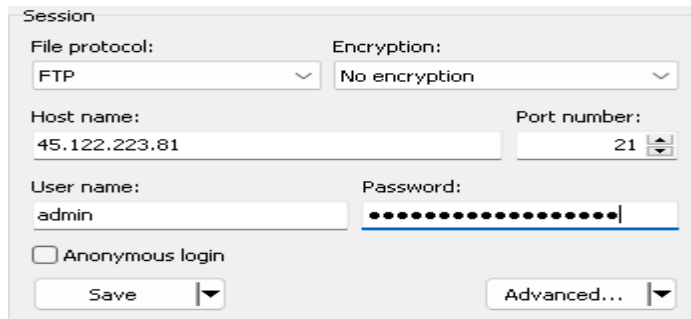
- Chỉ giữ lại FTP để chuyển file key(tất nhiên sẽ disable ngay sau đó), SSH để remote từ xa, www-ssl để truy cập qua website, winbox để truy cập qua app desktop.

2.2.3 Cài đặt để SSH vào MikroTik

- Đảm bảo đã mở dịch vụ FTP: `/ip service/enable ftp`

```
[admin@MikroTik] > /ip service/enable ftp
```

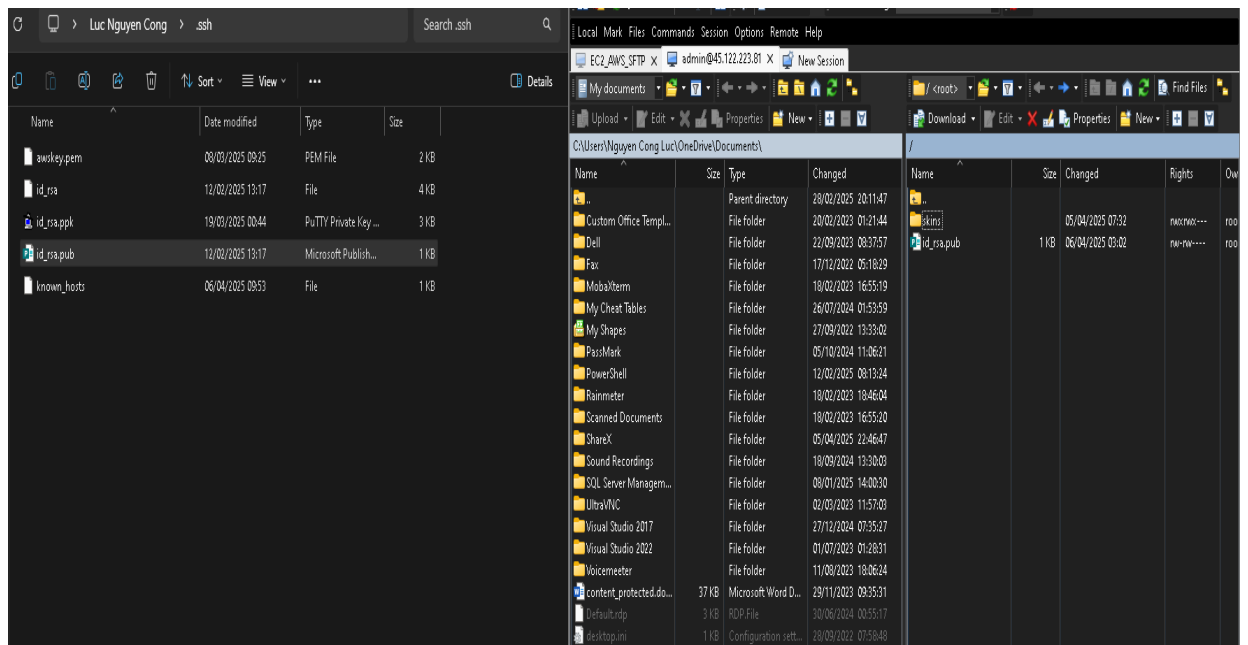
- FTP trong WinSCP:



The image shows the WinSCP Session configuration dialog box. It has the following fields and options:

- File protocol:** FTP (selected)
- Encryption:** No encryption (selected)
- Host name:** 45.122.223.81
- Port number:** 21
- User name:** admin
- Password:** [masked with dots]
- ☐ Anonymous login
- Buttons:** Save, Advanced...

- Chuyển file public key(id_rsa.pub) từ client qua folder gốc của MikroTik:



- Sau khi chuyển file xong, tắt ngay lập tức FTP và các service không dùng đến:

```
/ip service/disable telnet,ftp,www,api,api-ssl
```

```
[admin@MikroTik] > /ip service/disable ftp
```

- Update pubkey từ file : /user/ssh-keys/import public-key-file=id_rsa.pub user=admin

```
[admin@MikroTik] > /user/ssh-keys/import public-key-file=id_rsa.pub user=admin
```

- Để chống đăng nhập bằng password và tăng cường bảo mật, thực thi lệnh:

/ip/ssh/set allow-none-crypto=no always-allow-password-login=no strong-crypto=yes

```
[admin@MikroTik] > /ip/ssh/set allow-none-crypto=no always-allow-password-login=no strong-crypto=yes
```

- Thực hiện SSH từ client(windows): ssh admin@45.122.223.81

```
PS C:\Users\Nguyen Cong Luc> ssh admin@45.122.223.81

MMM      MMM      KKK      TTTTTTTTTT      KKK
MMMM     MMMM     KKK      TTTTTTTTTT      KKK
MMM MMMM MMM III KKK KKK RRRRRR      000000      TTT      III KKK KKK
MMM MM  MMM III KKKKK RRR RRR 000 000      TTT      III KKKKK
MMM     MMM III KKK KKK RRRRRR      000 000      TTT      III KKK KKK
MMM     MMM III KKK KKK RRR RRR 000000      TTT      III KKK KKK

MikroTik RouterOS 7.4 (c) 1999-2022      https://www.mikrotik.com/

ROUTER HAS NO SOFTWARE KEY
-----
You have 17h17m to configure the router to be remotely accessible,
and to enter the key by pasting it in a Telnet window or in Winbox.
Turn off the device to stop the timer.
See www.mikrotik.com/key for more details.

Current installation "software ID": CZWB-V2EP
Please press "Enter" to continue!

[admin@MikroTik] > |
```

2.2.4 Bảo mật nâng cao (Firewall) – Tùy chọn chỉ thêm khi cần

- Chặn toàn bộ truy cập từ WAN vào MikroTik, chỉ cho phép các giao thức cần thiết (như IPsec khi bạn cấu hình VPN).

/ip firewall filter

```
add chain=input in-interface=ether2 action=accept protocol=udp dst-port=500,4500  
comment="Allow IPsec IKE"
```

```
add chain=input in-interface=ether2 action=accept protocol=50 comment="Allow IPsec ESP"
```

```
add chain=input in-interface=ether2 action=drop comment="Drop all other WAN input"
```

```
[admin@MikroTik] /ip/firewall/filter> add chain=input in-interface=ether2 action=accept protocol=udp dst-port=500,4500 comment="Allow IPsec IKE"  
[admin@MikroTik] /ip/firewall/filter> add chain=input in-interface=ether2 action=accept protocol=50 comment="Allow IPsec ESP"  
[admin@MikroTik] /ip/firewall/filter> add chain=input in-interface=ether2 action=drop comment="Drop all other WAN input"
```

Giải thích:

- Rule 1: Cho phép UDP port 500 và 4500 (dùng cho IPsec IKE).
- Rule 2: Cho phép giao thức ESP – Port 50 (dùng cho mã hóa IPsec).
- Rule 3: Chặn mọi truy cập khác từ WAN (ether2 là interface WAN).

- Kiểm tra Xem danh sách rule:

/ip firewall filter print (Đảm bảo các rule được thêm đúng thứ tự (accept trước, drop sau).)

```
[admin@MikroTik] /ip/firewall/filter> print  
Flags: X - disabled, I - invalid, D - dynamic  
0      ;;; Allow IPsec IKE  
      chain=input action=accept protocol=udp in-interface=ether2 dst-port=500,4500  
  
1      ;;; Allow IPsec ESP  
      chain=input action=accept protocol=ipsec-esp in-interface=ether2  
  
2      ;;; Drop all other WAN input  
      chain=input action=drop in-interface=ether2
```

Phần 3. Cấu hình Client Server & check lưu lượng gửi đi

3.1 Cấu hình IP tại Client

- Tại Ubuntu Server site 1 set IP như sau:

addresses: [10.0.1.2/24], gateway4: 10.0.1.1

```
GNU nano 6.2 /etc/netplan/50-cloud-init.yaml
# This file is generated from information provided by the datasource. Changes
# to it will not persist across an instance reboot. To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  version: 2
  ethernets:
    eth0:
      addresses:
        - 10.0.1.2/24
      gateway4: 10.0.1.1
      match:
        macaddress: bc:24:11:26:31:91
      nameservers:
        addresses:
          - 103.232.121.8
        search:
          - vhost.vn
      set-name: eth0
```

- Tại Ubuntu Server site 2 set IP như sau:

addresses: [10.0.2.2/24], gateway4: 10.0.2.1

```
GNU nano 6.2 /etc/netplan/50-cloud-init.yaml
# This file is generated from information provided by the datasource. Changes
# to it will not persist across an instance reboot. To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  version: 2
  ethernets:
    eth0:
      addresses:
        - 10.0.2.2/24
      gateway4: 10.0.2.1
      match:
        macaddress: bc:24:11:c5:4b:7b
      nameservers:
        addresses:
          - 103.232.121.8
        search:
          - vhost.vn
      set-name: eth0
```

3.2 Kiểm tra kết nối

3.2.1 Ping từ Client Site 1 đến Gateway Mikrotik 1 và Net

- Vì trước đó trong Mikrotik đã cấu hình NAT để LAN ra net nên hiện tại client đã có thể ping ra gateway và internet

```
nguyencongluc@ns12-w09-lucnc:~$ ping 10.0.1.1
PING 10.0.1.1 (10.0.1.1) 56(84) bytes of data.
64 bytes from 10.0.1.1: icmp_seq=1 ttl=64 time=0.494 ms
64 bytes from 10.0.1.1: icmp_seq=2 ttl=64 time=0.526 ms
^C
--- 10.0.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.494/0.510/0.526/0.016 ms
nguyencongluc@ns12-w09-lucnc:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=30.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=30.0 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 29.981/29.988/29.996/0.007 ms
```

3.2.2 Ping từ Client Site 1 đến Gateway MirkroTik 2

- Trước đó Mikrotik đã cấu hình đường đi router, nên Client 1 có thể ping đến Gateway Mikrotik2 và Client2 với điều kiện cả 2 bên đều đã cấu hình đúng như vậy

```
root@ns12-w09-lucnc:~# ping 10.0.2.1
PING 10.0.2.1 (10.0.2.1) 56(84) bytes of data.
64 bytes from 10.0.2.1: icmp_seq=1 ttl=63 time=0.653 ms
64 bytes from 10.0.2.1: icmp_seq=2 ttl=63 time=0.900 ms
^C
--- 10.0.2.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.653/0.776/0.900/0.123 ms
```

3.2.3 Ping từ Client Site 1 đến Client Site

- Ping từ Client 1 đến Client 2:

```
root@ns12-w09-lucnc:~# ping 10.0.2.2
PING 10.0.2.2 (10.0.2.2) 56(84) bytes of data.
64 bytes from 10.0.2.2: icmp_seq=1 ttl=62 time=2.00 ms
64 bytes from 10.0.2.2: icmp_seq=2 ttl=62 time=1.60 ms
^C
--- 10.0.2.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.597/1.796/1.996/0.199 ms
```

Phần 4. Cấu hình VPN IPsec

4.1 Cấu hình tại 2 Site MikroTik

- Cấu hình tại MikroTik Site1:

+ Tạo cấu hình mã hóa Ipsec (**Chỉ tạo nếu không muốn dùng default, trong lab này là dùng cấu hình default**):

```
/ip ipsec/proposal/add name=proposal1 auth-algorithms=sha256 enc-algorithms=aes-256-cbc  
pfs-group=modp2048 lifetime=1h
```

```
[admin@MikroTik] > /ip ipsec/proposal/add name=proposal1 auth-algorithms=sha256 enc-algorithms=aes-256-cbc pfs-group=modp2048 lifetime=1h
```

+ Thiết lập peer IPsec với địa chỉ 45.122.223.85, dùng khóa chia sẻ VPN_CyberKing999999*

```
/ip ipsec/peer add address=45.122.223.85/32 exchange-mode=main
```

```
/ip ipsec/identity/add peer=[find peer =peer1 =45.122.223.85] auth-method=pre-shared-key  
secret="VPN_CyberKing999999"
```

```
[admin@MikroTik] > /ip ipsec/peer/add address=45.122.223.85/32 exchange-mode=main
```

```
[admin@MikroTik] > /ip ipsec/identity/add peer=[find peer =peer1 =45.122.223.85] auth-method=pre-shared-key secret="VPN_CyberKing999999"
```

+ Tạo chính sách Ipsec:

```
/ip ipsec policy add src-address=10.0.1.0/24 dst-address=10.0.2.0/24 tunnel=yes  
action=encrypt proposal=proposal1 peer=peer1
```

```
[admin@MikroTik] > /ip ipsec/policy/add src-address=10.0.1.0/24 dst-address=10.0.2.0/24 tunnel=yes action=encrypt proposal=default peer=peer1
```

+ Đảm bảo lưu lượng ICMP khớp với policy IPsec để mã hóa thành ESP:

```
/ip firewall nat add chain=srcnat src-address=10.0.1.0/24 dst-address=10.0.2.0/24  
action=accept place-before=0
```

```
[admin@MikroTik] > /ip firewall nat add chain=srcnat src-address=10.0.1.0/24 dst-address=10.0.2.0/24 action=accept place-before=0
```


- Kiểm tra các cấu hình đã thêm:

/ip ipsec/proposal/print

/ip ipsec/peer/print

/ip ipsec/identity/print

/ip ipsec/policy/print

/ip route/print

```
[admin@MikroTik] > /ip ipsec/proposal/print
Flags: X - disabled; * - default
0 * name="default" auth-algorithms=sha1 enc-algorithms=aes-256-cbc,aes-192-cbc,aes-128-cbc lifetime=30m
  pfs-group=modp1024
[admin@MikroTik] > /ip ipsec/peer/print
Flags: X - disabled; D - dynamic; R - responder
0 name="peer1" address=45.122.223.85/32 profile=default exchange-mode=main send-initial-contact=yes
[admin@MikroTik] > /ip ipsec/identity/print
Flags: D - dynamic; X - disabled
0 peer=peer1 auth-method=pre-shared-key secret="VPN_CyberKing999999*" generate-policy=no
[admin@MikroTik] > /ip ipsec/policy/print
Flags: T - TEMPLATE; * - DEFAULT
Columns: PEER, TUNNEL, SRC-ADDRESS, DST-ADDRESS, PROTOCOL, ACTION, LEVEL, PH2-COUNT
# PEER TUNNEL SRC-ADDRESS DST-ADDRESS PROTOCOL ACTION LEVEL PH2-COUNT
0 T* ::/0 ::/0 all 0
1 peer1 yes 10.0.1.0/24 10.0.2.0/24 all encrypt require 0
[admin@MikroTik] > /ip route/print
Flags: D - DYNAMIC; A - ACTIVE; c, s, y - COPY
Columns: DST-ADDRESS, GATEWAY, DISTANCE
# DST-ADDRESS GATEWAY DISTANCE
0 As 0.0.0.0/0 45.122.223.1 1
  DAc 10.0.1.0/24 ether2 0
1 As 10.0.2.0/24 45.122.223.85 1
  DAc 45.122.223.0/25 ether1 0
```

- Cấu hình ngược lại tại MikroTik Site 2:

/ip/ipsec/peer add address=45.122.223.81/32 exchange-mode=main

/ip ipsec/identity/add peer=[find peer =peer1 =45.122.223.81] auth-method=pre-shared-key
secret="VPN_CyberKing999999*"

/ip ipsec/policy/add src-address=10.0.2.0/24 dst-address=10.0.1.0/24 tunnel=yes
action=encrypt proposal=default peer=peer1

/ip firewall nat add chain=srcnat src-address=10.0.2.0/24 dst-address=10.0.1.0/24
action=accept place-before=0

4.2 Kiểm tra kết quả

- Check cấu hình IPSEC đã tồn tại trên 2 site, dưới đây là ảnh của mikrotik1 và sẽ tương tự trên mikrotik2:

/ip ipsec installed-sa print

```
[admin@mikrotik] > /ip ipsec installed-sa print
Flags: S - SEEN-TRAFFIC; E - ESP
Columns: SPI, STATE, SRC-ADDRESS, DST-ADDRESS, AUTH-ALGORITHM, ENC-ALGORITHM, ENC-KEY-SIZE
#  SPI      STATE  SRC-ADDRESS  DST-ADDRESS  AUTH-ALGORITHM  ENC-ALGORITHM  ENC-KEY-SIZE
0  SE 0x6C807BC  dying    45.122.223.85 45.122.223.81 sha1            aes-cbc        256
1  SE 0x1429514  dying    45.122.223.81 45.122.223.85 sha1            aes-cbc        256
2  E  0xF14AC3A  mature   45.122.223.85 45.122.223.81 sha1            aes-cbc        256
3  E  0x1529CC7  mature   45.122.223.81 45.122.223.85 sha1            aes-cbc        256
```

- Từ Client Site 1 ping đến Client Site 2 và ngược lại

- Quan sát lưu lượng đã mã hóa 2 site Mikrotik, các gói ICMP đã được mã hóa thành IPSEC-ESP, xem các gói ipsec-esp gửi đến bằng câu lệnh:

/tool sniffer quick interface=ether1 ip-protocol=ipsec-esp

+ Ảnh tại mikrotik1

```
[admin@mikrotik] > /tool sniffer quick interface=ether1 ip-protocol=ipsec-esp
Columns: INTERFACE, TIME, NUM, DIR, SRC-MAC, DST-MAC, SRC-ADDRESS, DST-ADDRESS, PROTOCOL, SIZE, CPU
INTERFACE  TIME  NUM  DIR  SRC-MAC          DST-MAC          SRC-ADDRESS      DST-ADDRESS      PROTOCOL  SIZE  CPU
ether1     0.781  1    <-   BC:24:11:5D:37:71 BC:24:11:45:A1:5E 45.122.223.85    45.122.223.81    ip:ipsec-esp 166  0
ether1     0.782  2    ->   BC:24:11:45:A1:5E BC:24:11:5D:37:71 45.122.223.81    45.122.223.85    ip:ipsec-esp 166  0
ether1     1.783  3    <-   BC:24:11:5D:37:71 BC:24:11:45:A1:5E 45.122.223.85    45.122.223.81    ip:ipsec-esp 166  0
ether1     1.784  4    ->   BC:24:11:45:A1:5E BC:24:11:5D:37:71 45.122.223.81    45.122.223.85    ip:ipsec-esp 166  0
ether1     2.785  5    <-   BC:24:11:5D:37:71 BC:24:11:45:A1:5E 45.122.223.85    45.122.223.81    ip:ipsec-esp 166  0
ether1     2.786  6    ->   BC:24:11:45:A1:5E BC:24:11:5D:37:71 45.122.223.81    45.122.223.85    ip:ipsec-esp 166  0
```

+ Ảnh tại mikrotik2

```
[admin@mikrotik] > /tool sniffer/quick interface=ether1 ip-protocol=ipsec-esp
Columns: INTERFACE, TIME, NUM, DIR, SRC-MAC, DST-MAC, SRC-ADDRESS
INTERF  TIME  NUM  DIR  SRC-MAC          DST-MAC          SRC-ADDRESS
ether1  0.761  1    ->   BC:24:11:5D:37:71 BC:24:11:45:A1:5E 45.122.223.85
ether1  0.762  2    <-   BC:24:11:45:A1:5E BC:24:11:5D:37:71 45.122.223.81
ether1  1.762  3    ->   BC:24:11:5D:37:71 BC:24:11:45:A1:5E 45.122.223.85
ether1  1.763  4    <-   BC:24:11:45:A1:5E BC:24:11:5D:37:71 45.122.223.81
ether1  2.764  5    ->   BC:24:11:5D:37:71 BC:24:11:45:A1:5E 45.122.223.85
ether1  2.765  6    <-   BC:24:11:45:A1:5E BC:24:11:5D:37:71 45.122.223.81
```

Phần 5. Cấu hình để truy cập MikroTik qua WinBox hoặc WebFig

- Ngoài cách truy cập MikroTik qua CLI, MikroTik còn cung cấp phương thức truy cập qua website (WebFig) hoặc phần mềm WinBox

5.1 Truy cập qua WinBox

- WinBox là công cụ giao diện đồ họa được MikroTik cung cấp để quản lý router. Nó có thể truy cập qua địa chỉ IP hoặc địa chỉ MAC.

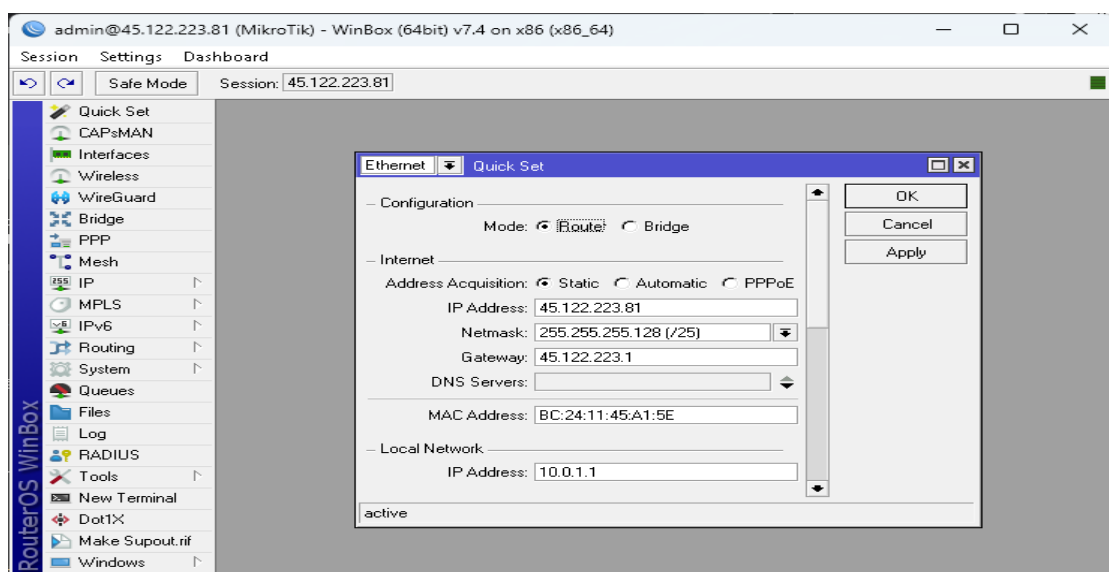
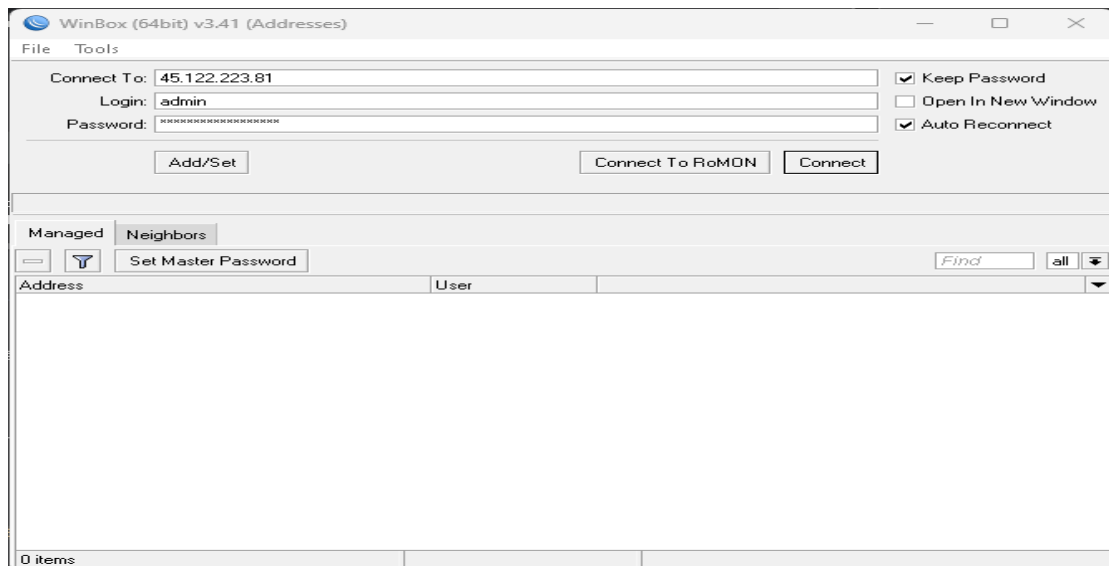
- Điều kiện cần thiết:

+ Máy tính cài WinBox (tải từ trang chính thức của MikroTik:
<https://mikrotik.com/download>).

+ Router MikroTik đã được kết nối với mạng và có địa chỉ IP hoặc có thể phát hiện qua MAC.

- Tại giao diện login nhập các thông tin quan trọng như IP, user, password và nhấn connect

- Giao diện chính của WinBox (Cửa sổ Quick Set):



5.2 Truy cập qua WebFig

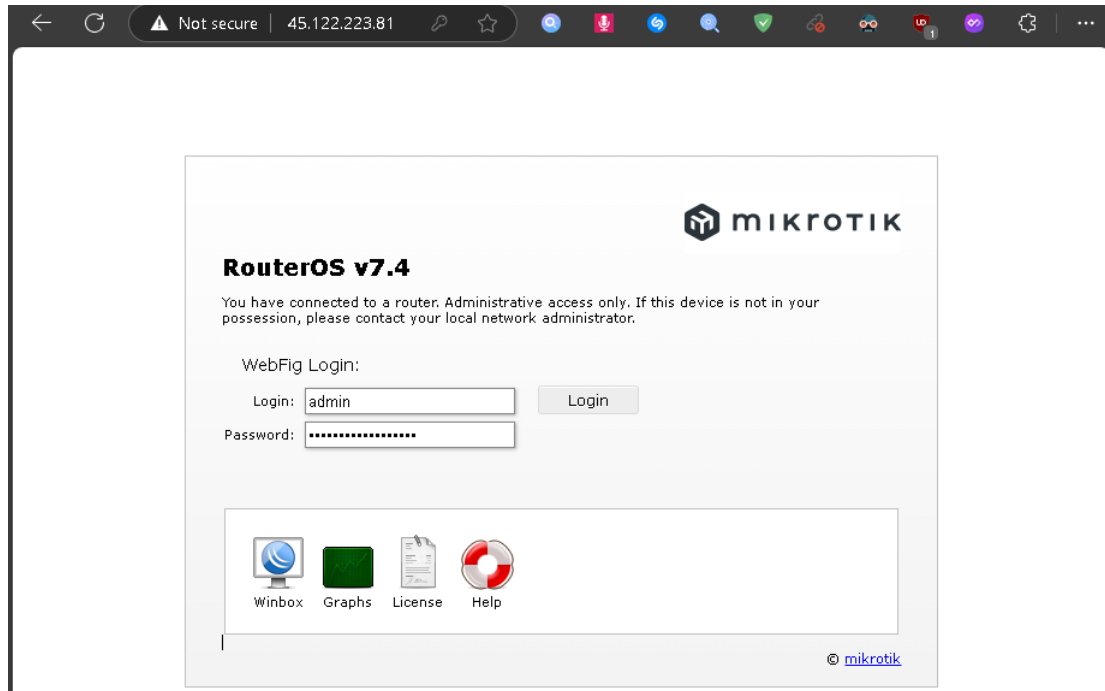
- WebFig là giao diện web của MikroTik, cho phép quản lý router qua trình duyệt.
- Để truy cập qua trình duyệt phải đảm bảo đã bật dịch vụ www

```
[admin@MikroTik] > ip service/enable www
```

- Mở trình duyệt:

Nhập <http://45.122.223.81> (IP của Server MikroTik) vào thanh địa chỉ.

Đăng nhập bằng tài khoản mặc định: admin, mật khẩu



- Giao diện chính tại WebFig.

