BÁO CÁO LAB 9

Sinh viên thực hiện	**Sinh viên 1** MSSV: Họ tên: Phan Võ Thiên Trường **Sinh viên 2** MSSV: Họ tên
Lớp	**NS011**
Tổng thời gian thực hiện Lab trung bình	
Phân chia công việc *(nếu là nhóm)*	**[Sinh viên 1]**: **[Sinh viên 2]**:
Link Video thực hiện *(nếu có yêu cầu)*	
Ý kiến *(nếu có)* *+ Khó khăn gặp phải* *+ Đề xuất, góp ý…*	
Điểm tự đánh giá *(bắt buộc)*	? /**10**

[Nội dung báo cáo chi tiết – Trình bày tùy sinh viên, Xuất file .PDF khi nộp]

Sử dụng CHR (Cloud Hosted Router) của Mikrotik để triển khai hệ thống VPN site to site kết nối 2 chi nhánh Hồ Chi Minh và Hà Nội

Môi trường: tạo 2 VM

- 1 VPS (ns011-w09-1) chạy CHR:có IP WAN và LAN.
  Trung: 103.232.123.214/24; LAN: 10.0.0.1/24
  Trường: 103.232.123.216/24; LAN: 10.0.1.1/24
  Giang: 103.232.123.218/24; LAN: 10.0.2.1/24
  Kha: 103.232.123.219/24; LAN: 10.0.3.1/24
- 1 VPS chạy Ubuntu chỉ có LAN, trỏ gateway về IP LAN của VPS CHR. (Sử dụng VM ns011-w9-2, card vmbr1)
  LAN network:
  Trung: 10.0.0.0/24
  Trường: 10.0.1.0/24
  Giang: 10.0.2.0/24
  Kha: 10.0.3.0/24

Yêu cầu làm việc team work: 2 bạn 1 team

- Team 1: Trung - Kha
- Team 2: Giang -Trường

Defaul login CHR: admin / trống

Disable tài khoản admin ngay lập tức, sử dụng tài khoản tên cá nhân. Đảm bảo mật khẩu phức tạp ítnhất 15 kí tự.

Tạo user mới

```
/user add name=truongpvt password=LionElJohnson_!q@w#e group=full
```

Sau đó disable user admin, thoát ra và đăng nhập lại bằng user đã tạo

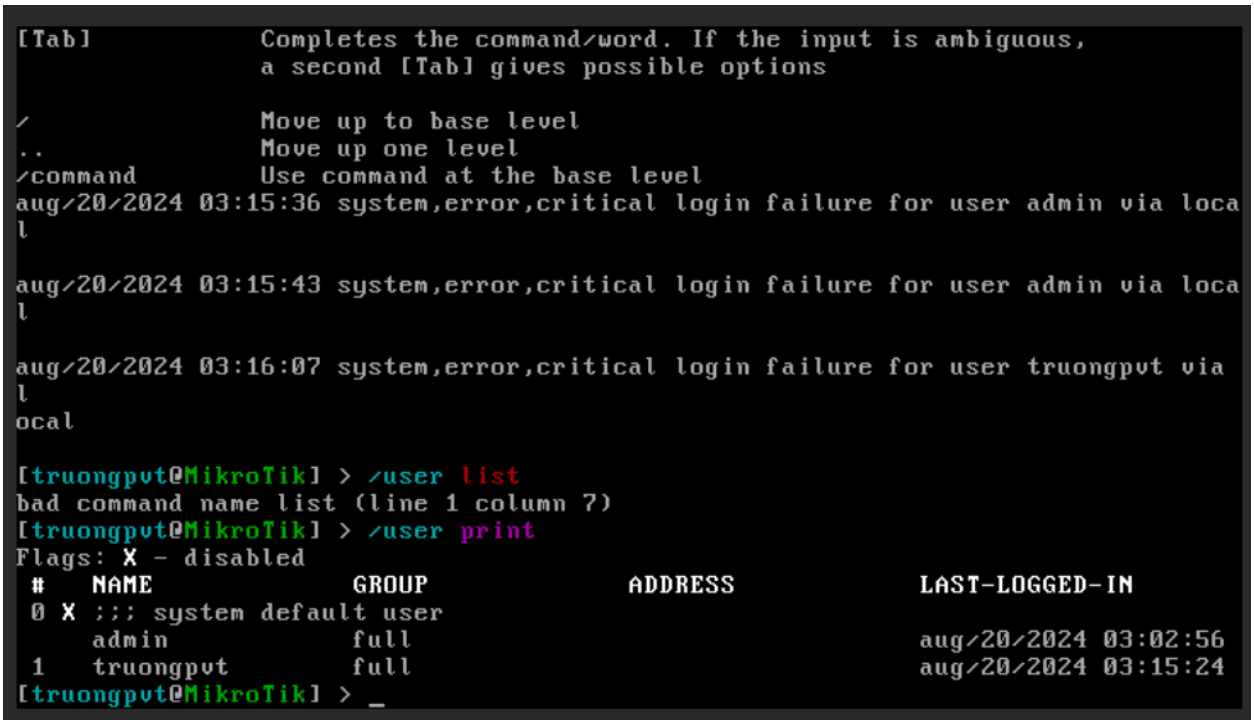
```
/user disable admin
/quit
```

Còn nếu xoá user admin

```
/user remove admin
```

Kiểm tra danh sách người dùng

```
/user print
```

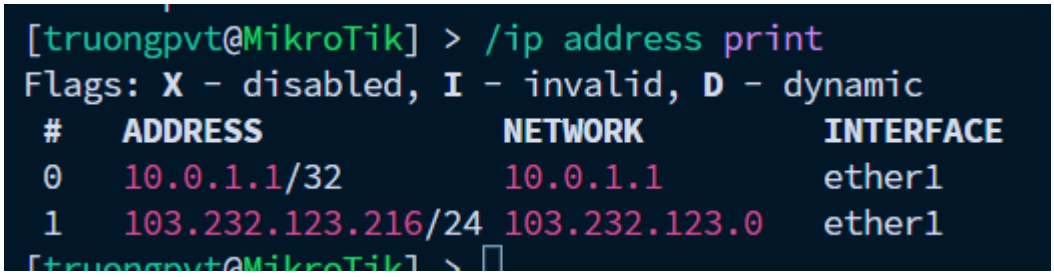


Đầu tiên em set IP WAN và LAN trên MikroTik

```
/ip address add address=103.232.123.216/24 interface=ether1

/ip address add address=10.0.1.1/24 interface=ether1
```

Kiểm tra cài đặt ip

```
/ip address print
```



Tiếp theo set gateway

```
/ip route add dst-address=0.0.0.0/0 gateway=103.232.123.1
```

Kiểm tra route

```
/ip route print
```

```
[truongpvt@MikroTik] > /ip route print
Flags: X - disabled, A - active, D - dynamic, C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 A S  0.0.0.0/0                          103.232.123.1             1
 1 ADC  10.0.1.1/32        10.0.1.1        ether1                    0
 2 ADC  103.232.123.0/24   103.232.123.216 ether1                    0
[truongpvt@MikroTik] >
```

Cấu hình DNS

```
/ip dns set servers=8.8.8.8,8.8.4.4
```

Restart lại system

```
/system reboot
```

Trên CHR tắt hết các dịch vụ, chỉ để lại dịch vụ SSH (7722), Winbox (7777).

Kiểm tra service đang chạy

```
/ip service print
```

Tắt các dịch vụ không cần

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

Set port cho SSH và Winbox

```
/ip service set ssh port=7722

/ip service set winbox port=7777
```

```
[truongpvt@MikroTik] > /ip service print
Flags: X - disabled, I - invalid
 #   NAME                          PORT ADDRESS                                 CERTIFICATE
 0 XI telnet                          23
 1 XI ftp                             21
 2 XI www                             80
 3    ssh                           7722
 4 XI www-ssl                        443                                        none
 5 XI api                           8728
 6    winbox                        7777
 7 XI api-ssl                       8729                                        none
```

Cấu hình GRE tunnel giữa 2 bạn với nhau dựa trên Mikrotik CHR. Đảm bảo có IPsec.

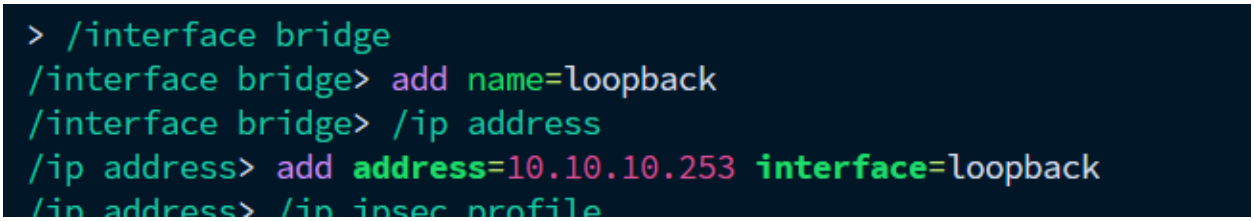
Link tham khảo: [GRE - RouterOS - MikroTik Documentation]

Trường: IPSEC: 10.10.10.253, GRE: 10.10.10.1

Giang: IPSEC: 10.10.10.254, GRE: 10.10.10.2

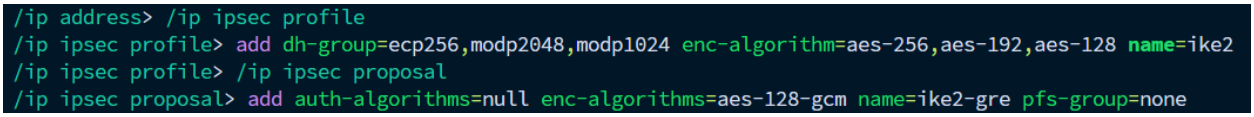
Đầu tiên tạo interface loopback bridge và gán IP cho nó

```
/interface bridge add name=loopback

/ip address add address=10.10.10.253 interface loopback
```



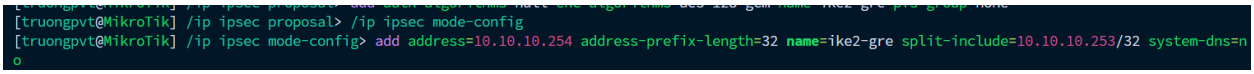
Tạo phase 1 profile và phase 2 proposal

```
/ip ipsec profile add dh-group=ecp256,modp2048,modp1024 enc-algorightm=aes-256,aes-192,aes-128 name=ike2

/ip ipsec proposal add auth-algorithms=null enc-algorithms=aes-128-gcm name=ike2-gre pfs-group=none
```



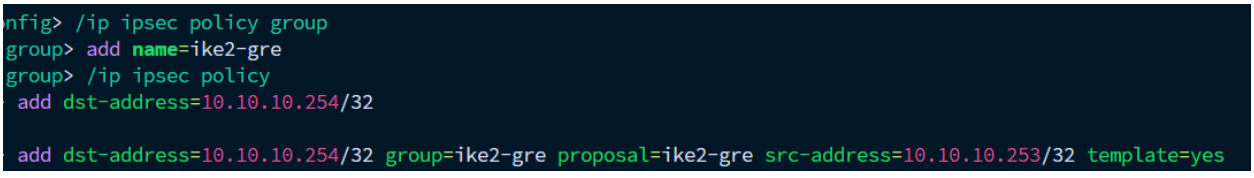
Tạo mode config entry với responder=yes

```
/ip ipsec mode-config add address=10.10.10.254 address-prefix-length=32 name=ike2-gre split-include=10.10.10.253/32 system-dns=no
```



Tạo policy group để tách riêng config này

```
/ip ipsec policy group add name=ike2-gre

/ip ipsec policy add dst-address=10.10.10.254/32 group=ike2-gre proposal=ike2-gre src-address=10.10.10.253/32 template=yes
```



Tạo peer config để lắng nghe tất cả IKEv2 requests

```
/ip ipsec peer add exchange-mode=ike2 name=ike2 passive=yes profile=ike2
```

```
y> /ip ipsec peer
 add exchange-mode=ike2 name=ike2 passive=yes profile=ike2
```

Tạo identity

/ip ipsec identity add generate-policy=port-strict mode-config=ike2-gre peer=ike2 policy-template-group=ike2-gre secret=test

```
/ip ipsec identity
ity> add generate-policy=port-strict mode-config=ike2-gre peer=ike2 policy-template-group=ike2-gre secret=test
```

Tạo interface gre-tunnel1 với ipsec local và ipsec remote

/interface gre add local-address=10.10.10.253 name=gre-tunnel1 remote-address=10.10.10.254

```
ity> /interface gre
 add local-address=10.10.10.253 name=gre-tunnel1 remote-address=10.10.10.254
```

Thêm ip address và route trên interface gre-tunnel1

/ip address add address=10.10.10.1/30 interface=gre-tunnel1

/ip route add dst-address=10.0.2.0/24 gateway=10.10.10.2

```
 gre> /ip address
s> add address=10.10.10.1

s> add address=10.10.10.1/30 interface=gre-tunnel1
s> /ip route
 add dst-network=10.0.2.0/24 gateway=10.10.10.2
 column 5)
 add dst-address=10.0.2.0/24 gateway=10.10.10.2
```

Kiểm tra bằng cách ping qua bên kia thông qua tunnel

```
truongpvt@MikroTik] > ping 10.10.10.2
 SEQ HOST                                     SIZE TTL TIME  STATUS
   0 10.10.10.2                                 56  64 0ms
   1 10.10.10.2                                 56  64 0ms
   2 10.10.10.2                                 56  64 0ms
   3 10.10.10.2                                 56  64 0ms
   4 10.10.10.2                                 56  64 0ms
   sent=5 received=5 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms

truongpvt@MikroTik] > ping 10.0.2.1
 SEQ HOST                                     SIZE TTL TIME  STATUS
   0 10.0.2.1                                   56  64 0ms
   1 10.0.2.1                                   56  64 0ms
   sent=2 received=2 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

Cấu hình LAN routing đảm bảo các VPS trong LAN của 2 bạn ping được IP của nhau.

Vì ip của VM nằm trong card mạng vmbr1 nên trên Mikrotic gán ip 10.0.1.1 trên interface ether2 thuộc vmbr1 là có thể ping tới.

```
Last login: Wed Aug 21 03:26:51 UTC 2024 on ttyS0
root@ns011-w09-truongpvt-2:~# 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=0.997 ms
64 bytes from 10.0.2.2: icmp_seq=2 ttl=62 time=1.55 ms
64 bytes from 10.0.2.2: icmp_seq=3 ttl=62 time=253 ms
64 bytes from 10.0.2.2: icmp_seq=4 ttl=62 time=571 ms
^C
--- 10.0.2.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 0.997/206.487/570.695/233.992 ms
```

Cấu hình Nat Outbound đảm bảo VM2 có thể đi ra internet thông qua CHR. Cấu hình Nat Inbound đảm bảo từ bên ngoài có thể SSH đến VM2 qua port 2222.

Thêm rule nat trong firewall vào với source từ lớp mạng 10.0.1.0/24

```
/ip firewall nat add chain=scrnat src-address=10.0.1.0/24 action=masquerade
```

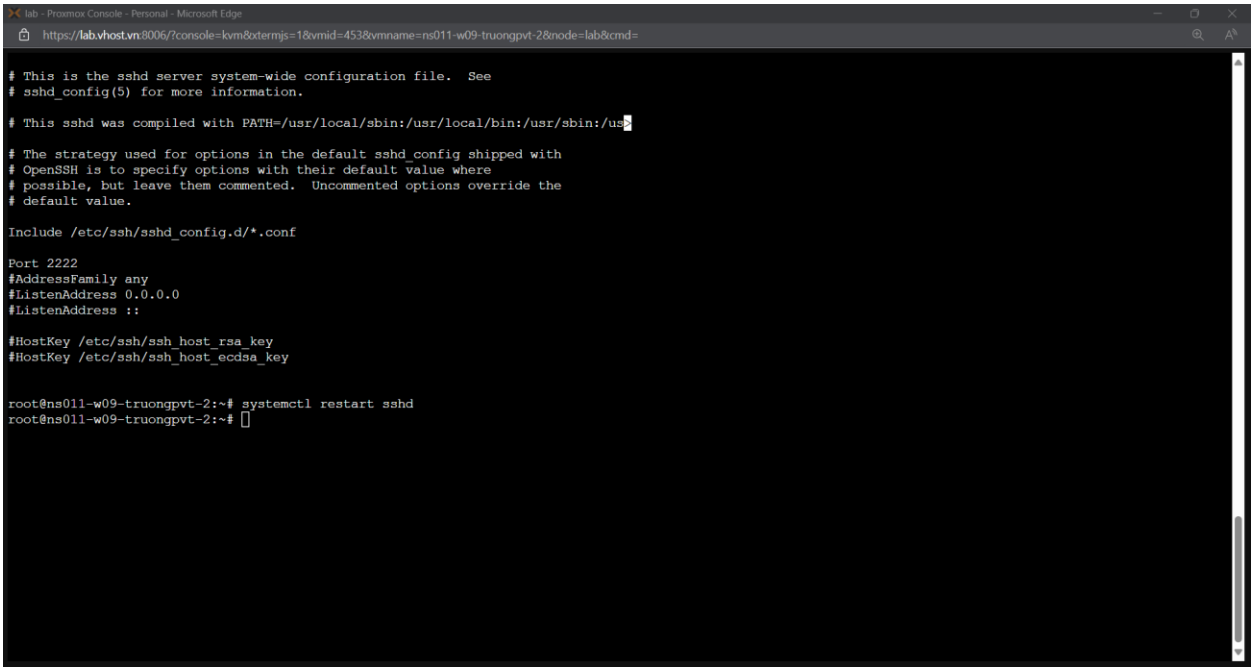
```
[truongpvt@MikroTik] > ip firewall nat add chain=srcnat src-address=10.0.1.0/24 action=masquerade
[truongpvt@MikroTik] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0    chain=srcnat action=masquerade src-address=10.0.1.0/24
```

Kiểm tra kết quả NAT ra ngoài

```
root@ns011-w09-truongpvt-2:~# 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=117 time=603 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=594 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=292 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=22.0 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=117 time=22.1 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=117 time=230 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=117 time=640 ms
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 7 received, 12.5% packet loss, time 7002ms
rtt min/avg/max/mdev = 21.979/343.344/640.124/250.765 ms
root@ns011-w09-truongpvt-2:~#
```

Tiếp đến thêm rule để có thể SSH từ bên ngoài vào VM2 thông qua port 2222

Thay đổi port SSH thành 2222 trên VM2 và restart SSHD



Thêm rule Firewall NAT từ ngoài vào và rule filter chấp nhận kết nối đến port 2222

```
/ip firewall nat add chain=dstnat protocol=tcp dst-port=2222 action=dst-nat to-addresses=10.0.1.2 to-ports=2222
```

/ip firewall filter add chain=input protocol=tcp dst-port=2222 action=accept

```
> /ip firewall nat add chain=dstnat protocol=tcp dst-port=2222 action=dst-nat to-addresses=10.0.1.2 to-ports=2222
> /ip firewall filter add chain=input protocol=tcp dst-port=2222 action=accept
>
```

Kiểm tra kết quả SSH

Tìm hiểu các tính năng có thể sử dụng của VPS trên trang https://members.vhost.vn

Kiểm tra các tính năng của VPS trên trang https://members.vhost.vn xem có hoạt động đúng như tên gọi không?