**Hướng dẫn lab: VPN Site to Site – MikroTik**

### **1. Chuẩn bị môi trường**

* **4 VM trên VMware:**
  + **VM 1:** MikroTik Site 1 (Router) - 2 NIC:
    - NIC 1 (LAN): Kết nối với mạng LAN Site 1.
    - NIC 2 (WAN): Kết nối với mạng WAN.
  + **VM 2:** MikroTik Site 2 (Router) - 2 NIC:
    - NIC 1 (LAN): Kết nối với mạng LAN Site 2.
    - NIC 2 (WAN): Kết nối với mạng WAN.
  + **VM 3:** Ubuntu Server Site 1 (Client) - 1 NIC:
    - Kết nối với mạng LAN Site 1.
  + **VM 4:** Ubuntu Server Site 2 (Client) - 1 NIC:
    - Kết nối với mạng LAN Site 2.
* **Cấu hình mạng trên VMware:**
  + Tạo 2 mạng LAN riêng biệt:
    - LAN Site 1: VMnet1 (Host-only) cho MikroTik Site 1 và Client Site 1.
    - LAN Site 2: VMnet2 (Host-only) cho MikroTik Site 2 và Client Site 2.
  + Tạo mạng WAN:
    - VMnet3 (Host-only hoặc NAT tùy ý) để kết nối WAN giữa MikroTik Site 1 và MikroTik Site 2.

### **2. Phân bổ IP**

* **Site 1:**
  + **Client Site 1:** IP: 10.0.1.2/24, Gateway: 10.0.1.1.
  + **MikroTik Site 1:**
    - LAN: 10.0.1.1/24 (ether1).
    - WAN: 45.122.223.81/24 (ether2).
* **Site 2:**
  + **Client Site 2:** IP: 10.0.2.2/24, Gateway: 10.0.2.1.
  + **MikroTik Site 2:**
    - LAN: 10.0.2.1/24 (ether1).
    - WAN: 45.122.223.85/24 (ether2).

### 3. Bảo mật MikroTik trước khi cấu hình IP ra Net

#### - Cả 2 máy MikroTik Site 1 và MikroTik Site 2 thực hiện các bước sau:

1. **Đổi lại mật khẩu mặc định nếu đang để đơn giản**

/user

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

1. **Tắt dịch vụ không cần thiết (Giữ lại winbox và ssh (tuỳ chọn)):**

/ip service

disable telnet

disable ftp

disable www

disable api

1. **Bảo mật nâng cao (Firewall)**

/ip address

/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=esp comment="Allow IPsec ESP"

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

### 4**. Cấu hình IP cơ bản trên MikroTik**

#### MikroTik Site 1

1. **Đăng nhập vào MikroTik Site 1**(qua Winbox hoặc terminal).
2. **Cấu hình IP:**

/ip address

add address=10.0.1.1/24 interface=ether1

add address=45.122.223.81/24 interface=ether2

1. **Cấu hình Gateway:**

/ip route

add gateway=45.122.223.85

1. **NAT (Masquerade) để Client Site 2 ra WAN:**

/ip firewall nat

add chain=srcnat out-interface=ether2 action=masquerade

#### **MikroTik Site 2**

1. **Đăng nhập vào MikroTik Site 2**.
2. **Cấu hình IP:**

/ip address

add address=10.0.2.1/24 interface=ether1

add address=45.122.223.85/24 interface=ether2

1. **Cấu hình Gateway:**

/ip route

add gateway=45.122.223.81

1. **NAT (Masquerade) để Client Site 2 ra WAN:**

/ip firewall nat

add chain=srcnat out-interface=ether2 action=masquerade

### **4. Cấu hình VPN IPsec Site-to-Site**

#### **MikroTik Site 1**

1. **Tạo IPsec Proposal:**

/ip ipsec proposal

add name=proposal1 auth-algorithms=sha1 enc-algorithms=aes-128-cbc pfs-group=modp1024

1. **Tạo IPsec Peer:**

/ip ipsec peer

add address=45.122.223.85/32 secret="your-secret-key" exchange-mode=main

**Lưu ý:** Thay "your-secret-key" bằng một chuỗi bí mật giống nhau trên cả hai MikroTik.

Đặt là: VPN\_CyberKing999

1. **Tạo IPsec Policy:**

/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=address=45.122.223.85

1. **Cấu hình route tĩnh để định tuyến qua VPN:**

/ip route

add dst-address=10.0.2.0/24 gateway=45.122.223.85

**Lưu ý:** Thay "your-secret-key" bằng một chuỗi bí mật giống nhau trên cả hai MikroTik.

Đặt là: VPN\_CyberKing999

#### **MikroTik Site 2**

1. **Tạo IPsec Proposal:**

/ip ipsec proposal

add name=proposal1 auth-algorithms=sha1 enc-algorithms=aes-128-cbc pfs-group=modp1024

1. **Tạo IPsec Peer:**

/ip ipsec peer

add address=45.122.223.81/32 secret="your-secret-key" exchange-mode=main

**Lưu ý:** Thay "your-secret-key" bằng một chuỗi bí mật giống nhau trên cả hai MikroTik.

Đặt là: VPN\_CyberKing999

1. **Tạo IPsec Policy:**

/ip ipsec policy

add src-address=10.0.2.0/24 dst-address=10.0.1.0/24 tunnel=yes action=encrypt proposal=proposal1 peer=address=45.122.223.81

1. **Cấu hình route tĩnh để định tuyến qua VPN:**

/ip route

add dst-address=10.0.1.0/24 gateway=45.122.223.81

### **5. Cấu hình Client**

#### **Client Site 1 (Ubuntu Server)**

1. **Cấu hình IP:**

sudo nano /etc/netplan/01-netcfg.yaml

Nội dung:

yaml

network:

version: 2

ethernets:

ens33:

addresses:

- 10.0.1.2/24

gateway4: 10.0.1.1

nameservers:

addresses: [8.8.8.8]

Áp dụng:

sudo netplan apply

#### **Client Site 2 (Ubuntu Server)**

1. **Cấu hình IP:**

sudo nano /etc/netplan/01-netcfg.yaml

Nội dung yaml:

network:

version: 2

ethernets:

ens33:

addresses:

- 10.0.2.2/24

gateway4: 10.0.2.1

nameservers:

addresses: [8.8.8.8]

Áp dụng:

sudo netplan apply

### **6. Kiểm tra VPN**

1. **Ping từ Client Site 1 sang Client Site 2:**
   * Trên Client Site 1:

ping 10.0.2.2

* + Nếu thành công, VPN đã hoạt động.

1. **Kiểm tra mã hóa trên MikroTik:**
   * Trên MikroTik Site 1 hoặc Site 2:

/ip ipsec installed-sa print

* + Nếu thấy SA (Security Association) được thiết lập, lưu lượng đã được mã hóa.

### **7. Xử lý sự cố (nếu cần)**

* **Không ping được:**
  + Kiểm tra firewall trên MikroTik: Đảm bảo không chặn ICMP hoặc IPsec (ESP, UDP 500, UDP 4500).
  + Kiểm tra IPsec Peer: Đảm bảo secret key khớp nhau.
* **Kiểm tra kết nối WAN:**
  + Từ MikroTik Site 1 ping 45.122.223.85 và ngược lại.

### **Kết quả mong đợi**

* Client Site 1 (10.0.1.2) ping được Client Site 2 (10.0.2.2).
* Lưu lượng giữa hai site được mã hóa qua VPN IPsec.