**CẤU HÌNH SITE-TO-SITE IPSEC VPN**

**4.1. Khái Niệm IPsec VPN**

**IPsec (Internet Protocol Security)** là bộ giao thức bảo mật mã hóa lưu lượng IP, bao gồm:

1. **IKE Phase 1 (ISAKMP)**: Thiết lập SA (Security Association) bảo mật
   * Xác thực: Pre-Shared Key (PSK) hoặc Certificate
   * Mã hóa: DES, 3DES, AES
   * Hashing: MD5, SHA
2. **IKE Phase 2 (IPsec)**: Thiết lập IPsec tunnel
   * ESP (Encapsulating Security Payload): Mã hóa + xác thực
   * AH (Authentication Header): Chỉ xác thực
3. **Crypto ACL**: Định nghĩa lưu lượng cần mã hóa

**4.2. Cấu Hình IPsec VPN trên HCM-EDGE**

enable

configure terminal

! ============================================

! BƯỚC 1: IKE PHASE 1 (ISAKMP Policy)

! ============================================

crypto isakmp policy 10

encryption aes 256

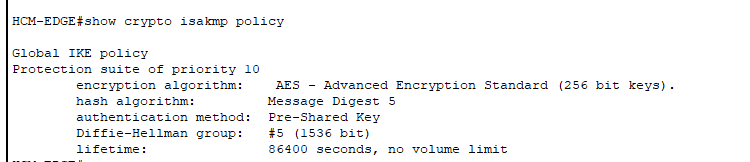
authentication pre-share

group 5

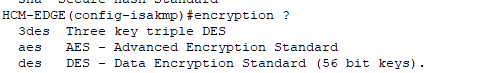
hash md5

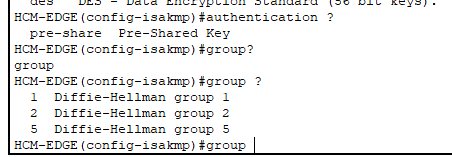
lifetime 86400

exit



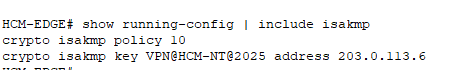






! === Pre-Shared Key ===

crypto isakmp key VPN@HCM-NT@2025 address 203.0.113.6



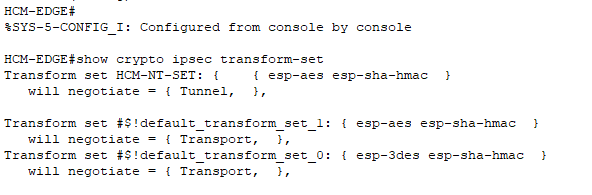
! ============================================

! BƯỚC 2: IKE PHASE 2 (IPsec Transform Set)

! ============================================

crypto ipsec transform-set HCM-NT-SET esp-aes esp-sha-hmac

exit



! ============================================

! BƯỚC 3: CRYPTO ACL (Lưu lượng cần mã hóa)

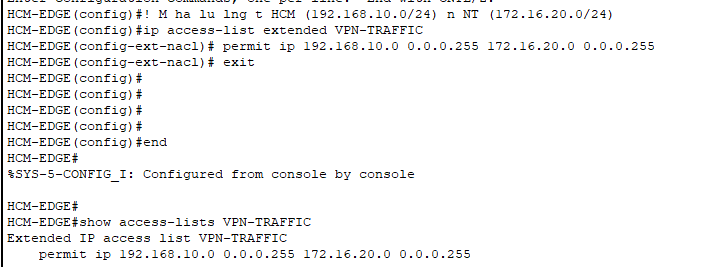
! ============================================

! Mã hóa lưu lượng từ HCM (192.168.10.0/24) đến NT (172.16.20.0/24)

ip access-list extended VPN-TRAFFIC

permit ip 192.168.10.0 0.0.0.255 172.16.20.0 0.0.0.255

exit



! ============================================

! BƯỚC 4: CRYPTO MAP

! ============================================

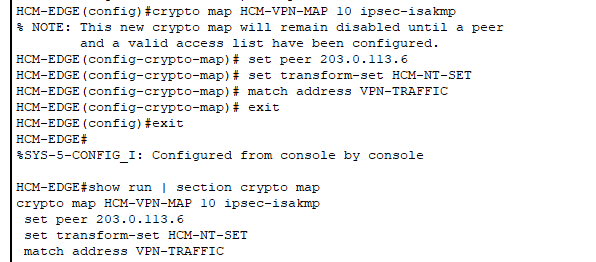
crypto map HCM-VPN-MAP 10 ipsec-isakmp

set peer 203.0.113.6

set transform-set HCM-NT-SET

match address VPN-TRAFFIC

exit



! ============================================

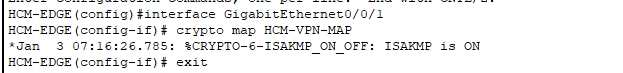
! BƯỚC 5: GẮN CRYPTO MAP VÀO INTERFACE OUTSIDE

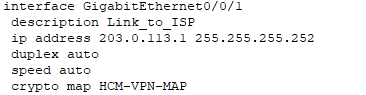
! ============================================

interface GigabitEthernet0/0/1

crypto map HCM-VPN-MAP

exit





! ============================================

! BƯỚC 6: ĐỊNH TUYẾN ĐẾN MẠNG REMOTE

! ============================================

! Route tĩnh đến mạng NT qua VPN

ip route 172.16.20.0 255.255.255.0 203.0.113.6

! ============================================

! BƯỚC 7: LOẠI TRỪ LƯU LƯỢNG VPN KHỎI NAT

! ============================================

! Sửa lại ACL 1 để loại trừ lưu lượng VPN

no access-list 1

access-list 1 permit 192.168.10.0 0.0.0.255

no access-list 1

! Dòng thứ hai: NAT toàn bộ lưu lượng nội bộ HCM ra Internet

access-list 1 permit 192.168.10.0 0.0.0.255

! =========================================

! CẤU HÌNH NAT OVERLOAD (PAT)

! =========================================

ip nat inside source list 1 interface GigabitEthernet0/0/1 overload

! =========================================

! PHÂN LOẠI INTERFACE NAT

! =========================================

interface GigabitEthernet0/0/0

description \*\*\* LAN interface to HCM-CORE \*\*\*

ip nat inside

!

interface GigabitEthernet0/0/1

description \*\*\* WAN interface to ISP \*\*\*

ip nat outside

*→ NAT chỉ dùng cho Internet, VPN vẫn hoạt động vì gói đến 172.16.20.0/24 đi qua tunnel, không bị NAT*

end

copy running-config startup-config

**4.3. Cấu Hình IPsec VPN trên NT-EDGE**

enable

configure terminal

! ============================================

! BƯỚC 1: IKE PHASE 1

! ============================================

crypto isakmp policy 10

encryption aes 256

authentication pre-share

group 5

hash md5

lifetime 86400

exit

! === Pre-Shared Key (PHẢI GIỐNG HCM) ===

crypto isakmp key VPN@HCM-NT@2025 address 203.0.113.2

! ============================================

! BƯỚC 2: IKE PHASE 2

! ============================================

crypto ipsec transform-set HCM-NT-SET esp-aes esp-sha-hmac

exit

! ============================================

! BƯỚC 3: CRYPTO ACL (Ngược lại với HCM)

! ============================================

ip access-list extended VPN-TRAFFIC

permit ip 172.16.20.0 0.0.0.255 192.168.10.0 0.0.0.255

exit

! ============================================

! BƯỚC 4: CRYPTO MAP

! ============================================

crypto map NT-VPN-MAP 10 ipsec-isakmp

set peer 203.0.113.2

set transform-set HCM-NT-SET

match address VPN-TRAFFIC

exit

! ============================================

! BƯỚC 5: GẮN CRYPTO MAP

! ============================================

interface GigabitEthernet0/0/1

crypto map NT-VPN-MAP

exit

! ============================================

! BƯỚC 6: ĐỊNH TUYẾN

! ============================================

ip route 192.168.10.0 255.255.255.0 203.0.113.2

! ============================================

! BƯỚC 7: LOẠI TRỪ VPN KHỎI NAT

! ============================================

! =========================================

! ACL CHO NAT LAN

! =========================================

no access-list 1

access-list 1 permit 172.16.20.0 0.0.0.255

! =========================================

! NAT OVERLOAD (PAT)

! =========================================

ip nat inside source list 1 interface GigabitEthernet0/0/1 overload

! =========================================

! GẮN NAT CHO INTERFACE

! =========================================

interface GigabitEthernet0/0/0

description \*\*\* LAN interface to NT-CORE \*\*\*

ip nat inside

!

interface GigabitEthernet0/0/1

description \*\*\* WAN interface to ISP \*\*\*

ip nat outside

end

copy running-config startup-config

**4.4. Cấu Hình ISP-ROUTER (Giả Lập Internet)**

enable

configure terminal

hostname ISP-ROUTER

! === Interface đến HCM ===

interface GigabitEthernet0/0

description \*\*\* Link to HCM \*\*\*

ip address 203.0.113.1 255.255.255.252

no shutdown

exit

! === Interface đến NT ===

interface GigabitEthernet0/1

description \*\*\* Link to NT \*\*\*

ip address 203.0.113.5 255.255.255.252

no shutdown

exit

! === Static Routes ===

ip route 203.0.113.2 255.255.255.255 GigabitEthernet0/0

ip route 203.0.113.6 255.255.255.255 GigabitEthernet0/1

end

copy running-config startup-config