**Lệnh kiểm tra:**

**Sh ru**

**Nội dung ôn tập cuối kỳ:**

**1. Định tuyến OSPF**

en

conf t

router ospf 100

network 192.168.1.0 0.0.0.255 area 0

network 192.168.2.0 0.0.0.3 area 0

**1.1. Định tuyến RIP**

en

conf t

ro ri

net 192.168.2.1

net 192.168.4.2

**1.2. Định tuyến EIGRP**

en

conf t

router ospf 100

network 192.168.1.0 0.0.0.255

network 192.168.2.0 0.0.0.3  
no auto-summary

**1.3. Định tuyến GHCP**

Router(config)# ip dhcp pool VLAN\_10

Router(dhcp-config)# network 172.16.10.0 255.255.255.0

Router(dhcp-config)# default-router 172.16.10.1

Router(dhcp-config)# dns-server 172.16.2.10

Router(config)# ip dhcp excluded-address 172.16.10.1 172.16.10.20

Router(dhcp-config)# option 150 ip 172.16.2.20

Router(config)# end

**1.4. Định tuyến NAT**

en

conf t

ip nat inside source list 1 interface se0/1/0 overload

**2. Cấu hình Trunk**

En

Conf t

Int rang g0/1 – 2

Switchport mode trunk

switchport access vlan 10

Switchport trunk native vlan 99

**2.1 Cấu hình VLAN**

Int gig0/1/0

switchport mode access

switchport access vlan 10

**3. Cấu hình port security**

Switch(config)# interface FastEthernet0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport port-security

Switch(config-if)# switchport port-security maximum 1

Switch(config-if)# switchport port-security mac-address sticky CAFE.CAFE.8000

**4. Cấu hình AAA**

En

Conf t

Hostname VPN-GW

enable secret 2112998

ip domain-name 2112998.com

crypto key generate rsa

1024

aaa new-model

aaa authentication login default group tacacs+ none

aaa authentication login telnet\_lines group tacacs+

aaa accounting exec default start-stop group tacacs+

tacacs-server host 192.168.99.200 key ciscosecret

line vty 0 4

logging synchronous

login authentication telnet\_lines

**5. Cấu hình VPN**

License boot module c1900 technology-package securityk9

Yes

Wri

Reload

Crypto isakmp policy 10

Authentication pre-share

Encryption 3des

Hash sha

Gpoup 5

Crypto isakmp key cisco address 192.168.3.2

crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac

crypto map VPN-MAP 10 ipsec-isakmp

match address 100

set transform-set VPN-SET

192.168.1.254

set peer 192.168.1.254

exit

int g0/0/0

crypto map VPN-MAP

**6. Lý thuyết chương IDS/IPS**

**Hệ thống phát hiện xâm nhập (IDS)** là một khái niệm quen thuộc trong lĩnh vực bảo mật. Hãy cùng tìm hiểu về nó:

1. **IDS là gì?**
   * **IDS** (Intrusion Detection System) là hệ thống phát hiện xâm nhập. Nó là một phần của các công cụ bảo mật lớn hơn và có nhiệm vụ giám sát lưu lượng truy cập mạng, phát hiện và thông báo về các hoạt động nghi ngờ.
   * IDS không có khả năng “phản ứng” lại các xâm nhập, chỉ giám sát và báo cáo.
   * IDS là một phần quan trọng trong hệ thống bảo mật, giúp duy trì vận hành ổn định cho toàn mạng lưới.
2. **Chức năng chính của IDS:**
   * Giám sát lưu lượng truy cập mạng, phát hiện hoạt động nghi ngờ.
   * Cảnh báo xâm nhập cho đội quản trị mạng.
   * Phối hợp với tường lửa và phần mềm diệt virus để tạo nên hệ thống bảo mật hoàn chỉnh.
3. **Phân loại IDS:**
   * **Network IDS**: Bố trí tại vị trí dễ bị tấn công nhất trong một hệ thống. Theo dõi lưu lượng truy cập, phát hiện bất thường.
   * **Nod Network IDS**: Tương tự Network IDS, nhưng chỉ tác dụng cho một máy chủ trong khoảng thời gian xác định.
   * **Host IDS**: Hoạt động trên mọi thiết bị có kết nối internet trong hệ thống, bao gồm cả phần còn lại của mạng lưới doanh nghiệp.
4. **Ưu điểm và nhược điểm của IDS:**
   * **Ưu điểm**: Phát hiện sớm bất thường, giúp bảo mật hiệu quả hơn.
   * **Nhược điểm**: Không thể phát hiện đợt tấn công theo dạng truy cập mã hóa và đôi khi cần thao tác thủ công để điều chỉnh cấu hình.
5. **Phân biệt giữa IDS, IPS và tường lửa**:
   * **IDS**: Giám sát và báo cáo xâm nhập.
   * **IPS (Intrusion Prevention System)**: Ngăn chặn xâm nhập.
   * **Tường lửa**: Kiểm soát luồng dữ liệu giữa mạng nội bộ và mạng bên ngoài.
6. **Cách triển khai IDS trong mạng doanh nghiệp**:
   * **Đặt ở vị trí giữa router và firewall**: Giám sát lưu lượng truy cập từ bên ngoài vào mạng nội bộ.
   * **Đặt sau firewall**: Giám sát lưu lượng truy cập từ mạng nội bộ ra bên ngoài.
7. **Lý thuyết chương layer 2 security**

**Layer 2 security** là một khía cạnh quan trọng trong bảo mật mạng, đặc biệt là khi chúng ta xem xét các thiết bị **switch**. Dưới đây là một số khái niệm và thực hành quan trọng liên quan đến bảo mật tại **Layer 2**:

1. **Port Security**:
   * **Port security** là tính năng bảo mật tại **Layer 2** trên các cổng của switch.
   * Nó giới hạn việc truy cập vào cổng dựa trên địa chỉ MAC của các thiết bị kết nối.
   * Chỉ cho phép các địa chỉ MAC an toàn truy cập, từ chối tất cả các thiết bị khác.
   * **Port security** giúp kiểm soát mở rộng không ủy quyền của mạng và bảo vệ khỏi tấn công bằng bảng địa chỉ MAC.
2. **Các thực hành tốt cho Layer 2 security**:
   * **Quản lý switch một cách an toàn**:
     + Sử dụng SSH, cơ chế xác thực, danh sách truy cập và đặt cấp độ đặc quyền.
     + Hạn chế truy cập quản lý để không cho phép mạng không đáng tin cậy khai thác giao diện quản lý và giao thức SNMP.
   * **Sử dụng VLAN ID riêng cho các cổng trunk**:
     + Tránh sử dụng VLAN 1 cho bất kỳ mục đích nào khác.
   * **Tắt DTP (Dynamic Trunking Protocol) trên các cổng không phải trunk**:
     + Ngăn chặn việc tự động thiết lập trunking trên các cổng không cần thiết.
   * **Triển khai tính năng Port Security**:
     + Ngăn chặn truy cập trái phép từ các cổng chuyển mạch.
   * **Sử dụng Private VLAN** (nếu phù hợp):
     + Phân chia lưu lượng mạng tại **Layer 2**.
   * **Sử dụng MD5 authentication** (nếu phù hợp).
   * **Tắt CDP (Cisco Discovery Protocol)** nếu không cần thiết.
   * **Ngăn chặn tấn công từ chối dịch vụ và khai thác khác**:
     + Tắt các dịch vụ và giao thức không sử dụng.
     + Vô hiệu hóa các cổng không sử dụng trên switch và đặt chúng vào một VLAN không được sử dụng cho hoạt động bình thường.
   * **Sử dụng các cơ chế bảo mật cổng**:
     + Bảo vệ khỏi tấn công tràn bảng địa chỉ MAC.
     + Sử dụng các tính năng bảo mật cấp cổng như DHCP Snooping, IP Source Guard và ARP security (nếu phù hợp).
   * **Kích hoạt các tính năng Spanning Tree Protocol** (ví dụ: BPDU Guard, Loopguard và Root Guard).
   * **Sử dụng ACLs (Access Control Lists) trên Switch IOS** để lọc lưu lượng không mong muốn (IP và không phải IP).

**8. ACL**

Access-list 100 per ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255

**9. Tunnel IPv4**

int Tunnel1

Tunnel source g0/0/0

tunnel destination 209.165.201.2

ip add 192.168.99.1 255.255.255.252

no shut

**10. Tunnel IPv6**

**Đề giữa kỳ**

**Câu 1: gắn địa chỉ phụ**

en

conf t

int Gi0/0

no shut

int gi0/0.10

encapsulation dot1Q 10

ip add 172.16.10.1 255.255.255.0

no shut

int gi0/0.20

encapsulation dot1Q 20

ip add 172.16.20.1 255.255.255.0

no shut

int gi0/0.30

encapsulation dot1Q 30

ip add 172.16.30.1 255.255.255.0

no shut

**ROUTER**

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

ip nat inside source list 100 interface GigabitEthernet0/0/0 overload

ip classless

ip route 10.0.0.0 255.255.255.252 10.0.0.5

ip route 10.0.0.12 255.255.255.252 192.168.99.2

ip route 10.0.0.6 255.255.255.255 GigabitEthernet0/1/0

ip route 172.16.10.0 255.255.255.0 10.0.0.5

ip route 172.16.20.0 255.255.255.0 10.0.0.5

ip route 172.16.30.0 255.255.255.0 10.0.0.5

ip route 192.168.1.0 255.255.255.0 10.0.0.5

ip route 192.168.10.0 255.255.255.0 192.168.99.2

ip route 209.165.200.0 255.255.255.252 GigabitEthernet0/0/0

ip route 0.0.0.0 0.0.0.0 209.165.200.2

**VLAN**

crypto isakmp policy 10

encr 3des

authentication pre-share

group 5

crypto isakmp key antoan address 192.168.1.254

crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac

crypto map VPN-MAP 10 ipsec-isakmp

set peer 192.168.1.254

set transform-set VPN-SET

match address 100

access-list 100 permit ip 172.16.20.0 0.0.0.255 192.168.10.0 0.0.0.255

access-list 100 permit ip 172.16.30.0 0.0.0.255 192.168.10.0 0.0.0.255

crypto map VPN-MAP 10 ipsec-isakmp

set peer 10.0.0.14

crypto isakmp key antoan address 10.0.0.1

**AAA**

En

Conf t

Hostname VPN-GW

enable secret 2112998

ip domain-name 2112998.com

crypto key generate rsa

1024

aaa new-model

aaa authentication login default group tacacs+ none

aaa authentication login telnet\_lines group tacacs+

aaa accounting exec default start-stop group tacacs+

tacacs-server host 192.168.99.200 key ciscosecret

line vty 0 4

logging synchronous

login authentication telnet\_lines

**NAT**

en

conf t

ip nat inside source list 1 interface g0/0/0 overload

**Tunnel1**

int Tunnel1

Tunnel source g0/0/0

tunnel destination 209.165.201.2

ip add 192.168.99.1 255.255.255.252

no shut

**RIP**

En

Conf t

Router rip

Ver 2

No au

Net 10.0.0.0

Net 10.0.0.4

**Gắn ip helper-address**

int gi0/0/0.10

ip helper-address 192.168.99.99

no shut

int gi0/0/0.20

ip helper-address 192.168.99.99

no shut

int gi0/0/0.70

ip helper-address 192.168.99.99

no shut

int gi0/0/0.88

ip helper-address 192.168.99.99

no shut

**GW**

**Gắn tunnel**

en

conf t

int Tunnel1

ip add 1.1.1.1 255.255.255.252

no shut

int Tunnel2

Tunnel source s0/1/1

tunnel destination 209.165.203.2

ip add 2.2.2.1 255.255.255.252

no shut

en

conf t

int Se0/1/0

no shut

en

conf t

int Se0/1/1

no shut

en

conf t

ro ri

net 10.0.0.2

net 209.165.201.1

default-information originate

**Nha Trang**

en

conf t

int Tunnel2

Tunnel source s0/1/0

tunnel destination 209.165.201.1

ip add 2.2.2.2 255.255.255.252

no shut

en

conf t

ro ri

net 209.165.202.2

net 192.168.4.1

en

conf t

ip nat inside source list 1 interface se0/1/0 overload

**DL01\_VPN\_Gateway**

en

conf t

ro ri

net 192.168.2.1

net 192.168.4.2

**Đà lạt**

en

conf t

ip nat inside source list 1 interface se0/1/0 overload