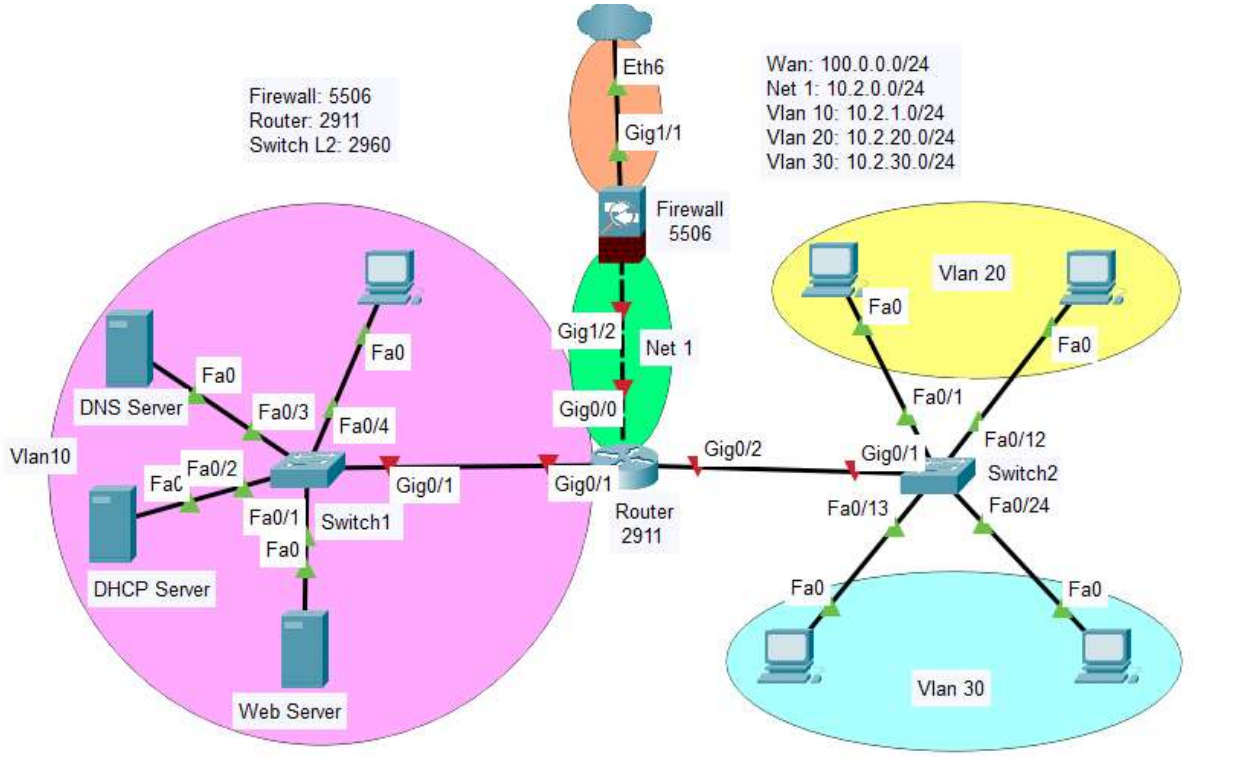
ĐỀ SỐ 2

ĐỀ KIỂM TRA
MÔN: PHÂN TÍCH THIẾT KẾ HỆ THỐNG MẠNG
Thời gian: 90 phút (không tính thời gian giao đề)

1. SƠ ĐỒ



2. MÔ TẢ THIẾT BỊ VÀ KẾT NỐI

Thiết bị	Cổng	IP Address/subnet	Kết nối	Chức năng / Ghi chú
Cloud	—	100.0.0.1/24		(Internet)
Firewall 5506	Gig1/1 (outside)	100.0.0.2/24		Cloud
	Gig1/2 (inside)	10.2.0.1/24	Gig0/0 Router	Kết nối Router
Router 2911	Gig0/0	10.2.0.2/24	Gig1/2 Firewall	Kết nối ASA (inside)
	Gig0/1	10.2.1.1/24	Gig0/1 Switch1	Mạng Server
	Gig0/2.20	10.2.20.1/24	VLAN 20	Subinterface
	Gig0/2.30	10.2.30.1/24	VLAN 20	Subinterface
Switch1 2960	Fa0/21–24	—		VLAN10 (DMZ)
	Gig0/1; Gig0/2	trunk	Gig0/1 Router	Mạng server
Switch2 2960	Gig0/1, Gig0/2	trunk	Gig0/2 Router	Vlan 20/30
	Fa0/1–12	—		VLAN20
	Fa0/13–24	—		VLAN30
Web Server		10.2.1.2/24	Fa0/1 Switch 1	
DHCP Server		10.2.1.3/24	Fa0/2 Switch 1	
DNS Server		10.2.1.4/24	Fa0/3 Switch 1	
PC		IP động	Fa0/3 Switch 1	DHCP Server cấp

3. YÊU CẦU:

Câu 1: Dựng sơ đồ mạng với các chú thích đầy đủ; phân vùng các mạng rõ ràng

Câu 2: Cấu hình Switch L2 và Router tạo các VLAN: VLAN10, VLAN20, VLAN30, Gán port tương ứng tại các Switch L2 và trunk kết nối lên Router

Câu 3: Cấu hình các Server trong VLAN10 gồm:

- Web Server (10.2.1.2) với các thông tin sinh viên : Họ tên, Lớp, thi môn;
- DHCP Server (10.2.1.3) cấp phát IP động cho VLAN 10/20/30.
- DNS Server (10.2.1.4) với tên miền www.cntt.com trỏ vào máy Web Server

Câu 4: Cấu hình Router:

- Định tuyến nội bộ giữa các VLAN và bật ip routing.
- Sử dụng lệnh ip helper-address tại các VLAN để chuyển yêu cầu DHCP về server.
- Tạo ACL nội bộ tại Router để:
    + Cấm máy 10.2.1.254 truy cập các Vlan 20/30
    + Cấm máy 10.2.20.254 truy cập vào máy Web Server

Câu 5: Cấu hình ASA firewall

- NAT Overload toàn mạng nội bộ ra ngoài Internet.
- Cấu hình NAT tĩnh ánh xạ Web Server (10.2.1.2) ra địa chỉ công cộng trên ASA (Interface Outside)
- Cho phép IP 203.11.1.1 truy cập Web Server qua cổng 80; Chặn IP 203.113.1.2 truy cập Web Server qua cổng 80
- Cho phép các kết nối khác truy cập vào bên trong

Lưu ý: *Sinh viên không sử dụng tài liệu, không trao đổi bài*

CÂU LỆNH

1. SWITCH1

```
enable
configure terminal
hostname switch1
vlan 10
name DMZ
exit
interface range fa0/1-24
switchport mode access
switchport access vlan 10
exit
interface gig0/1
switchport mode trunk
exit
interface gig0/2
switchport mode trunk
exit
end
copy running-config startup-config
```

2. SWITCH2

```
enable
configure terminal
hostname switch2
vlan 20
name VLAN20
exit
vlan 30
name VLAN30
exit
interface range fa0/1-12
switchport mode access
switchport access vlan 20
no shutdown
exit
interface range fa0/13-24
switchport mode access
switchport access vlan 30
no shutdown
exit
interface gig0/1
```

```
switchport mode trunk
no shutdown
exit
interface gig0/2
switchport mode trunk
no shutdown
exit
end
copy running-config startup-config
```

3. ROUTER

```
enable
configure terminal
hostname R1
interface gig0/0
ip address 10.2.0.2 255.255.255.0
no shutdown
exit
interface gig0/1
no ip address
no shutdown
exit
interface gig0/2
no ip address
no shutdown
exit
interface gig0/1.10
encapsulation dot1Q 10
ip address 10.2.1.1 255.255.255.0
no shutdown
exit
interface gig0/2.20
encapsulation dot1Q 20
ip address 10.2.20.1 255.255.255.0
ip helper-address 10.2.1.3
no shutdown
exit
interface gig0/2.30
encapsulation dot1Q 30
ip address 10.2.30.1 255.255.255.0
ip helper-address 10.2.1.3
no shutdown
exit
```

ip routing
ip route 0.0.0.0 0.0.0.0 10.2.0.1
ip access-list extended BLOCK_DMZ
deny ip host 10.2.1.254 10.2.20.0 0.0.0.255
deny ip host 10.2.1.254 10.2.30.0 0.0.0.255
permit ip any any
exit
ip access-list extended BLOCK_VLAN20_WEBSERVER
deny ip host 10.2.20.254 host 10.2.1.2
permit ip any any
exit
interface vlan 10
ip access-group BLOCK_DMZ in
exit
interface vlan 20
ip access-group BLOCK_VLAN20_WEBSERVER in
end
copy running-config startup-config

4. FIREWALL(ASA 5506)

* Xóa cấu hình nếu cần để viết lại lệnh
write erase
reload
* Bắt đầu viết lệnh
enable
Password:
configure terminal
interface GigabitEthernet1/1
no nameif
exit
interface GigabitEthernet1/2
no nameif
exit
interface GigabitEthernet1/1
nameif outside
security-level 0
ip address 100.0.0.2 255.255.255.0
no shutdown
exit
interface GigabitEthernet1/2
nameif inside
security-level 100
ip address 10.2.0.1 255.255.255.0
no shutdown

exit
configure terminal
route inside 0.0.0.0 0.0.0.0 10.2.0.2
exit
configure terminal
object network INTERNAL
subnet 10.21.0.0 255.255.0.0
nat (inside,outside) dynamic interface
exit
configure terminal
object network WEB
host 10.2.1.2
nat (inside,outside) static 100.0.0.100
exit
configure terminal
access-list OUTSIDE_IN extended permit tcp host 203.11.1.1 host 100.0.0.100 eq 80
access-list OUTSIDE_IN extended deny tcp host 203.113.1.2 host 100.0.0.100 eq 80
access-list OUTSIDE_IN extended permit ip any any
exit
configure terminal
access-group OUTSIDE_IN in interface outside
exit
configure terminal
access-list INSIDE_IN extended permit icmp any any
access-group INSIDE_IN in interface inside
policy-map global_policy
class inspection_default
inspect icmp
end
copy running-config startup-config

Lưu ý: Lệnh này viết cho ASA 5506; nếu sử dụng lệnh ASA5505 thì gán IP các cổng ASA thông qua Vlan

----------HẾT ĐỀ 2----------