**ĐỒ ÁN CUỐI KỲ - HK2/2021-2022**

**MÔN: AN NINH MÁY TÍNH**

--------------

**Câu 1.** (3,0 đ) Bảo vệ dịch vụ Web

* Tóm tắt lý thuyết
* Các hình thức tấn công vào dịch vụ Web
* Giải pháp phòng chống.

**Câu 2.** (7,0 đ) Cho sơ đồ mạng



**Mô tả hệ thống:**

* SV thay chữ **X** bằng **2 số cuối** trong **MSSV** của mình.
* Các cổng gắn PC với Switch, SV tự chọn theo ý mình
* SV có thể bổ sung địa chỉ IP ở các kết nối mà đề bài chưa cho để phù hợp với cách làm của mình.
* *Địa chỉ IP của các máy tính:* SV tự cho sao cho thuộc địa chỉ mạng đã quy định
* ***HQ: Hội sở***
* Gồm có **CoreSwitch** đặt ở toàn nhà trung tâm (**Building 1**)
* **2 Distribution Switch**, mỗi Distribution Switch đặt ở mỗi tòa nhà (gọi là **Building2** và **Building 3**)
* Building 1 có *2 phòng ban (kết nối vào* ***CoreSW*** *– khu vực VP TNTT)*, Building 2 có *3 phòng ban (kết nối vào* ***Dist-SW1****)*, Building 3 có *2 phòng ban (kết nối vào* ***Dist-SW2****).* Số lượng phòng ban có thể thay đổi theo thời gian cho phù hợp với tình hình hoạt động của doanh nghiệp.
* Có các Server cung cấp dịch vụ ra bên ngoài Internet gồm: *Web server, Email server*
* Có các Server nội bộ cung cấp dịch vụ cho mạng nội bộ như *DHCP server, DNS server*
* Có khu vực quản trị: gồm máy tính của người quản trị, thực hiện các chức năng quản trị như cấu hình từ xa các thiết bị mạng thông qua **Telnet/SSH.**
* Có Firewall để bảo vệ cho hệ thống mạng nội bộ.
* ***Branch: Chi nhánh***
* Công ty có 1 chi nhánh, có 3 phòng ban.
* Có DHCP Server để cung cấp địa chỉ IP cho các máy tính trong mạng
* Các ứng dụng nội bộ đặt ở HQ. Do đó, chi nhánh cần có kết nối với mạng nội bộ bên HQ để sử dụng dịch vụ (VPN Site-to-Site).
* Có Firewall để bảo vệ cho hệ thống mạng nội bộ.

**Yêu cầu:**

1. *(3,0 đ)* ***Cấu hình cơ bản:***

* SV điền lại đầy đủ các thông tin về địa chỉ IP sau khi thay chữ **X** bằng **2 số cuối** trong **MSSV** của mình trong sơ đồ mạng.
* Cấu hình các kỹ thuật VLAN, VTP, Trunk,… để đáp ứng yêu cầu đầu bài.
* Cấu hình định tuyến cho hệ thống mạng nội bộ *(SV tự chọn cách cấu hình định tuyến tĩnh hoặc định tuyến động)*
* Cấu hình NAT cho phép người dùng bên trong ra ngoài Internet *(NAT Overloading)*
* Cấu hình để cung cấp các dịch vụ Web, Email để người dùng ở ngoài Internet có thể sử dụng được *(Cấu hình Static NAT, với IP public cho Web server là* ***4.4.4.4*** *và Email Server là* ***5.5.5.5****)*

1. *(3,0 đ)* ***Cấu hình bảo mật***

* *Cấu hình Hardening trên Switch* (SV chỉ cần làm trên *Access-SW1* ): Giả sử ***Access-SW1*** chỉ cho sử dụng 2 máy tính, các port không sử dụng phải tắt đi.
* *Cấu hình tính năng Port Secutity trên các Access-Switch* (SV chỉ cần làm trên *Access-SW1* ) để người dùng không thể tự ý thay đổi thiết bị gắn vào các Switch.
* Ở các thiết bị mạng: CoreSW, Distribution Switch (*Dist-SW1, Dist-SW2*), Access-Switch (*chỉ cần làm trên Access-SW1*) mở cho phép truy cập từ xa bằng dịch vụ **SSH**.
* Hệ thống có DHCP server đặt ở khu vực Internal Server để cung cấp IP động cho tất cả các người dùng trong hệ thống. *Cấu hình tính năng DHCP Snooping* để ngăn các DHCP giả cung cấp IP các người dùng trong mạng (SV làm ở mạng của Hội sở, không cần làm ở chi nhánh).
* *Cấu hình ACL* thực hiện một số yêu cầu sau:
  + Cấm các PC thuộc phòng ban VLAN10 truy cập vào khu vực quản trị (có địa chỉ là 172.X.111.0/24)
  + Chỉ cho phép các máy thuộc khu vực quản trị được quyền truy cập từ xa bằng dịch vụ SSH vào các thiết bị
* *Cấu hình Firewall (ở Hội sở)*
  + Các máy ở VLAN20 chỉ được truy cập ra ngoài bằng dịch vụ PING và dịch vụ FTP
  + Các máy tính khác trong mạng truy cập được tất cả các dịch vụ bên ngoài Internet.
* *Cấu hình Firewall (ở chi nhánh)*
  + Cho phép tất cả các dịch vụ ra ngoài Internet
* Mạng WiFi *(ở Hội sở)*:
  + Chứng thực cho người dùng mạng WiFi bằng WPA2 *(password SV tự cho & ghi vào trong báo cáo)*
  + SSID: SV tự cho

1. *(1,0 đ)* ***Cấu hình VPN Site-to-Site (IPSec VPN) đế kết nối HQ và Branch***.

--- Hết ----