**KIỂM TRA LÝ THUYẾT PHẦN TỰ LUẬN (70%)**

**Môn: An toàn thông tin**

**Đề bài:**

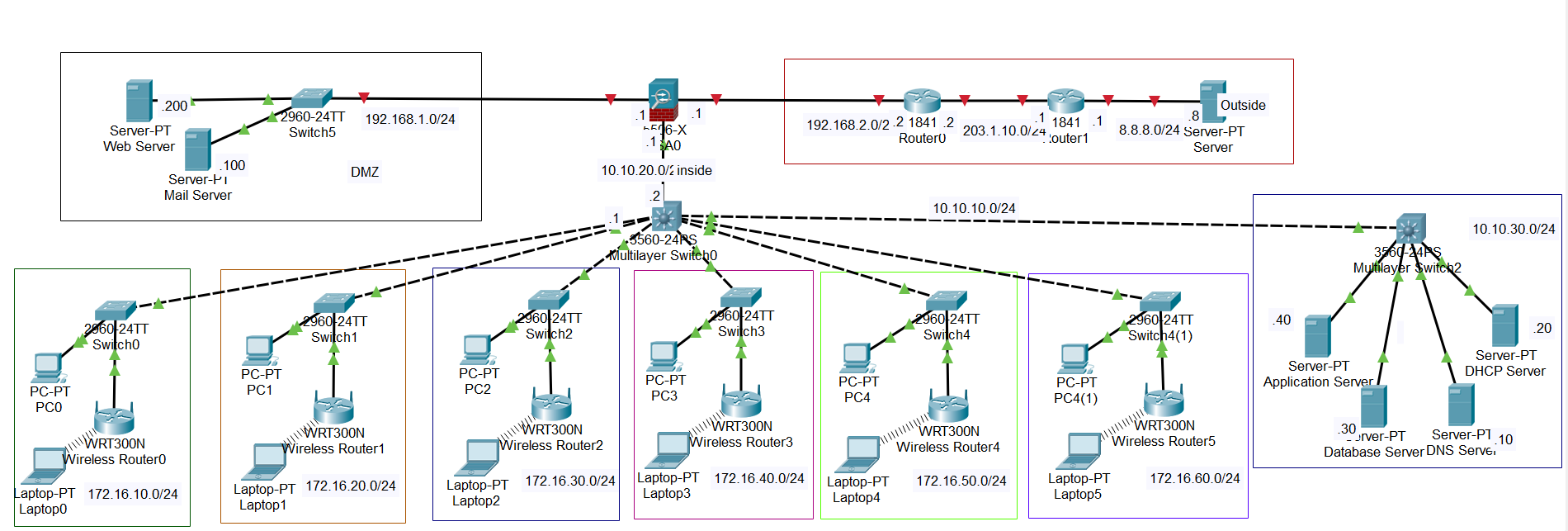
1. ***( 3,0 điểm)* Tấn công từ chối dịch vụ là gì? Giải pháp hạn chế kiểu tấn công này?**

* Tấn công từ chối dịch vụ (DoS) là cuộc tấn công nhằm làm sập một máy chủ hoặc mạng, khiến người dùng khác không thể truy cập vào máy chủ/mạng đó. Kẻ tấn công thực hiện điều này bằng cách “tuồn” ồ ạt traffic hoặc gửi thông tin có thể kích hoạt sự cố đến máy chủ, hệ thống hoặc mạng mục tiêu, từ đó khiến người dùng hợp pháp (nhân viên, thành viên, chủ tài khoản) không thể truy cập dịch vụ, tài nguyên họ mong đợi. Nạn nhân của tấn công DoS thường là máy chủ web của các tổ chức cao cấp như ngân hàng, doanh nghiệp thương mại, công ty truyền thông, các trang báo, mạng xã hội... DoS có các dạng tấn công như sau: Tấn công over-buffer; Tấn công Ping of Death hoặc ICMP flood; tấn công Teardrop Attack; SYN flood, UDP flood, HTTP flood,...
* Tấn công DDoS là nỗ lực làm sập một dịch vụ trực tuyến bằng cách làm tràn ngập nó với traffic từ nhiều nguồn. Tấn công từ chối dịch vụ phân tán (DDoS) là dạng tấn công DoS nguy hiểm nhất khi nguồn tấn công nhiều và phân bố trên diện rộng trên mạng Internet toàn cầu, rất khó ngăn chặn triệt để. Đây là kiểu tấn công phân tán vì kẻ tấn công sử dụng nhiều máy tính, bao gồm có cả máy tính của bạn để thực hiện tấn công Dos. Có 03 loại tấn công cơ bản: Volume-based, Protocol, Application.
* Chúng ta không thể ngăn chặn hoàn toàn tấn công từ chối dịch vụ (DOS hoặc DDoS), nhưng có một số biện pháp có thể giảm thiểu khả năng người dùng trở thành công cụ nhằm tấn công các máy tính khác. Giải pháp để hạn chế tấn công từ chối dịch vụ là:
* Cài đặt và duy trì một phần mềm diệt virus (Antivirus Software).
* Giám sát và giớ hạn lưu lượng truy cập
* Cài đặt một Firewall (tường lửa) và cấu hình nó để hạn chế các lưu lượng truy cập vào và đi từ máy tính của bạn.
* Mua thêm băng thông, thiết lập nhiều server hơn và dùng các giải pháp cân bằng tải tốt
* Làm theo các hướng dẫn thực hành an toàn về phân phối địa chỉ email của bạn.
* Dùng các bộ lọc email để giúp bạn quản lý lưu lượng không mong muốn.
* Tối ưu hóa các thuật toán xử lý, mã nguồn của máy chủ web; Nâng cấp hệ thống máy chủ; Nâng cấp đường truyền và các thiết bị liên quan; Cài đặt đầy đủ các bản vá cho hệ điều hành và các phần mềm khác để phòng ngừa khả năng bị lỗi tràn bộ đệm, cướp quyền điều khiển, …
* Sử dụng các tường lửa cho phép lọc nội dung thông tin (tầng ứng dụng) để ngăn chặn các kết nối nhằm tấn công hệ thống.
* Phân tích luồng tin (traffic) để phát hiện các dấu hiệu tấn công và cài đặt các tường lửa cho phép lọc nội dung thông tin (tầng ứng dụng) ngăn chặn theo các dấu hiệu đã phát hiện.
* Sử dụng phương pháp - định tuyến hố đen: tạo một tuyến đường lỗ đen để chuyển cá traffic vào đó. Nhằm tránh tình trạng quá tải trên hệ thống. Khi website gặp phải một cuộc tấn công từ chối dịch vụ, nhà cung cấp dịch vụ internet có thể đưa tất cả lưu lượng truy cập quá tải từ website vào lỗ đen để tự bảo vệ mình
* Anycast Network Diffusion: phương pháp này giúp máy chủ tránh khỏi tình trạng quá tải. Cách thức xử lý này cho phép chuyển lượng traffic Dos/DDos đến các điểm có thể quản lý được.
* Sử dụng hệ thống thiết bị, phần mềm hoặc dịch vụ giám sát an toàn mạng (đặc biệt về lưu lượng) để phát hiện sớm các tấn công từ chối dịch vụ.
* Sử dụng thiết bị bảo vệ mạng có dịch vụ chống tấn công DDoS chuyên nghiệp kèm theo, ví dụ như: Arbor, Checkpoint, Imperva, Perimeter,…

1. ***( 3,0 điểm)* Vẽ sơ đồ logic cho một công ty có các đặc điểm sau:**

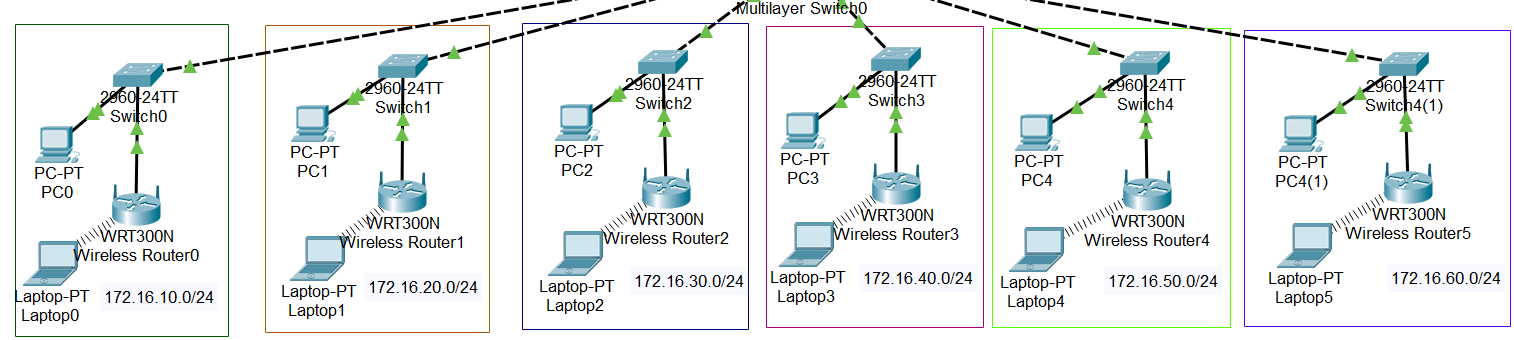
* 6 phòng ban
* 01 khu vực đặt các server nội bộ bên trong như: DNS server, DHCP server, Database Server, Application Server
* 01 khu vực đặt các server public gồm: Web server, Mail server
* Công ty có triển khai mạng WiFi

Sử dụng các thiết bị mạng đã biết: Router, Switch, Firewall, IDS/IPS,… thiết kế cho hệ thống mạng trên.

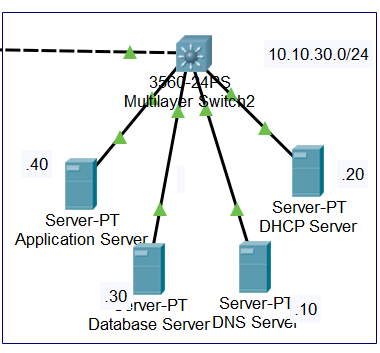


1. ***(4,0 điểm)* Dựa vào sơ đồ mạng ở câu 2, SV thực hiện các yêu cầu sau:**
   1. **Đặt địa chỉ IP cho các khu vực trong sơ đồ đã vẽ (SV có thể ghi địa chỉ trực tiếp trên sơ đồ mạng ở câu 2).**

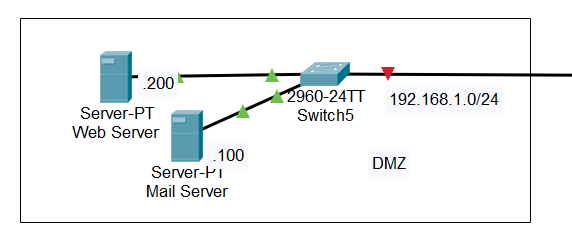
* Địa chỉ IP cho các phòng ban lần lượt là: 172.16.x.0/24(x lần lượt là 10, 20, 30, 40, 50, 60)



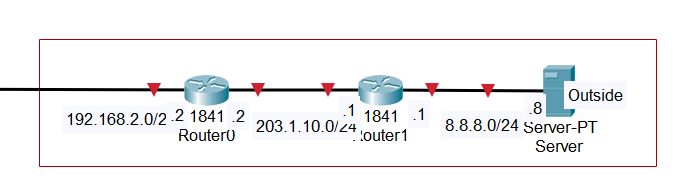
* Khu vực Server nội bộ có ip là **10.10.30.0/24**

****

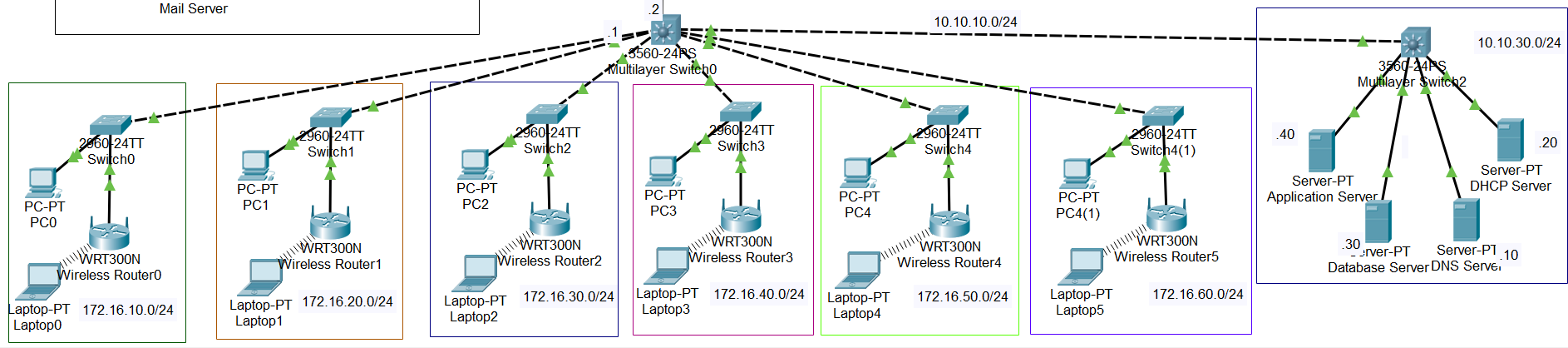
* Khu vực server public có ip **192.168.1.0/24**

****

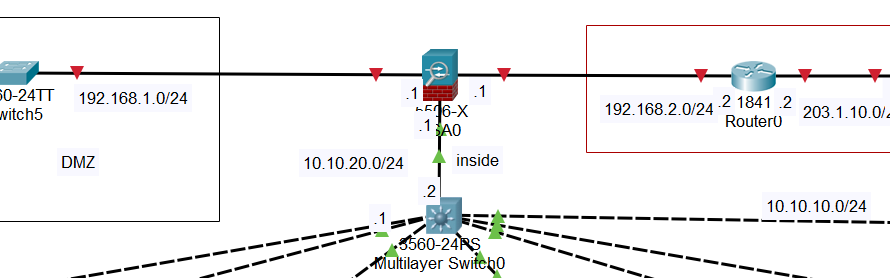
* Khu vực outside

****

* Khu vực inside

****

* Địa chỉ IP cho các đường truyền kết nối: **10.10.10.0/24**, **10.10.20.0/24**, **192.168.1.0/24**, **192.168.2.0/24**

****

* 1. **Mô tả ngắn gọn cách thiết kế cho công ty trên, các thiết kế như vậy mang lại các lợi ích gì ?**
* Máy Server Web, Email-Server… cung cấp dịch vụ ra ngoài Internet trong mạng DMZ để tránh bị truy cập trái phép từ bên trong.
* Các máy chủ không cung cấp trực tiếp cung cấp dịch vụ mạng ra ngoài: DNS, DHCP, Database,.. nên đặt trong mạng DMZ để tránh bị tấn công từ bên ngoài và phía bên mạng nội bộ.
* Đặt Firewall hoặc IDS/IPS để bảo vệ hệ thống, phân luồng thông tin truy cập cũng như chống tấn công từ bên ngoài. Nên đặt Firewall giữa kết nối vào mạng Internet (chống tấn công bên ngoài) và giữa mạng nội bộ với DMZ để tránh tấn công nội bộ.
* Các phòng ban có mạng riêng, giúp tránh việc truy cập trái phép từ phòng ban khác. Các phòng ban chung nhau Multiswitch, tạo ra mạng nội bộ. Trong đó, các máy trong mỗi phòng có thể truy cập vào.
* Thiết lập 3 vùng mạng inside, outside, DMZ và nối chúng với Firewall để tránh tấn công từ bên ngoài vào hệ thống, đồng thời ngăn chặn sự tấn công hay truy cập trái phép từ mạng nội bộ.
* Chia các phòng ban do nhiều MultileSwitch nhằm mục đích: đảm bảo lượng máy mà MultiSwitch có thể phục vụ; nếu có tấn công hoặc gặp sự cố sẽ dễ phát hiện và xử lý.
  1. **Phân tích một số giải pháp có thể sử dụng để bảo vệ hệ thống mạng nội bộ (khu vực mạng LAN – hay gọi là khu vực INSIDE) trong thiết kế trên.**
* Thiết kế theo tầng: đảm bảo tính dự phòng đường truyền, lưu lượng mạng được phân bố đều, toàn mạng được chia thành nhiều phân đoạn để dễ dàng kiểm soát và bảo mật.
* Đối với các hệ thống thông tin yêu cầu có mức bảo mật cao, hoặc có nhiều cụm máy chủ khác nhau có thể chia vùng Server Nội bộ thành các vùng nhỏ hơn độc lập để nâng cao tính bảo mật.
* Lựa chọn tường lữa thích hợp .
* Dùng phần mềm lọc nội dung cho HTTP, FTP và SMTP.
* Đóng hết các cổng truy cập để tránh bị mất dữ liệu từ các phương tiện ngoài.

***Hướng dẫn nộp bài:***

* Đặt tên file: ***MSSV*\_*HoTen*\_Ktra\_PartII** (file word hoặc pdf)
* Nộp bài trên hệ thống mục **Bài KT tự luận**