Tên: Lê Hải Đăng

MSSV: 20110243

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

**Môn: An toàn thông tin**

1. *( 3,0 điểm)*
   1. Trình bày sự khác nhau giữa IDS và IPS?

* IDS (Intrusion Detection Systems) - Hệ thống phát hiện xâm nhập: Có khả năng phát hiện xâm nhập và cảnh báo, nhưng không có khả năng ngăn chặn lại các xâm nhập.
* IPS (Intrusion Prevention System) là Hệ thống Ngăn chặn Xâm nhập: có khả năng phát hiện xâm nhập và ngăn chặn sự xâm nhập hoặc tấn công đó.
  1. Trình bày về firewall và firewall rules?

**FireWall**

* Một phần của hệ thống máy tính hoặc mạng được thiết kế để ngăn chặn truy cập trái phép đi qua nó.
* Chia mạng ra thành nhiều phần: inside – outside (trusted and untrusted)
* Phân biệt mạng thành các khu vực có độ bảo mật khác nhau
* Chức năng chính là lọc dữ liệu (filtering) dựa vào các rule mà người ta đã thiết lập trước đó để chống lại các truy cập bất hợp pháp hay các tấn công.

Yêu cầu của Firewall

* Tất cả truy cập giữa các vùng tin cậy phải vượt qua tường lửa.
* Chỉ truy cập được phép, như được xác định bởi chính sách bảo mật, mới được phép đi qua.
* Bản thân Firewall phải miễn nhiễm với sự xâm nhập, nghĩa là sử dụng một hardened system với Hệ điều hành được bảo mật.

Policy

* User control: Kiểm soát quyền truy cập của người dùng
* Service control: Kiểm soát các dịch vụ, giao thức
* Direction control: Kiểm soát hướng (inbound/ outbound)

Firewall actions

* Permit/ Allow/ accepted: Cho phép truy cập
* Deny/ Drop/ Rejected: Từ chối truy cập

Type firewall

Phân loại dựa vào cách xử lý:

* Packet Filter Firewall/ Stateless Firewall / Per packet: Xử lý từng gói riêng lẻ
* Stateful Firewall/ Per flow Firewall: Xử lý một lúc nhiều gói có mối liên quan với nhau
* Application/Proxy Firewall

Phân loại dựa vào vị trí:

* External Firewall: bên ngoài
* Internal Firewall: Nội bộ

**Firewall Rules**

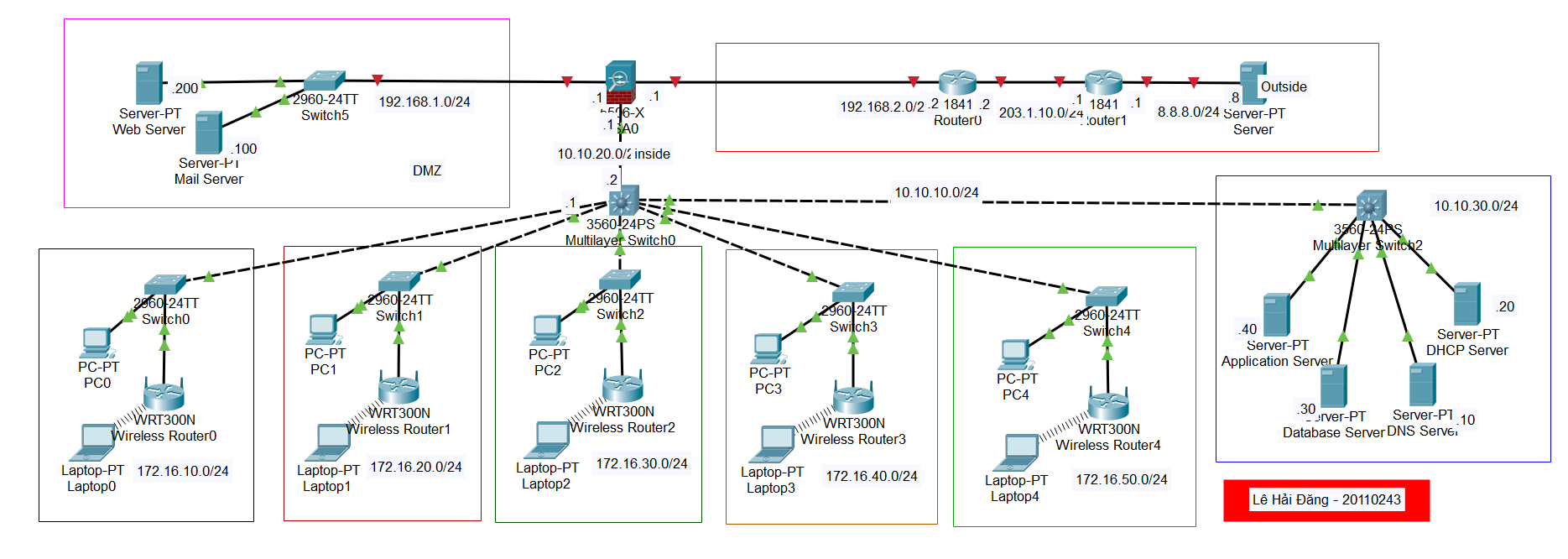
* **Cấu trúc:** Rule\_name, action, source, destination
* Có tính thứ tự
* Xác định lưu lượng mà tường lửa của bạn cho phép và những gì bị chặn.
* Kiểm tra thông tin điều khiển trong các gói riêng lẻ và chặn hoặc cho phép chúng theo các tiêu chí mà bạn xác định.
* Kiểm soát cách tường lửa bảo vệ mạng của bạn khỏi các chương trình độc hại và truy cập trái phép.
* Quản lý các quy tắc tường lửa trên các thiết bị của bạn và trong toàn bộ mạng của bạn là rất quan trọng đối với an ninh mạng.

Với các Firewall Rules, có thể triển khai các chính sách và hành động để thực thi các biện pháp kiểm soát bảo mật và ưu tiên lưu lượng truy cập

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

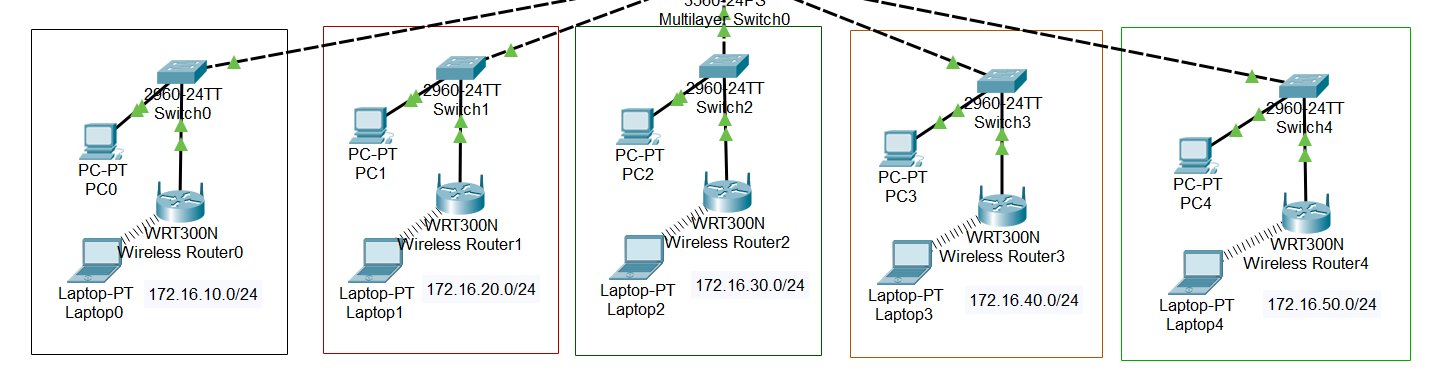
* 5 phòng ban
* 01 khu vực đặt các server nội bộ bên trong như: DNS server, DHCP server, Database Server, Application Server
* 01 khu vực đặt các server public gồm: Web server, Mail server
* Công ty có triển khai mạng WiFi

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

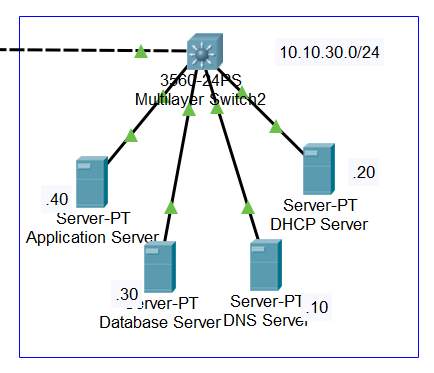


1. *(4,0 điểm)* Dựa vào sơ đồ ở câu 2, SV thực hiện các yêu cầu sau:
   1. Đặt địa chỉ IP cho các khu vực trong sơ đồ đã vẽ (SV có thể ghi địa chỉ trực tiếp trên sơ đồ mạng ở câu 2).

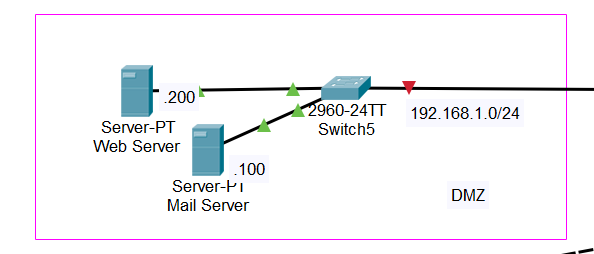
* Địa chỉ IP Cho các phòng ban lần lượt là: **172.16.x.0/24(x lần lượt là 10, 20, 30, 40, 50)**



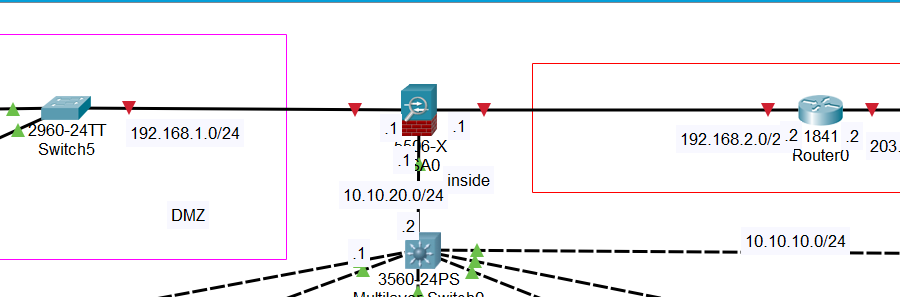
* Khu vực Server nội bộ có ip là **10.10.30.0/24**



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



* 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, thiết kế như vậy mang lại các lợi ích gì ?
* Thiết kế mạng theo mô hình sao có tốc độ nhan. Khi xảy ra xự cố cáp mạng bị đứt thì thông thường chỉ làm hỏng kết nối của một máy, các máy khác vẫn hoạt động được. Khi có lỗi mạng, ta dễ dàng kiểm tra sửa chữa.
* Tất cả các truy cập bên ngoài khi muốn truy cập vào hệ thống phải thông qua Firewall, từ đó có thể quản lý được lưu lượng truy cập nhằm tránh bị tấn công Dos, Ddos.
* FireWall chia hệ thống thành nhiều khu vực riêng biệt: Inside, DMZ, Outside. Mỗi khu vực có mức độ bảo mật khác nhau.
* Cụm DMZ gồm Mail Server và Web Server có thể liên kết với internet bên ngoài nhưng vẫn phải qua Firewall và hệ thống IPS để đảm bảo an toàn.
* Khu vực Inside cũng được tách riêng biệt với nhau để dễ quản lý.
  1. Phân tích một số giải pháp để bảo vệ và nâng cao tính sẵn sàng của Web server và Email server trong thiết kế trên.
* Cài đặt chứng chỉ SSL là cách bảo mật website được nhiều người biết đến. SSL bảo mật dựa theo cơ chế mã hóa thông tin giữa trình duyệt client và server, giúp thông tin được bảo vệ.
* Cập nhật web application: Cập nhật các phần mềm ứng dụng giúp sửa lại các lỗ hổng, lỗi của phiên bản trước. Đây cũng là một trong những biện pháp đơn giản nhưng hữu hiệu để tránh khỏi sự tấn công của các hacker.
* Web application firewall (WAF)- tường lửa ứng dụng web: Tường lửa ứng dụng web có chức năng tự động phân tích các lỗ hổng có thể bị xâm nhập, chống lại các code độc, sự tấn công của các hacker hoặc virus.
* Sử dụng VPN (Virtual Private Network): mã hóa dữ liệu, xác thực danh tính người dùng, quản lý phiên truy cập của người dùng.
* Sử dụng chữ ký số (Digital Signature): nhằm mục đích xác định người chủ của dữ liệu đó.