**Võ Văn Đức 20110635**

**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 là nỗ lực phá vỡ lưu lượng truy cập, có nghĩa là sử dụng nhiều hệ thống máy tính để truy cập vào lưu lượng, khiến máy chủ và mạng bị nhắm đến bị tràn lưu lượng, dẫn đến việc từ chối truy cập đối với những lưu lượng truy cập bình thường.

\_ Cách thức tấn công từ chối dịch vụ: những người tấn công sẽ cố gắng chiếm quyền kiểm soát mạng lưới máy trực tuyến bằng cách lây nhiễn các phần mềm bị hại đến các máy tính và các loại thiết bị khác (tương tự như thiết bị nhúng IoT) để biến chúng thành các botnet, và điều khiển chúng xâm nhập vào lưu lượng được quản lý bởi máy chủ hoặc mạng. Các botnet sẽ gửi yêu cầu đến máy chủ (mạng) bị nhắm đến, vì chưa có biện pháp phân biệt đâu là việc truy cập bình thường, đâu là tấn công, khiến lưu lượng của máy chủ, mạng bị tràn; từ đó từ chối dịch vụ khi những truy cập bình thường.

\_ Thông thường một cuộc tấn công DdoS sẽ tấn công dưới dạng đa vector để tấn công mục tiêu bằng nhiều con đường khác nhau, có nghĩa là sẽ tấn công nhiều lớp cùng một lúc (Trong mô hình OSI có 7 lớp riêng biệt, việc tấn công vào mỗi lớp có một mục đích cụ thể)

+) Tấn công lớp application: làm cạn kiệt tài nguyên của mục tiêu

+) Tấn công giao thức chủ yếu ở lớp session layer và transport layer: gây gián đoạn dịch vụ để mục tiêu không thể truy cập được

+) Tấn công Volumetric : tiêu thụ tất cả băng thông bằng cách khuếch đại để khuếch địa dữ liệu được gửi.

\_ Các giải pháp:

+) DdoS blackhole routing: khi lỗ đen được triển khai mà không có tiêu chí cụ thể, cả lưu lượng truy cập mạng hợp pháp và độc hại đều định tuyến đến đường rỗng.

+) Giới hạn tỷ lệ: giảm thiểu số lượng yêu cầu mà máy chủ nhận trong thời gian cụ thể.

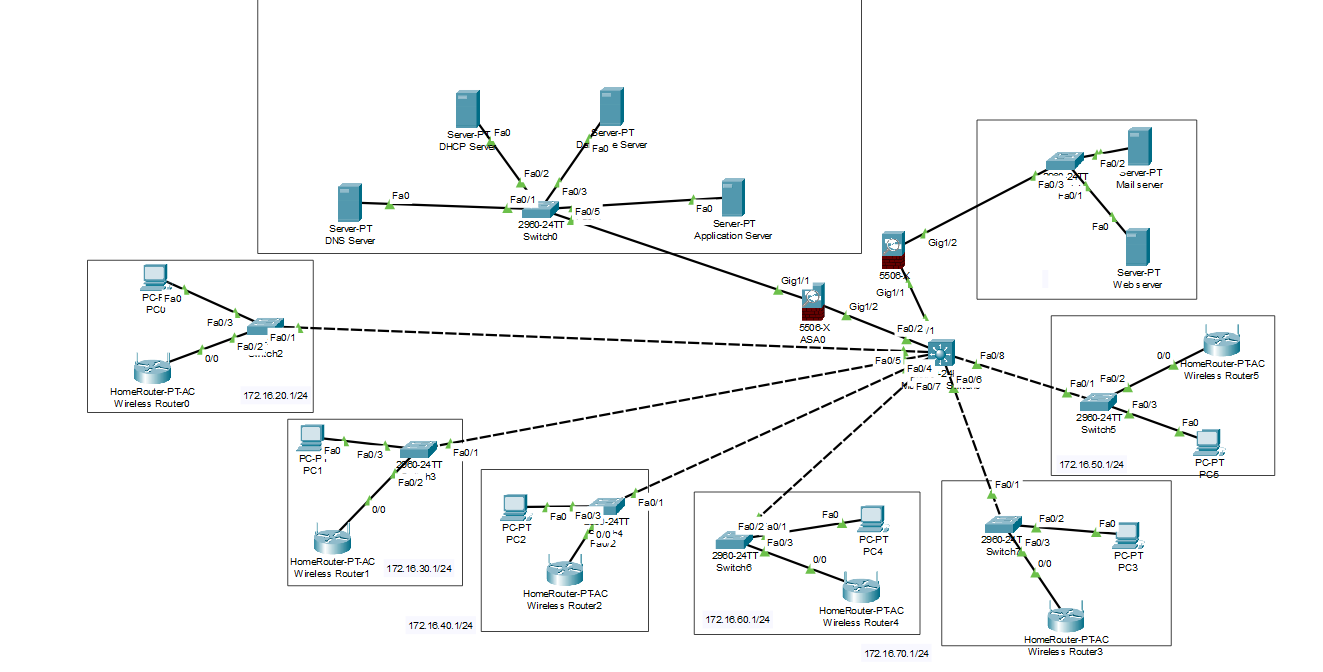
+) Sử dụng Web application firewall: giảm thiểu tấn công DdoS lớp Application bằng quy tắc mà nó yêu cầu.

+) Anycast Network Diffusion: phân tán lưu lượng tấn công.

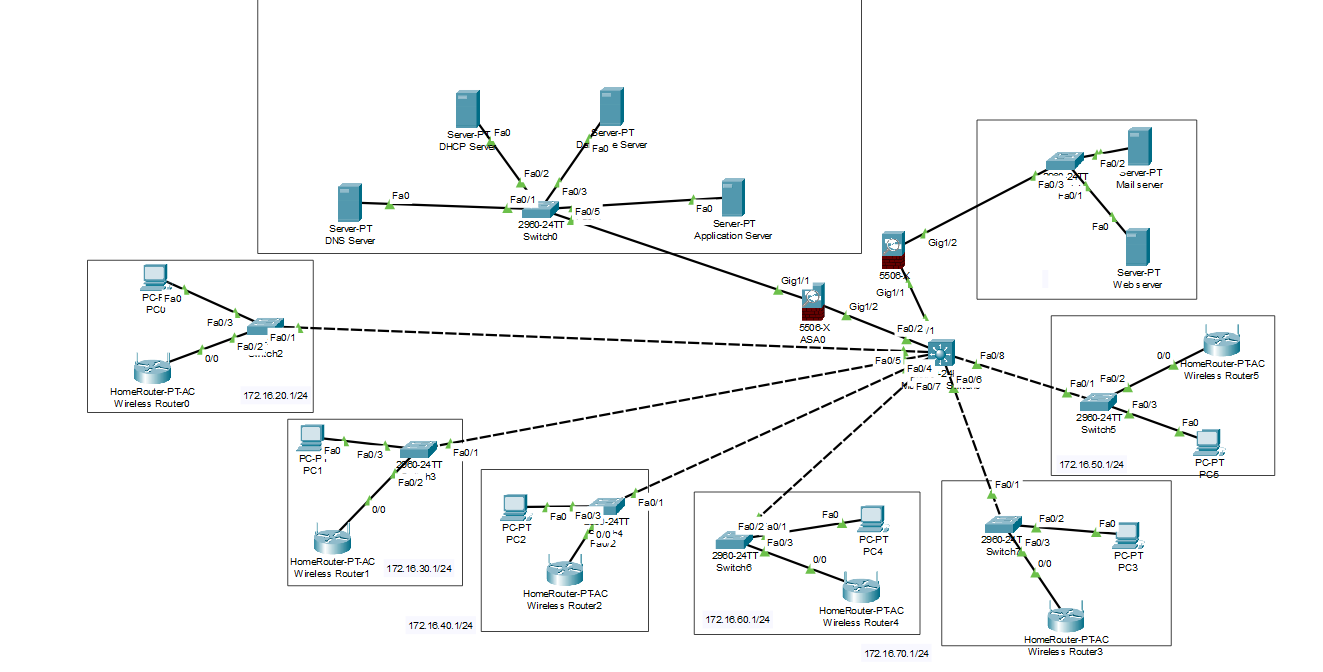
1. *( 3,0 điểm)* Vẽ sơ đồ logic cho một công ty có các đặc điểm sau:

* 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).



* 1. Mô tả ngắn gọn cách thiết kế cho công ty trên, các thiết kế như vậy mang lại các lợi ích gì ?

\_ Công ty có 6 phòng ban, các máy được nhận IP từ DHCP server, 1 khu vực bao gồm web-server và mail server, mỗi phòng ban có 1 cục wifi. Mỗi phòng ban có 1 switch để pc kết nối với dhcp server. Hệ thống sử dụng 2 tường lửa trước 2 khu vực.

* 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.

\_ DHCP snooping: để PC có IP được DHCP server cấp phát, nếu có một AP gắn vào switch để cung cấp 1 IP khác thì PC cũng không nhận.

\_ MAC address filtering

\_ Wireless Security Techniques như mã hoá, thay đổi password

\_ Sao lưu dữ liệu

\_ Đật mật khẩu BIOS

\_ Phân quyền máy

\_ Cấu hình port security tại switch

***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**