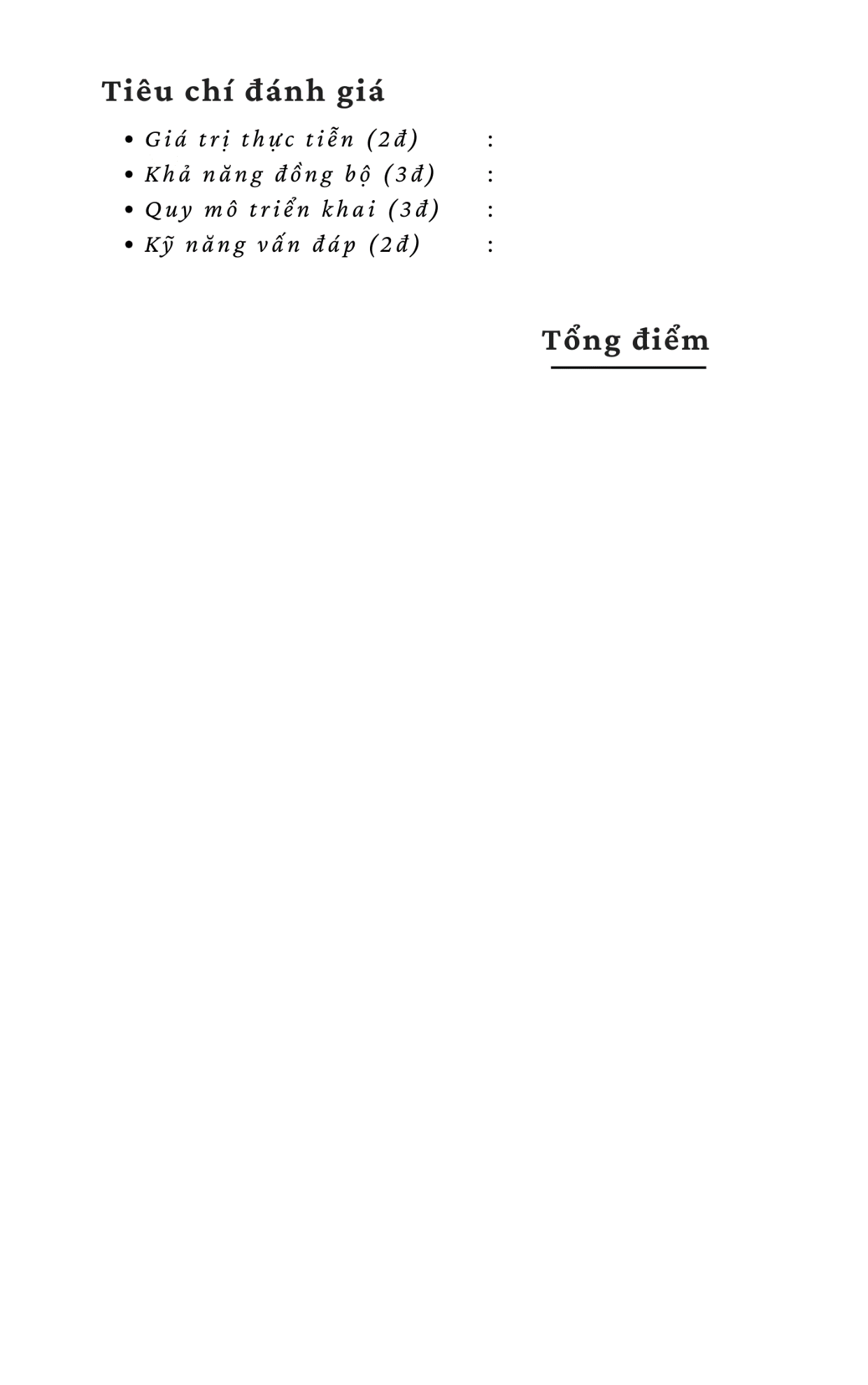


**Bùi Đăng Khoa 21DH113768**

**Trần Nguyễn Thiên Phúc 21DH114023**

**Huỳnh Phúc Đăng Quang 21DH114500**





MỤC LỤC

[CHƯƠNG 1 CƠ SỞ LÝ THUYẾT 1](#_Toc161257123)

[1. Các kiểu tấn công 1](#_Toc161257124)

[Tấn công từ chối dịch vụ - Denial of Service (DoS) 1](#_Toc161257125)

[SYN FLood 1](#_Toc161257126)

[Smurf Attack 1](#_Toc161257127)

[Ping of Death 2](#_Toc161257128)

[UDP Flood 2](#_Toc161257129)

[ICMP Flood 2](#_Toc161257130)

[DHCP Starvation 2](#_Toc161257131)

[HTTP Post DoS 2](#_Toc161257132)

[PDoS 2](#_Toc161257133)

[Distributed Reflection Denial of Service (DRDoS) 2](#_Toc161257134)

[Buffer Overflow Attack 3](#_Toc161257135)

[IP Spoofing 3](#_Toc161257136)

[Session Hijacking 3](#_Toc161257137)

[Phishing 3](#_Toc161257138)

[Tấn công bằng Virus và Trojan 3](#_Toc161257139)

[2. Hệ thống firewall và proxy 5](#_Toc161257140)

[CHƯƠNG 2 THIẾT KẾ HỆ THỐNG 7](#_Toc161257141)

[1. Ý tưởng 7](#_Toc161257142)

[2. Ưu – nhược điểm hệ thống mạng 7](#_Toc161257143)

[3. Bảng quy hoạch IP 8](#_Toc161257144)

[4. Sơ đồ Logic 10](#_Toc161257145)

[5. Sơ đồ vật lí. 11](#_Toc161257146)

[CHƯƠNG 3 TRIỂN KHAI 13](#_Toc161257147)

[1. Domain Controller và Group Policy 13](#_Toc161257148)

[1.1. Cài đặt dịch vụ Active Directory Domain Services 13](#_Toc161257149)

[1.2. Nâng cấp server lên Domain Controller 13](#_Toc161257150)

[1.3. Tạo OU và User cho Domain 14](#_Toc161257151)

[1.4. Cấu hình Group Policy Object (GPO) 14](#_Toc161257152)

[2. Additional Domain Controller: 16](#_Toc161257153)

[2.1 Cài đặt dịch vụ Active Domain Service: 17](#_Toc161257154)

[2.2 Cấu hình Additional Domain Controller: 17](#_Toc161257155)

[3. Web Server: 18](#_Toc161257156)

[4. DNS Server 18](#_Toc161257157)

[**5.** DHCP Server 19](#_Toc161257158)

[5.1 Cài đặt dịch vụ DHCP 19](#_Toc161257159)

[5.2 Cấu hình dịch vụ DHCP 19](#_Toc161257160)

[6. Symantec Endpoint Protection 20](#_Toc161257161)

[7. Fortigate. 22](#_Toc161257162)

[8. PRTG Network Monitor 23](#_Toc161257163)

[9. Snort 24](#_Toc161257164)

[10. Xây dựng các chính sách (luật) trong công ty 25](#_Toc161257165)

[Sử dụng thiết bị mạng: 25](#_Toc161257166)

[Bảo mật thông tin: 25](#_Toc161257167)

[Quyền hạn: 25](#_Toc161257168)

[Bảo trì và Bảo dưỡng thiết bị: 25](#_Toc161257169)

[Tài liệu tham khảo 26](#_Toc161257170)

# CHƯƠNG 1 CƠ SỞ LÝ THUYẾT

## Các kiểu tấn công

Trong thời đại kĩ thuật số ngày nay việc bảo vệ thông tin cá nhân hoặc doanh nghiệp trước các cuộc tấn công mạng là việc làm cần thiết. Đặt biệt là đối với các thông tin nhạy cảm của cá nhân và doanh nghiệp không thể tiết lộ. Các hình thức tấn công mạng hiện nay rất đa dạng và những thiệt hại mà các cuộc tấn công này gây ra thì vô cùng lớn về thông tin và tài sản. Từ những cuộc tấn công phá hoại như DDoS làm ngưng trệ hệ thống thông tin cho đến những cuộc tấn công quy mô lớn như sử dụng virus, mã độc trojan tấn công và lấy cắp những thông tin quan trọng. Càng ngày các hình thức tấn công càng trở nên tinh vi và quy mô hơn gây thách thức lớn cho những người làm công việc bảo mật mạng. Vì vậy ta cần phải biết và hiểu được các kiểu tấn công mà những kẻ tấn công mạng sử dụng đồng thời cần phải cập nhật và tăng cường các biện pháp bảo mật cao hơn nữa đề ngăn ngừa và đối phó với những mối đe dọa này.

### Tấn công từ chối dịch vụ - Denial of Service (DoS)

Tấn công từ chối dịch vụ là kiểu tấn công với mục đích ngăn cho người dùng sử dụng dịch vụ của hệ thống đang bị tấn công.Cuộc tấn công DoS dựa trên cơ sở bất kì thiết bị nào cũng có giới hạn hoạt động bao gồm cả các máy tính. Và ta sẽ làm cho máy tính phải hoạt động quá khả năng của nó thì sẽ khiến cho hệ thống bị dừng hoạt động. Đây là phương thức tấn công không xâm nhập vào hệ thống hay chiếm những thông tin quan trọng, mục tiêu của cuộc tấn công là ngăn chặn người dùng hợp pháp truy cập vào hệ thống. Đây là 1 trong những loại tấn công phổ biến nhất vì rất dễ để thực thi 1 cuộc tấn công DoS.

### SYN FLood

Phiên bản phổ biến của tấn công DoS là SYN Flood. Khi diễn ra quá trình “bắt tay” giữa máy chủ và người dùng sử dụng cổng TCP, hacker sẽ gửi hàng loạt yêu cầu kết nối đến máy chủ và sau đó hủy bỏ quá trình “bắt tay”, điều này sẽ làm cho các kết nối với máy chủ mở một nửa và khiến cho các bộ nhớ đệm được cấp phát cho những kết nối đó, không còn có thể thực thi những việc khác. Cuộc tấn công sẽ gây ảnh hưởng đến quá trình phản hồi của các phiên giao dịch trên mạng.

### Smurf Attack

Smurf Attack cũng là một hình thức tấn công DoS sử dụng các gói tin ICMP được gửi đến địa chỉ broadcast của mạng và được trả về 1 địa chỉ giả thay thế trùng với địa chỉ của 1 máy tính trong hệ thoogns mạng đó. Các máy tính của hệ thống mạng sẽ phản hồi bằng cách ping máy tính đó, vì địa chỉ các gói tin đã gửi là địa chỉ broadcast nên nó sẽ tiếp tục gửi các gói tin đó đến tất cả máy trong hệ thống mạng và gửi đến địa chỉ giả. Những gói tin được gửi liên tục sẽ làm cho hệ thống mạng bị DoS. Smurf Attack là phương thức tấn công khiến cho hệ thống mạng tự làm DoS chính nó.

### Ping of Death

Hình thức tấn công Ping of Death (PoD) là hình thức tấn công DoS đơn giản nhất dựa trên cơ sở làm quá tải hệ thống. Khi các gói tin TCP với kích thước lớn được gửi đi có thể làm tắt máy tính mục tiêu. Hình thức tấn công này trở nên ít phổ biến dần do người dùng có thể khởi động lại máy và các hệ điều hành có những bản cập nhật để xử lí những gói tin TCP có kích thước lớn dùng cho việc tấn công PoD.

### UDP Flood

Cuộc tấn công bằng UDP Flood dựa trên cơ sở các gói tin UDP không cần các giao thức kết nối và quy trình kết nối để truyền dữ liệu. Các gói tin TCP kết nối và chờ được xử lí trước khi gửi gói dữ liệu tiếp theo. Gói tin UDP sẽ gửi nhiều gói tin mà không cần xác nhận. Điều này sẽ khiến cho các gói tin được gửi nhanh hơn làm cho diễn ra cuộc tấn công DoS. Hacker lợi dụng điều này khi gửi gói tin UDP đến 1 port bất kì trên hệ thống nạn nhân. Khi hệ thống đó nhận được gói tin UDP, nó sẽ xác định xem port đích có ứng dụng nào đang trong trạng thái chờ hay không. Khi phát hiện ra không có ứng dụng nào đang trong trạng thái chờ, nó sẽ tạo ra một gói tin ICMP mà địa chỉ giả không thể truy cập được, nếu đủ các gói UDP được gửi đến port của nạn nhân thì hệ thống sẽ bị tê liệt.

### ICMP Flood

ICMP Flood là tên gọi khác của Ping Flood, các gói tin ICMP được gửi đi gây tắc nghẽn hệ thống.

### DHCP Starvation

DHCP Starvation là hình thức tấn công khi đủ các yêu cầu truy cập mạng, hacker hoàn toàn có thể chiếm dụng hết không gian địa chỉ của các máy chủ DHCP.

### HTTP Post DoS

Là cuộc tấn công gửi gói tin HTTP Post, các gói tin HTTP Post sẽ có nội dung với độ dài lớn. Hacker lời dụng điều này để gửi nội dung gói tin với tốc độ rất chậm làm cho máy chủ web phải treo để chờ tin nhắn đó hoàn tất.

### PDoS

Tấn cộng từ chối dịch vụ vĩnh viễn Permanent Denial of Service (PDoS) là hình thức tấn công làm hỏng hệ thống nghiêm trọng khiến cho máy của nạn nhân cần cài đặt lại hệ thống hoặc thậm chí sử dụng phần cứng mới.

### Distributed Reflection Denial of Service (DRDoS)

Đây là hình thức đặc biệt trong tấn công DoS, thay vì sử dụng nhiều máy tính như những cuốc tấn công DoS khác, DRDoS lợi dụng các router để tấn công mục tiêu. Nhiều router giao tiếp với nhau bằng port 179. Phương thức tấn công này lợi dụng port 179 này để khiến các router tấn công mục tiêu. Hacker gửi 1 luồng gói tin đến những router và yêu cầu kết nối, các gói tin này được thay đổi để được gửi đi từ địa chỉ cần tấn công. Các router khi này phản hồi bằng cách kết nối với hệ thống đó, quá nhiều router kết nối đến 1 hệ thống khiến cho hệ thống đó không thể truy cập được bất kì điều gì.

### Buffer Overflow Attack

Một hình thức tấn công hệ thống khác nữa là Buffer Overflow Attack (Làm tràn bộ nhớ đệm). Cuộc tấn công làm tràn bộ nhớ đệm diễn ra dựa trên cơ sở bất kì chương trình nào tương tác với Internet hay mạng riêng tư đều phải nhận được một vài dữ liệu. Những dữ liệu này được lưu trữ tạm thời trong bộ nhớ được gọi là bộ nhớ đệm. Nếu có nhiều dữ liệu hơn khả năng lưu trữ của bộ nhớ đệm nó sẽ ghi đè lên các vị trí bộ nhớ liền kề đó. Nếu như dữ liệu đó là dữ liệu độc hại thì nó được đưa vào trong bộ nhớ và chạy trên hệ thống của máy mục tiêu. Điều này làm tràn bộ nhớ của hệ thống khiến dữ liệu ghi đè lên các mục khác trong bộ nhớ làm chúng gặp sự cố bị treo, dẫn tới khả năng bị các hacker lợi dụng xâm nhập vào hệ thống máy tính của nạn nhân từ xa

### IP Spoofing

IP Spoofing là kĩ thuật được hacker sử dụng để che giấu IP thật và sử dụng IP giả nhằm truy cập trái phép vào hệ thống máy tính. Hacker có thể sử dụng nhiều cách để tìm ra địa chỉ IP của máy tin cậy. Sau dó hacker sẽ gửi các gói tin từ IP giả có nguồn tin cậy đó để truy cập trái phép vào hệ thống

### Session Hijacking

Hình thức khác của tấn công mạng là Session Hijacking (Chiếm quyền điều khiển). đây là quá trình hacker chiếm quyền điều khiển TCP sessioin khi đang có tương tác giữa 2 máy. Hacker có khả năng xâm nhập vào lúc tương tác giữa 2 máy và chiếm quyền điều khiển của phiên sử dụng đó. Phương thức tấn công phổ biến là sử dụng các gói IP định tuyến nguồn, điều này cho phép hacker ở vị trí A trên mạng có thể tham gia vào hoạt động giữa B và C bằng cách thúc đẩy các gói tin IP đi qua máy của hacker. Điểm mấu chốt của hijacking là chiếm quyền kiểm soát một kết nối để tạo tin cậy và truy cập vào hệ thống mà hacker không truy cập được.

### Phishing

Phishing là kĩ thuật tấn công mạng bằng cách giả mạo. Hacker sẽ tạo ra 1 trang web giả mạo, email giả mạo với mục tiêu lấy được thông tin cá nhân hoặc tài khoản của nạn nhân. Khi nạn nhân nhập thông tin cá nhân vào trang web giả mạo đó, hacker sẽ biết được tất cả thông tin mà nạn nhân cung cấp sau đó nạn nhân sẽ được đưa về trang web đúng.

### Tấn công bằng Virus và Trojan

Virus là loại hình tấn công mạng phổ biến hiện nay. Virus là chương trình tự sao chép và lây lan nhanh. Khả năng tự sao chép và lây lan của virus khiến cho hệ thống mạng bị nhiễm độc dẫn đến lưu lượng mạng trong hệ thống bị tăng đột ngột khiến cho toàn bộ hệ thống không hoạt động ổn định thậm chí là ngưng hoạt động.

Trojan horses là chương trình nhìn bề ngoài thì bình thường nhưng bản chất bên trong thì có chứa mã độc dùng cho mục đích phá hoại. Trojan có thể xuất hiện khi tải những phần mềm crack hoặc các file có đính kèm mã độc, khi mở những chương trình này thì nó sẽ bắt đầu lây lan trong hệ thống máy tính. Hacker có thể sử dụng trojan để lấy cắp thông tin của người sử dụng

## Hệ thống firewall và proxy

Hệ thống tường lửa (Firewall) là hệ thống ngăn cách giữa mạng nội bộ với mạng Internet bên ngoài. Chứng năng chính và cơ bản nhất của firewall là kiểm soát và lọc các gói tin ra vào hệ thống. Ta có 4 loại firewall được phân chia dựa vào khả năng của thiết bị:

- Pack Filtering (Tường lửa lọc gói tin): là firewall cơ bản nhất, chỉ có khả năng lọc gói tin cho phép hoặc chặn gói tin đó. Nó cung cấp khả năng bảo vệ mạng khỏi những mối đe dọa bằng khả năng lọc những gói tin chuyển tiếp có dấu hiệu là mã độc. Tuy nhiên khả năng lọc gói bị hạn chế trong việc xử lí các gói tin và dễ bị qua mặt bởi các hình thức tấn công phức tạp.

- Stateful Packet Filtering (Tường lửa lọc gói tin theo trạng thái): là loại tường lửa nâng cao hơn của Packet Filtering, loại tường lửa này lọc gói tin bằng cách theo dõi trạng thái của các kết nối mạng, đảm bảo rằng các gói tin chỉ được chấp nhận nếu thiết bị đã kết nối từ trước. Điều này giúp ngăn chặn các cuộc tấn công SYN Flood

- User Authentication Firewall (Tường lửa xác thực người dùng): là loại tường lửa yêu cầu người dùng phải xác thực trước khi truy cập vào mạng. Người dùng phải cung cấp thông tin đăng nhập để xác minh danh tính trước khi sử dụng dịch vụ mạng mong muốn.

- User Appliance Authentication (Tường lửa xác thực thiết bị người dùng): là loại tường lửa nâng cấp của tường lửa xác thực người dùng. Nó yêu cầu không chỉ người dùng xác thực danh tính mà cả thiết bị mà họ sử dụng cũng phải được xác thực trước khi truy cập vào mạng. Điều này đảm bảo chỉ có các thiết bị được ủy quyền mới có thể kết nối và truy cập vào hệ thống mạng.

- Application Gateway: Thay vì kiểm tra giao thức và cổng mà gói tin được sử dụng nó sẽ kiểm tra ứng dụng ở phía khách và máy chủ mà cả 2 đang cố gắng kết nối để quyết định xem lưu lượng truy cập của ứng dụng đó có được phép thông qua hay không nhằm đảo bảo tính an toàn và hợp lệ.

- Circuit Level Gateway: là phần mở rộng hơn của Application Gateway, loại tường lửa này cũng sử dụng phương thức xác thực người dùng. Việc xác thực người dùng được thực hiện ở bước đầu tiên, người dùng được cấp quyền truy cập.

Hệ thống Proxy là một máy chủ trung gian nằm giữa ứng dụng khách và máy chủ đảm nhận vai trò truyền tải và bảo vệ dữ liệu. Proxy được sử dụng chung với tường lửa nhằm mục đích ẩn địa chỉ IP của mạng nội bộ và sử dụng 1 địa chỉ IP với Internet bên ngoài. Nó có tác dụng ngăn tin tặc nhìn thấy địa chỉ IP của các máy trong nội bộ hệ thống mạng và thông tin về hệ thống mạng đó. Sử dụng máy chủ Proxy thì các giao thực sử dụng HTTP ra ngoài hoặc vào trong mạng nội bộ đều phải qua máy chủ Proxy trước tiên, nó có thể được chuyển hướng truy cập trang web. Nhờ khả năng này mà khi một máy trong mạng nội bộ truy cập 1 trang web, web đó chỉ phát hiện IP của Proxy. Nhờ sử dụng Proxy Server ta có thể tránh được các cuộc tấn công bằng IP Spoofing do ta đã ẩn địa chỉ IP của mạng nội bộ và sử dụng IP của Proxy khiến cho hacker không phát hiện được IP chính xác.

# CHƯƠNG 2 THIẾT KẾ HỆ THỐNG

## Ý tưởng

Công ty Giao hàng nhóm 8 xây dựng công ty gồm khoảng 40 nhân viên. 29 nhân viên thuộc phòng nhân sự, 5 nhân viên marketing, 5 nhân viên quản lý và kinh doanh. Và một nhân viên trực thuộc phòng quản trị hệ thống mạng.

Đây là công ty giao hàng nên nhóm sẽ triền khai web quản lý các đơn hàng. Hơn nữa hệ thống có nhóm của còn có DC,DHCP,DNS server để quản lý nhân viên và thiết bị. Hệ thống mạng có thể đáp ứng mọi nhu cầu ở mức tiêu chuẩn ổn định chịu tải tốt và có khả năng dự phòng. Những yếu tố đó nằm ở một chức năng mà nhóm rất tâm đắc đó là triển khai Etherchannel cho các cable bên trong hệ thống.

Sau khi xem xét, dựa trên yếu tố kinh tế và nhu cầu của doanh nghiệp. Nhóm quyết định triển khai mô hình Screened Host. MÔ hình có đủ những yếu tố cần thiết như cung cấp dịch vụ tốt, đảm bảo độ an toàn cho mô hình vừa và nhỏ. Ở mô hình này nhóm sẽ chú ý phần cung cấp dịch vụ DMZ phải được phân tách ra khỏi vùng server nội bộ. Mỗi khi các client muốn truy cập trang web của doanh nghiệp thì phải truy cập public để tránh bị tấn công từ các attacker sử dụng VPN tấn công bên trong nội bộ

Hệ thống mạng sẽ sử dụng công cụ bảo mật firewall fortigate giúp tiến hành ngăn chặn các truy cập trái phép từ bên trong và bên ngoài.

## Ưu – nhược điểm hệ thống mạng

Ưu điểm của hệ thống mạng:

* Dễ triển khai
* Giá thành của số lượng các thiết bị phù hợp với doanh nghiệp vừa và nhỏ
* Có tính ổn định và khả năng dự phòng
* Hạn chế được các cuộc tấn công từ bên ngoài và từ bên trong nội bộ.
* Có tính mở rộng
* Các nhân viên trong công ty chỉ được truy cập vào web của công ty bằng IP public để hạn chế các cuộc tấn công vào Web Server từ nội bộ
* Có sử dụng thêm Additional Domain để phòng khi máy Domain chính gặp sự cố thì sẽ có Additional Domain luôn sẵn sàng lên thay thế để đảm bảo được hiệu suất tốt nhất.

Khuyết điểm của hệ thống mạng :

* Chưa triển khai được bastion host quản lý các truy cập trái phép.
* Yêu cầu người quản trị phải có kiến thức và trình độ.

## Bảng quy hoạch IP

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Unit | Network | DG | Usable Range | Broadcast | Subnet Mask |
| Server | 172.16.0.64/29 | 172.16.0.65 | 172.16.0.66  –  172.16.2.70 | 172.16.0.71/29 | 255.255.255.248 |
| Marketing | 172.16.0.40/29 | 172.16.0.41 | 172.16.0.42  –  172.16.0.46 | 172.16.0.47/29 | 255.255.255.248 |
| Quản lý | 172.16.0.32/29 | 172.16.0.33 | 172.16.0.34  –  172.16.0.38 | 172.16.0.39/29 | 255.255.255.248 |
| Nhân sự | 172.16.0.0/27 | 172.16.0.1 | 172.16.0.2  –  172.16.0.30 | 172.16.0.31/27 | 255.255.255.224 |
| Network Devices | 192.168.34.0/24 |  | 192.168.34.1  –  192.168.34.2 |  | 255.255.255.0 |

*Bảng 1. Bảng quy hoạch địa chỉ ip*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| No  . | Devices | Interface | IP | Routing | | Notes |
| Destination | Gateway |
| 1 | Router | F0/0 | 192.168.69.144/ 24 | 0.0.0.0/0 | 192.168.69.2/ 24 | Static IP |
| F1/0 | 192.168.34.1/24 | - | 192.168.69.2/ 24 | Static IP |
| 2 | Core Switch | E0/0 | 192.168.33.2/24 | 0.0.0.0/0 | 192.168.33.1/24 | - |
| VLAN  2 | 172.16.0.1/27 | - | 192.168.33.2/24 | DG to NhanSu |
| VLAN  3 | 172.16.0.33/29 | - | DG to  Marketing |
| VLAN  4 | 172.16.0.41/29 | - | DG to Quan ly |
|  |  |  |  |
|  |  | VLAN  5 | 172.16.0.65/29 | - |  | DG to Server |
| 3 | Firewall Fortinet | Port1 | 192.168.34.2/24 | 0.0.0.0/0 | 192.168.34.1/24 | - |
| Port2 | 192.168.33.1/24 | - | - | - |
| 4 | DC + DNS | Eth0 | 172.16.0.66/29 | - | 172.16.0.65/29 | - |
| 5 | Subdomain | Eth0 | 172.16.0.69/29 | - | - |
| 6 | DHCP | Eth0 | 172.16.0.67/29 | - | - |
| 7 | Web -Server | Eth0 | 172.16.0.68/29 | - | - |

*Bảng 2. Bảng quy hoạch địa chỉ ip của thiết bị mạng*

## Sơ đồ Logic

A diagram of a computer network

Description automatically generated

Hình 1 Sơ đồ Logic

## Sơ đồ vật lí.

A floor plan of a house

Description automatically generated

Hình 2 Sơ đồ Vật Lý tầng trệt

A diagram of a computer room

Description automatically generated

Hình 3 Sơ đồ vật lý tầng 1

# CHƯƠNG 3 TRIỂN KHAI

## Domain Controller và Group Policy

* Công ty Giao Hàng QQExpress lấy tên miền là nhom8.com
* Các bước dưới đây sẽ mô tả chi tiết các giai đoạn tạo tên miền cho công ty, đồng thời tạo các chính sách cho các phòng ban của công ty.
* Ta có cấu hình IP của DC như sau :
  + IP address : 172.16.0.66
  + Subnet mask : 255.255.255.248
  + Default gateway : 172.16.0.65
  + DNS server : 1722.16.0.66

### Cài đặt dịch vụ Active Directory Domain Services

* Ở Server Manager tại tab dashboard , chọn Add roles and features để vào giao điện cài đặt.
* Tại Before you begin -> next.
* Tại Select installation type -> Role-based or feature-based installation -> next.
* Tại Select destination roles, chọn server của nhóm cài đặt dịch vụ Active Directory -> next.
* Tại màn hình Select server roles, nhấp chuột vào ô Active Directory Domain Services.
* Tại màn hình select Features -> next.
* Màn hình hiển thị thông tin về dịch vụ Active Directory, đọc nó -> next
* Tại màn hình Confirmation, chọn Install sau khi xác nhận mọi thứ đã ổn. Finish and Close

### Nâng cấp server lên Domain Controller

* Nếu cài đặt thành công, biểu tượng Flag trên cùng sẽ có Notification màu vàng. Ta nhấp vào và chọn Promote this server to a domain controller.
* Tại màn hình Deployment Configuration, ta ấn vào Add a new forest -> nhập tên domain (nhom8.com) -> next.
* Tại màn hình Domain Controller Options, chọn roles Domain Name System (DNS) server và Global Catalog (GC). Nhập mật khẩu DSRM -> next
* Tại màn hình DNS -> next
* Tại màn hình Prerequisite check -> install. Sau khi thành công máy sẽ tự động khởi động lại

### Tạo OU và User cho Domain

* Sau khi nâng cấp lên DC, ta tiến hành tạo OU chính là CONGTYGIAOHANG, và 4 OU con là Admin, Marketing, Quản Lí, Nhân Sự. Mỗi OU sẽ có chính sách phù hợp với từng phòng ban.
* Trong mỗi OU tạo user cho các phòng ban join vào Domain để nhận được chính sách tương ứng cho OU của mình và dùng tài khoản này để đăng nhập mấy.

Các bước tạo :

* Tại giao diện Administrator, góc bên trái -> Tools -> Active Directory Usrs and Computers.
* Tại OU CONGTYGIAOHANG -> OU QUANLY, nhâp chuột phải New -> User.
* Tại giao diện tạo User, điền đầy đủ thông tin vào -> next.
* Sau khi điền mật khẩu ta nhấn vào 2 tùy chọn là User cannot change pass và Pass never expires -> next.
* Tại mục Confirmation ta kiểm tra lại thứ và ấn finish.
* Đối với OU khác ta tiến hành tạo dựng tương tự

### Cấu hình Group Policy Object (GPO)

#### 1.4.1 Tạo khoá Registry

Chính sách mà nhóm cấu hình dưới đây sẽ giúp người dung hạn chế truy cập và can thiệp vào phần mềm gây ra các sự cố không mong muốn. Registry là cơ sở dữ liệu lưu trữ của window. Lưu lại thông tin về phần cứng, phần mềm, thông tin người sử dụng và registry luôn được cập nhật mỗi khi có sự thay đổi về các file quan trọng hay các hành động đụng đến rule của người sử dụng máy.

Các bước tiến hành :

* Mở Windows Administrator Tools, click chuột phải chọn Create a GPO on this domain -> link it here -> đặt tên Block\_Registry.
* Tại giao diện Management, nhấp vào edit .
* Tại giao điện editor, chọn User Configuration -> Policies -> Administrative Template -> System -> Prevent access to Registry Editing Tools -> Enable -> apply -> OK
* Cuối cùng ta mở cmd lên và gõ câu lệnh gpupdate /force để cập nhật chính sách cho các user

#### 1.4.2 Cấm Command Prompt:

Chính sách tiếp theo sẽ là chính sách cấm người dung truy cập vào Command Prompt nhằm không cho người dùng có những truy cập trái phép.

Các bước tiến hành:

* Mở Windows Administrative Tools, để cấu hình chính sách.
* Chọn OU CONGTYGIAOHANG, click chuột phải chọn Create a GPO on this domain, and link it here. Đặt tên GPO là Block Command Prompt.
* Nhấp chuột phải vào chính sách vừa tạo và chọn Edit.
* Tại Group Policy Management Editor, chọn User Configuration -> Policies -> Administrative Templates. Chọn System -> Prevent access to the Command Prompt.
* Enable chính sách để có thể áp dụng cho OU -> Apply -> OK.
* Mở cmd và nhập dòng lệnh gpupdate /force để cập nhật chính sách.

#### 1.4.3 Cấm Task Manager:

Chính sách tiếp theo sẽ cấm người dùng truy cập vào Task Manager nhằm tránh người dùng tắt những tiến trình của máy hay phần mềm quan trọng của công ty.

Các bước tiến hành:

* Mở Windows Administrative Tools, chọn Group Policy Management để cấu hình chính sách.
* Chọn OU CONGTYGIAOHANG, click chuột phải chọn Create a GPO on this domain. Sau đó, đặt tên chính sách là Block Task Manager.
* Nhấp chuột phải vào chính sách vừa tạo và chọn Edit.
* Chọn User Configuration tại màn hình Group Policy Management Editor -> Policies -> Administrative Template. Trong Administrative Template chọn System -> Ctrl + Alt + Del Opitons -> Remove Task Manager.
* Enable chính sách để áp dụng cho OU -> Apply -> OK.
* Mở cmd và nhập dòng lệnh gpupdate /force để cập nhật chính sách.

#### 1.4.4 Chỉ hiển thị những tác vụ cơ bản bên trong Control Panel

Ở Chính sách này nhóm triển khai policy là chỉ cho phép máy tính user hiển thị hạn chế các mục bên trong Control Panel. Các hiển thị cho phép chỉ gồm Mouse, System, Display. Việc này sẽ giúp người dùng hạn chế can thiệp trái phép vào cấu hình máy tính.

Các bước tiếp theo sẽ mô tả chi tiết quá trình tạo chính sách này:

- Mở Windows Administrative Tools, chọn Group Policy Management để cấu hình các chính sách.

- Chọn OU CONGTYDULICH, click chuột phải chọn Create a GPO on this domain, and link it here. Sau đó tạo một GPO đặt tên là Control Panel

- Nhấp chuột phải vào chính sách vừa tạo và chọn Edit

- Tại màn hình Group Policy Management Editor, Chọn User Configuration →

Policies → Administrative Templates. Trong Administrative Template chọn Control Panel → Show only specified Control Panel items

- Tại màn hình của chính sách này chọn Enable để bật chính sách này lên áp cho OU

- Bên dưới ở mục Options có một ô List of allowed Control Panel items, ta nhấn chọn

vào Show Contents

- Nhập lần lượt Fonts, Mouse, Display, System vào cột Value. Sau khi nhập xong thì nhấn OK

- Khi đã ra lại bàn hình cấu hình chính sách, nhấp vào Apply, sau đó nhấn OK

- Mở cmd lên và gõ câu lênh gpupdate /force để cập nhật chính sách cho user

## Additional Domain Controller:

Máy Additional Domain Controller là một máy được xây dựng để back up cho Domain Controller nhằm trường hợp máy Domain Controller gặp những rủi ro như: hệ thống hoạt động chập chạm do có quá nhiều máy Client truy cập xác thực, và nguy hiểm hơn là Domain Controller bị sự cố đặc biệt thì toàn bộ cơ sở dữ liệu trong Active Directory sẽ mất. Vì vậy, đây là giải pháp tối ưu giúp việc chia tải, phân giải giữa các Domain Controller cũng như cơ sở dữ liệu được lưu trữ trên các máy Domain Controller.

Công ty Giao hàng sẽ triển khai thêm Additional Controller, và đương nhiên cơ sở dữ liệu của Domain sẽ luôn đồng bộ với nhau. Nếu máy Primary Domain gặp sự cố thì máy Additional sẽ thay thế nhằm duy trì tính liên tục của Server.

Trước tiên, ta sẽ thiết lập IP cho máy chủ Sub Domain Controller như sau:

* IP Address: 172.16.0.69
* Subnet Mask: 255.255.255.248
* Default Gateway: 172.16.0.65
* Preferred DNS Server: 172.16.0.69

Sau khi nhập xong, ta sẽ kiểm tra kết nối từ máy Domain Controller đến máy Additional Domain Controller bằng lệnh Ping. Sau khi đã ping được thành công thì ta sẽ tiến hành cài đặt và cấu hình Additional Domain Controller.

### 2.1 Cài đặt dịch vụ Active Domain Service:

* Chúng ta sẽ nhấp vào Add roles and features từ giao diện Server Manager để hiển thị các dịch vụ cài đặt.
* Tại màn hình Before you begin, Next.
* Chọn Role-based or feature-based installation, Next.
* Tại Select Destination Roles, chọn Server mà ta muốn cài Active Directory, Next.
* Tại màn hình menu các dịch vụ, click chọn Active Directory Domain Services, Next cho đến khi thấy Install button và chọn Install.
* Sau khi đã Install thành công, Close.

### 2.2 Cấu hình Additional Domain Controller:

* Sau khi đã cài đặt ADDS thành công, ở màn hình Server Manager ta sẽ nhìn thấy một biểu tượng tam giác vàng, nhấp chọn nó và Promote this server to a Domain Controller.
* Tiếp theo, ta sẽ cấu hình nó bằng cách chọn mục Add a domain controller to an existing domain ở màn hình Deployment Configuration nhằm tạo thêm một domain vào domain có sẵn là nhom8.com.
* Nhập tên domain có sẵn nhom8.com và chọn Select.
* Nhập tài khoản và mật khẩu, Next.
* Đến mục Select a domain from the forest ta chọn nhom8.com và OK.
* Tại màn hình Domain Controller Options, chọn Domain Name System (DNS) và Global Catalog (GC). Nhập mật khẩu và Next.
* Sau đó, ta sẽ nhận được cảnh báo của DNS Options, bỏ qua tùy chọn Update DNS Delegation và Next.
* Chọn Replicate from Any Domain Controller ở mục Additional Opiton.
* Ta sẽ tiếp tục Next đến phần Install.
* Sau khi install thành công, ta sẽ restart lại.

## Web Server:

* Ở Dashboard, ta chọn Add roles and features để tiến hành cài đặt Web Server.
* Tại màn hình Before you begin, Next.
* Chọn Role-based or feature-based installation, Next.
* Tại Select Destination Roles, chọn Server mà ta muốn cài Active Directory, Next.
* Chọn Web Server (IIS), Next.
* Ta sẽ tiếp tục next đến phần install.
* Sau khi cài đặt thành công, ta sẽ vào ổ đĩa C và chọn folder web -> tạo file nhom8.html bên trong.
* Vào Administrative Tools, chọn Internet Information Services (IIS) Manager.
* Vào được phần dashboard Application Pools and Sites. Vào folder Sites, vào Default Web Site -> Default Document -> Action -> Add -> Nhập tên file trangchu.html . Sau khi add raw file vào ta tiến hành deploy bằng cách ấn vào góc phải hoặc vào trình duyệt nhập tên web www.nhom8.com.

## DNS Server

Sau khi cài đặt DNS thành công, ta sẽ tiến hành cấu hình phân giải tên miền cho Công ty giao hang nhóm 8 . Ở đây nhóm sử dụng địa chỉ www.nhom8.com và đây cũng sẽ là địa chỉ truy cập web của Công ty.

Các bước dưới đây sẽ mô tả chi tiết quá trình phân giải tên miền như sau:

- Mở Server Manager, ở tab Tools click chọn dịch vụ DNS

- Khi giao diện cấu hình xuất hiện, nhấp vào tên miền nhom8.com, nhấp chuột phải vào Forward Lookup Zones và chọn New Zone, sau đó nhấn Next

- Ở phần Zone Type, ta tích vào Primary zone và nhấn Next.

- Đến phần Zone Name, ta nhập Zone Name: nhom8.com.

- Ở giao diện mục Zone File, ta tích vào Create a new file with this file name, và nhấn Next.

- Sau đó, đến mục Dynamic Update ta tích vào Allow both nonsecure and secure dynamic updates rồi nhấn Finish

- Kết thúc phần Foward Lookup Zone, ta click chuột phải vào Reverse Lookup Zones và chọn New Zone.

- Ở phần Zone Type, ta tích vào Primary Zone và nhấn Next

- Đến mục Reverse Lookup Zone Name , ta tích vào Ipv4 Reverse Lookup Zone rồi nhấn Next.

- Ở Reverse Lookup Zone Name, ta nhập vào Network ID: 172.16.0

- Tại mục Zone File, ta tích vào Create a new file this file name và nhấn vào Next

Ngay phần Dynamic Update, ta tích vào Allow both nonsecure and secure dynamic updates, sau đó nhấn Finish để hoàn thành.

* Ở bên trong mục Foward Lookup Zone, ta nhấp chuột phải vào nhom2.com, chọn New Host (A or AAAA)
* Ở cửa sổ New Host, gõ vào như sau:

|  |  |
| --- | --- |
| Name | www |
| IP address | 172.16.0.68 |

* Sau đó chọn “Create associated pointer(PTR)” -> add Host.
* Sau khi xong hết các bước trên tiến hành restart lại DNS .
* Cuối cùng vào một máy tính bất kì đã join Domain và thực hiện nslookup về tên miền [www.nhom8.com](http://www.nhom8.com) . Nếu nó phân giải được ra IP nghĩa ra ta đã thành công.

## DHCP Server

### 5.1 Cài đặt dịch vụ DHCP

* Ở Dashboard, ta chọn Add roles and features để tiến hành cài đặt DHCP Server
* Tại màn hình Before you begin, Next.
* Tại Select Destination Roles, chọn Server mà ta muốn cài Active Directory, Next.
* Tại màn hình menu các dịch vụ, click chọn DHCP Server Tools, Next cho đến khi thấy Install button và chọn Install.
* Sau khi đã Install thành công, Close.
* Ở Dashboard trên có thông báo màu vàng ở trên cùng bên phải
* Nhấp vào “Complete DHCP configuration” để hoàn thành cấuu hình DHCP
* Ở phần Description nhấn Next
* Sau đó đến phần Authorization, chọn Use the following user’s credentials
* Nhấn Commit
* Khi xuất hiện bảng Summary nhấn Close.

### 5.2 Cấu hình dịch vụ DHCP

* Ở Server manager chọn Tools chọn DHCP để cấu hình
* Chọn mục Ipv4, click chuột phải chọn New scope để tạo scope cho mạng Lan
* Sau đó đặt tên cho scope dự theo phòng các phòng như Makerting, Quản lí và Nhân sự sau đó nhấn Next
* Ở mục IP address range, nhập địa chỉ IP đầu cuối dựa theo bảng phân hoạch địa chỉ IP đã tính trước đó cũng như subnet mask, sau đó nhấn Next
* Ở mục Add Exclusion and delay dùng để không cấp các IP của các thiết bị được cấp cố định như Server, router…Sau đó nhấn Next.
* Nhấn Next cho tới Finish để hoàn thành việc tạo scope cấp DHCP.

## Symantec Endpoint Protection

Sysmantec Endpoint Protection (SEP) là phần mềm anti-virus khá phổ thông và được biết đến rộng rãi trong giới bảo mật. Là lớp phòng vệ cuối cùng trong hệ thống mạng giúp thoát khỏi các mối đe dọa từ các phần mềm độc hại như virus, mã độc, phần mềm gián điệp.

Khi kẻ tấn công vượt qua được firewall thì vẫn còn anti-virus chặn lại. Công ty giao hang nhóm 8 sẽ chọn triển khai phần mềm Symantect Endpoint Protection lên máy server Monitor-Backup vì server này luôn trong (trạng thái sẵn sàng).

Các bước sau đây sẽ mô tả chi tiết quá trình cài đặt và cấu hình một Anti-virus server

- Đầu tiên, ta tải file setup Symantect Endpoint Protection về máy

- Chạy file setup .exe -> cửa sổ Symantect Endpoint Protect Installation Program -> chọn option Install Symantect Endpoint Protection Manager.

- Nhấn Next ở mục Install the management server and console -> Lincense -> chọn I accept the terms in the license agreement -> Next

- Đến cửa sổ Destination Folder, chọn ổ đĩa đích để chứa folder của phần mềm-> Next

– Ở cửa sổ Ready to Install the Program ta nhấn Install và chờ đợi phần mềm được cài đặt.

- Sau khi cài đặt thành công sẽ trở về cửa sổ đầu tiên, khi đó ta sẽ nhấn Next ở mục Configure the management server

- Khi nhấn Next thì hệ thống sẽ hiển thị ra một cửa sổ mới là Management Server Configuration Wizard thì ta dể option mặc định là Default configuration for new installation rồi ta nhấn Next

- Đến cửa sổ Create a system administrator account, ta điền lần lượt các thông tin như sau:

• Company name: Cong ty Giao Hang Nhom 8

• User name: admin

• Password: @Admin1234

• Confirm password: @Admin1234

• Email address: [congtygiaohangnhom8@gmail.com](mailto:congtygiaohangnhom8@gmail.com)

- Sau đó thì ta nhấn Next thì sẽ hiện lên một thông báo Email Address Not Validated. Khi đó ta nhấp vào No

- Trong mục Partner Information (Optional) thì ta nhấn Next

- Ta tiếp tục nhấn Next ở phần Server Data Collection và nhấn Finish khi đã hoàn tất quá trình Configuration

- Sau khi cài đặt thành công, ta nhập tìm Symantect Endpoint Protection, sau đó nhấn chọn Symantect Endpoint Protection Manager

- Khi đó cửa sổ đăng nhập hiện ra và ta nhập user name và password để đăng nhập vào hệ thống

- Ta vào tab Client, chọn Install a client, một cửa sổ Client Deploymonent Wizard sẽ xuất hiện. Ta chọn Next ở các bước đầu tiên.

- Tại Specify the folder, ta chọn Browse rồi chọn Desktop làm nơi xuất file. Sau đó nhấn Next đến bước Ready to save the package. Trong quá trình Creating Installation Files, một cửa sổ Warning yêu cầu ta chạy Live Update

- Nhấn Ok rồi chờ quá trình tạo file. Sau khi tạo xong thì ta nhấn Finish.

- Bắt đầu quá trình chạy file cài đặt Client mà ta đã tải xuống trước đó.

- Các bước setup tương tự như khi cài bản Symantec Endpoint Protection Manager. Hoàn thành xong bước cài đăt thì ta nhấn Finish.

- Sau khi cài xong file client, ta vào Start, nhấn chọn Symantec Endpoint Protection Client trên máy server.

- Quay lại Protection Manager để kiểm tra xem máy DC đã trở thành một client của hệ thống Symantec chưa. Như vậy thì ta cũng có thể dùng phần mềm này để quét luôn cả máy DC.

- Để cài đặt Symantec Enpoint Protection cho các máy client trong hệ thống, ta chia sẻ folder chứa file setup cho các máy trong nội bộ. Bằng cách nhấp chuột phải vào folder chọn Properties → chọn tab Sharing → Advance Sharing → rồi tick vào o share this folder. Sau đó chọn Permissions, rồi cấp quyền cho Everyone với Full Control. Nhấn Apply, rồi nhấn OK.

- Chuyển sang máy client trong hệ thống, mở File Explorer rồi đến địa chỉ share của folder. Rồi copy file setup ra màn hình Desktop và bắt đầu quá trình cài đặt.

- Hoàn thành xong bước cài đặt Symantec Endpoint Protection Client trên các máy trong nội bộ thì ta quay lại DC để kiểm tra xem trong mục Client đã xuất hiện thông tin của các máy nội bộ trong hệ thống không. Nếu nhìn thấy thông tin thì ta đã cài đặt thành công.

## Fortigate.

Với mô hình Firewall screened host, nhóm đưa ra giải pháp sử dụng thiết bị Fortigate để đảm bảo tính bảo mật, ổn định của website, an toàn trong các tính hiệu truyền đi trong mạng. Lọc các gói tin cũng như thiết lập các chính sách hợp lí giữa các thiết bị trong mạng với nhau và các thiết bị ngoài mạng. Cùng với dịch vụ Filter lưu lượng có sẵn bên trong thiết bị sẽ giúp hệ thống mạng của công ty hạn chế các truy cập trái phép từ bên trong và bên ngoài

Các bước cài đặt và tiến hành thiết lập chính sách:

- Kết nối port 1 (WAN) trên Fortigate với port f0/0 trên router, port 2 (LAN) tương ứng với port e0/0 trên core switch.

- Tiến hành vào static route set IP gateway là 192.168.34.1(cổng f0/0 của router) và cổng outgoing là cổng Wan (port1).

- Thiết lập OSPF cho vùng router area 0. Ta nhấp chuột vào phần Network -> OSPF -> Nhập IP cổng Wan : 192.168.34.1 -> tạo area : 0.0.0.0

- Tạo thêm 2 vùng mạng interrior và exterrior là : 192.168.33.0/24 và 192.168.34.0/24

- Tiến hành thêm policy/rule firewall :

+ Outgoing : lan

+ Incoming : wan

+ permit : all

+ Web filter : rules block web facebook

## PRTG Network Monitor

PRTG là một phần mềm giám sát mạng hỗ trợ bản miễn phí cho các người dùng không phải doanh nghiệp giúp kiểm tra và khắc phực các vấn đề việc kết nối mạng trong window

Sau đây là bước triển khai phần mềm Monitor

- Install phần mềm trển Internet -> chọn ngôn ngữ

- Ở phần license Agreement -> i accept the agreement -> nhập email vào mục Your Email Address -> next.

- Tại mục Installation -> chọn Express mmode (recommend) -> sau khi chọn các bước trên thì chúng ta thành công và đợi PRTG được deploy lên địa chỉ Localhost

- Tiến hành login với tài khoản và mật khẩu mặc định : {"username" : "prtgadmin" ; "password" : "prtgadmin" }

- Sau khi vào được giao diện Dashboard -> ta thiết lập lại account (nếu cần thiêt)

- Tạo thêm group nhom8.com vào Network Discovery

- Tiến hành thêm sensor từ các thiết bị vào Nhấn vào Add Device -> điền Device name -> điền IPv4 của máy cần giám sát.

- Ở mục Auto-Discovery Settings -> Default auto-discovery Settings -> Default auto-discovery (recommend) -> Default -> ok.

- Sau khi add các sensor mặc định thì nó sẽ list ra cho chúng ta (sau khi scan đến thiết bị đó đạt 100%)

Nhóm chúng em cũng triền khai được phần gửi các thông báo sang một bot chat tại Telegram :

- Ta lên telegram search chữ /botfather và chọn nick có tích tròn xanh -> nhập lệnh /addbot.

- Ta nhận được một Token : (5452821230:AAG79EYrDC0WabcxzddPXLpH8XSTZLG) lưu nó lại vào đâu đó

- Sau khi đã đặt tên thành công thì ta sẽ vào tạo một roomchat và add bot Alert vào đó.

- Vào PRTG mục Setup > Notification hoặc Notification Template > Add new Notification.

- Trong mục URL nhập : https://web.telegram.org/bot(mã token của bạn)>/sendMessage

- Mục Post data : chat\_id= -4195394749&text=

[%sensor](%linksensor)

Last Value %lastvalue

Last Message %lastmessage

Down since %since

Device %device

Group %group&parse\_mode=Markdown

## Snort

Nhóm sẽ triển khai phần mêm Snort IDS trên máy Monitor. Đây là phần mềm mã nguồn mở được đánh giá cao trong việc phát hiện xâm nhập.

Ưu điểm cao nhất là mặc dù nó miễn phí nhưng các tính năng của nó rất tuyệt vời giúp tăng cường bảo mật cho hệ thống.

- Ta cần tải trước các phần mềm như : npcap, winpcap, notepad++, snort.exe và snortrule.

- Tiến hành cài đặt -> chạy file snort.exe -> copy & paste 2 file pre\_procrule và rules vào bên trong c:\Snort.

- Sau khi thực hiện các bước trên ta vào config và đôi đường dẫn các biến cho phù hợp với đường dẫn hiện hành trên máy tính.

- Sau khi thành công ta vào test thử đã xây dựng Snort thành công chưa bằng câu lệnh : snort.exe -V.

- Tiến hành chạy Snort console bằng câu lệnh : Snort -i 1 c:\Snort\etc\snort.conf -A console

## Xây dựng các chính sách (luật) trong công ty

### Sử dụng thiết bị mạng:

+ Sử dụng đúng mục đích trong công việc

+ Không truy cập hoặc download các dữ liệu lạ hoặc không liên quan đến công việc

### Bảo mật thông tin:

+ Không được chia sẻ thông tin tài khoản mật khẩu của mình cho người khác

+ Bảo mật thông tin của công ty và của khách hàng

### Quyền hạn:

+ Không được ra vào phòng Server khi chưa có sự cấp phép của Admin

+ Khi các thiết bị mạng xảy ra vấn đề cần liên hệ kỹ thuật hỗ trợ

### Bảo trì và Bảo dưỡng thiết bị:

+ Khi xảy ra vấn đề cháy nổ ở phòng Server chỉ được dùng bình xịt cứu hỏa ( bình bọt ) để xử lý vụ cháy

+ Các thiết bị mạng chỉ sử dụng trong 5 năm sau đó cần thay mới và chính hãng hoàn toàn

# Tài liệu tham khảo

[network-defense.pdf](C:/Users/mrtri/Downloads/Documents/network-defense.pdf)

[the-pfsense-documentation.pdf](C:/Users/mrtri/Downloads/Documents/the-pfsense-documentation.pdf)

<https://learn.microsoft.com/en-us/windows-server/>

[Top 20 Most Common Types Of Cyber Attacks | Fortinet](https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks)

[Cyber-Security-1.pdf](C:/Users/mrtri/Downloads/Documents/Cyber-Security-1.pdf)

<https://www.paessler.com/manuals/prtg/quick_start_guide>

<https://www.snort.org/documents>

<https://ttcshelbyville.wordpress.com/2014/03/30/defending-your-network-with-snort-for-windows/>

<https://cnttshop.vn/blogs/fortinet/huong-dan-cau-hinh-config-firewall-fortigate-1111>