

BỘ THÔNG TIN VÀ TRUYỀN THÔNG  
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



BÁO CÁO ĐỊNH KỲ THỰC  
TẬP TỐT NGHIỆP ĐẠI  
HỌC

*Đề tài: “XÂY DỰNG HỆ THỐNG  
GIÁM SÁT MẠNG VỚI SNORT”*

Người hướng dẫn : NGUYỄN HOÀNG THÀNH  
Sinh viên thực hiện : NGÔ ĐỨC TUÂN  
Mã số sinh viên : N20DCAT054  
Lớp : D20CQAT01-N  
Khoa : 2020  
Ngành : AN TOÀN THÔNG TIN  
Hệ : CHÍNH QUY

BỘ THÔNG TIN VÀ TRUYỀN THÔNG  
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



BÁO CÁO THỰC TẬP  
TỐT NGHIỆP ĐẠI HỌC

*Đề tài:* “XÂY DỰNG HỆ THỐNG GIÁM SÁT  
MẠNG VỚI SNORT”

Người hướng dẫn : **NGUYỄN HOÀNG THÀNH**  
Sinh viên thực hiện : **NGÔ ĐỨC TUẤN**  
**Mã số sinh viên** : **N20DCAT054**  
Lớp : **D20CQAT01-N**  
Khoa : **2020**  
Ngành : **AN TOÀN THÔNG TIN**  
Hệ : **CHÍNH QUY**

TP.HCM, tháng 07/2024

## NHẬN XÉT QUÁ TRÌNH THỰC TẬP CỦA SINH VIÊN

Họ và tên sinh viên : Ngô Đức Tuấn

Lớp : D20CQAT01-N

Nơi thực tập : Công ty Cổ phần An ninh mạng THD

Họ tên người nhận xét : Trần Tuấn Anh

Nội dung đánh giá	Xếp loại (dán dấu vào ô được chọn)				
	Tốt	Khá	Trung bình	Trung bình yếu	Yếu
<b>I. Tính kỷ luật và tư chất</b>					
I.1. Thực hiện nội quy	X				
I.2. Thái độ làm việc	X				
I.3. Năng lực tiếp thu	X				
I.4. Khả năng vượt khó	X				
I.5. Giao tiếp và ứng xử	X				
<b>II. Khả năng chuyên môn</b>					
II.1. Kiến thức	X				
II.2. Kỹ năng thực hành	X				
II.3. Năng lực ngoại ngữ		X			
II.4. Kỹ năng làm việc nhóm	X				
II.5. Tinh sáng tạo		X			
<b>III. Kết quả thực hiện đề tài được giao</b>					
I.1. Thực hiện yêu cầu về nội dung		X			
I.2. Thực hiện yêu cầu về tiến độ		X			
<b>IV. Nhận xét khác và lời khuyên cho sinh viên:</b>					
Hiệu quả công việc: Hoàn thành hầu hết các nhiệm vụ đúng hạn và đạt yêu cầu. Công việc ít lỗi và đáp ứng yêu cầu của cấp trên.					
Mục tiêu: Giám sát, xử lý cảnh báo cho hệ thống giám sát SOC Tier 1 – Tier 2					
Kỹ năng làm việc: Có thể sử dụng các công cụ ở mức cơ bản. Các vấn đề đề chuyên môn cao hơn thì vẫn cần được hỗ trợ và hướng dẫn và đã được cải thiện tốt hơn. Đạt kỳ vọng của phòng ban và công ty đối với nhân sự					
Thái độ: Tích cực, nhiệt tình và có trách nhiệm cao trong công việc. Thể hiện sự sẵn sàng học hỏi và cải thiện bản thân.					
Tinh thần hợp tác: Dễ dàng làm việc nhóm, chủ động nhờ hỗ trợ khi cần.					
<b>V. Điểm tổng kết thực tập tốt nghiệp (thang điểm 10): ...8.....</b>					

XÁC NHẬN CỦA TỔ CHỨC/DOANH NGHIỆP



Phạm Thị Hồng Hảo  
TỔNG GIÁM ĐỐC

NGƯỜI NHẬN XÉT  
(ký tên ghi rõ họ tên)

Trần Tuấn Anh

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

Độc lập- Tự do- Hạnh phúc

TP. Hồ Chí Minh, ngày tháng năm 20...

**NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN**

**THỰC TẬP TỐT NGHIỆP ĐẠI HỌC**

1. **Tên đề tài:** Xây dựng hệ thống giám sát mạng với Snort

2. **Sinh viên:** Ngô Đức Tuấn

**Lớp:** D20CQAT01-N

3. **Giáo viên hướng dẫn:** Nguyễn Hoàng Thành

4. **Nơi công tác:** khoa Công nghệ thông tin 2

**NỘI DUNG NHẬN XÉT**

1. Đánh giá chung:

.....  
.....  
.....

2. Đánh giá chi tiết:

.....  
.....

3. Nhận xét về tinh thần, thái độ làm việc:

.....  
.....

4. Kết luận:

.....  
.....

5. Điểm hướng dẫn:

**GIÁO VIÊN HƯỚNG DẪN**

(Ký, ghi rõ họ tên)

## LỜI CẢM ƠN

Em xin bày tỏ lòng biết ơn sâu sắc đến thầy Nguyễn Hoàng Thành, người đã tận tình hướng dẫn và hỗ trợ em trong suốt quá trình thực hiện đề tài "Xây dựng hệ thống giám sát với Snort". Sự chỉ dẫn nhiệt tình, những góp ý quý báu và sự kiên nhẫn của thầy đã giúp em hoàn thiện đề tài này.

Em đã học hỏi được rất nhiều từ thầy, không chỉ về kiến thức chuyên môn mà còn về tinh thần nghiên cứu, làm việc nghiêm túc và trách nhiệm. Những kỹ năng và kinh nghiệm mà em có được từ quá trình thực hiện đề tài này sẽ là hành trang quý giá cho chúng em trong tương lai.

Em xin chân thành cảm ơn thầy đã luôn đồng hành, động viên và truyền đạt những kiến thức quý báu, giúp em vượt qua những khó khăn và thử thách trong suốt quá trình nghiên cứu. Một lần nữa, em xin gửi đến thầy lời cảm ơn chân thành và sâu sắc nhất.

Tp. Hồ Chí Minh, tháng 08 năm 2024

Sinh viên thực hiện

Tuấn

Ngô Đức Tuấn

**MỤC LỤC**

<b>LỜI CẢM ƠN .....</b>	i
<b>MỤC LỤC .....</b>	ii
<b>DANH MỤC BẢNG VÀ HÌNH ẢNH .....</b>	iv
<b>KÍ HIỆU VÀ CÁC CỤM TỪ VIẾT TẮT .....</b>	vii
<b>LỜI MỞ ĐẦU .....</b>	1
<b>CHƯƠNG 1: GIỚI THIỆU .....</b>	2
<b>1.1 Bối cảnh chọn đề tài .....</b>	2
<b>1.2 Mục tiêu đề tài.....</b>	2
<b>1.3 Cấu trúc báo cáo.....</b>	2
<b>CHƯƠNG 2: CƠ SỞ LÝ THUYẾT .....</b>	3
<b>2.1 An ninh mạng và các mối đe dọa .....</b>	3
<b>2.1.1 Khái niệm an ninh mạng .....</b>	3
<b>2.1.2 Các loại tấn công phổ biến.....</b>	3
<b>2.2 Hệ thống phát hiện xâm nhập (IDS) và ngăn chặn xâm nhập (IPS) .....</b>	3
<b>2.2.1 Khái niệm và vai trò của IDS và IPS .....</b>	3
<b>2.2.2 Các phương pháp phát hiện xâm nhập.....</b>	3
<b>2.3 Giới thiệu về Snort .....</b>	4
<b>2.3.1 Lịch sử và phát triển của Snort .....</b>	4
<b>2.3.2 Chức năng và các thành phần của Snort .....</b>	4
<b>2.3.3 Ưu và nhược điểm của Snort .....</b>	4
<b>2.4 Graylog .....</b>	5
<b>2.4.1 Giới thiệu về Graylog.....</b>	5
<b>2.4.2 Chức năng chính của Graylog .....</b>	5
<b>2.4.3 Các thành phần chính của Graylog .....</b>	5
<b>2.4.4 Tích hợp Snort với Graylog .....</b>	5
<b>2.4.5 Ưu và nhược điểm của Graylog .....</b>	5
<b>CHƯƠNG 3: TRIỂN KHAI MÔ HÌNH.....</b>	7
<b>3.1 Giới thiệu.....</b>	7
<b>3.2 Mô hình hệ thống .....</b>	7
<b>3.3 Thiết kế chi tiết các thành phần .....</b>	8
<b>3.3.1 PfSense với Snort .....</b>	8
<b>3.3.3 Mạng DMZ .....</b>	8
<b>3.4 Xây dựng mô hình mạng doanh nghiệp.....</b>	9
<b>3.4.1 Thông số máy ảo .....</b>	9
<b>3.4.2. Cấu hình phần mềm .....</b>	9
<b>3.4.3 Cấu hình NAT .....</b>	16

3.4.4 Tạo user cho LAN .....	18
3.4.5 Remote từ Lan đến Windows server .....	20
3.4.6 OpenVPN và Remote desktop từ máy Internet vào LAN.....	22
3.4.7 Cài đặt Graylog.....	28
<b>3.5 Cấu hình Snort và gửi log về Graylog trên firewall Pfsense.....</b>	<b>29</b>
3.5.1 Cấu hình Snort .....	29
3.5.2 Gửi log từ Pfsense về Graylog.....	31
<b>3.6 Cấu hình Web server và Nginx, gửi log Nginx về Graylog.....</b>	<b>33</b>
3.6.1 Cài đặt Apache Tomcat và Nginx .....	33
3.6.2 Chuyển log nginx đến Graylog.....	35
<b>3.7 Cấu hình custom rules.....</b>	<b>38</b>
<b>3.8 Tạo Alert trên Graylog.....</b>	<b>39</b>
<b>3.9 Demo tấn công.....</b>	<b>40</b>
3.9.1 SQL injection .....	40
3.9.2 Brute Force SSH Attack.....	42
3.9.3 DOS Attack.....	44
<b>CHƯƠNG 4: KẾT LUẬN.....</b>	<b>46</b>
4.1 Tìm hiểu và phân tích các chức năng của Snort.....	46
4.2 Xây dựng mô hình mạng doanh nghiệp.....	46
4.3 Xây dựng và triển khai mô hình giám sát mạng sử dụng Snort và Graylog .....	46
4.4 Đánh giá hiệu quả của mô hình thông qua các kịch bản kiểm thử .....	46
4.5 Tổng kết.....	46
<b>TÀI LIỆU THAM KHẢO.....</b>	<b>47</b>

**DANH MỤC BẢNG VÀ HÌNH ẢNH**

Hình 3.1 - Mô hình hệ thống .....	7
Bảng 3.1 – Bảng thông số các máy ảo .....	9
Hình 3.2 - Cấu hình Web interface trên cổng LAN.....	10
Hình 3.3 - Giao diện web mặc định của pfsense .....	10
Hình 3.4 - Cấu hình hostname, domain, dns .....	10
Hình 3.5 - Đặt mật khẩu admin .....	11
Hình 3.6 - Thêm interface DMZ .....	11
Hình 3.7 - Cấu hình interface DMZ .....	12
Hình 3.8 - IP configuration của Windows Server 2019 .....	12
Hình 3.9 - Add roles and features .....	13
Hình 3.10 - Active Directory Domain Services.....	13
Hình 3.11 - Tạo Root domain name .....	14
Hình 3.12 - Thêm DHCP .....	14
Hình 3.13 - Đặt IP range.....	15
Hình 3.14 - Authorize DHCP server .....	15
Hình 3.15 - Cấu hình DHCP relay .....	16
Hình 3.16 - Cấu hình NAT trên port HTTP .....	16
Hình 3.17 - Cấu hình NAT trên port HTTP của interface DMZ .....	17
Hình 3.18 - Rule cho phép kết nối mạng trên DMZ .....	17
Hình 3.19 - Tạo group .....	18
Hình 3.20 - Cho phép remote desktop trên user Tuanuser1 .....	18
Hình 3.21 - Login vào máy windows 10 bằng user Tuanuser1 .....	19
Hình 3.22 - Login user Tuanuser1 thành công .....	19
Hình 3.23 - Ping từ máy windows 10 đến windows server 2019 .....	20
Hình 3.24 - Thêm group Remote Desktop Users vào Local Security Setting.....	20
Hình 3.25 - Remote desktop từ máy windows 10.....	21
Hình 3.26 - Remote thành công .....	21
Hình 3.27 - Tạo Organization Unit và thêm group user vừa tạo vào unit đó .....	22
Hình 3.28 - Cấu hình Authentication Server .....	23
Hình 3.29 - Các thông tin của Unit đã tạo .....	23
Hình 3.30 - Setting user manager.....	24
Hình 3.31 - Thành công tạo Authentication Server.....	24
Hình 3.32 - Thông tin yêu cầu của OpenVPN.....	25
Hình 3.33 - Cài thêm package OpenVPN client export .....	25

---

Hình 3.34 - Chọn phiên bản Client Export phù hợp .....	26
Hình 3.35 - Kết nối VPN sử dụng máy thật .....	26
Hình 3.36 - Kết nối thành công .....	27
Hình 3.37 - Ping tới máy trong LAN từ máy thật .....	27
Hình 3.38 - Remote Desktop thành công từ máy thật .....	27
Hình 3.39 – Cài đặt môi trường java .....	28
Hình 3.40 – Cấu hình Elasticsearch.....	28
Hình 3.41 – Kiểm tra status của MongoDB .....	28
Hình 3.42 – Cấu hình Graylog .....	29
Hình 3.43 – Cài đặt Snort.....	29
Hình 3.44 – Cấu hình mẫu của Snort .....	30
Hình 3.45 – Update rule Snort .....	30
Hình 3.46 – Cấu hình Snort interface .....	31
Hình 3.47 – Chọn các rule sẽ được áp dụng .....	31
Hình 3.48 – Cấu hình gửi log từ firewall đến máy Graylog .....	32
Hình 3.49 – Cấu hình input cho log từ firewall .....	32
Hình 3.50 – Log alert của Snort trên firewall .....	33
Hình 3.51 – Website chính thức của “Apache Tomcat” .....	33
Hình 3.52 – Build thành công file “.War” .....	34
Hình 3.53 – Kết quả sau khi cài đặt và cấu hình thành công Website.....	34
Hình 3.54 – Cấu hình Nginx.....	35
Hình 3.55 – Cấu hình WinSCP.....	35
Hình 3.56 – Script Powershell.....	36
Hình 3.57 – Cấu hình chạy tự động trên Task Scheduler .....	36
Hình 3.58 – Log đã được gửi đến máy Graylog.....	36
Hình 3.59 – Cấu hình input cho log đến từ Nginx.....	36
Hình 3.60 – Cấu hình filebeat .....	37
Hình 3.61 – Cấu hình NAT Port Forward.....	37
Hình 3.62 – Kiểm tra cấu hình NAT .....	38
Hình 3.63 – Rule SQL injection, Bruteforce Attack, Dos .....	39
Hình 3.64 – Thông tin cấu hình Event definitions.....	40
Hình 3.65 – Cấu hình Notifications.....	40
Hình 3.66 – Tấn công SQL injection vào form đăng nhập.....	41
Hình 3.67 – Graylog Alert SQL injection.....	41
Hình 3.68 – Email cảnh báo từ Graylog .....	41

---

<i>Hình 3.69 – Tạo list password sử dụng Crunch.....</i>	42
<i>Hình 3.70 – Tấn công ssh authentication sử dụng hydra.....</i>	43
<i>Hình 3.71 – Graylog Alert Brute Force .....</i>	43
<i>Hình 3.72 – Email cảnh báo Brute Force từ Graylog.....</i>	43
<i>Hình 3.73 – Tấn công sử dụng hping3 .....</i>	44
<i>Hình 3.74 – Graylog Alert Dos Attack .....</i>	45
<i>Hình 3.75 – Email cảnh báo Dos Attack từ Graylog .....</i>	45

**KÍ HIỆU VÀ CÁC CỤM TỪ VIẾT TẮT**

ADSI: Active Directory Service Interfaces	Giao diện Dịch vụ Active Directory
AD-DS: Active Directory Domain Service	Dịch vụ lưu trữ thông tin thư mục và xử lý tương tác của người dùng với domain
BASE DN: Base Distinguished Name	Tên phân biệt cơ sở
DHCP: Dynamic Host Configuration Protocol	Giao thức cấu hình động máy chủ
DMZ: Demilitarised Zone	Khu vực chứa các Server
HTTP/S	HTTP và HTTPS
Input	Đầu vào
ICMP: Internet Control Message Protocol	Giao thức Thông điệp Điều khiển Internet
IP: Internet Protocol	Giao thức internet
Log	Nhật ký của ứng dụng
LAN: Local Area Network	Mạng nội bộ
LDAP: Lightweight Directory Access Protocol	Phương thức đăng nhập trực tiếp
NoSQL	Cơ sở dữ liệu phi quan hệ
NAT: Network Address Translation	Biên dịch địa chỉ mạng
TCP: Transmission Control Protocol	Giao thức điều khiển truyền vận
UDP: User Datagram Protocol	Giao thức truyền thông không kết nối
VPN: Virtual Private Network	Mạng riêng ảo
WAN: Wide Area Network	Mạng diện rộng

**LỜI MỞ ĐẦU**

Ngày nay, với sự phát triển không ngừng của công nghệ thông tin và Internet, vấn đề an ninh mạng trở thành một trong những mối quan tâm hàng đầu của các tổ chức và cá nhân. Các cuộc tấn công mạng ngày càng tinh vi và đa dạng, đòi hỏi các biện pháp bảo vệ phải được cải tiến và nâng cao liên tục. Trong bối cảnh đó, việc giám sát và phát hiện các hành vi xâm nhập trái phép trở nên vô cùng quan trọng.

Snort là một trong những công cụ mã nguồn mở phổ biến và mạnh mẽ nhất hiện nay, được sử dụng rộng rãi trong việc phát hiện xâm nhập (Intrusion Detection System - IDS) và ngăn chặn xâm nhập (Intrusion Prevention System - IPS). Với khả năng phân tích lưu lượng mạng, phát hiện các cuộc tấn công dựa trên chữ ký và các quy tắc, Snort đã chứng minh được tính hiệu quả và độ tin cậy của mình trong việc bảo vệ hệ thống mạng.

Đề tài “Xây dựng hệ thống giám sát mạng với Snort” nhằm mục đích nghiên cứu và triển khai một hệ thống giám sát mạng dựa trên Snort, giúp phát hiện kịp thời các hành vi xâm nhập và bảo vệ an ninh cho hệ thống mạng. Trong quá trình thực hiện đề tài, em đã tiến hành nghiên cứu các khái niệm cơ bản về an ninh mạng, phân tích chức năng và cách sử dụng của Snort, cũng như triển khai mô hình giám sát trên môi trường thực tế.

Em hy vọng rằng đề tài này sẽ góp phần cung cấp thêm kiến thức và giải pháp thực tiễn cho việc bảo vệ an ninh mạng, đồng thời mở ra những hướng nghiên cứu và ứng dụng mới trong lĩnh vực này.

## CHƯƠNG 1: GIỚI THIỆU

### 1.1 Bối cảnh chọn đề tài

Trong thời đại công nghệ thông tin phát triển nhanh chóng, các hệ thống mạng ngày càng trở nên phức tạp và dễ bị tấn công hơn. Các cuộc tấn công mạng không chỉ gây thiệt hại về tài chính mà còn ảnh hưởng đến uy tín và hoạt động của tổ chức. Việc phát hiện và ngăn chặn kịp thời các hành vi xâm nhập là một trong những nhiệm vụ quan trọng hàng đầu trong bảo mật thông tin. Snort, một công cụ mã nguồn mở mạnh mẽ, đã chứng tỏ khả năng hiệu quả trong việc phát hiện và ngăn chặn các cuộc tấn công mạng. Chính vì vậy, chúng em quyết định chọn đề tài " Xây dựng hệ thống giám sát mạng với Snort " để nghiên cứu và triển khai hệ thống giám sát mạng nhằm nâng cao an ninh cho các hệ thống thông tin.

### 1.2 Mục tiêu đề tài

Đề tài này hướng tới các mục tiêu sau:

- Tìm hiểu và phân tích các chức năng của Snort.
- Tìm hiểu tổng quan về hệ thống phát hiện xâm nhập.
- Xây dựng mô hình mạng doanh nghiệp.
- Xây dựng và triển khai một mô hình giám sát mạng sử dụng Snort và Graylog.
- Đánh giá hiệu quả của mô hình thông qua các kịch bản kiểm thử.

### 1.3 Cấu trúc báo cáo

Báo cáo được chia thành các chương như sau:

- **Chương 1: Giới thiệu** - Trình bày bối cảnh, lý do chọn đề tài, mục tiêu nghiên cứu và cấu trúc của báo cáo.
- **Chương 2: Cơ sở lý thuyết** - Cung cấp các kiến thức cơ bản về an ninh mạng, hệ thống phát hiện xâm nhập, giới thiệu về Snort và Graylog.
- **Chương 3: Triển khai và kiểm thử mô hình** - Phân tích yêu cầu hệ thống và thiết kế mô hình giám sát. Cài đặt, cấu hình, triển khai và kiểm thử mô hình giám sát.
- **Chương 4: Kết luận và hướng phát triển** - Tóm tắt kết quả đạt được, những khó khăn và hạn chế, và đề xuất hướng phát triển trong tương lai.

## CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

### 2.1 An ninh mạng và các mối đe dọa

#### 2.1.1 Khái niệm an ninh mạng

An ninh mạng là thực tiễn bảo vệ hệ thống máy tính và mạng khỏi các cuộc tấn công, truy cập trái phép, tổn hại hoặc các mối đe dọa khác nhằm bảo vệ tính toàn vẹn, bí mật và sẵn có của dữ liệu và hệ thống. Điều này bao gồm việc bảo vệ các thiết bị, phần mềm, và thông tin truyền qua mạng khỏi các mối đe dọa như virus, malware, tấn công từ chối dịch vụ (DDoS), và các hành vi gian lận khác [1].

#### 2.1.2 Các loại tấn công phổ biến

- Tấn công từ chối dịch vụ (DoS/DDoS): Tấn công từ chối dịch vụ (DoS/DDoS) nhằm làm tê liệt dịch vụ bằng cách gửi một lượng lớn lưu lượng truy cập đến hệ thống mục tiêu, làm cho hệ thống không thể xử lý các yêu cầu hợp lệ từ người dùng [2].

- Phishing: Phishing là hình thức lừa đảo qua email hoặc các trang web giả mạo nhằm đánh cắp thông tin cá nhân của người dùng, chẳng hạn như mật khẩu và số thẻ tín dụng [3].

- Malware: Malware là phần mềm độc hại như virus, worm, trojan, ransomware, và spyware được thiết kế để gây hại cho hệ thống máy tính, phá hoại dữ liệu hoặc đánh cắp thông tin cá nhân [4].

- SQL Injection: SQL Injection là một phương pháp tấn công trong đó mã SQL độc hại được chèn vào các truy vấn cơ sở dữ liệu, cho phép kẻ tấn công truy cập hoặc thao tác dữ liệu không được phép [5].

- Man-in-the-Middle (MitM): Tấn công Man-in-the-Middle (MitM) xảy ra khi một kẻ tấn công nghe trộm hoặc can thiệp vào giao tiếp giữa hai bên mà không bị phát hiện, nhằm đánh cắp hoặc thao túng thông tin trao đổi [6].

### 2.2 Hệ thống phát hiện xâm nhập (IDS) và ngăn chặn xâm nhập (IPS)

#### 2.2.1 Khái niệm và vai trò của IDS và IPS

- IDS (Intrusion Detection System): Hệ thống phát hiện xâm nhập (IDS) là một hệ thống giám sát mạng hoặc hệ thống để phát hiện các hoạt động độc hại hoặc vi phạm chính sách. IDS phân tích lưu lượng mạng và/hoặc nhật ký hệ thống để xác định các dấu hiệu của hành vi xâm nhập, ghi nhận các sự kiện đáng ngờ và cảnh báo quản trị viên về các mối đe dọa tiềm tàng [7].

- IPS (Intrusion Prevention System): Hệ thống ngăn chặn xâm nhập (IPS) là một hệ thống giám sát mạng hoặc hệ thống có khả năng ngăn chặn các hoạt động độc hại hoặc vi phạm chính sách. IPS không chỉ phát hiện các mối đe dọa như IDS, mà còn thực hiện hành động để ngăn chặn các mối đe dọa này, chẳng hạn như chặn lưu lượng đáng ngờ, hoặc khởi động lại các kết nối mạng [8].

#### 2.2.2 Các phương pháp phát hiện xâm nhập

- **Phát hiện dựa trên chữ ký (Signature-based Detection):** So sánh lưu lượng mạng với các chữ ký của các cuộc tấn công đã biết.

- **Phát hiện dựa trên bất thường (Anomaly-based Detection):** Xác định các hành vi bất thường bằng cách so sánh với hành vi bình thường của hệ thống.

### 2.3 Giới thiệu về Snort

#### 2.3.1 Lịch sử và phát triển của Snort

Snort được phát triển bởi Martin Roesch vào năm 1998 như một công cụ mã nguồn mở để phát hiện xâm nhập mạng (IDS). Ban đầu, Snort được phát triển như một công cụ kiểm tra gói tin đơn giản, nhưng nhanh chóng phát triển thành một hệ thống phát hiện xâm nhập toàn diện nhờ vào sự hỗ trợ mạnh mẽ từ cộng đồng mã nguồn mở và các đóng góp của các nhà phát triển bảo mật trên toàn thế giới.

Năm 2001, Sourcefire, công ty do Roesch sáng lập, đã thương mại hóa Snort bằng cách cung cấp các phiên bản cao cấp của phần mềm và các dịch vụ hỗ trợ chuyên nghiệp. Snort đã trở thành một trong những IDS phổ biến nhất trong ngành bảo mật mạng, được sử dụng rộng rãi trong nhiều tổ chức và doanh nghiệp trên toàn cầu [9], [10].

#### 2.3.2 Chức năng và các thành phần của Snort

##### - Chức năng chính của Snort:

- + Phân tích lưu lượng mạng.
- + Phát hiện các cuộc tấn công dựa trên chữ ký.
- + Phát hiện các bất thường trong lưu lượng mạng.
- + Ghi lại và cảnh báo về các hành vi xâm nhập.

##### - Các thành phần chính của Snort:

- + **Sniffer Mode:** Chế độ “người” gói tin, cho phép Snort đọc và hiển thị lưu lượng mạng.
- + **Packet Logger Mode:** Chế độ ghi gói tin, cho phép Snort ghi lại lưu lượng mạng vào tệp tin.
- + **Network Intrusion Detection Mode:** Chế độ phát hiện xâm nhập mạng, cho phép Snort phân tích lưu lượng mạng và phát hiện các hành vi xâm nhập.

#### 2.3.3 Ưu và nhược điểm của Snort

##### - Ưu điểm:

- + Mã nguồn mở và miễn phí.
- + Cộng đồng hỗ trợ rộng rãi và tài liệu phong phú.
- + Linh hoạt và có thể tùy chỉnh cao.
- + Hỗ trợ nhiều nền tảng hệ điều hành.

##### - Nhược điểm:

- + Yêu cầu cấu hình và quản lý phức tạp.
- + Hiệu suất có thể giảm khi lưu lượng mạng lớn.
- + Dễ bị tấn công từ chối dịch vụ (DoS) nếu không được cấu hình và bảo vệ đúng cách.

## 2.4 Graylog

### 2.4.1 Giới thiệu về Graylog

Graylog là một nền tảng mã nguồn mở mạnh mẽ và linh hoạt dùng để quản lý và phân tích log. Graylog giúp thu thập, phân tích và hiển thị các log từ nhiều nguồn khác nhau, giúp quản trị viên hệ thống phát hiện và giải quyết các vấn đề một cách nhanh chóng và hiệu quả.

### 2.4.2 Chức năng chính của Graylog

- Thu thập log: Graylog có khả năng thu thập log từ nhiều nguồn khác nhau như hệ điều hành, ứng dụng, thiết bị mạng và các công cụ bảo mật.
- Phân tích log: Graylog cung cấp các công cụ mạnh mẽ để phân tích log, bao gồm tìm kiếm, lọc và tạo các báo cáo.
- Hiển thị log: Graylog cung cấp giao diện đồ họa trực quan để hiển thị các log, giúp người dùng dễ dàng theo dõi và phân tích các sự kiện.
- Cảnh báo: Graylog có khả năng thiết lập các cảnh báo dựa trên các điều kiện cụ thể, giúp người dùng phản ứng kịp thời với các sự kiện quan trọng.

### 2.4.3 Các thành phần chính của Graylog

- Graylog Server: Thành phần chính chịu trách nhiệm thu thập, phân tích và lưu trữ log.
- MongoDB: Cơ sở dữ liệu NoSQL được sử dụng để lưu trữ các cấu hình và metadata của Graylog.
- Elasticsearch: Công cụ tìm kiếm và phân tích được sử dụng để lưu trữ và tìm kiếm log.
- Graylog Web Interface: Giao diện người dùng đồ họa cho phép quản trị viên truy cập, tìm kiếm và phân tích log.

### 2.4.4 Tích hợp Snort với Graylog

Việc tích hợp Snort với Graylog giúp tạo ra một hệ thống giám sát mạng hiệu quả, kết hợp khả năng phát hiện xâm nhập của Snort với khả năng quản lý và phân tích log mạnh mẽ của Graylog. Quy trình tích hợp bao gồm các bước sau:

- Cấu hình Snort để gửi log: Trên PfSense, cấu hình Snort để gửi log đến Graylog thông qua giao thức Syslog hoặc trực tiếp qua GELF (Graylog Extended Log Format).
- Cấu hình Graylog để nhận log: Trên máy Windows Server trong mạng DMZ, thiết lập Graylog để nhận và xử lý log từ Snort. Điều này bao gồm việc tạo các input trên Graylog để nhận log và cấu hình các extractor để phân tích và trích xuất thông tin từ log.
- Tạo các dashboard và cảnh báo: Sử dụng Graylog để tạo các dashboard hiển thị log từ Snort và thiết lập các cảnh báo dựa trên các điều kiện cụ thể để giám sát các sự kiện quan trọng.

### 2.4.5 Ưu và nhược điểm của Graylog

#### - Ưu điểm:

- + Mã nguồn mở và miễn phí.

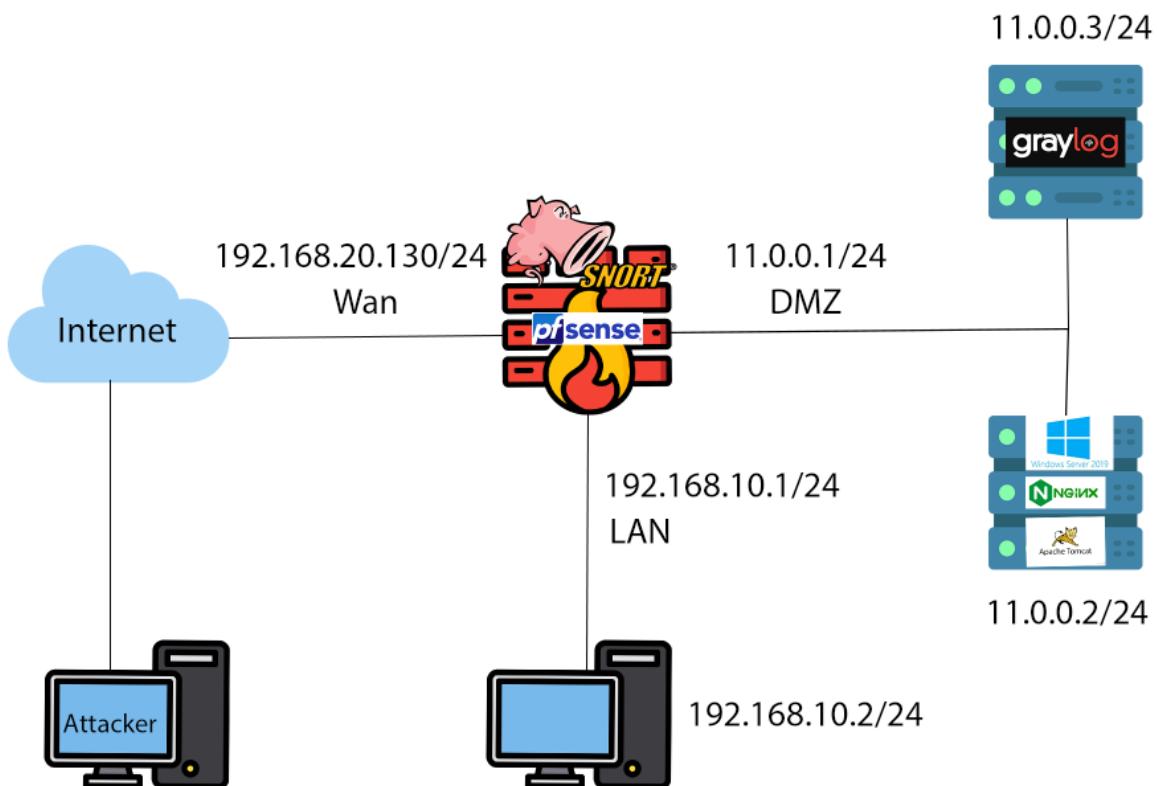
- + Giao diện người dùng thân thiện và dễ sử dụng.
  - + Khả năng mở rộng tốt với Elasticsearch.
  - + Tích hợp tốt với nhiều nguồn log và hệ thống khác nhau.
- Nhược điểm:
- + Yêu cầu kiến thức kỹ thuật để cấu hình và quản lý.
  - + Hiệu suất có thể bị ảnh hưởng khi lượng log lớn.
  - + Cần tài nguyên hệ thống đáng kể để chạy Graylog, MongoDB và Elasticsearch.

## CHƯƠNG 3: TRIỂN KHAI MÔ HÌNH

### 3.1 Giới thiệu

Trong chương này, chúng ta sẽ đi vào chi tiết phân tích và thiết kế mô hình giám sát mạng với Snort. Mô hình này được triển khai trong một môi trường giả lập doanh nghiệp, bao gồm một máy firewall pfSense tích hợp Snort, một mạng LAN với một máy Windows 10, một mạng DMZ với một máy Windows Server 2019 được cấu hình với nhiều dịch vụ doanh nghiệp quan trọng và một máy Ubuntu cài Graylog.

### 3.2 Mô hình hệ thống



*Hình 3.1 - Mô hình hệ thống*

Mô hình hệ thống được trình bày như ở Hình 3.1 bao gồm các thành phần chính sau:

- **PfSense Firewall:** Được tích hợp với Snort để giám sát và phát hiện các hành vi xâm nhập mạng. Firewall này sẽ đóng vai trò bảo vệ và phân tách các mạng LAN và DMZ.
- **Mạng LAN:** Bao gồm một máy tính Windows 10, đại diện cho các máy trạm người dùng trong mạng doanh nghiệp.
- **Mạng DMZ:** Bao gồm Máy Graylog có chức năng thu thập log từ các nguồn như firewall pfSense và nginx, và một máy Windows Server 2019, được cấu hình với các dịch vụ sau:
  - + Active Directory (AD): Quản lý người dùng và quyền truy cập.
  - + DHCP: Cấp phát địa chỉ IP động cho các thiết bị trong mạng.
  - + DNS: Hệ thống phân giải tên miền.

- + LDAP: Dịch vụ thư mục nhẹ để quản lý thông tin người dùng và tài nguyên mạng.
- + OpenVPN: Thiết lập kết nối VPN bảo mật.
- + Tomcat: Máy chủ web ứng dụng để triển khai các ứng dụng web.
- + Nginx: Có chức năng reverse tcp tạo load balancer mô phỏng cho máy chủ web Tomcat.

### 3.3 Thiết kế chi tiết các thành phần

#### 3.3.1 PfSense với Snort

##### - Cấu hình pfSense:

- + Thiết lập các luật firewall để kiểm soát lưu lượng truy cập giữa mạng LAN và DMZ, và từ Internet vào DMZ.
- + Tích hợp Snort vào pfSense để giám sát và phân tích lưu lượng mạng, thiết lập các luật phát hiện xâm nhập.

##### - Cấu hình Snort:

- + Thiết lập Snort để giám sát các giao diện mạng trên pfSense.
- + Cấu hình các luật phát hiện dựa trên chữ ký và bất thường.
- + Cấu hình Snort để gửi log đến Graylog thông qua giao thức Syslog hoặc GELF.

#### 3.3.2 Mạng LAN

##### - Windows 10:

- + Cấu hình máy Windows 10 để kết nối và nhận địa chỉ IP từ máy chủ DHCP trong DMZ.
- + Thiết lập các ứng dụng và dịch vụ để mô phỏng hoạt động của người dùng trong mạng doanh nghiệp.

#### 3.3.3 Mạng DMZ

##### - Windows Server 2019:

- + Active Directory: Cài đặt và cấu hình Active Directory để quản lý người dùng và quyền truy cập.
- + DHCP: Cấu hình dịch vụ DHCP để cấp phát địa chỉ IP cho các thiết bị trong mạng LAN và DMZ.
- + DNS: Cài đặt và cấu hình dịch vụ DNS để phân giải tên miền nội bộ.
- + LDAP: Cài đặt dịch vụ LDAP để quản lý thông tin người dùng và tài nguyên mạng.
- + OpenVPN: Cài đặt và cấu hình OpenVPN để thiết lập kết nối VPN bảo mật cho người dùng từ xa.
- + Tomcat: Cài đặt và cấu hình máy chủ web Tomcat để triển khai các ứng dụng web.

##### - Ubuntu 22.04:

- + Cài đặt Graylog trên máy Ubuntu 22.04 trong mạng DMZ.
- + Cài đặt MongoDB và Elasticsearch làm cơ sở dữ liệu cho Graylog.
- + Thiết lập các input để nhận log từ Snort, nginx.
- + Cấu hình các alert để tạo cảnh báo dựa trên các điều kiện cụ thể.

### 3.4 Xây dựng mô hình mạng doanh nghiệp

#### 3.4.1 Thông số máy ảo

Dưới đây là thông số của các máy ảo sẽ được cài đặt:

	Memory	Processors	Hard Disk	Network Adapter
Firewall Pfsense	512 MB	2	30 GB	1: NAT 2: LAN Segment(lan) 3: LAN Segment(dmz)
Windows Server 2019	4 GB	4	40 GB	1: LAN Segment(dmz)
Windows 10	4 GB	4	40 GB	1: LAN Segment(lan)
Ubuntu (Graylog)	4 GB	4	40 GB	1: LAN Segment(dmz)

Bảng 3.1 – Bảng thông số các máy ảo

#### 3.4.2. Cấu hình phần mềm

- Cấu hình cổng LAN cho firewall Pfsense:

Enter an option: 2

Available interfaces:

```
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static, dhcp6)
```

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

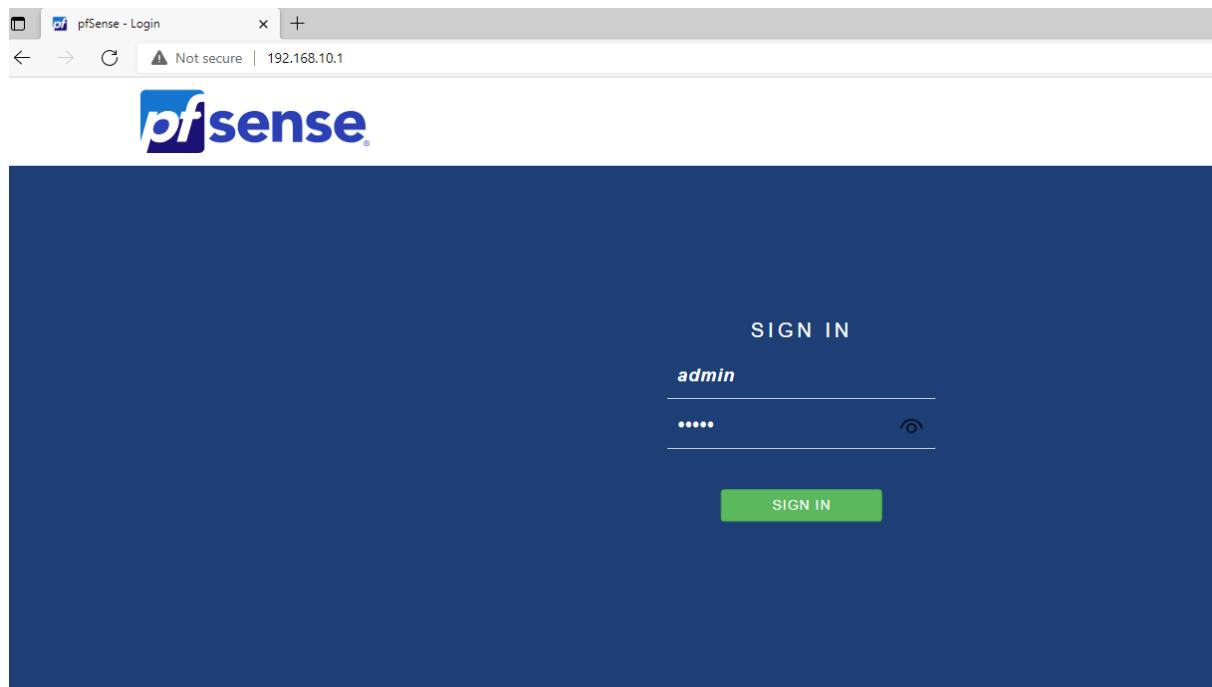
Enter the new LAN IPv4 address. Press <ENTER> for none:  
> 192.168.10.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.  
e.g. 255.255.255.0 = 24  
255.255.0.0 = 16  
255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):  
> 24

*Hình 3.2 - Cấu hình Web interface trên cổng LAN*

- Đăng nhập vào giao diện web của pfsense để tiếp tục cấu hình với tài khoản mặc định là “admin”, mật khẩu là “pfsense”.

*Hình 3.3 - Giao diện web mặc định của pfsense*

- Cài các cấu hình ban đầu cho Pfsense:

General Information	
On this screen the general pfSense parameters will be set.	
<b>Hostname</b>	<input type="text" value="pfSense"/> Name of the firewall host, without domain part. Examples: pfsense, firewall, edgefw
<b>Domain</b>	<input type="text" value="pfSense.com"/> Domain name for the firewall. Examples: home.arpa, example.com Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used in Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Quic	
<b>Primary DNS Server</b>	<input type="text" value="8.8.8.8"/>
<b>Secondary DNS Server</b>	<input type="text" value="8.8.4.4"/>
<b>Override DNS</b>	<input checked="" type="checkbox"/> Allow DNS servers to be overridden by DHCP/PPP on WAN

*Hình 3.4 - Cấu hình hostname, domain, dns*

- Đặt lại mật khẩu cho tài khoản admin Pfsense:

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

**Set Admin WebGUI Password**

On this screen the admin password will be set, which is used to access the WebGUI.

Admin Password:

Admin Password AGAIN:

**>> Next**

Hình 3.5 - Đặt mật khẩu admin

- Trên giao diện web của Pfsense, chọn Interface, sau đó chọn Interface Assignments, chọn Add để thêm vùng DMZ:

Interfaces / Interface Assignments

Interface has been deleted.

Interface	Network port
WAN	em0 (00:0c:29:1b:6f:96)
LAN	em1 (00:0c:29:1b:6f:a0) <span style="color: red;">Delete</span>
Available network ports:	em2 (00:0c:29:1b:6f:aa) <span style="color: green; border: 1px solid green; padding: 2px;">+ Add</span>

**Save**

Hình 3.6 - Thêm interface DMZ

**Enable**  **Enable interface**

**Description** DMZ  
Enter a description (name) for the interface here.

**IPv4 Configuration Type** Static IPv4

**IPv6 Configuration Type** None

**MAC Address** XX:XX:XX:XX:XX:XX  
This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xxxx:xxxx:xx or leave blank.

**MTU**   
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

**MSS**   
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

**Speed and Duplex** Default (no preference, typically autoselect)  
Explicitly set speed and duplex mode for this interface.  
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

**Static IPv4 Configuration**

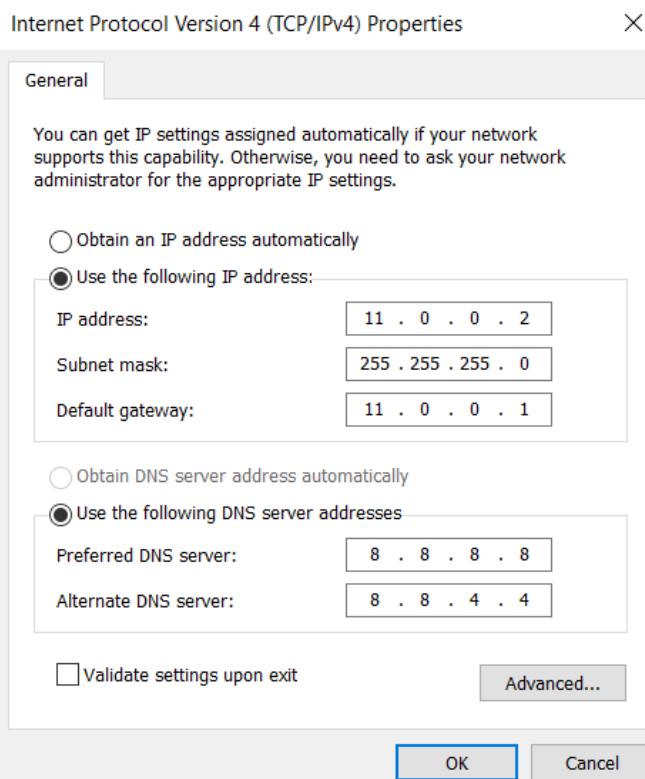
<b>IPv4 Address</b>	11.0.0.1	/ 24
<b>IPv4 Upstream gateway</b>	None	<b>+ Add a new gateway</b>

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.  
On local area network interfaces the upstream gateway should be "none".

*Hình 3.7 - Cấu hình interface DMZ*

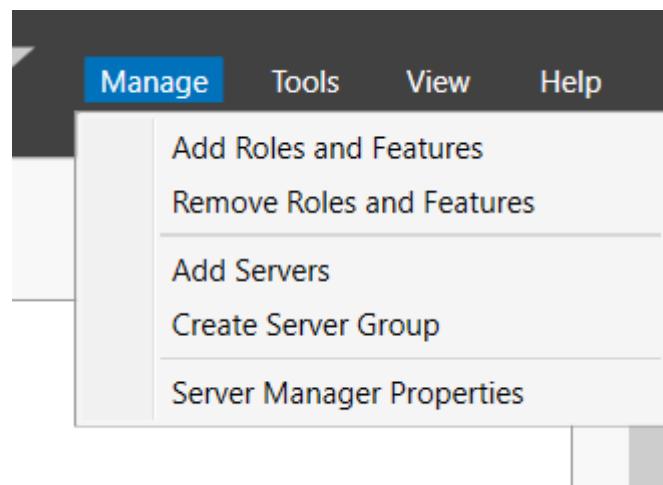
- Cấu hình vùng DMZ:

- Cấu hình IP tĩnh cho máy Windows Server 2019 (DMZ):

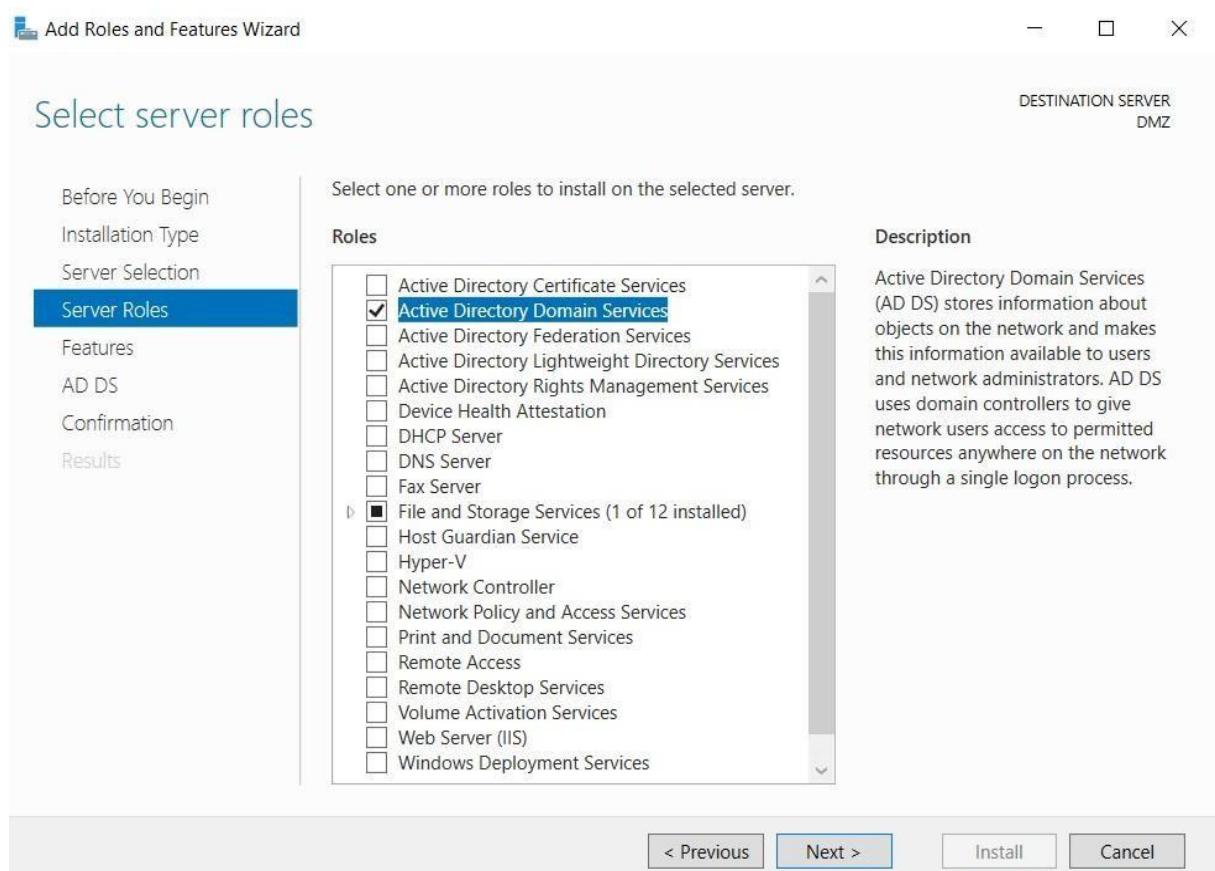
*Hình 3.8 - IP configuration của Windows Server 2019*

- Tiếp theo cấu hình AD-DS trên DMZ:

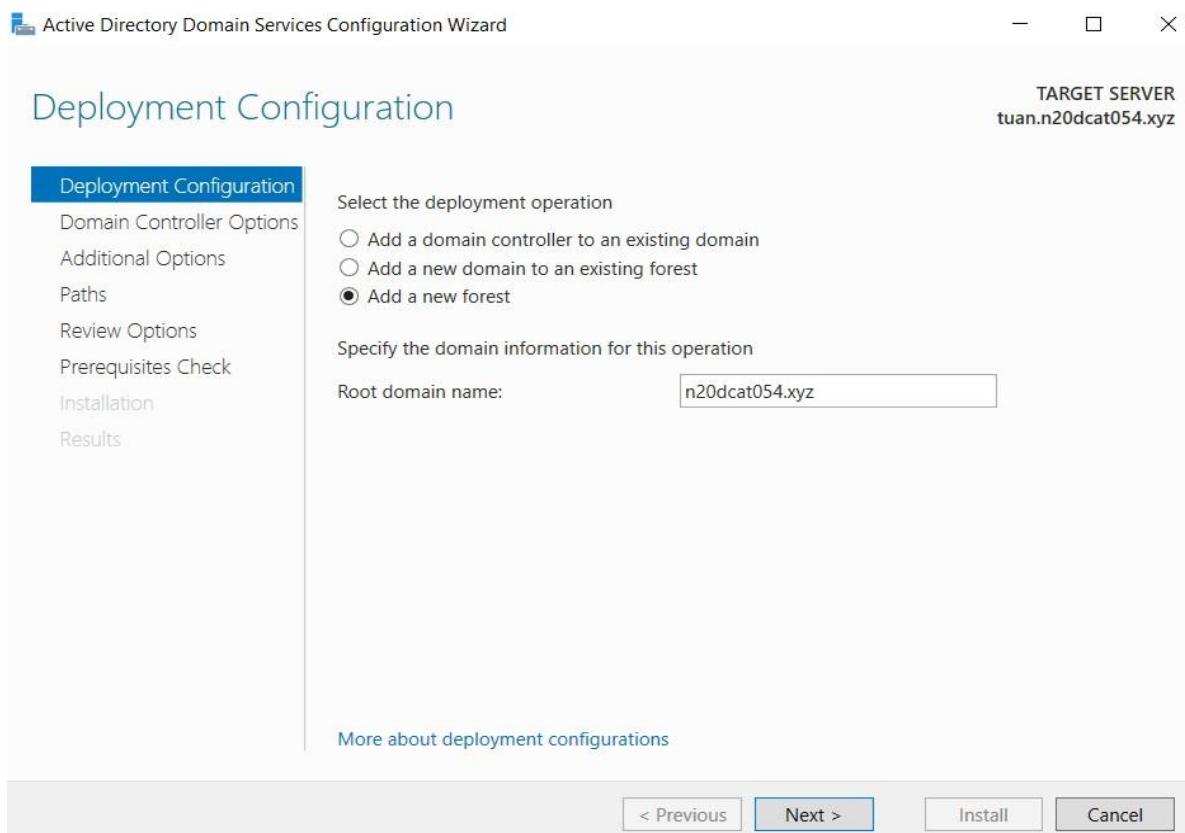
+ Chọn Manage > Add Roles and Features.

*Hình 3.9 - Add roles and features*

+ Chọn Active Directory Domain Services.

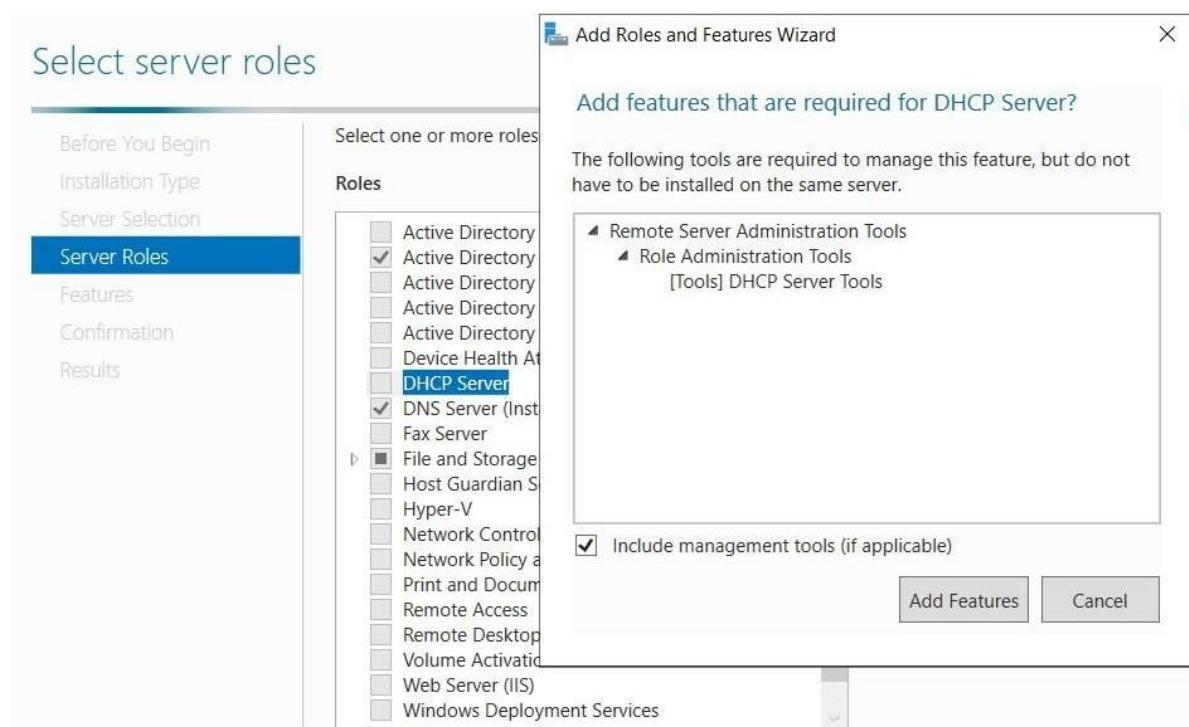
*Hình 3.10 - Active Directory Domain Services*

+ Cấu hình domain.



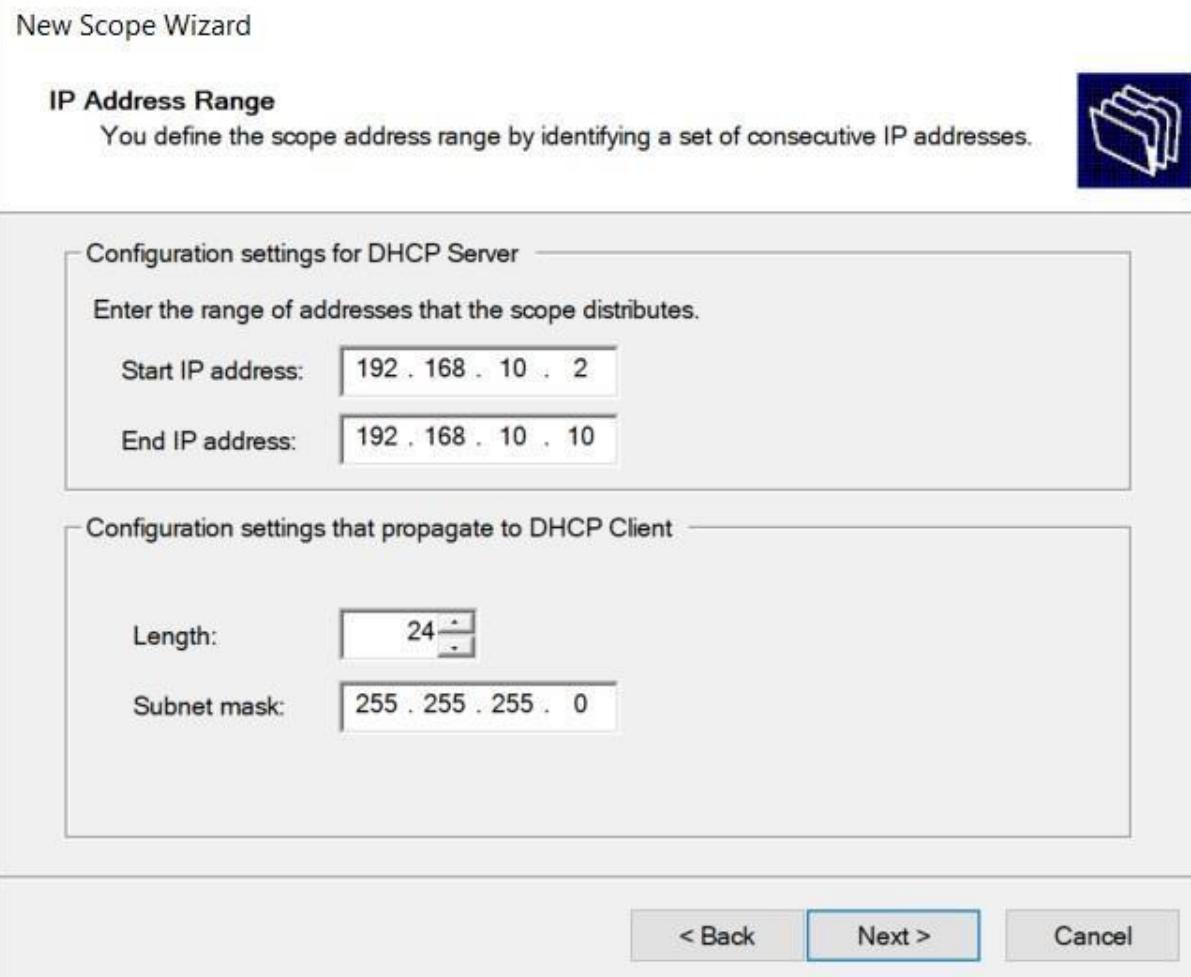
*Hình 3.11 - Tạo Root domain name*

- Cài đặt DHCP server cho window server.



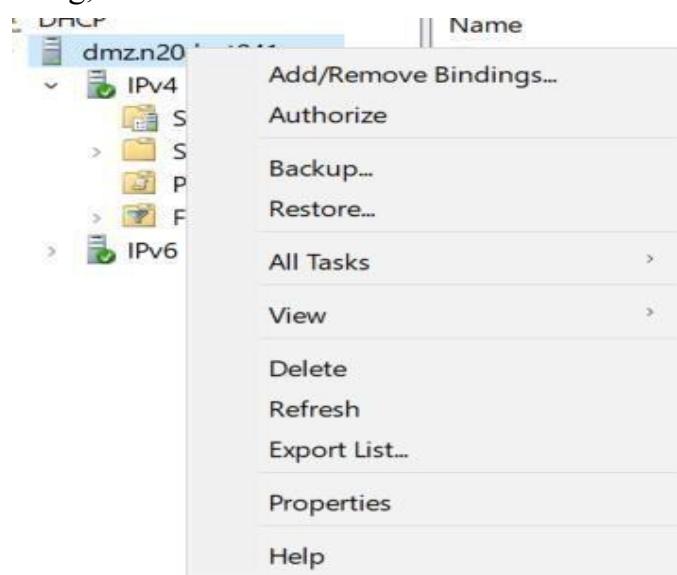
*Hình 3.12 - Thêm DHCP*

- Cấu hình DHCP server trên window server.



Hình 3.13 - Đặt IP range

- Sau khi tạo thành công, Authorize DHCP server.



Hình 3.14 - Authorize DHCP server

- Cấu hình DHCP relay trên pfSense.

The screenshot shows the 'DHCP Relay Configuration' section of the pfSense web interface. Under the 'Enable' heading, there is a checked checkbox for 'Enable DHCP Relay on interface'. Below it, under 'Interface(s)', the 'LAN' interface is selected from a dropdown menu. A note states: 'Interfaces without an IP address will not be shown.' In the 'CARP Status VIP' section, the dropdown is set to 'none'. A note explains: 'Used to determine the HA MASTER/BACKUP status. DHCP Relay will be stopped when the chosen VIP is in status.' There is also an unchecked checkbox for 'Append circuit ID and agent ID to requests', with a note explaining its function. The 'Destination server' field is set to '11.0.0.2'. At the bottom right are two buttons: a blue 'Save' button and a green '+ Add server' button.

Hình 3.15 - Cấu hình DHCP relay

### 3.4.3 Cấu hình NAT

- Trên giao diện web của pfSense, vào Firewall, chọn NAT, Chọn Port Forward, sau đó click Add để thêm cấu hình.

#### - Cấu hình NAT cho cổng LAN:

The screenshot shows the 'Port Forwarding' configuration page in pfSense. It includes fields for 'Interface' (WAN), 'Address Family' (IPv4), 'Protocol' (TCP/UDP), and 'Source' (Display Advanced). Under 'Destination', there are fields for 'Type' (WAN address), 'Address/mask', and 'From port' (HTTP). Under 'Destination port range', there are fields for 'To port' (HTTP) and 'Custom'. The 'Redirect target IP' field is set to 'LAN address' with 'Address' (Custom). The 'Redirect target port' field is set to 'HTTP' with 'Port' (Custom). Notes explain the mapping rules for both IPv4 and IPv6 addresses.

Hình 3.16 - Cấu hình NAT trên port HTTP

- Cấu hình NAT cho DMZ:

The screenshot shows a configuration page for a NAT rule. The fields are as follows:

- Interface:** WAN
- Address Family:** IPv4
- Protocol:** TCP/UDP
- Source:** Display Advanced
- Destination:** WAN address (Type: / /)
- Destination port range:** HTTP (From port: Custom, To port: Custom)
- Redirect target IP:** DMZ address (Type: Address)
- Redirect target port:** HTTP (Port: Custom)

Notes: "Choose which interface this rule applies to. In most cases "WAN" is specified." and "Select the Internet Protocol version this rule applies to."

*Hình 3.17 - Cấu hình NAT trên port HTTP của interface DMZ*

- Cấu hình rule để cho phép DMZ kết nối mạng.

The screenshot shows a configuration page for a firewall rule. The fields are as follows:

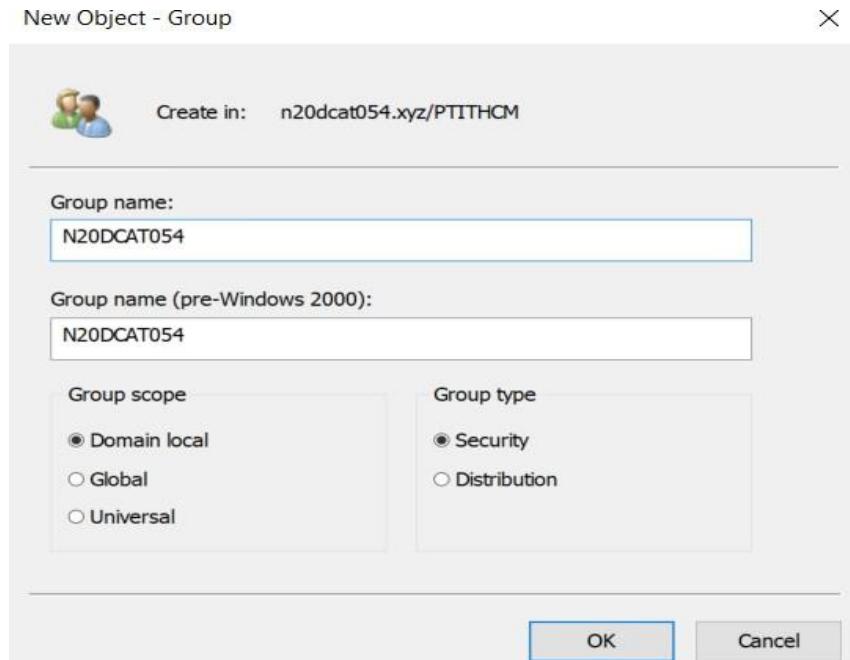
- Action:** Pass
- Disabled:**  Disable this rule
- Interface:** DMZ
- Address Family:** IPv4
- Protocol:** Any
- Source:** Source (Invert match: DMZ net, Source Address: )
- Destination:** Destination (Invert match: any, Destination Address: )

Notes: "Choose what to do with packets that match the criteria specified below.", "Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender whereas with block the packet is dropped silently. In either case, the original packet is discarded.", "Set this option to disable this rule without removing it from the list.", "Choose the interface from which packets must come to match this rule.", "Select the Internet Protocol version this rule applies to.", "Choose which IP protocol this rule should match.", "Choose which interface this rule applies to. In most cases "WAN" is specified.", "Select the Internet Protocol version this rule applies to."

*Hình 3.18 - Rule cho phép kết nối mạng trên DMZ*

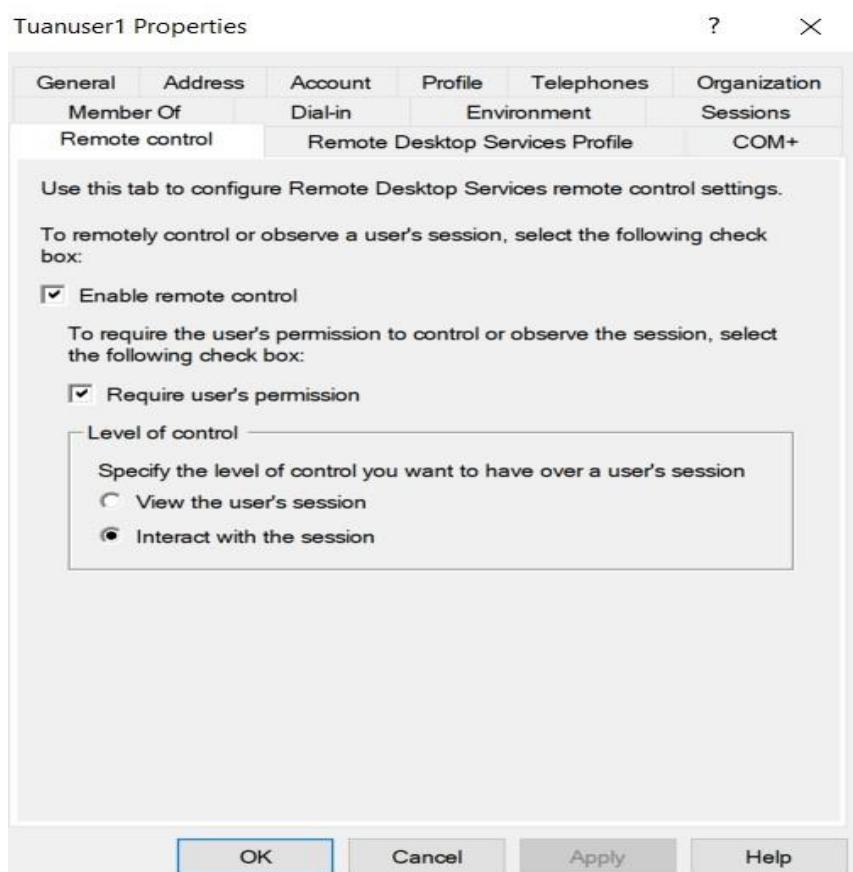
### 3.4.4 Tao user cho LAN

- Join domain cho máy Lan
- Tạo Group user



Hình 3.19 - Tao group

- Enable remote control cho user 1:



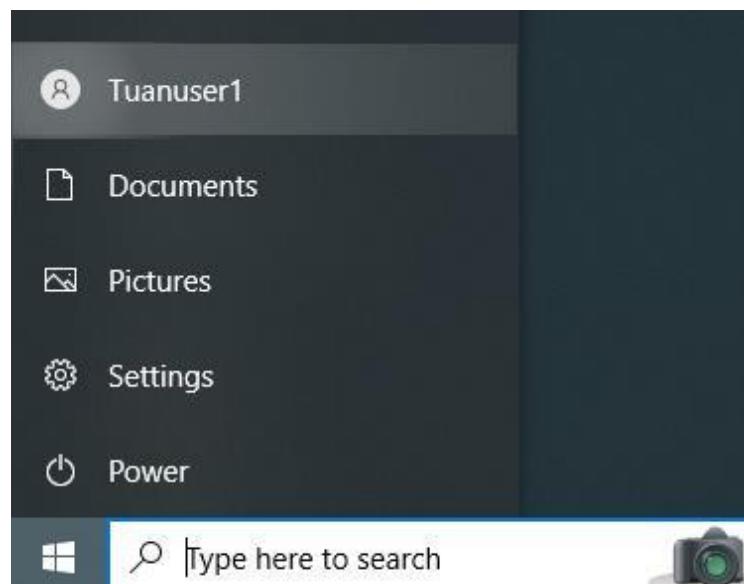
Hình 3.20 - Cho phép remote desktop trên user Tuanuser1

- Login vào win 10 bằng user



Hình 3.21 - Login vào máy windows 10 bằng user Tuanuser1

- Login thành công.



Hình 3.22 - Login user Tuanuser1 thành công

### 3.4.5 Remote từ Lan đến Windows server

#### - Ping từ Lan đến Windows server

```
Microsoft Windows [Version 10.0.19045.2965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Tuanuser11>ping 11.0.0.2

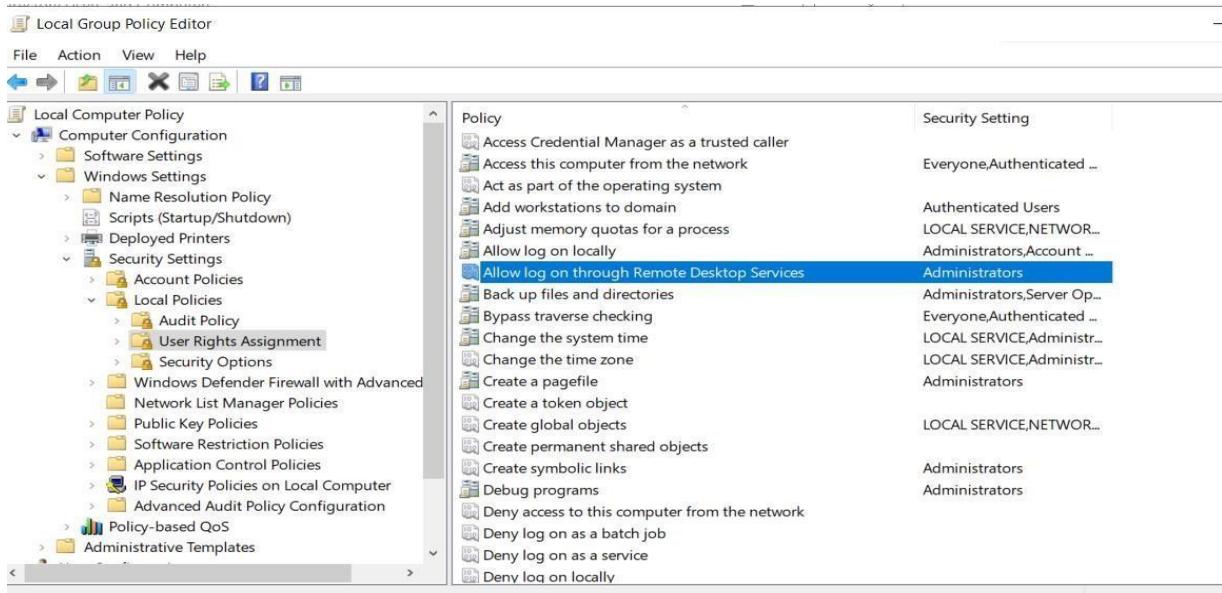
Pinging 11.0.0.2 with 32 bytes of data:
Reply from 11.0.0.2: bytes=32 time=1ms TTL=127

Ping statistics for 11.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Tuanuser11>
```

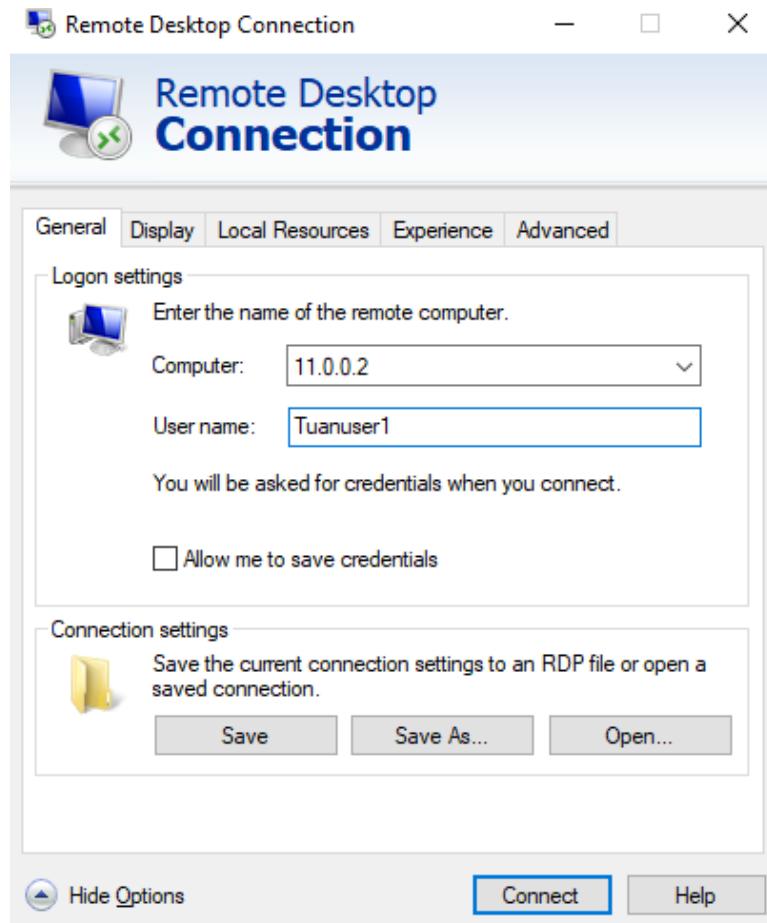
Hình 3.23 - Ping từ máy windows 10 đến windows server 2019

#### - Cho phép remote desktop trên máy Windows server 2019.



Hình 3.24 - Thêm group Remote Desktop Users vào Local Security Setting

- Remote bằng Tuanuser1:



Hình 3.25 - Remote desktop từ máy windows 10

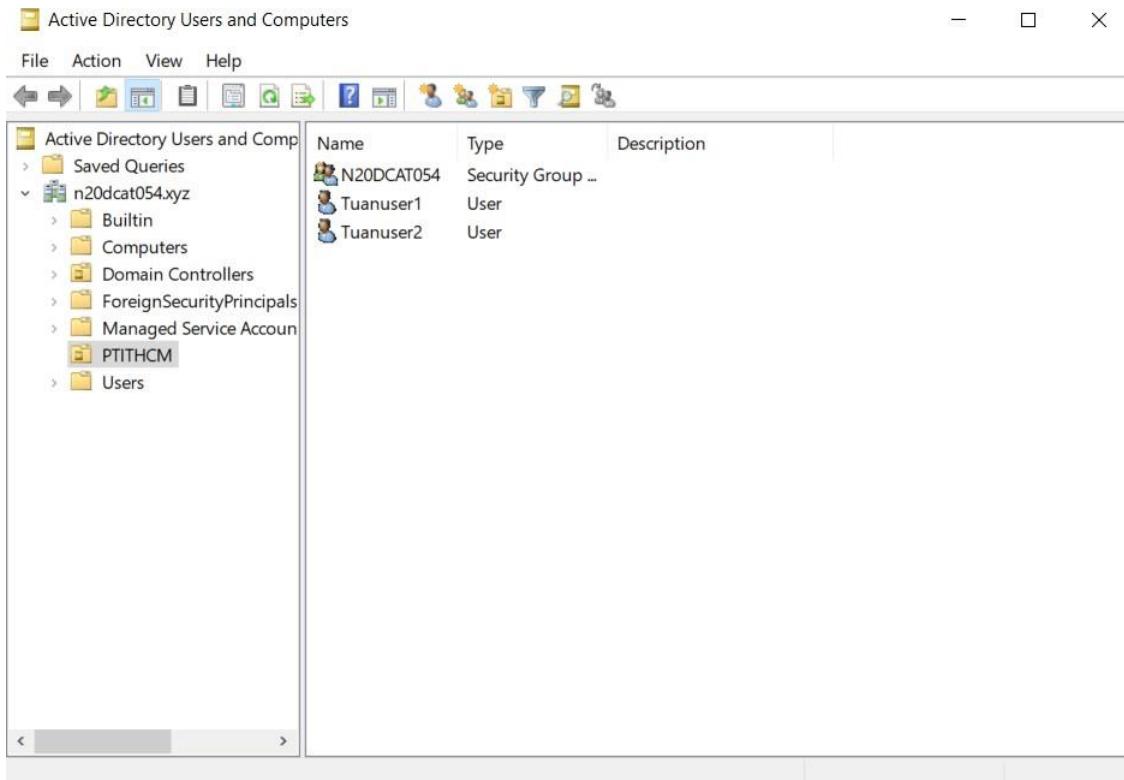
- Remote thành công



Hình 3.26 - Remote thành công

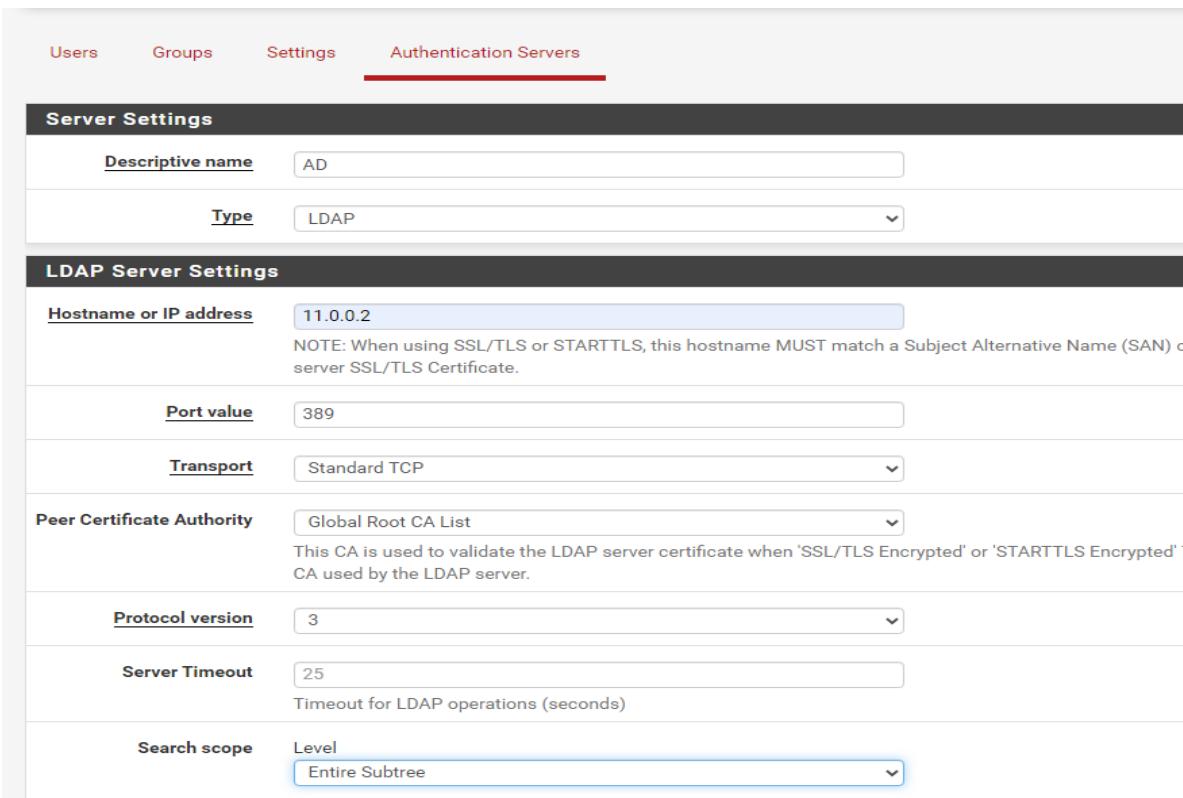
### 3.4.6 OpenVPN và Remote desktop từ máy Internet vào LAN

- Tạo LDAP để liên kết tài khoản windows server với pfsense
- Tạo Organization Unit pfsense trong AD và chuyển 2 tài khoản đã tạo vào unit vừa tạo.



Hình 3.27 - Tạo Organization Unit và thêm group user vừa tạo vào unit đó

- Tạo Authentication Server.

*Hình 3.28 - Cấu hình Authentication Server*

- Sử dụng ADSI để lấy Base DN, Authentication containers, Bind credentials.

Name	Class	Distinguished Name	Actions
CN=Builtin	builtinDomain	CN=Builtin,DC=n20dcat054,DC=xyz	DC=n20dcat05...
CN=Computers	container	CN=Computers,DC=n20dcat054,DC=xyz	More Acti...
OU=Domain Controllers	organization...	OU=Domain Controllers,DC=n20dcat054,DC=xyz	OU=PTITHCM
CN=ForeignSecurityPrincipals	container	CN=ForeignSecurityPrincipals,DC=n20dcat054,DC=xyz	More Acti...
CN=Keys	container	CN=Keys,DC=n20dcat054,DC=xyz	
CN=LostAndFound	lostAndFound	CN=LostAndFound,DC=n20dcat054,DC=xyz	
CN=Managed Service Accounts	container	CN=Managed Service Accounts,DC=n20dcat054,DC=xyz	
CN=NTDS Quotas	msDS-Quota...	CN=NTDS Quotas,DC=n20dcat054,DC=xyz	
CN=Program Data	container	CN=Program Data,DC=n20dcat054,DC=xyz	
<b>OU=PTITHCM</b>	organization...	<b>OU=PTITHCM,DC=n20dcat054,DC=xyz</b>	
CN=System	container	CN=System,DC=n20dcat054,DC=xyz	
CN=TPM Devices	msTPM-Infor...	CN=TPM Devices,DC=n20dcat054,DC=xyz	
CN=Users	container	CN=Users,DC=n20dcat054,DC=xyz	
CN=Infrastructure	infrastructure...	CN=Infrastructure,DC=n20dcat054,DC=xyz	

*Hình 3.29 - Các thông tin của Unit đã tạo*

- Setting User manager.

**System / User Manager / Settings**

Users Groups **Settings** Authentication Servers

**Settings**

**Session timeout**  Time in minutes to expire idle management sessions. The default is 4 hours (240 m risk!

**Authentication Server**

**Password Hash Algorithm**  Selects which algorithm the firewall will use when creating hashes for local user pa The most secure option is currently bcrypt. Some users may prefer SHA-512-based

**Shell Authentication**  Use Authentication Server for Shell Authentication  
If RADIUS or LDAP server is selected it is used for console and SSH authentication. To allow logins with RADIUS credentials, equivalent local users with the expected pi To allow logins with LDAP credentials, Shell Authentication Group DN must be spec

**Auth Refresh Time**  Time in seconds to cache authentication results. The default is 30 seconds, maxim to authentication servers.

**Save** **Save & Test**

*Hình 3.30 - Setting user manager*

### LDAP settings

Test results		
Attempting connection to	11.0.0.2	OK
Attempting bind to	11.0.0.2	OK
Attempting to fetch Organizational Units from	11.0.0.2	OK
Organization units found		
OU=Domain Controllers,DC=N20DCAT041,DC=com		
OU=pfsense,DC=N20DCAT041,DC=com		
CN=Users,DC=N20DCAT041,DC=com		
CN=Users,CN=BuiltIn,DC=N20DCAT041,DC=com		

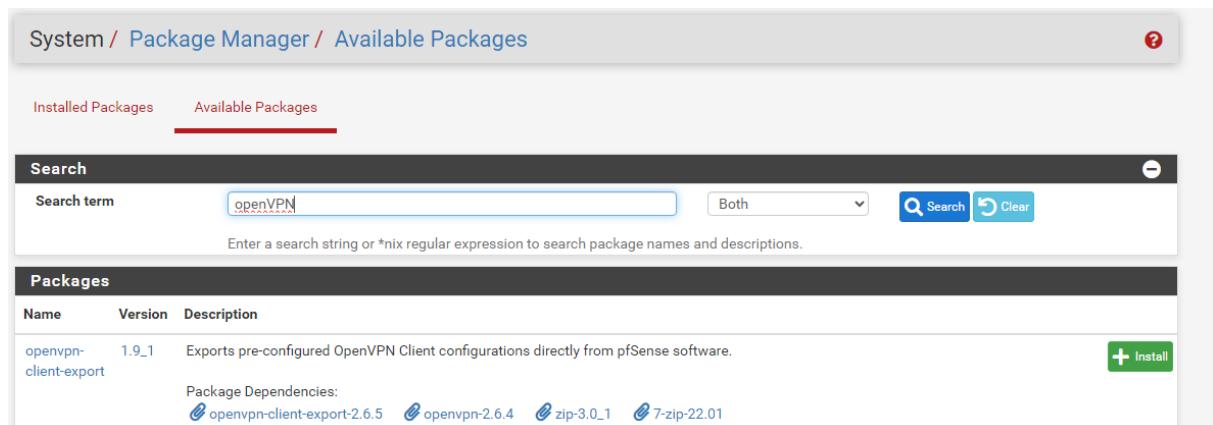
*Hình 3.31 - Thành công tạo Authentication Server*

- Cấu hình OpenVPN:

<b>Descriptive name</b>	CA-VPN	A name for administrative reference, to identify this certificate.
<b>Randomize Serial</b>	<input checked="" type="checkbox"/> Use random serial numbers when signing certificates. When enabled, serial numbers for certificates signed by this CA will be auto sequential values.	
<b>Key length</b>	2048 bit	
Size of the key which will be generated. The larger the key, the more security slightly longer to validate leading to a slight slowdown in setting up new sessions. Most common selection and 4096 is the maximum in common use. For more information, see the RSA Key Size page.		
<b>Lifetime</b>	3650	
Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)		
<b>Common Name</b>		
The internal name of the CA, used as a part of the CA subject. If left blank, the common name will be the descriptive name.		
<b>Country Code</b>	VN	
Two-letter ISO country code (e.g. US, AU, CA)		
<b>State or Province</b>	Ho Chi Minh	
Full State or Province name, not abbreviated (e.g. Texas, Indiana, Ontario).		
<b>City</b>	Thu Duc	
City or other Locality name (e.g. Austin, Indianapolis, Toronto).		
<b>Organization</b>	PTIT	
Organization name, often the company or group name.		
<b>Organizational Unit</b>	PTIT	

Hình 3.32 - Thông tin yêu cầu của OpenVPN

- Cài thêm package OpenVPN client export



Hình 3.33 - Cài thêm package OpenVPN client export

- Vào OpenVPN > Client Export tải phiên bản phù hợp.

OpenVPN Clients

User	Certificate Name	Export
Authentication Only (No Cert)	none	<ul style="list-style-type: none"> <li>- Inline Configurations:</li> <li><a href="#">Most Clients</a></li> <li><a href="#">Android</a></li> <li><a href="#">OpenVPN Connect (iOS/Android)</a></li> </ul> <ul style="list-style-type: none"> <li>- Bundled Configurations:</li> <li><a href="#">Archive</a></li> <li><a href="#">Config File Only</a></li> </ul> <ul style="list-style-type: none"> <li>- Current Windows Installer (2.6.5-ix001):</li> <li><a href="#">64-bit</a></li> <li><a href="#">32-bit</a></li> </ul> <ul style="list-style-type: none"> <li>- Previous Windows Installer (2.5.9-ix601):</li> <li><a href="#">64-bit</a></li> <li><a href="#">32-bit</a></li> </ul> <ul style="list-style-type: none"> <li>- Legacy Windows Installers (2.4.12-ix601):</li> <li><a href="#">10/2016/2019</a></li> <li><a href="#">7/8/8.1/2012/2</a></li> </ul> <ul style="list-style-type: none"> <li>- Viscosity (Mac OS X and Windows):</li> <li><a href="#">Viscosity Bundle</a></li> <li><a href="#">Viscosity Inline Config</a></li> </ul>

Only OpenVPN-compatible user certificates are shown

*Hình 3.34 - Chọn phiên bản Client Export phù hợp*

- Cài đặt trên máy thật và tiến hành kết nối vpn

OpenVPN Connection (pfSense-TCP-1194-config)

Current State: Connecting

Fri Oct 20 17:43:49 2023 OpenVPN 2.6.5 [git:v2.6.5/cbc9e0ce412e7b42] Windows-MSVC [SSL (OpenSSL)] [LZO]

Fri Oct 20 17:43:49 2023 Windows version 10.0 (Windows 10 or greater), amd64 executable

Fri Oct 20 17:43:49 2023 library versions: OpenSSL 3.1.1.30 May 2023 LZO 2.10

Fri Oct 20 17:43:49 2023 pfSense-TCP-1194-config

Username:

Password:

Save password

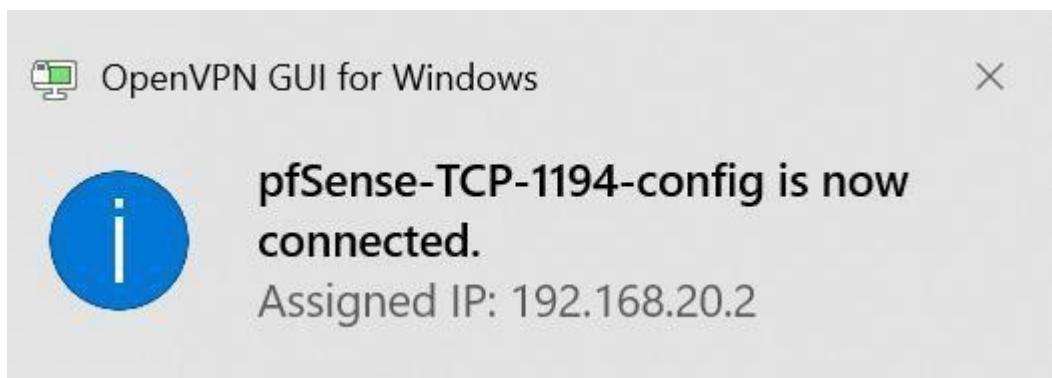
OK Cancel

OpenVPN GUI 11.43.0.0/2.6.5

Disconnect Reconnect Hide

*Hình 3.35 - Kết nối VPN sử dụng máy thật*

- Kết nối thành công.

*Hình 3.36 - Kết nối thành công*

- Ta đã có thể ping tới máy trong Lan

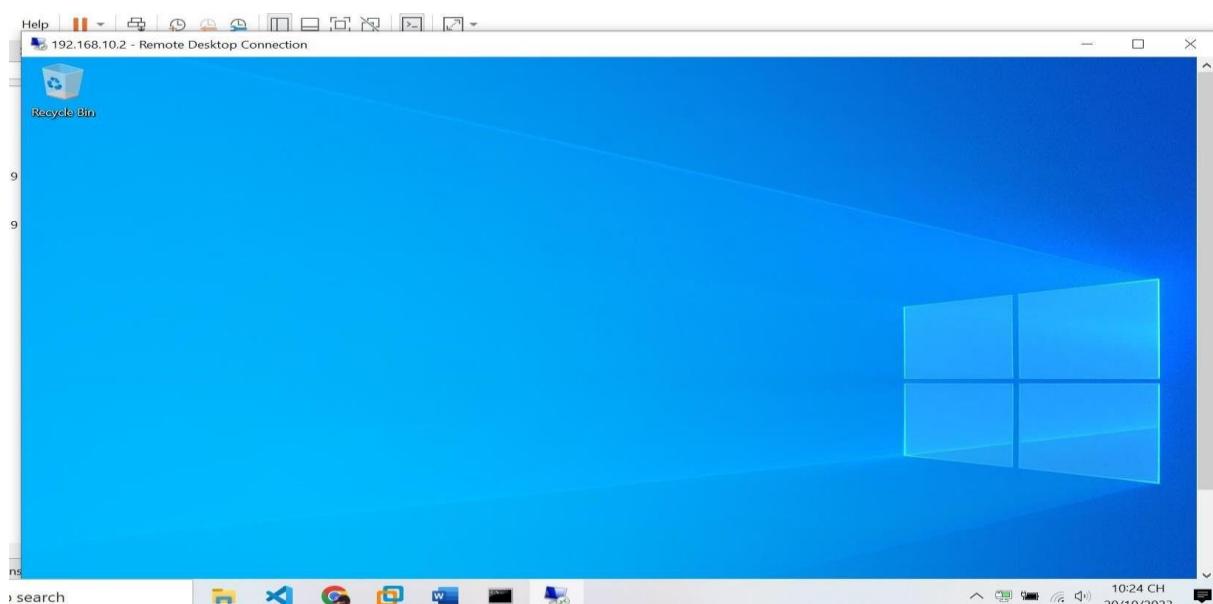
```
C:\Users\DELL>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=1368ms TTL=127
Reply from 192.168.10.2: bytes=32 time=1ms TTL=127
Reply from 192.168.10.2: bytes=32 time=14ms TTL=127
Reply from 192.168.10.2: bytes=32 time=6ms TTL=127

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1368ms, Average = 347ms
```

*Hình 3.37 - Ping tới máy trong LAN từ máy thật*

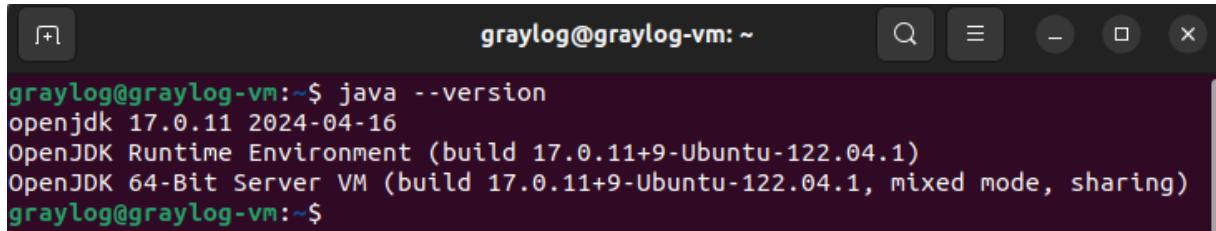
- Remote Desktop thành công.

*Hình 3.38 - Remote Desktop thành công từ máy thật*

### 3.4.7 Cài đặt Graylog

Trước khi cài Graylog, cần phải cài các thành phần phụ thuộc mà Graylog yêu cầu, bao gồm môi trường java, elasticsearch và MongoDB.

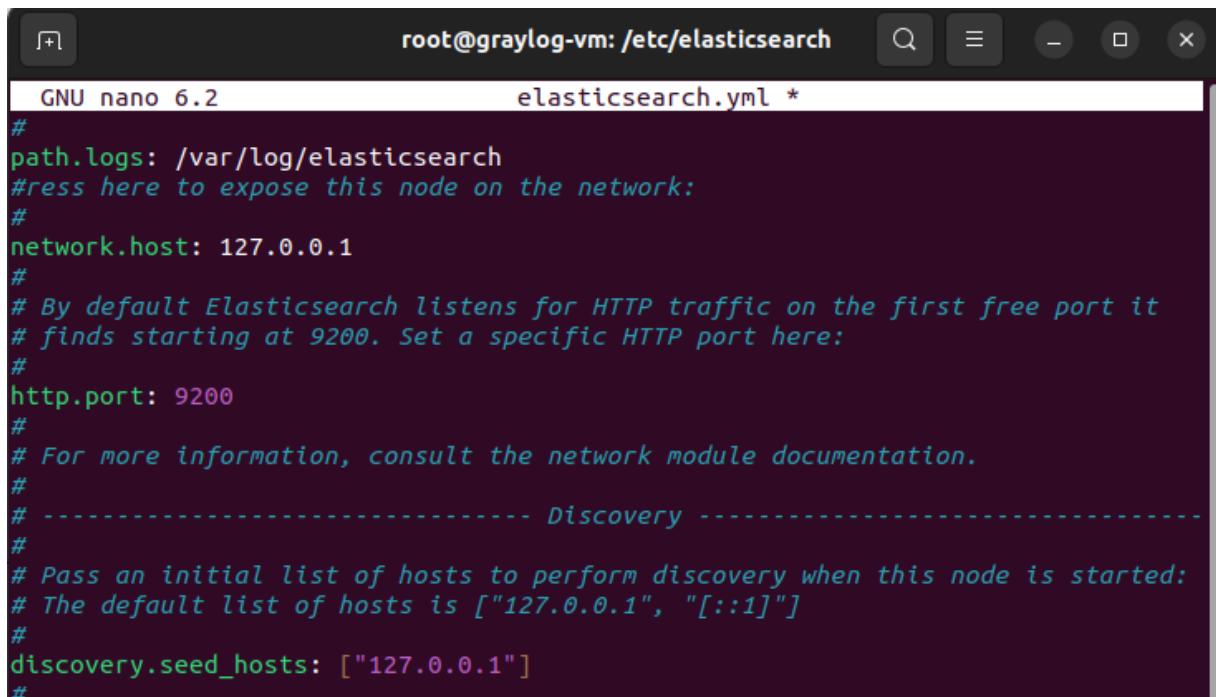
- Cài đặt môi trường java:



```
graylog@graylog-vm:~$ java --version
openjdk 17.0.11 2024-04-16
OpenJDK Runtime Environment (build 17.0.11+9-Ubuntu-122.04.1)
OpenJDK 64-Bit Server VM (build 17.0.11+9-Ubuntu-122.04.1, mixed mode, sharing)
graylog@graylog-vm:~$
```

Hình 3.39 – Cài đặt môi trường java

- Cài đặt elasticsearch, cần cấu hình hợp lý để máy chủ Graylog có thể kết nối đến, cấu hình mẫu như hình 3.40.

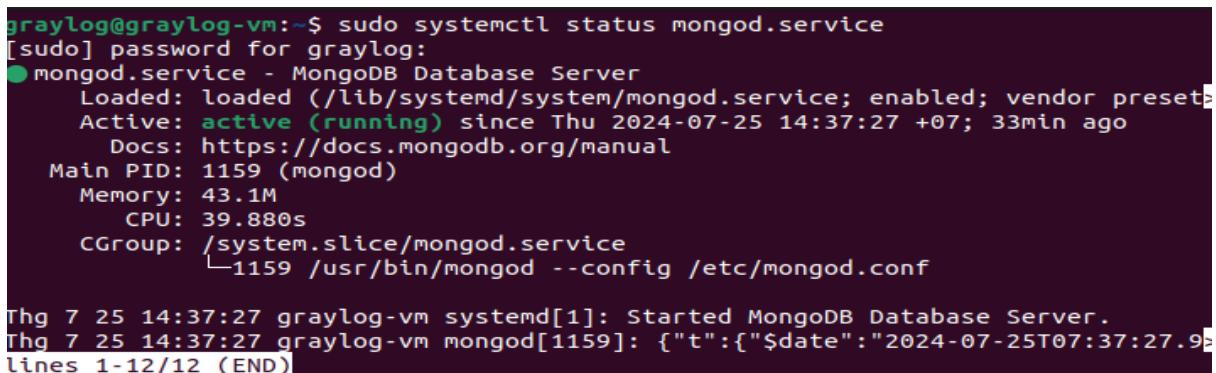


```
root@graylog-vm: /etc/elasticsearch
GNU nano 6.2
elasticsearch.yml *

#
#path.logs: /var/log/elasticsearch
#ress here to expose this node on the network:
#
network.host: 127.0.0.1
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9200
#
# For more information, consult the network module documentation.
#
# ----- Discovery -----
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]
#
discovery.seed_hosts: ["127.0.0.1"]
#
```

Hình 3.40 – Cấu hình Elasticsearch

- Cài đặt MongoDB, đảm bảo rằng MongoDB đã hoạt động.

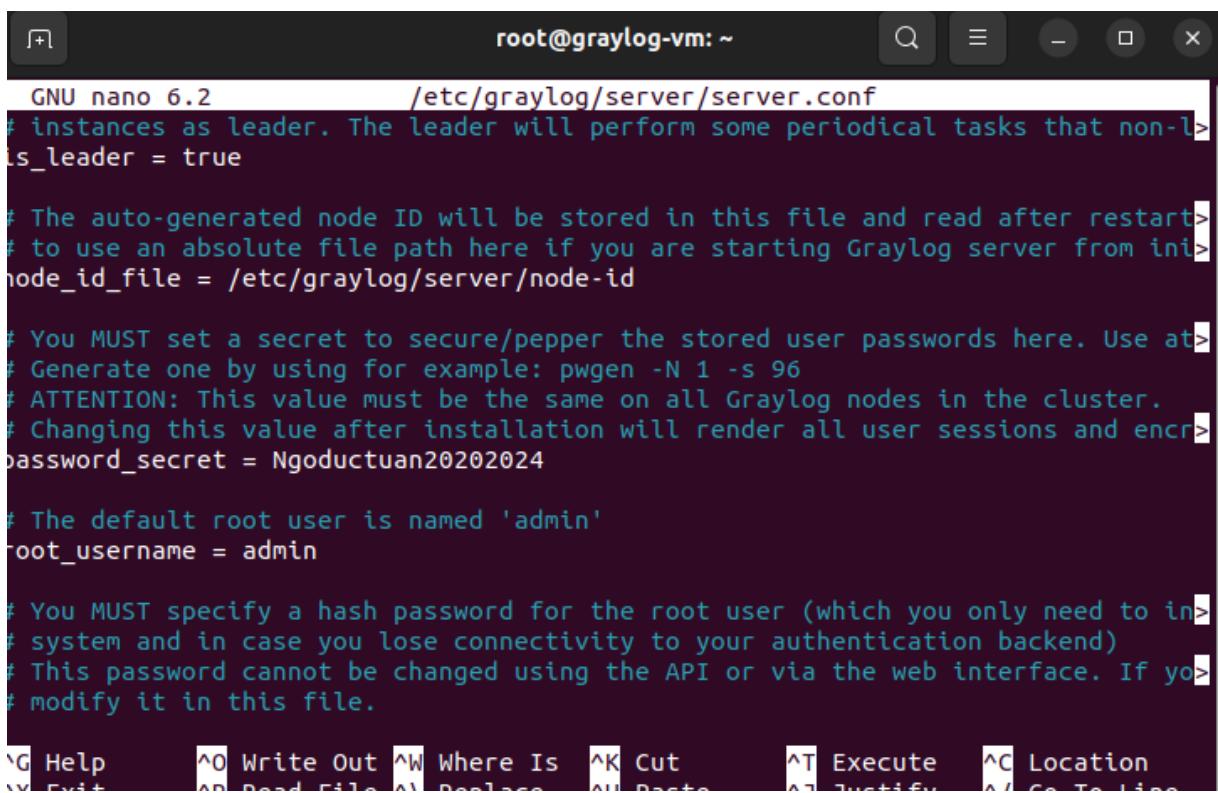


```
graylog@graylog-vm:~$ sudo systemctl status mongod.service
[sudo] password for graylog:
● mongod.service - MongoDB Database Server
   Loaded: loaded (/lib/systemd/system/mongod.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2024-07-25 14:37:27 +07; 33min ago
     Docs: https://docs.mongodb.org/manual
 Main PID: 1159 (mongod)
    Memory: 43.1M
       CPU: 39.880s
      CGROUP: /system.slice/mongod.service
                  └─1159 /usr/bin/mongod --config /etc/mongod.conf

Thg 7 25 14:37:27 graylog-vm systemd[1]: Started MongoDB Database Server.
Thg 7 25 14:37:27 graylog-vm mongod[1159]: {"t":{"$date":"2024-07-25T07:37:27.952Z"}}
lines 1-12/12 (END)
```

Hình 3.41 – Kiểm tra status của MongoDB

Sau khi đã cài đầy đủ các thành phần phụ thuộc, tiến hành cài graylogs, sau đó cấu hình file config của graylog, cấu hình mẫu như hình 3.42.



```

GNU nano 6.2          /etc/graylog/server/server.conf
# instances as leader. The leader will perform some periodical tasks that non-leader = true

# The auto-generated node ID will be stored in this file and read after restart
# to use an absolute file path here if you are starting Graylog server from init
node_id_file = /etc/graylog/server/node-id

# You MUST set a secret to secure/pepper the stored user passwords here. Use at least 96 characters.
# Generate one by using for example: pwgen -N 1 -s 96
# ATTENTION: This value must be the same on all Graylog nodes in the cluster.
# Changing this value after installation will render all user sessions and encrypted log messages unusable.
password_secret = Ngductuan20202024

# The default root user is named 'admin'
root_username = admin

# You MUST specify a hash password for the root user (which you only need to install once)
# system and in case you lose connectivity to your authentication backend
# This password cannot be changed using the API or via the web interface. If you forget it, you will have to
# modify it in this file.

^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File  ^V Replace    ^U Undo      ^J Justify   ^L Go To Line

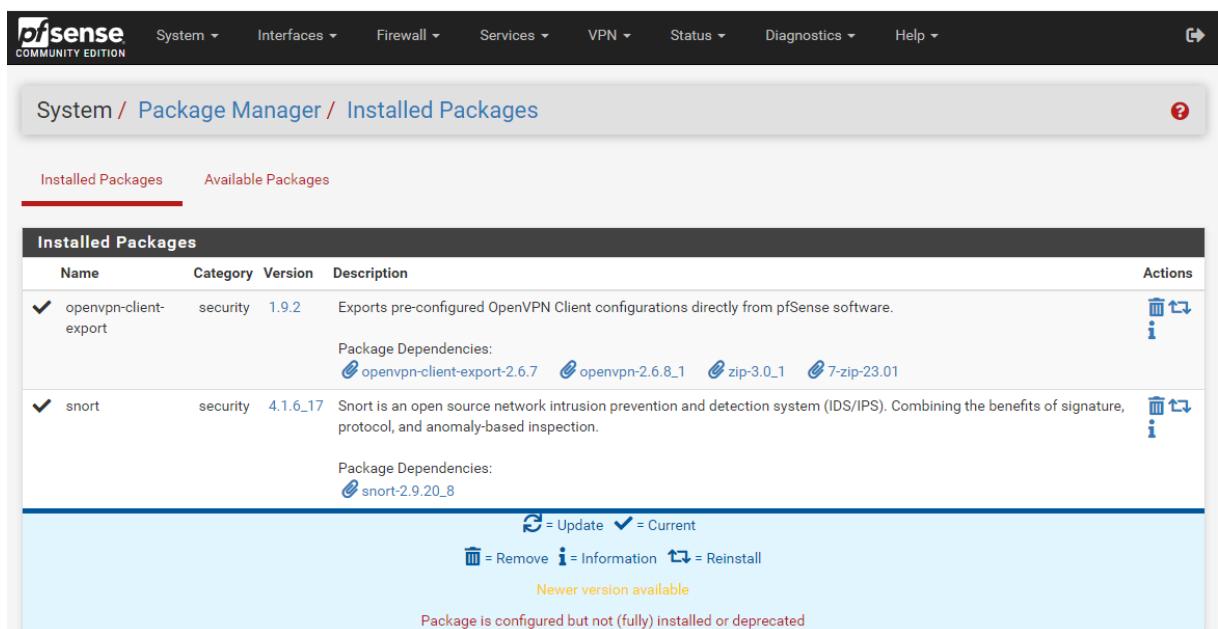
```

Hình 3.42 – Cấu hình Graylog

### 3.5 Cấu hình Snort và gửi log về Graylog trên firewall Pfsense

#### 3.5.1 Cấu hình Snort

Cài đặt Snort từ Package Manager của Pfsense.



Installed Packages				
Name	Category	Version	Description	Actions
✓ openvpn-client-export	security	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software. Package Dependencies: ● openvpn-client-export-2.6.7 ● openvpn-2.6.8.1 ● zip-3.0.1 ● 7-zip-23.01	<span style="color: blue;">Delete</span> <span style="color: blue;">Update</span> <span style="color: blue;">Information</span>
✓ snort	security	4.1.6_17	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. Package Dependencies: ● snort-2.9.20_8	<span style="color: blue;">Delete</span> <span style="color: blue;">Update</span> <span style="color: blue;">Information</span>

S = Update   ✓ = Current  
Delete   Information   Update = Reinstall  
 Never version available  
 Package is configured but not (fully) installed or deprecated

Hình 3.43 – Cài đặt Snort

Trong tab Services, chọn Snort, sau đó vào Global Settings để tiến hành cấu hình tổng thể cho Snort.

The screenshot shows the 'Global Settings' tab selected in the top navigation bar. Under the 'Snort Subscriber Rules' section, there is a checkbox for 'Enable Snort VRT' which is checked, followed by a note: 'Click to enable download of Snort free Registered User or paid Subscriber rules'. Below this are links to 'Sign Up for a free Registered User Rules Account' and 'Sign Up for paid Snort Subscriber Rule Set (by Talos)'. In the 'Snort GPLv2 Community Rules' section, there is another checked checkbox for 'Enable Snort GPLv2' with a similar note. A note below states: 'The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.' Under the 'Emerging Threats (ET) Rules' section, there are two checkboxes: 'Enable ET Open' (checked) and 'Enable ET Pro' (unchecked), each with their respective notes and links to sign up for accounts.

*Hình 3.44 – Cấu hình mẫu của Snort*

Qua tab Updates để cập nhật các rule đã được tích chọn trong lúc cấu hình ở Global Settings.

The screenshot shows the 'Updates' tab selected in the top navigation bar. Under the 'Installed Rule Set MD5 Signature' section, a table lists various rule sets with their MD5 signatures and update dates:

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	9f06b9e4f057a82bb7edfd885c229221	Saturday, 20-Jul-24 16:56:18 +07
Snort GPLv2 Community Rules	773cb91d72dc264e142a2d00d74dc617	Saturday, 20-Jul-24 16:56:18 +07
Emerging Threats Open Rules	ff86a0e1418dc6ef3d03269fcab621	Saturday, 20-Jul-24 16:56:19 +07
Snort OpenAppID Detectors	c726cf937d84c651a20f2ac7c528384e	Saturday, 20-Jul-24 16:56:18 +07
Snort AppID Open Text Rules	2c26cb4f6a3bc03ab9c8e02befcf6fe1	Saturday, 20-Jul-24 16:56:18 +07
Feodo Tracker Botnet C2 IP Rules	2575d915c1694b75df710f0246568696	Monday, 22-Jul-24 00:32:34 +07

Under the 'Update Your Rule Set' section, it shows the last update was on Jul-22 2024 00:34 and the result was 'Success'. There are buttons for 'Update Rules' (with a checkmark) and 'Force Update'. A note below says: 'Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.'

*Hình 3.45 – Update rule Snort*

Tiến hành cấu hình Snort interface để xác định interface mà Snort sẽ kiểm soát, đồng thời chọn loại system log facility, cũng như system log priority để log đổ về Graylog được phân loại cụ thể.

The screenshot shows the configuration interface for a Snort instance. At the top, there are tabs for WAN Settings, WAN Categories, WAN Rules, WAN Variables, WAN Preprocs, WAN IP Rep, and WAN Logs. The WAN Settings tab is active.

**General Settings**

- Enable:**  Enable interface
- Interface:** WAN (em0) - A dropdown menu showing the selected interface.
- Description:** WAN - A text input field for a descriptive name.
- Snap Length:** 1518 - A text input field for the snaplen value in bytes.

**Alert Settings**

- Send Alerts to System Log:**  Snort will send Alerts to the firewall's system log. Default is Not Checked.
- System Log Facility:** LOG\_LOCAL1 - A dropdown menu for the system log facility.
- System Log Priority:** LOG\_ALERT - A dropdown menu for the system log priority.
- Enable Packet Captures:**  Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file.
- Enable Unified2 Logging:**  Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.

*Hình 3.46 – Cấu hình Snort interface*

Thiết lập Categories để xác định các loại rule sẽ được sử dụng bởi Snort. Các rule này là các rule đã được cập nhật từ tab Update.

The screenshot shows the configuration interface for Snort Subscriber IPS Policy Selection. At the top, there are tabs for Snort Interfaces, Global Settings, Updates, Alerts, Blocked, Pass Lists, Suppress, IP Lists, SID Mgmt, Log Mgmt, and Sync. The WAN Categories tab is active.

**Automatic Flowbit Resolution**

- Resolve Flowbits:**  If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.
- Auto-Flowbit Rules:** A button labeled "View". Below it, a note: Disabling auto-flowbit rules is strongly discouraged for security reasons. Auto-enabled flowbit rules that generate unwanted alerts should have their GID:SID added to the Suppression List for the interface instead of being disabled.

**Snort Subscriber IPS Policy Selection**

- Use IPS Policy:**  If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.
- IPS Policy Selection:** Security - A dropdown menu for selecting the policy.

*Hình 3.47 – Chọn các rule sẽ được áp dụng*

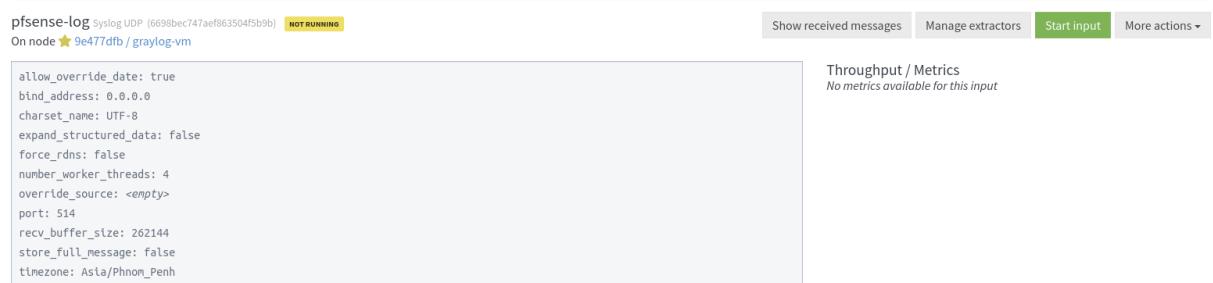
### 3.5.2 Gửi log từ Pfsense về Graylog

Trên giao diện web của Pfsense, vào tab Status, chọn System logs, sau đó chọn Settings, trong Log Message Format chọn “syslog”. Tại mục Remote Logging Options, tích vào Enable Remote Logging, chọn Everything ở Remote Syslogs Contents và lưu lại cấu

hình. Cấu hình này là để cho phép firewall Pfsense gửi toàn bộ log đến máy Graylog.

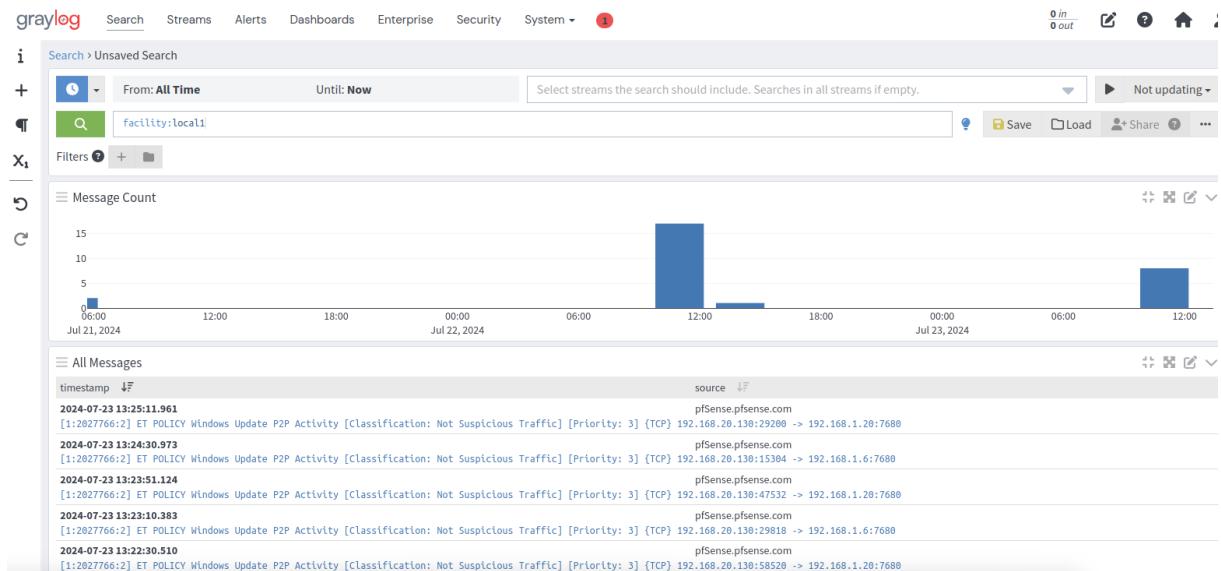
*Hình 3.48 – Cấu hình gửi log từ firewall đến máy Graylog*

Trên máy Ubuntu, truy cập vào giao diện web của Graylog, sau đó vào tab System, chọn Input, ở đây, cài input với dạng log là “Syslog UDP” cho log gửi tới từ firewall theo cấu hình dưới đây.



*Hình 3.49 – Cấu hình input cho log từ firewall*

Sử dụng chức năng “Search” của Graylog để xác minh log từ firewall đã được Graylog tiếp nhận. Với câu search theo “facility=local1”, đã xác nhận được việc nhận log alert của Snort từ firewall.

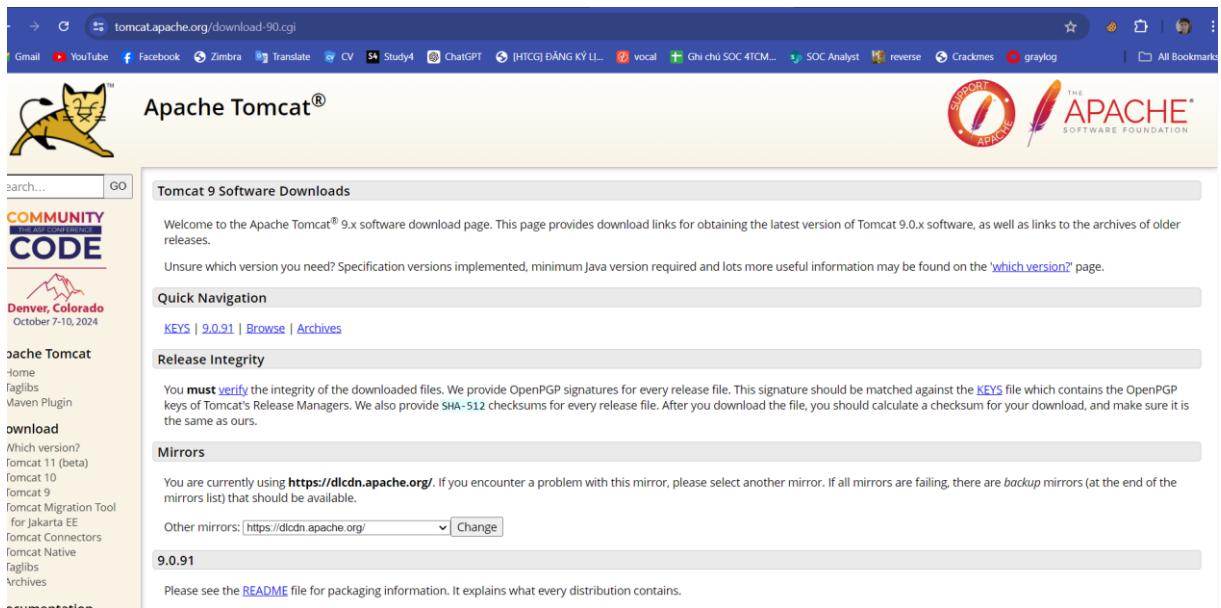
*Hình 3.50 – Log alert của Snort trên firewall*

### 3.6 Cấu hình Web server và Nginx, gửi log Nginx về Graylog

Cấu hình này phù hợp trong trường hợp kẻ tấn công vượt qua được firewall, lúc này các log tại Nginx sẽ đóng vai trò điều tra các sự cố xảy ra.

#### 3.6.1 Cài đặt Apache Tomcat và Nginx

Tiến hành tải và cài đặt Tomcat 9 từ trang chủ của tomcat

*Hình 3.51 – Website chính thức của “Apache Tomcat”*

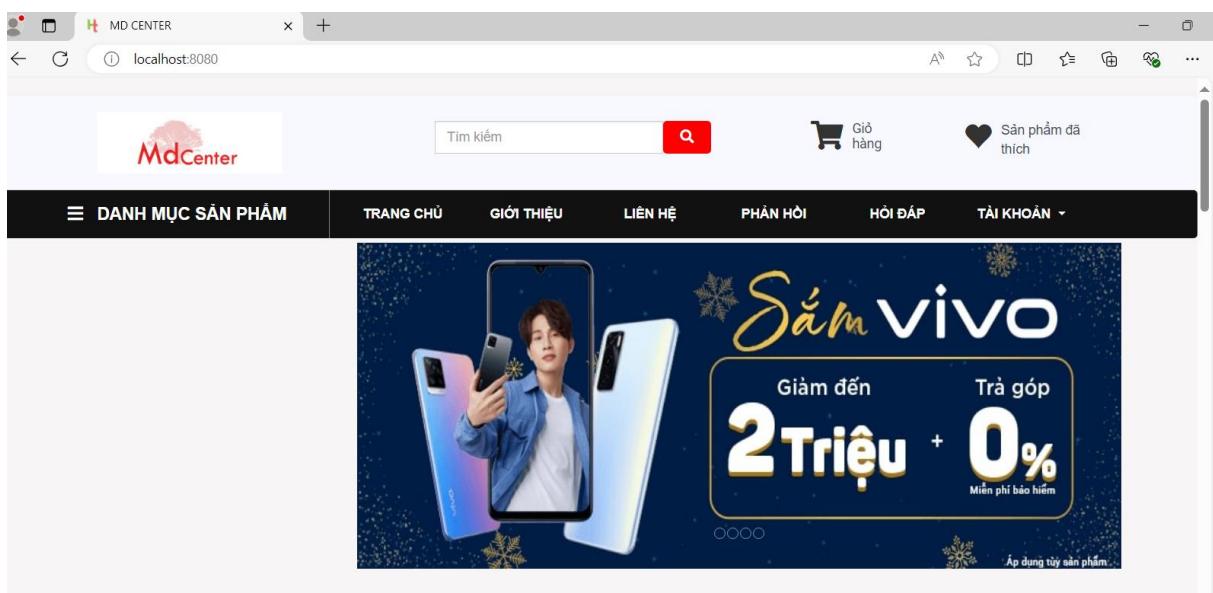
Tiếp theo cài Maven để build artifact từ source code java spring boot. File “.War” sau khi build sẽ đóng vai trò là thành phần xử lý các yêu cầu đến trang web.

```
Select Administrator: C:\Windows\System32\cmd.exe
t 45 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/apache/maven/shared/maven-dependency-tree/3.0.1/maven-dependency-tree-3.0.1.jar
Downloaded from central: https://repo.maven.apache.org/maven2/org/ow2/asm/asm-commons/7.0/asm-commons-7.0.jar (80 kB at 109 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/vafer/jdependency/2.1.1/jdependency-2.1.1.jar
Downloaded from central: https://repo.maven.apache.org/maven2/org/ow2/asm/asm-tree/7.0/asm-tree-7.0.jar (50 kB at 69 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/org/ow2/asm/asm-util/7.0-beta/asm-util-7.0-beta.jar
Downloaded from central: https://repo.maven.apache.org/maven2/org/ow2/asm/asm-util/7.0-beta/asm-util-7.0-beta.jar (81 kB at 101 kB/s)
Downloading from central: https://repo.maven.apache.org/maven2/com/google/guava/guava/19.0/guava-19.0.jar
Downloaded from central: https://repo.maven.apache.org/maven2/org/apache/maven/shared/maven-dependency-tree/3.0.1/maven-dependency-tree-3.0.1.jar (37 kB at 45 kB/s)
Downloaded from central: https://repo.maven.apache.org/maven2/commons-codec/commons-codec/1.13/commons-codec-1.13.jar (344 kB at 424 kB/s)
Downloaded from central: https://repo.maven.apache.org/maven2/org/jdom/jdom2/2.0.6/jdom2-2.0.6.jar (305 kB at 368 kB/s)
Downloaded from central: https://repo.maven.apache.org/maven2/org/vafer/jdependency/2.1.1/jdependency-2.1.1.jar (186 kB at 217 kB/s)
Downloaded from central: https://repo.maven.apache.org/maven2/com/google/guava/guava/19.0/guava-19.0.jar (2.3 MB at 1.7 MB/s)
[INFO] Replacing main artifact with repackaged archive
[INFO] -----
[INFO] BUILD SUCCESS
[INFO] -----
[INFO] Total time: 01:10 min
[INFO] Finished at: 2024-07-23T22:55:39+07:00
[INFO] -----
```

C:\Users\Administrator\Desktop\security-web-selling-phone>

*Hình 3.52 – Build thành công file “.War”*

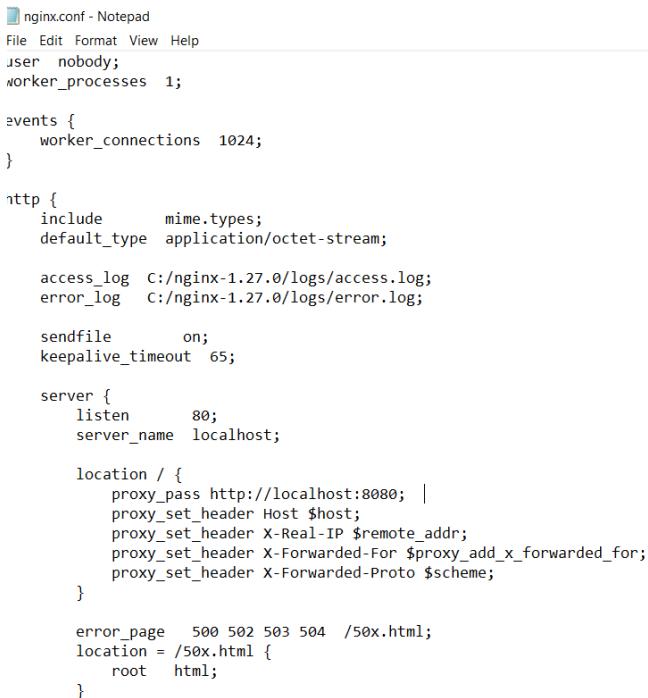
Đổi tên file artifact đã build thành “ROOT.war” và chuyển vào thư mục webapp của tomcat, sau đó restart lại tomcat.

*Hình 3.53 – Kết quả sau khi cài đặt và cấu hình thành công Website*

Chọn phiên bản Nginx phù hợp với máy chủ windows server 2019 và giải nén file tải về để cài đặt Nginx. Nginx đóng vai trò là một reverse proxy giúp phân phối các yêu cầu đến đúng địa chỉ, ở đây là đến Web server Tomcat.

Cấu hình Nginx để có thể chuyển hướng đến Web server và lưu lại access.log, error.log. Ở đây, cần quan tâm đến khóa “server” và khóa “location”, hai khóa này đóng vai trò xác định điểm đích của yêu cầu (location), và địa chỉ mà nó sẽ đại diện cho đích đến đó

(server).



```

nginx.conf - Notepad
File Edit Format View Help
user nobody;
worker_processes 1;

events {
    worker_connections 1024;
}

http {
    include mime.types;
    default_type application/octet-stream;

    access_log C:/nginx-1.27.0/logs/access.log;
    error_log C:/nginx-1.27.0/logs/error.log;

    sendfile on;
    keepalive_timeout 65;

    server {
        listen 80;
        server_name localhost;

        location / {
            proxy_pass http://localhost:8080;
            proxy_set_header Host $host;
            proxy_set_header X-Real-IP $remote_addr;
            proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
            proxy_set_header X-Forwarded-Proto $scheme;
        }

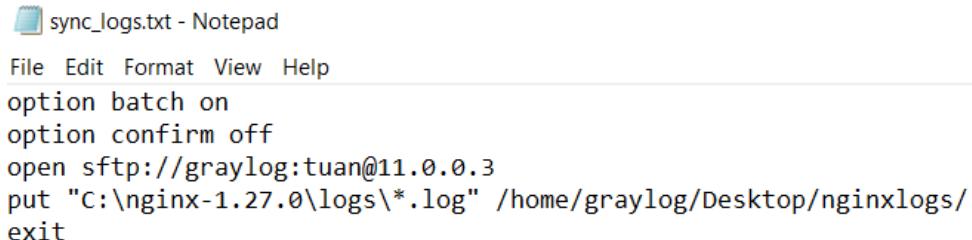
        error_page 500 502 503 504 /50x.html;
        location = /50x.html {
            root html;
        }
    }
}

```

Hình 3.54 – Câu lệnh Nginx

### 3.6.2 Chuyển log nginx đến Graylog

Để chuyển log của nginx đến Graylog, đầu tiên cài WinSCP để có thể chuyển file thông qua ssh sử dụng một file txt làm cấu hình.



```

sync_logs.txt - Notepad
File Edit Format View Help
option batch on
option confirm off
open sftp://graylog:tuan@11.0.0.3
put "C:\nginx-1.27.0\logs\*.log" /home/graylog/Desktop/nginxlogs/
exit

```

Hình 3.55 – Câu lệnh WinSCP

Sau đó tạo một file “.ps1” để thực hiện chạy lệnh gửi log tự động, ở đây tạo điều kiện cho vòng while là true để có thể lặp lại câu lệnh gửi log. Chọn địa chỉ của WinSCP và file cấu hình của nó để có thể chuyển file theo lệnh powershell.



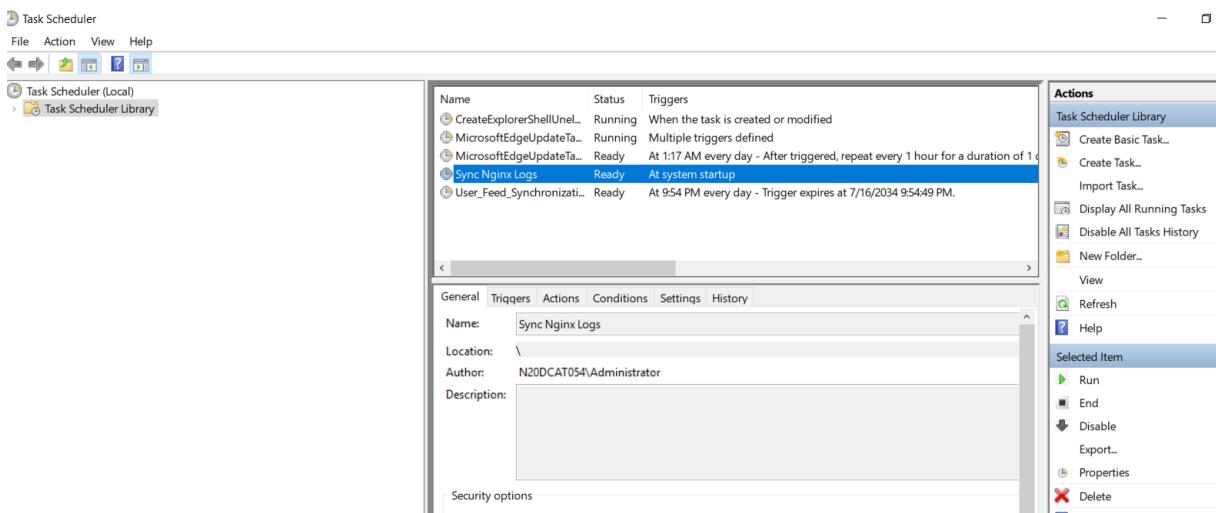
```

sync_logs.ps1 - Notepad
File Edit Format View Help
while ($true) {
    & "C:\Program Files (x86)\WinSCP\WinSCP.com" /script="C:\Users\Administrator\Desktop\sync_logs.txt"
    Start-Sleep -Seconds 5
}

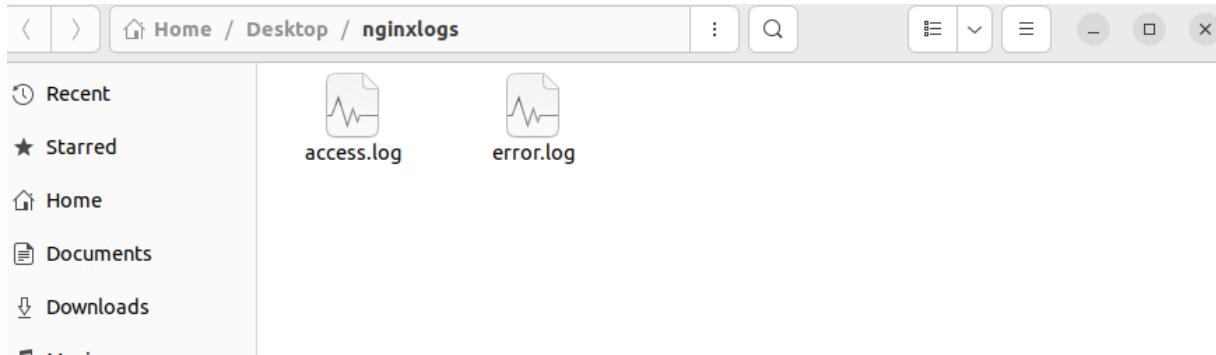
```

*Hình 3.56 – Script Powershell*

Cuối cùng tạo Task Scheduler để thiết lập lịch chạy tập lệnh trong file sync\_logs.ps1

*Hình 3.57 – Cấu hình chạy tự động trên Task Scheduler*

Vào tệp đích trên máy Graylog để xác nhận log đã được chuyển đến thành công.

*Hình 3.58 – Log đã được gửi đến máy Graylog*

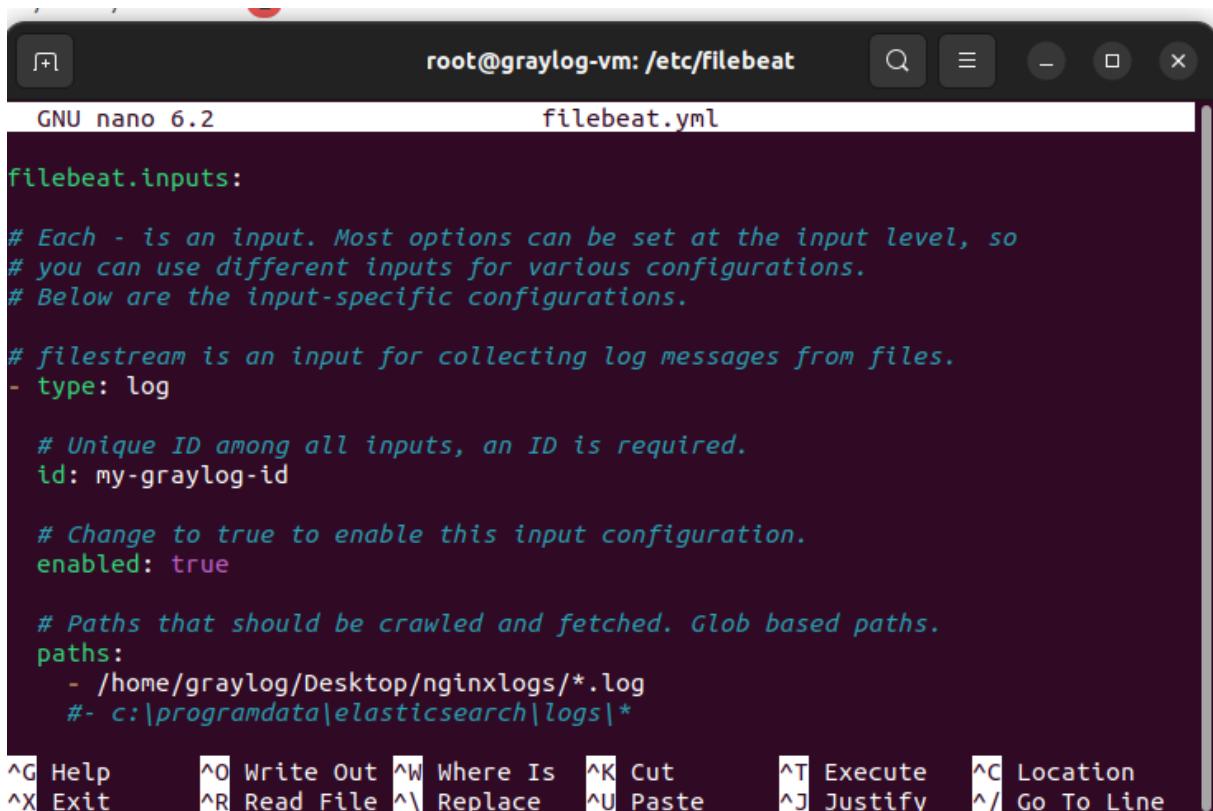
Cấu hình input cho log của nginx với loại log là “Beats”, theo các thông số như hình dưới đây.

```
bind_address: 0.0.0.0
charset_name: UTF-8
decompress_size_limit: 8388608
number_worker_threads: 4
override_source: <empty>
port: 5044
recv_buffer_size: 262144
```

Throughput / Metrics  
No metrics available for this input

*Hình 3.59 – Cấu hình input cho log đến từ Nginx*

Cài đặt và cấu hình filebeat để tải log lên Graylog. Filebeat có chức năng tiếp nhận và đổi sang định dạng mà Graylog có thể tiếp nhận.



```

root@graylog-vm: /etc/filebeat
GNU nano 6.2           filebeat.yml

filebeat.inputs:
  # Each - is an input. Most options can be set at the input level, so
  # you can use different inputs for various configurations.
  # Below are the input-specific configurations.

  # filestream is an input for collecting log messages from files.
  - type: log

    # Unique ID among all inputs, an ID is required.
    id: my-graylog-id

    # Change to true to enable this input configuration.
    enabled: true

    # Paths that should be crawled and fetched. Glob based paths.
    paths:
      - /home/graylog/Desktop/nginxlogs/*.log
      #- c:\programdata\elasticsearch\logs\*

```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location  
 ^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line

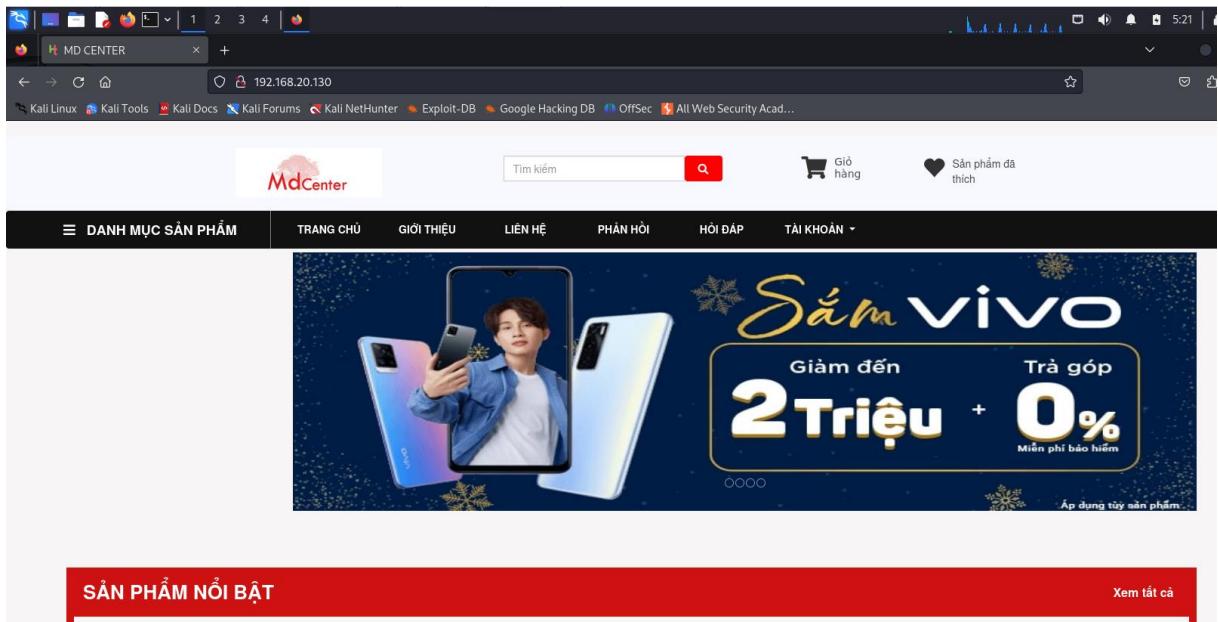
Hình 3.60 – Cấu hình filebeat

### 3.6.2 Cấu hình NAT Port Forward trên firewall pfsense

Cấu hình này giúp cho các IP từ WAN có thể chuyển hướng đến trang web đã được triển khai trên Windows server 2019. Pfsense ở đây sẽ đóng vai trò là người dẫn đường cho các yêu cầu được gửi đến port 80 của nó.

Hình 3.61 – Cấu hình NAT Port Forward

Kiểm tra đã thành công hay chưa bằng cách sử dụng máy kali đang có cùng lớp mạng WAN với firewall để truy cập đến web.



Hình 3.62 – Kiểm tra cấu hình NAT

### 3.7 Cấu hình custom rules

Ngoài các rule có sẵn của Snort, ta cần viết thêm các rule để Snort có thể phát hiện các kiểu tấn công mới và các loại tấn công chưa có trong rule mặc định.

- Rule SQL injection:

- + alert: Đây là hành động Snort sẽ thực hiện khi rule được kích hoạt. Trong trường hợp này, Snort sẽ gửi một cảnh báo.
- + tcp: Rule này áp dụng cho giao thức TCP.
- + any any -> any 80: Rule này áp dụng cho tất cả các địa chỉ nguồn và đích, trên tất cả các cổng nguồn, và cổng đích là 80 (HTTP).
- + msg: "AND SQL Injection Detected": Thông điệp cảnh báo sẽ được ghi lại khi rule này được kích hoạt.
- + content: "and": Rule sẽ tìm kiếm chuỗi "and" trong payload của gói tin.
- + nocase: Tùy chọn này chỉ định rằng việc so sánh chuỗi sẽ không phân biệt chữ hoa chữ thường.
- + sid:100000060: Đây là số định danh duy nhất của rule này.

- Rule Brute Force Attack:

- + alert: Snort sẽ gửi một cảnh báo khi rule này được kích hoạt.
- + tcp: Rule này áp dụng cho giao thức TCP.
- + any any -> any 22: Rule này áp dụng cho tất cả các địa chỉ nguồn và đích, trên tất cả các cổng nguồn, và cổng đích là 22 (SSH).
- + msg: "Possible SSH brute forcing!": Thông điệp cảnh báo sẽ được ghi lại khi

rule này được kích hoạt.

- + flags: S+: Rule này tìm các gói TCP SYN.
- + threshold: type both, track by\_src, count 5, seconds 30: Rule này sẽ kích hoạt nếu có 5 gói SYN từ cùng một nguồn trong vòng 30 giây.
- + sid:10000001: Đây là số định danh duy nhất của rule này.
- + rev: 1: Đây là số phiên bản của rule.

#### - Rule Dos:

- + alert: Snort sẽ gửi một cảnh báo khi rule này được kích hoạt.
- + tcp: Rule này áp dụng cho giao thức TCP.
- + any any -> any any: Rule này áp dụng cho tất cả các địa chỉ và cổng.
- + flags: S: Rule này tìm các gói TCP SYN (chỉ có cờ SYN được bật).
- + msg:"Possible SYN DoS": Thông điệp cảnh báo sẽ được ghi lại khi rule này được kích hoạt.
- + flow: stateless: Rule này áp dụng cho các gói tin không duy trì trạng thái.
- + threshold: type both, track by\_dst, count 1000, seconds 3: Rule này sẽ kích hoạt nếu có 1000 gói SYN trong vòng 3 giây đến cùng một đích.
- + sid:10002: Đây là số định danh duy nhất của rule này.
- + rev:1: Đây là số phiên bản của rule.

The screenshot shows the pfSense Community Edition interface with the following details:

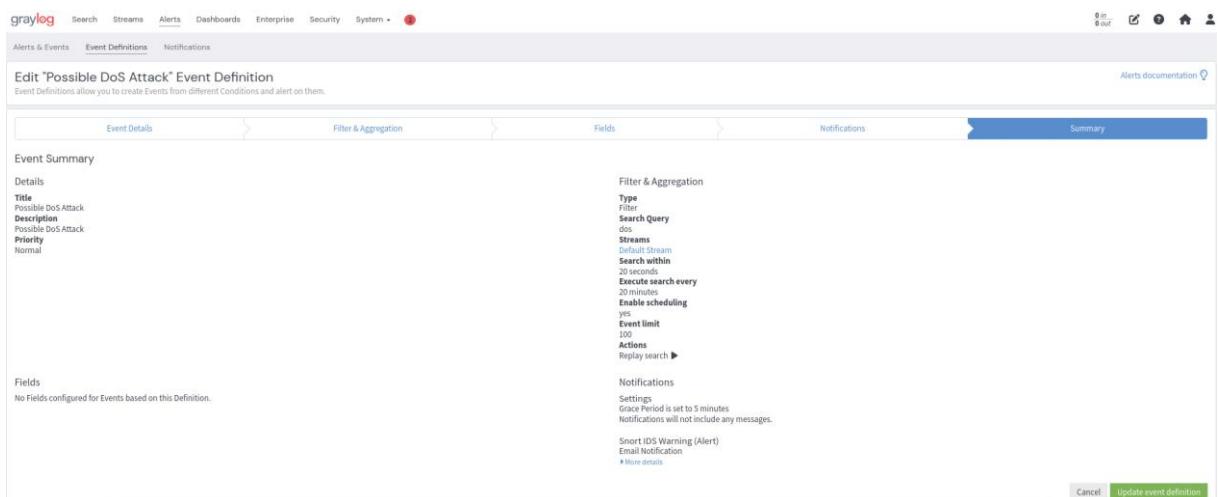
- Header:** Services / Snort / Interface Settings / WAN - Rules
- Top Navigation:** System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help
- Sub-navigation:** Snort Interfaces, Global Settings, Updates, Alerts, Blocked, Pass Lists, Suppress, IP Lists, SID Mgmt, Log Mgmt, Sync
- Current Tab:** WAN Rules
- Available Rule Categories:** Category Selection dropdown set to "custom.rules". A note says "Select the rule category to view and manage."
- Defined Custom Rules:**

```
# RULE SQL
alert tcp any any -> any 80 (msg: "AND SQL Injection Detected"; content: "and"; nocase; sid:100000060; )
alert tcp any any -> any 80 (msg: "OR SQL Injection Detected"; content: "--"; nocase; sid:100000061; )
#DOS ATTACK DETECTION
alert tcp any any -> any any (flags: S; msg:"Possible SYN DoS"; flow: stateless; threshold: type both, track by_dst, count 5; )
alert tcp any any -> any any (flags: A; msg:"Possible ACK DoS"; flow: stateless; threshold: type both, track by_dst, count 1000; )
alert tcp any any -> any any (flags: R; msg:"Possible RST DoS"; flow: stateless; threshold: type both, track by_dst, count 1000; )
alert tcp any any -> any any (flags: F; msg:"Possible FIN DoS"; flow: stateless; threshold: type both, track by_dst, count 1000; )
alert udp any any -> any any (msg:"Possible UDP DoS"; flow: stateless; threshold: type both, track by_dst, count 1000; )
alert icmp any any -> any any (msg:"Possible ICMP DoS"; threshold: type both, track by_dst, count 250, seconds 3; sid:100000062; )
# RULE SSH BRUTE FORCE ATTACK
alert tcp any any -> any 22 (msg:"Possible SSH brute forcing!"; flags: S+; threshold: type both, track by_src, count 5, seconds 30; )
```

Hình 3.63 – Rule SQL injection, Bruteforce Attack, Dos

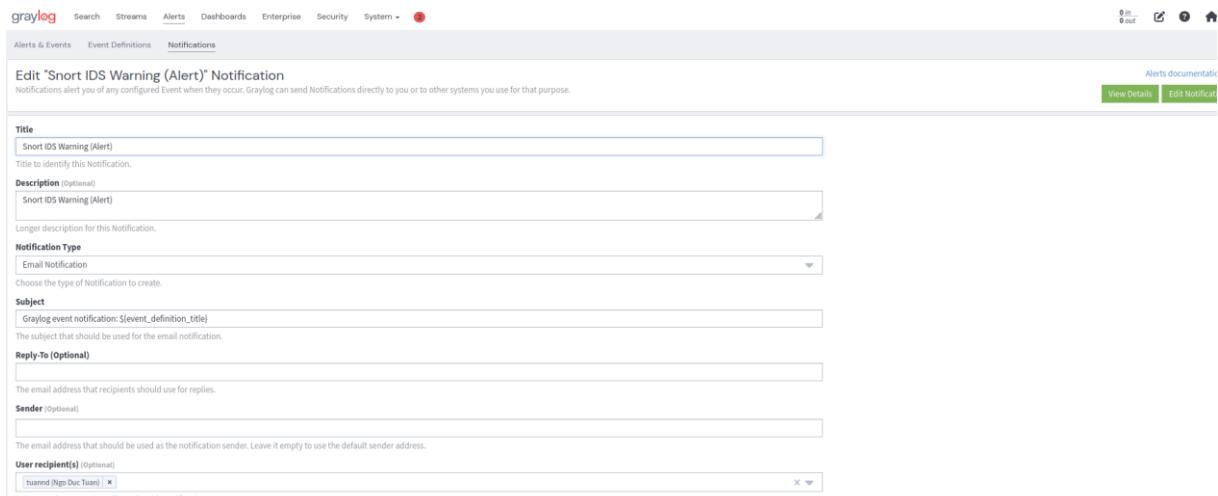
### 3.8 Tạo Alert trên Graylog

Để tạo alert trên Graylog trước hết cần tạo Event definitions. Mục đích của việc này là để Graylog có thể xác định loại cảnh báo và điều kiện để kích hoạt cảnh báo.



*Hình 3.64 – Thông tin cấu hình Event definitions*

Nhưng để alert thực sự được tạo, cần cấu hình thêm Notifications, có thể lựa chọn loại thông báo như thông báo qua email như hình 3.65.



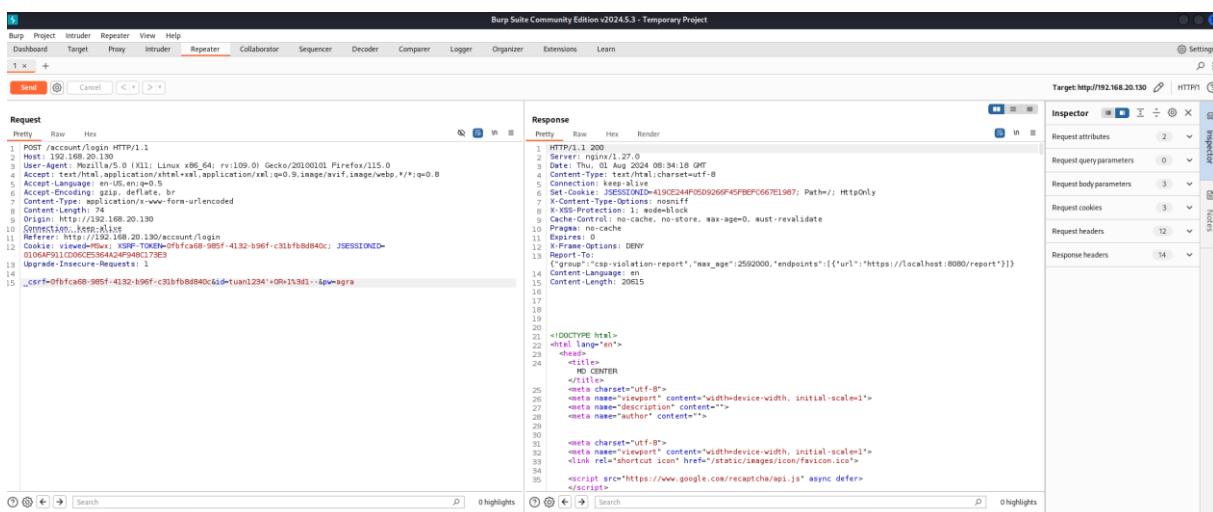
*Hình 3.65 – Cấu hình Notifications*

### 3.9 Demo tấn công

#### 3.9.1 SQL injection

Burp Suite là một bộ công cụ dùng để kiểm thử bảo mật cho các ứng dụng web, phát triển bởi PortSwigger. Các tính năng chính của Burp Suite bao gồm Burp Proxy (cho phép chặn, kiểm tra và sửa đổi lưu lượng HTTP/S giữa trình duyệt và ứng dụng web), Burp Spider (thu thập và lập bản đồ các ứng dụng web), Burp Scanner (quét lỗ hổng bảo mật tự động), Burp Intruder (tấn công brute force và kiểm tra điểm yếu bảo mật), Burp Repeater (gửi lại các yêu cầu HTTP/S tùy chỉnh), Burp Sequencer (phân tích độ ngẫu nhiên của các chuỗi token), Burp Decoder (giải mã hoặc mã hóa dữ liệu), và Burp Comparer (so sánh văn bản hoặc mã).

Trong kịch bản tấn công SQL injection vào trang web đã tạo ở các phần trước. Sử dụng Burp Suite tấn công vào form đăng nhập



Hình 3.66 – Tấn công SQL injection vào form đăng nhập

Sau khi tấn công, Snort trên firewall Pfsense sẽ so sánh gói tin được truyền đến với custom rules đã được tạo ở phần trước. Sau khi bắt được gói tin phù hợp với rule đã tạo. Snort sẽ tạo ra cảnh báo, cảnh báo này được lưu trên log của firewall Pfsense và được gửi về Graylog với facility là “local1”.

Event definitions đã tạo có điều kiện thỏa với các loại cảnh báo được gửi về, vì vậy nó sẽ tạo ra alert, đồng thời cũng sẽ gửi email cảnh báo như cấu hình notifications.

Description	Key	Type	Event Definition	Timestamp
SQL Injection Detected	none	Alert	SQL Injection Detected	2024-08-01 15:46:02
SQL Injection Detected	none	Alert	SQL Injection Detected	2024-08-01 15:46:02

Hình 3.67 – Graylog Alert SQL injection

Graylog event notification: SQL Injection Detected [Hủy thư đến]

V ngoductuanvn4@gmail.com  
đến tôi 15:46 (6 phút trước) ★ ☺ ← ::

**Event Definition**

Title	SQL Injection Detected
Description	SQL Injection Detected
Type	aggregation-v1

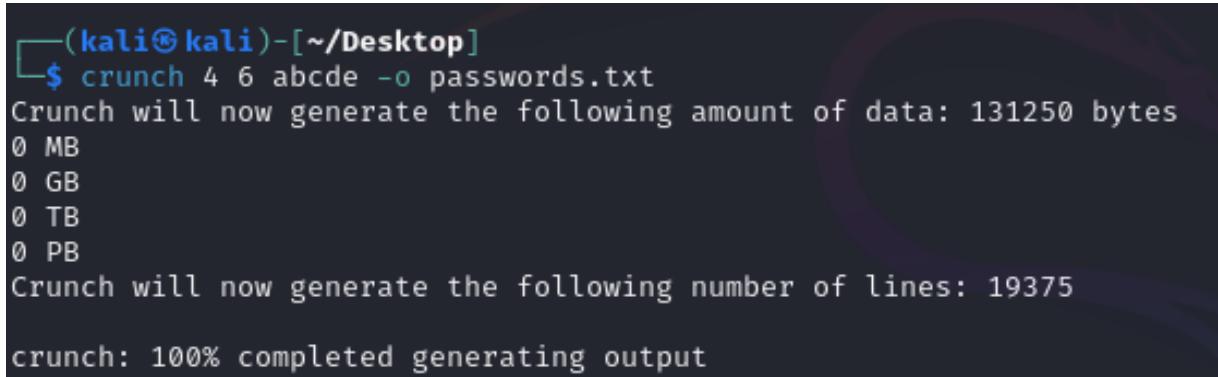
**Event**

Alert Replay	http://alerts/01J46HXG98H9R2YWAWSCE9ZQZR/replay-search
Timestamp	2024-08-01T15:46:02.963+07:00
Message	SQL Injection Detected

Hình 3.68 – Email cảnh báo từ Graylog

### 3.9.2 Brute Force SSH Attack

Để tiến hành thử nghiệm tấn công Brute Force, cần tạo list password bằng crunch – một công cụ tạo list từ khóa dựa trên các kí tự đã cho. Công cụ này sẽ tạo ra số từ bằng n giai thừa kí tự nhập vào.



```
(kali㉿kali)-[~/Desktop]
$ crunch 4 6 abcde -o passwords.txt
Crunch will now generate the following amount of data: 131250 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 19375
crunch: 100% completed generating output
```

*Hình 3.69 – Tạo list password sử dụng Crunch*

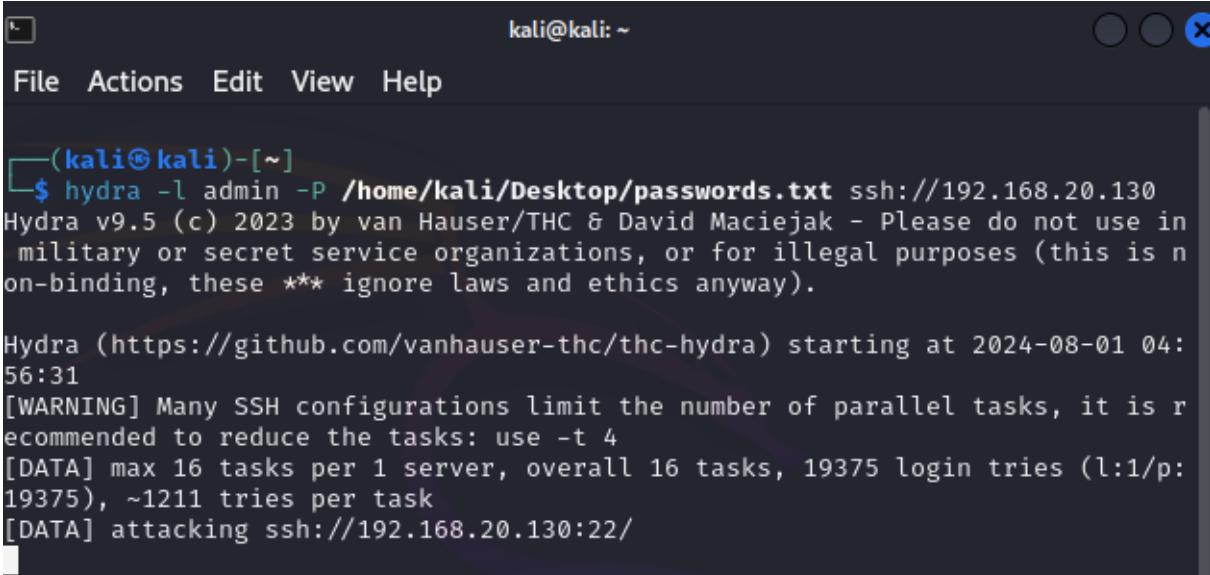
Hydra là một công cụ mã nguồn mở mạnh mẽ được sử dụng để tấn công brute force trên nhiều dịch vụ mạng khác nhau. Được phát triển bởi Van Hauser, Hydra hỗ trợ kiểm tra mật khẩu trên nhiều giao thức và dịch vụ, bao gồm SSH, FTP, HTTP, HTTPS, Telnet, và nhiều dịch vụ khác. Công cụ này có khả năng thực hiện các cuộc tấn công brute force nhanh chóng và hiệu quả nhờ vào việc sử dụng các danh sách mật khẩu và tên người dùng có sẵn. Hydra rất linh hoạt, cho phép người dùng tùy chỉnh các tham số tấn công như số lượng kết nối đồng thời, thời gian chờ giữa các lần thử, và thậm chí cấu hình các mô-đun tùy chỉnh để mở rộng khả năng của nó. Công cụ này thường được sử dụng bởi các chuyên gia bảo mật để kiểm tra độ mạnh của mật khẩu và phát hiện các lỗ hổng bảo mật liên quan đến xác thực.

Lần thử nghiệm tấn công này là nhắm vào dịch vụ ssh của firewall Pfsense, sử dụng câu lệnh dưới đây:

“hydra -l admin -P /home/kali/Desktop/passwords.txt ssh://192.168.20.130” trong đó:

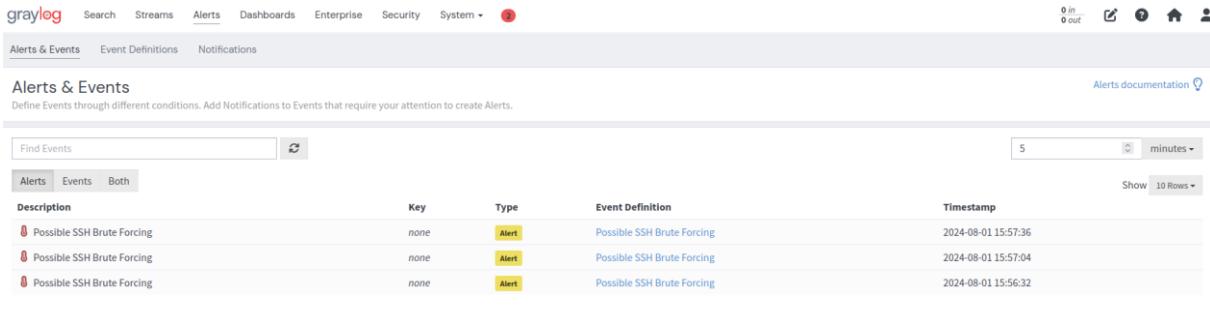
- “hydra”: Gọi chương trình Hydra để thực hiện tấn công brute force.
- “-l admin”: Chỉ định tên người dùng để thử nghiệm đăng nhập. Trong trường hợp này, tên người dùng là admin.
- “-P /home/kali/Desktop/passwords.txt”: Chỉ định đường dẫn đến file chứa danh sách mật khẩu để thử nghiệm. File passwords.txt nằm trên desktop của người dùng kali.
- “ssh://192.168.20.130”: Chỉ định giao thức và địa chỉ IP của máy chủ mục tiêu. Trong trường hợp này, giao thức là SSH và địa chỉ IP là 192.168.20.130.

Tóm lại, lệnh này sẽ thử tất cả các mật khẩu trong file passwords.txt để đăng nhập vào máy chủ SSH tại địa chỉ IP 192.168.20.130 với tên người dùng admin.

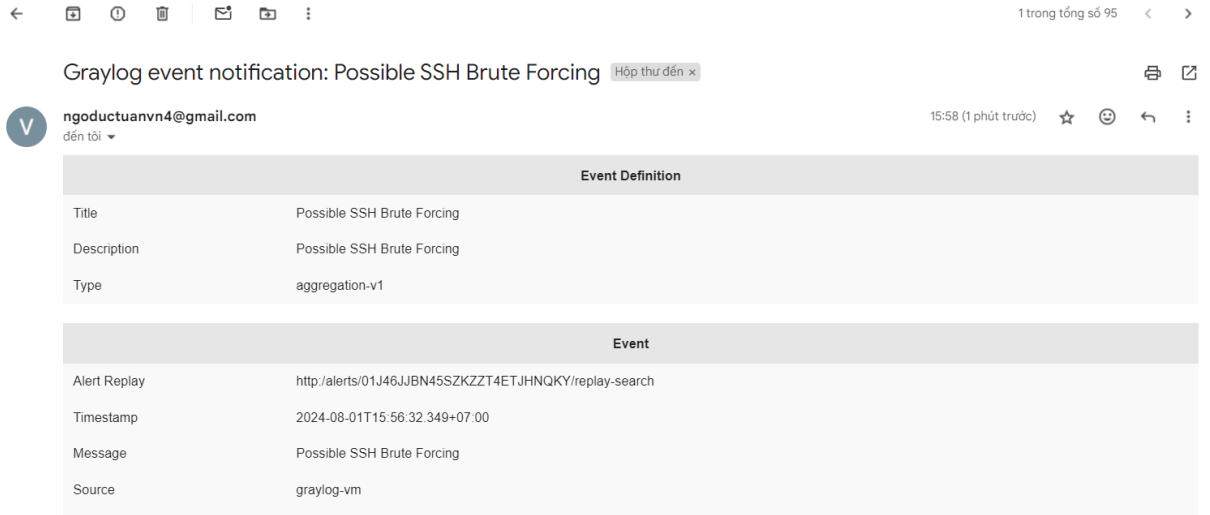


```
(kali㉿kali)-[~]
$ hydra -l admin -P /home/kali/Desktop/passwords.txt ssh://192.168.20.130
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-08-01 04:
56:31
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 19375 login tries (l:1/p:
19375), ~1211 tries per task
[DATA] attacking ssh://192.168.20.130:22/
```

*Hình 3.70 – Tấn công ssh authentication sử dụng hydra*


Description	Key	Type	Event Definition	Timestamp
Possible SSH Brute Forcing	none	Alert	Possible SSH Brute Forcing	2024-08-01 15:57:36
Possible SSH Brute Forcing	none	Alert	Possible SSH Brute Forcing	2024-08-01 15:57:04
Possible SSH Brute Forcing	none	Alert	Possible SSH Brute Forcing	2024-08-01 15:56:32

*Hình 3.71 – Graylog Alert Brute Force*


Graylog event notification: Possible SSH Brute Forcing

nguctuanvn4@gmail.com  
đến tôi

Event Definition

Title	Possible SSH Brute Forcing
Description	Possible SSH Brute Forcing
Type	aggregation-v1

Event

Alert Replay	http://alerts/01J46JJBN45SZKZT4ETJHNQKY/replay-search
Timestamp	2024-08-01T15:56:32.349+07:00
Message	Possible SSH Brute Forcing
Source	graylog-vm

*Hình 3.72 – Email cảnh báo Brute Force từ Graylog*

### 3.9.3 DOS Attack

Hping3 là một công cụ mạnh mẽ dùng để kiểm thử và phân tích mạng, cũng như thực hiện các cuộc tấn công mạng. Đây là phiên bản cải tiến của Hping, tương tự như công cụ ping truyền thống nhưng có nhiều tính năng mở rộng. Hping3 cho phép gửi các gói tin TCP, UDP, ICMP, và RAW-IP để kiểm tra kết nối mạng, đo độ trễ và theo dõi đường đi của gói tin. Nó cũng hỗ trợ các cuộc tấn công DoS, DDoS, quét cổng, tạo gói tin tùy chỉnh, và IP spoofing. Hping3 còn có thể thực hiện chức năng tương tự như traceroute để theo dõi đường đi của các gói tin qua mạng.

Thử nghiệm lần này sử dụng câu lệnh “sudo hping3 -S -p 80 -i u1 192.168.20.130” để tấn công Dos đến Web server trong đó:

- “sudo”: Chạy lệnh với quyền quản trị (superuser) để đảm bảo có đủ quyền truy cập cần thiết.
- “hping3”: Gọi chương trình Hping3 để thực hiện gửi gói tin mạng.
- “-S”: Chỉ định cờ SYN trong gói tin TCP, thường được sử dụng để bắt đầu một kết nối TCP.
- “-p 80”: Chỉ định cổng đích là 80, thường là cổng HTTP.
- “-i u1”: Chỉ định khoảng thời gian giữa các gói tin được gửi đi là 1 microsecond, điều này làm tăng tốc độ gửi gói tin.
- “192.168.20.130”: Địa chỉ IP của máy chủ mục tiêu.

Tóm lại, lệnh này sẽ gửi một loạt các gói tin TCP SYN đến cổng 80 của máy chủ có địa chỉ IP 192.168.20.130 với tần suất rất cao.

```
(root㉿kali)-[~]
# sudo hping3 -S -p 80 -i u1 192.168.20.130
HPING 192.168.20.130 (eth0 192.168.20.130): S set, 40 headers + 0 data bytes
len=46 ip=192.168.20.130 ttl=127 DF id=17800 sport=80 flags=SA seq=1 win=6539
2 rtt=3.5 ms
len=46 ip=192.168.20.130 ttl=127 DF id=17801 sport=80 flags=SA seq=0 win=6539
2 rtt=3.8 ms
len=46 ip=192.168.20.130 ttl=127 DF id=17807 sport=80 flags=SA seq=11 win=653
92 rtt=9.4 ms
len=46 ip=192.168.20.130 ttl=127 DF id=17808 sport=80 flags=SA seq=13 win=653
92 rtt=9.1 ms
len=46 ip=192.168.20.130 ttl=127 DF id=17809 sport=80 flags=SA seq=15 win=653
92 rtt=8.7 ms
len=46 ip=192.168.20.130 ttl=127 DF id=17811 sport=80 flags=SA seq=17 win=653
92 rtt=8.3 ms
len=46 ip=192.168.20.130 ttl=127 DF id=17812 sport=80 flags=SA seq=18 win=653
92 rtt=8.1 ms
len=46 ip=192.168.20.130 ttl=127 DF id=17813 sport=80 flags=SA seq=20 win=653
92 rtt=7.7 ms
len=46 ip=192.168.20.130 ttl=127 DF id=17814 sport=80 flags=SA seq=22 win=653
92 rtt=7.3 ms
len=46 ip=192.168.20.130 ttl=127 DF id=17815 sport=80 flags=SA seq=24 win=653
92 rtt=6.9 ms
len=46 ip=192.168.20.130 ttl=127 DF id=17825 sport=80 flags=SA seq=43 win=653
92 rtt=3.4 ms
```

Hình 3.73 – Tấn công sử dụng hping3

## Cảnh báo sẽ được Graylog kích hoạt

The screenshot shows the Graylog web interface under the 'Alerts & Events' tab. A search bar at the top left contains 'Find Events'. To its right are buttons for '0 in' and '0 out' log counts, and icons for refresh, search, and user. Below the search bar are tabs for 'Alerts & Events', 'Event Definitions', and 'Notifications'. A note says 'Define Events through different conditions. Add Notifications to Events that require your attention to create Alerts.' On the right, a link points to 'Alerts documentation'. A table below lists four alerts:

Description	Key	Type	Event Definition	Timestamp
Possible DoS Attack	none	Alert	Possible DoS Attack	2024-08-01 15:51:29
Possible DoS Attack	none	Alert	Possible DoS Attack	2024-08-01 15:51:28
Possible DoS Attack	none	Alert	Possible DoS Attack	2024-08-01 15:51:23
Possible DoS Attack	none	Alert	Possible DoS Attack	2024-08-01 15:51:20

At the bottom right of the table are buttons for 'Show' and '10 Rows'.

*Hình 3.74 – Graylog Alert Dos Attack*

The screenshot shows an email message from 'ngductuanvn4@gmail.com' to 'nguctuanvn4@gmail.com' at 15:53 (0 phút trước). The subject is 'Graylog event notification: Possible DoS Attack'. The message body contains two sections: 'Event Definition' and 'Event'.

**Event Definition**

Title	Possible DoS Attack
Description	Possible DoS Attack
Type	aggregation-v1

**Event**

Alert Replay	<a href="http://alerts/01J46J9G56VFRZKAZ19PCQQ2XM/replay-search">http://alerts/01J46J9G56VFRZKAZ19PCQQ2XM/replay-search</a>
Timestamp	2024-08-01T15:51:20.796+07:00
Message	Possible DoS Attack
Source	graylog-vm
Key	
Priority	

*Hình 3.75 – Email cảnh báo Dos Attack từ Graylog*

## CHƯƠNG 4: KẾT LUẬN

Trong quá trình thực hiện đề tài, các mục tiêu chính đã được hoàn thành như sau:

### 4.1 Tìm hiểu và phân tích các chức năng của Snort

Đã tiến hành nghiên cứu chi tiết về các chức năng và khả năng của Snort, một trong những hệ thống phát hiện xâm nhập (IDS) phổ biến nhất hiện nay. Qua đó, hiểu rõ cách Snort hoạt động, các chế độ hoạt động và các thành phần chính của Snort.

### 4.2 Xây dựng mô hình mạng doanh nghiệp

Đã xây dựng một mô hình mạng doanh nghiệp giả lập, bao gồm một hệ thống mạng với các thành phần như máy chủ, máy trạm, và các thiết bị mạng. Mô hình này được thiết kế để phản ánh các cấu hình và kiến trúc mạng thực tế trong môi trường doanh nghiệp, tạo điều kiện thuận lợi cho việc triển khai và kiểm thử Snort.

### 4.3 Xây dựng và triển khai mô hình giám sát mạng sử dụng Snort và Graylog

Đã triển khai Snort trên mô hình mạng doanh nghiệp và tích hợp với Graylog để thu thập và phân tích các log sự kiện. Quá trình này bao gồm việc cấu hình Snort để phát hiện các hoạt động xâm nhập và thiết lập Graylog để lưu trữ và phân tích log từ Snort. Sự tích hợp này đã cung cấp cái nhìn toàn diện và kịp thời về các sự kiện bảo mật xảy ra trong mạng.

### 4.4 Đánh giá hiệu quả của mô hình thông qua các kịch bản kiểm thử

Đã tiến hành một loạt các kịch bản kiểm thử để đánh giá hiệu quả của mô hình giám sát mạng sử dụng Snort và Graylog. Các kịch bản này bao gồm việc giả lập các cuộc tấn công phổ biến như DoS, SQL injection, và Brute Force Attack. Kết quả kiểm thử cho thấy mô hình giám sát đã hoạt động hiệu quả trong việc phát hiện và ghi nhận các hành vi xâm nhập, cung cấp thông tin quan trọng để đưa ra các biện pháp phòng ngừa kịp thời.

### 4.5 Tổng kết

Qua đề tài này, đã chứng minh được khả năng của Snort trong việc phát hiện các hoạt động xâm nhập và sự kết hợp mạnh mẽ giữa Snort và Graylog trong việc giám sát và phân tích log sự kiện. Các kết quả đạt được không chỉ cung cấp cái nhìn chi tiết về hoạt động của hệ thống phát hiện xâm nhập mà còn khẳng định tầm quan trọng của việc triển khai các biện pháp bảo mật mạng trong môi trường doanh nghiệp. Hy vọng rằng những kết quả này sẽ đóng góp tích cực vào công tác bảo mật thông tin và nâng cao nhận thức về an ninh mạng trong cộng đồng.

**TÀI LIỆU THAM KHẢO**

- [1] N. I. o. S. a. T. (NIST), “Computer Security Resource Center,” [Trực tuyến]. Available: <https://csrc.nist.gov>. [Đã truy cập 23 July 2024].
- [2] S. Institute, “What is a DDoS Attack?,” [Trực tuyến]. Available: <https://www.sans.org/white-papers/36621>. [Đã truy cập 23 July 2024].
- [3] F. T. C. (FTC), “What is Phishing?,” [Trực tuyến]. Available: <https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>. [Đã truy cập 23 July 2024].
- [4] Microsoft, “What is malware?,” [Trực tuyến]. Available: <https://www.microsoft.com/en-us/security/portal/mmpc/shared/malware.aspx>. [Đã truy cập 23 July 2024].
- [5] O. Foundation, “SQL Injection.,” [Trực tuyến]. Available: [https://owasp.org/www-community/attacks/SQL\\_Injection](https://owasp.org/www-community/attacks/SQL_Injection). [Đã truy cập 23 July 2024].
- [6] N. I. o. S. a. T. (NIST), “Guide to Bluetooth Security,” [Trực tuyến]. Available: <https://csrc.nist.gov/publications/detail/sp/800-121/rev-2/final>. [Đã truy cập 23 July 2024].
- [7] R. Bejtlich, *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*, No Starch Press, 2013.
- [8] A. C. J. A. John McHugh, “Defending Yourself: The Role of Intrusion Detection Systems,” *IEEE Software*, tập 17, số 5, pp. 42-51, Sept.-Oct. 2000.
- [9] J. C. Mogul, “Snort: Lightweight Intrusion Detection for Networks,” *IEEE Security & Privacy*, tập 1, pp. 91-95, Jul.-Aug. 2003.
- [10] C. Kolde, *Network Security with Snort: Intrusion Detection, Prevention, and Analysis*, No Starch Press, 2004.