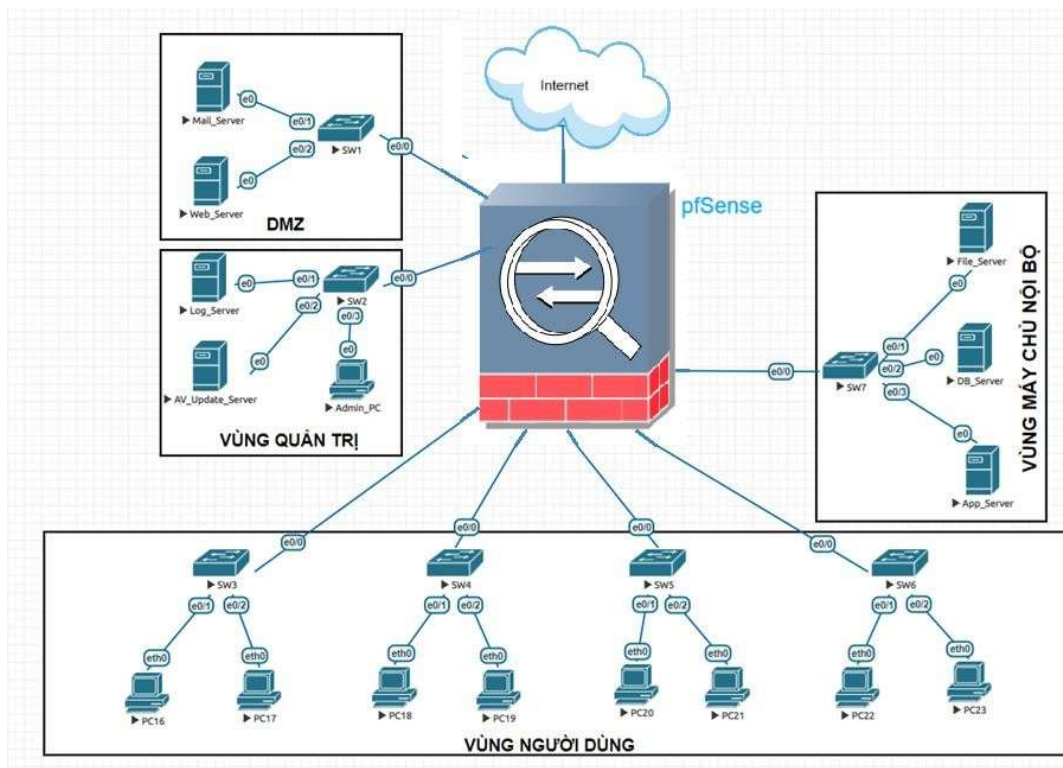


### CHƯƠNG 3. XÂY DỰNG HỆ THỐNG MẠNG AN TOÀN SỬ DỤNG CÔNG CỤ VÀ KỸ THUẬT QUẢN LÝ, PHÁT HIỆN MỐI ĐE DỌA TỰ ĐỘNG / BÁN TỰ ĐỘNG TRÊN HỆ THỐNG MẠNG INTRANET/INTERNET

#### 3.1. Mô hình triển khai



Hình 3. 1. Mô hình

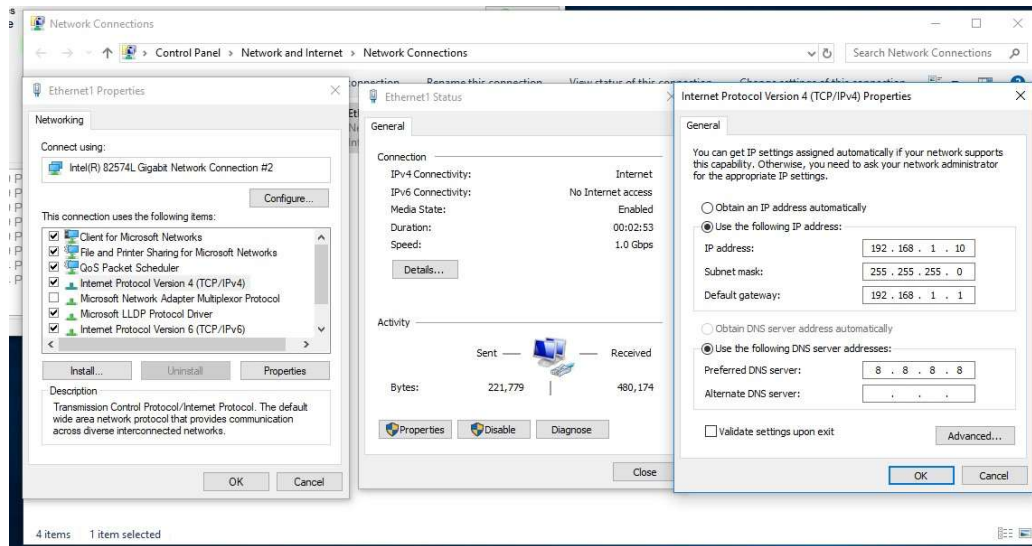
- pfSense được thiết lập như 1 môi trường được cài đặt các công cụ: Snort làm IDS và Suricata làm IDS. Pfsense sử dụng card NAT nối đến vùng mạng ngoài, card VMnet6 nối đến vùng DMZ, card VMnet7 nối đến vùng người dùng, card VMnet 5 nối đến vùng máy chủ nội bộ và VMnet4 nối đến vùng quản trị.

- Vùng DMZ được triển khai trên Windows 10, cài đặt công cụ XAMPP làm web server. Dùng card VMnet6 nối đến môi trường

pfSense.

- Vùng người dùng được triển khai trên card mạng LAN,
- Attacker sử dụng máy thật gán card NAT và có thể truy cập được vùng DMZ.

### 3.2. Triển khai DMZ



Hình 3. 2. Trên vùng DMZ đặt ip

```
C:\Users\Ngoc Dai>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=36ms TTL=128
Reply from 8.8.8.8: bytes=32 time=34ms TTL=128
Reply from 8.8.8.8: bytes=32 time=38ms TTL=128
Reply from 8.8.8.8: bytes=32 time=33ms TTL=128

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 33ms, Maximum = 38ms, Average = 35ms

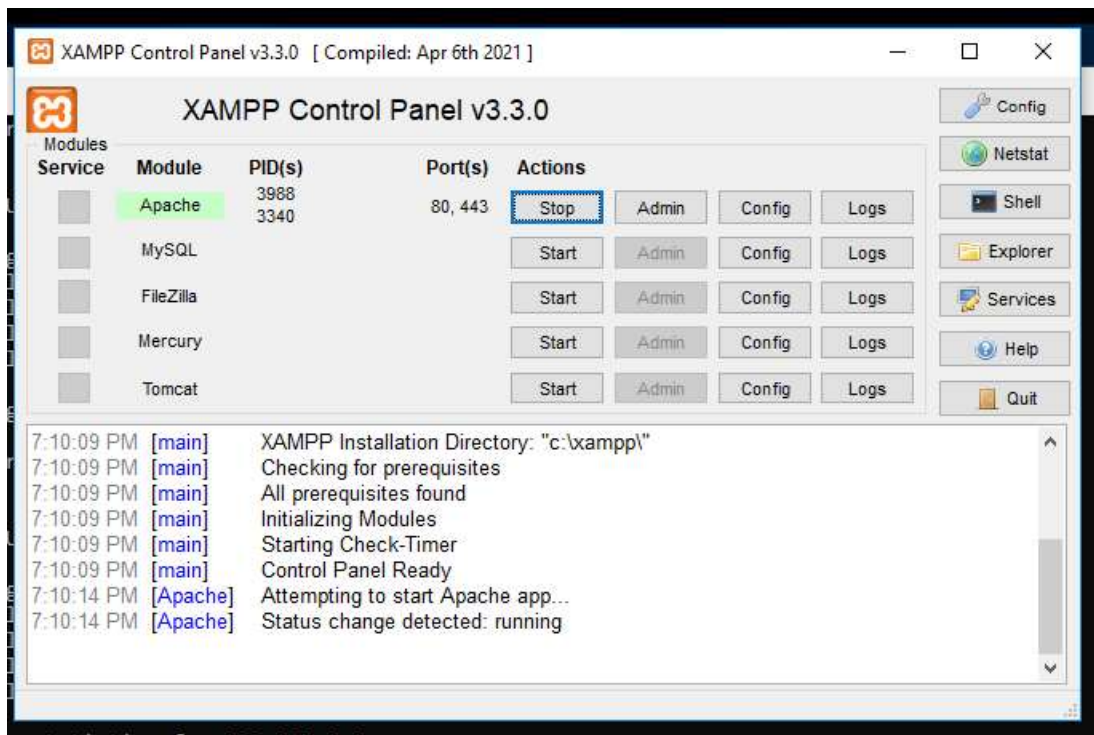
C:\Users\Ngoc Dai>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

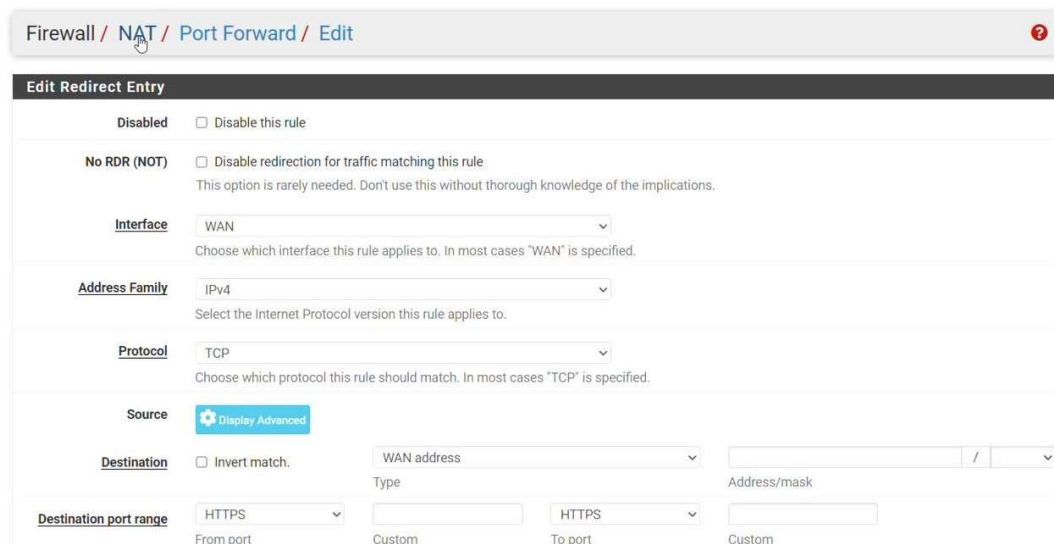
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Ngoc Dai>
```

Hình 3. 3. Đảm bảo có thể ping ra được pfSense và Internet



Hình 3. 4. Cài đặt và triển khai web server sử dụng XAMPP



Hình 3. 5. Cấu hình để có thể public web server trong Firewall / NAT / Port Forward / Edit

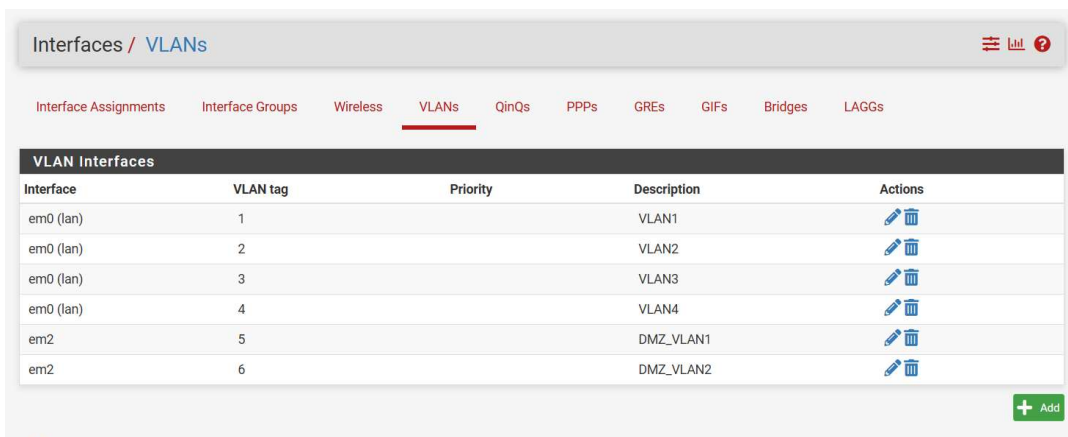


Hình 3. 6. Ấn save và chọn Apply Changes



Hình 3. 7. Đảm bảo mạng ngoài có thể truy cập pfSense

### 3.3. Triển khai VLAN trên vùng DMZ, vùng người dùng và vùng quản trị




Hình 3. 8: Trong Interfaces /Vlan chọn add để tạo vlan mới

Interfaces / VLANs / Edit

### VLAN Configuration

Parent Interface	em0 (00:0c:29:f5:4d:8c) - lan
Only VLAN capable interfaces will be shown.	
VLAN Tag	1
802.1Q VLAN tag (between 1 and 4094).	
VLAN Priority	0
802.1Q VLAN Priority (between 0 and 7).	
Description	VLAN1
A group description may be entered here for administrative reference (not parsed).	

 Save

Hình 3. 9: Chọn card LAN và đặt Vlan tag là 1


Lặp lại nhiều lần và tạo ra lần lượt từ Vlan 1 đến Vlan 4 cho lớp mạng người dùng

· Tiếp tục và tạo ra với vùng DMZ.

Interfaces / VLANs / Edit

### VLAN Configuration

Parent Interface	em2 (00:0c:29:f5:4d:a0)
Only VLAN capable interfaces will be shown.	
VLAN Tag	5
802.1Q VLAN tag (between 1 and 4094).	
VLAN Priority	0
802.1Q VLAN Priority (between 0 and 7).	
Description	DMZ_VLAN1
A group description may be entered here for administrative reference (not parsed).	

 Save

Hình 3. 10: Vùng DMZ

Tiếp tục và tạo ra với vùng quản trị.

Interfaces / VLANs / Edit


### VLAN Configuration

**Parent Interface**  ▼  
 Only VLAN capable interfaces will be shown.

**VLAN Tag**   
 802.1Q VLAN tag (between 1 and 4094).











**VLAN Priority**   
 802.1Q VLAN Priority (between 0 and 7).

**Description**   
 A group description may be entered here for administrative reference (not parsed).

 Save

Hình 3. 11: Vlan cho vùng Manager

Trong phần Interfaces / Interface Assignments chọn lần lượt các lớp mạng vừa tạo và nhấn add.

Interface	Network port
WAN	<input type="text" value="em1 (00:0c:29:f5:4d:96)"/> <span>▼</span>
LAN	<input type="text" value="em0 (00:0c:29:f5:4d:8c)"/> <span>▼</span>  Delete
DMZ	<input type="text" value="BRIDGE0 (bri)"/> <span>▼</span>  Delete
VLAN1	<input type="text" value="VLAN 1 on em0 - lan (VLAN1)"/> <span>▼</span>  Delete
VLAN2	<input type="text" value="VLAN 2 on em0 - lan (VLAN2)"/> <span>▼</span>  Delete
VLAN3	<input type="text" value="VLAN 3 on em0 - lan (VLAN3)"/> <span>▼</span>  Delete
VLAN4	<input type="text" value="VLAN 4 on em0 - lan (VLAN4)"/> <span>▼</span>  Delete
DMZ_VLAN1	<input type="text" value="VLAN 5 on em2 - opt8 (DMZ_VLAN1)"/> <span>▼</span>  Delete
DMZ_VLAN2	<input type="text" value="VLAN 6 on em2 - opt8 (DMZ_VLAN2)"/> <span>▼</span>  Delete
Manager	<input type="text" value="em2 (00:0c:29:f5:4d:a0)"/> <span>▼</span>  Delete
Manager_VLAN1	<input type="text" value="VLAN 9 on em2 - opt8 (Manager_VLAN1)"/> <span>▼</span>  Delete

Hình 3. 12: Sau đó nhấn Save

Tiếp đến vào ấn đúp chuột vào từng lớp

Vlan. Ta đặt lại tên và chọn như hình.



Interfaces / OPT2 (em0.1)

**General Configuration**

Enable ☐ Enable interface

Description **VLAN1**  
Enter a description (name) for the interface here.

IPv4 Configuration Type **DHCP**

IPv6 Configuration Type **None**

MAC Address **XXXXXXXXXXXX**  
The MAC address of a VLAN interface must be set on its parent interface

MTU   
If this field is blank, the adapter's default MTU will be used. This is typically 15

MSS   
If a value is entered in this field, then MSS clamping for TCP connections to th  
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

Hình 3. 13: Đặt tên hiển thị cho Vlan

Sau đó nhấn Save để lưu cấu hình.

Đó là cách cấu hình đối với DHCP, còn đối với static IP thì ta cấu hình như sau:

Interfaces / OPT4 (em0.3)

**General Configuration**

Enable ☐ Enable interface

Description **VLAN3**  
Enter a description (name) for the interface here.

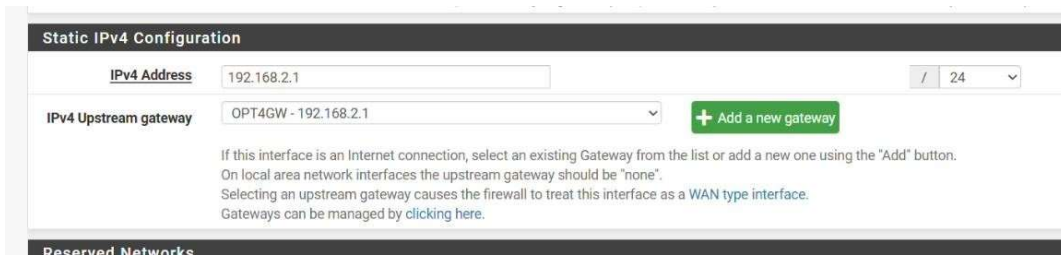
IPv4 Configuration Type **Static IPv4**

IPv6 Configuration Type **None**

MAC Address

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.

Hình 3. 14: Chọn Static ip trong ipv4 configuration types

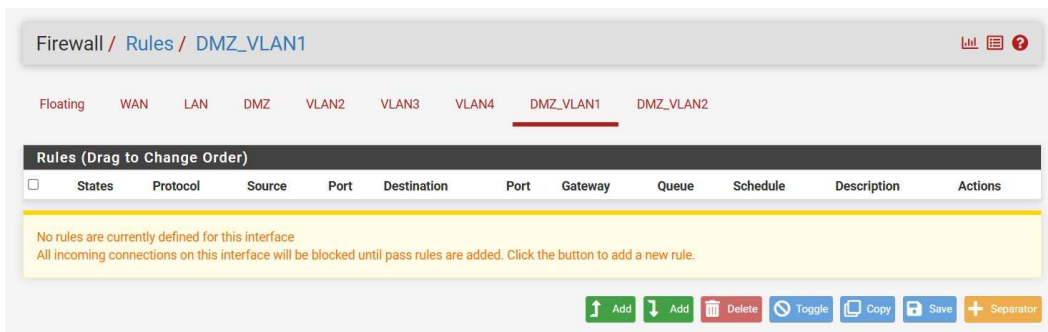


Hình 3. 15: Kéo xuống và đặt ip cho lớp mạng VLAN

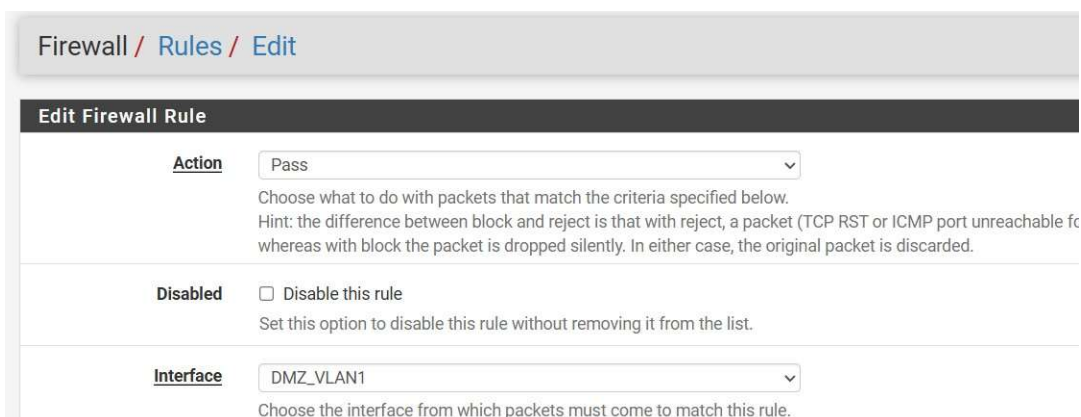
Đối với nhu cầu xây dựng hệ thống khác nhau thì ta sẽ sử dụng những cách đặt khác nhau.

Để cho Vlan có thể đi thông ra Internet thì ta đặt rule cho các lớp mạng VLAN.

Trong Firewall / Rules.



Hình 3. 16: Chọn lớp mạng cần thêm rule



Hình 3. 17: Chọn Pass và để mặc định

Nhấn Save để lưu cấu hình. Tiếp tục lặp đối với các Vlan còn lại.

Quay lại phần CLI của pfsense, ta đã thấy xuất hiện dần các IP cho từng lớp Vlan.

```
WAN (wan)      -> em1      -> v4/DHCP4: 192.168.182.175/24
LAN (lan)      -> em0      -> v4: 192.168.1.1/24
DMZ (opt1)     -> bridge0  -> v4: 192.168.4.10/24
VLAN1 (opt2)   -> em0.1    ->
VLAN2 (opt3)   -> em0.2    -> v4: 192.168.3.10/24
VLAN3 (opt4)   -> em0.3    -> v4: 192.168.2.1/24
VLAN4 (opt5)   -> em0.4    ->
DMZ_VLAN1 (opt6) -> em2.5    -> v4: 192.168.6.1/24
DMZ_VLAN2 (opt7) -> em2.6    -> v4: 192.168.5.10/24
MANAGER (opt8) -> em2      -> v4: 192.168.8.10/24
MANAGER_VLAN1 (opt9) -> em2.9    -> v4: 192.168.9.30/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

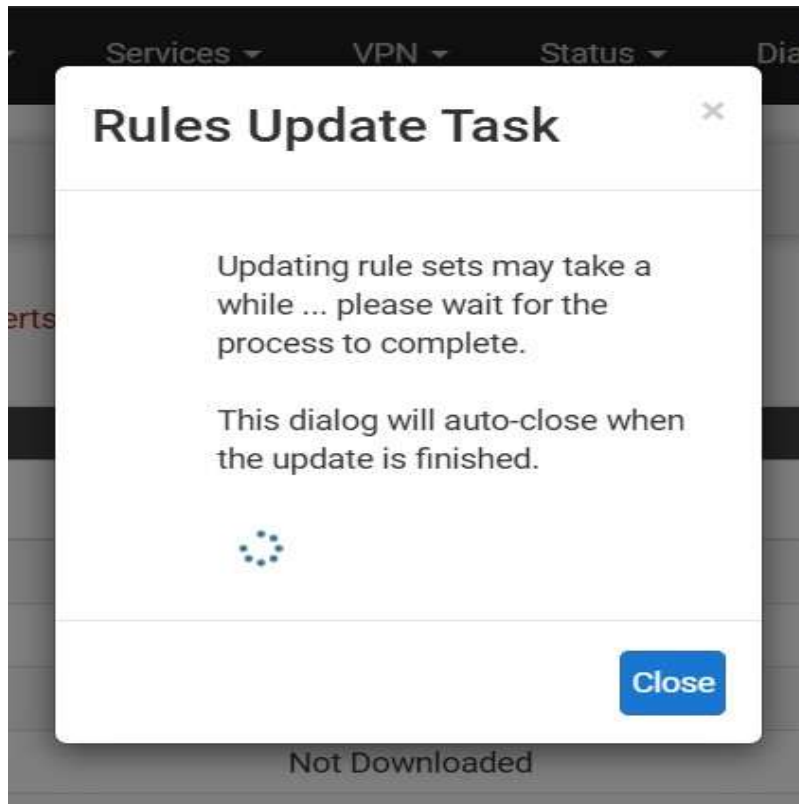
Enter an option: █
```

Hình 3. 18: Đã xuất hiện tất cả các phân vùng

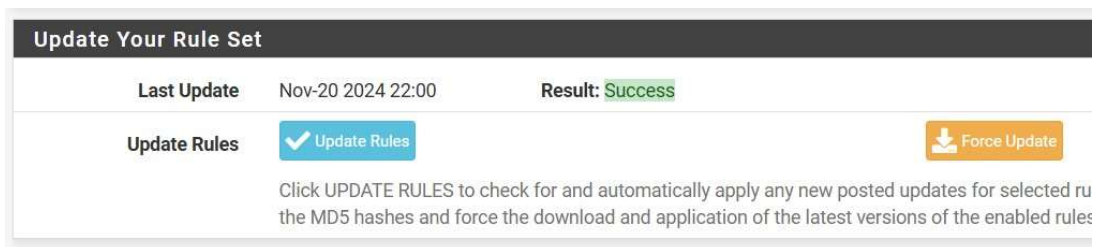
### 3.4. Sử dụng Snort làm IDS

Trong pfSense, mục Services / Snort/ Global Settings Enable một số tính năng như: Snort VRT, Snort GPLv2, ET Open, OpenAppID, FEODO Tracker Botnet C2 IP Rules.

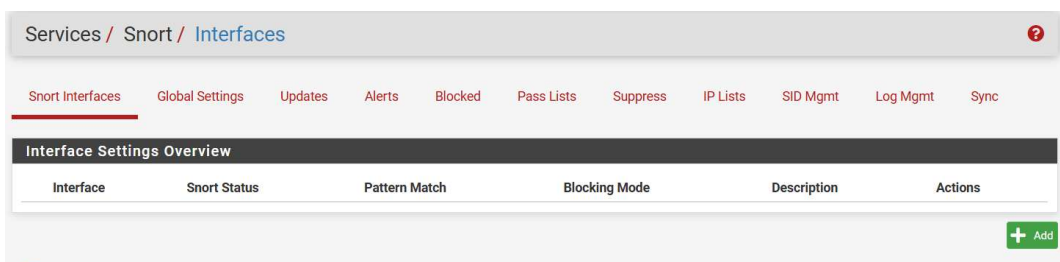




Hình 3. 21. Mạng mạnh thì đợi update rule tầm 5 phút



Hình 3. 22. Kết quả download thành công



Hình 3. 23. Để kích hoạt Snort thì trong Services / Snort / Interfaces chọn Add

## - Cấu hình alert trên WAN

The screenshot shows the 'WAN Settings' page in pfSense. It is divided into two main sections: 'General Settings' and 'Alert Settings'.

**General Settings:**

- Enable:** A checkbox labeled 'Enable interface' is checked.
- Interface:** A dropdown menu is set to 'WAN (em0)'. Below it, a note says 'Choose the interface where this Snort instance will inspect traffic.'
- Description:** A text input field contains 'WAN'. Below it, a note says 'Enter a meaningful description here for your reference.'
- Snap Length:** A text input field contains '1518'. Below it, a note says 'Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.'

**Alert Settings:**

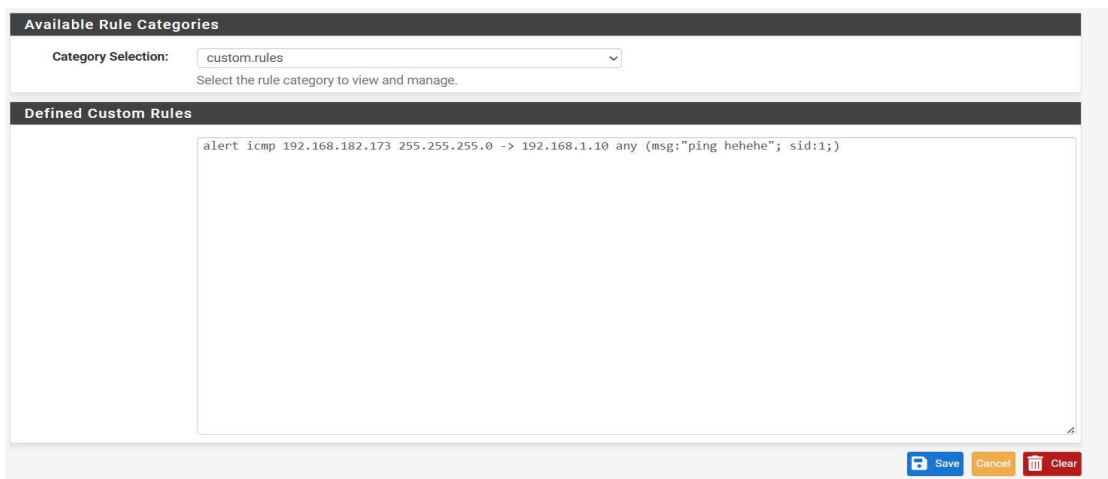
- Send Alerts to System Log:** A checkbox is checked. A note says 'Snort will send Alerts to the firewall's system log. Default is Not Checked.'
- System Log Facility:** A dropdown menu is set to 'LOG\_AUTH'. A note says 'Select system log Facility to use for reporting. Default is LOG\_AUTH.'
- System Log Priority:** A dropdown menu is set to 'LOG\_ALERT'. A note says 'Select system log Priority (Level) to use for reporting. Default is LOG\_ALERT.'
- Enable Packet Captures:** An unchecked checkbox. A note says 'Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file.'
- Enable Unified2 Logging:** An unchecked checkbox. A note says '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. 24. Chọn cổng WAN và bật tính năng alert

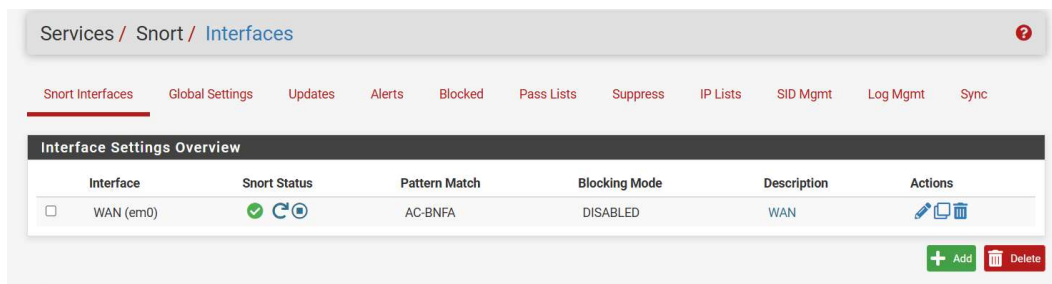
## Trong Services / Snort / Interface Settings / WAN – Rules

The screenshot shows the 'WAN Rules' page in pfSense. The breadcrumb trail at the top reads 'Services / Snort / Interface Settings / WAN - Rules'. Below the breadcrumb, there are several tabs: 'Snort Interfaces', 'Global Settings', 'Updates', 'Alerts', 'Blocked', 'Pass Lists', 'Suppress', 'IP Lists', 'SID Mgmt', 'Log Mgmt', and 'Sync'. The 'Alerts' tab is selected. Below the tabs, there are several sub-sections: 'WAN Settings', 'WAN Categories', 'WAN Rules', 'WAN Variables', 'WAN Preprocs', 'WAN IP Rep', and 'WAN Logs'. The 'WAN Rules' sub-section is selected. Below the sub-sections, there is a section titled 'Available Rule Categories' with a 'Category Selection:' dropdown menu set to 'custom.rules'. A note below the dropdown says 'Select the rule category to view and manage.' Below this, there is a section titled 'Defined Custom Rules' which is currently empty.

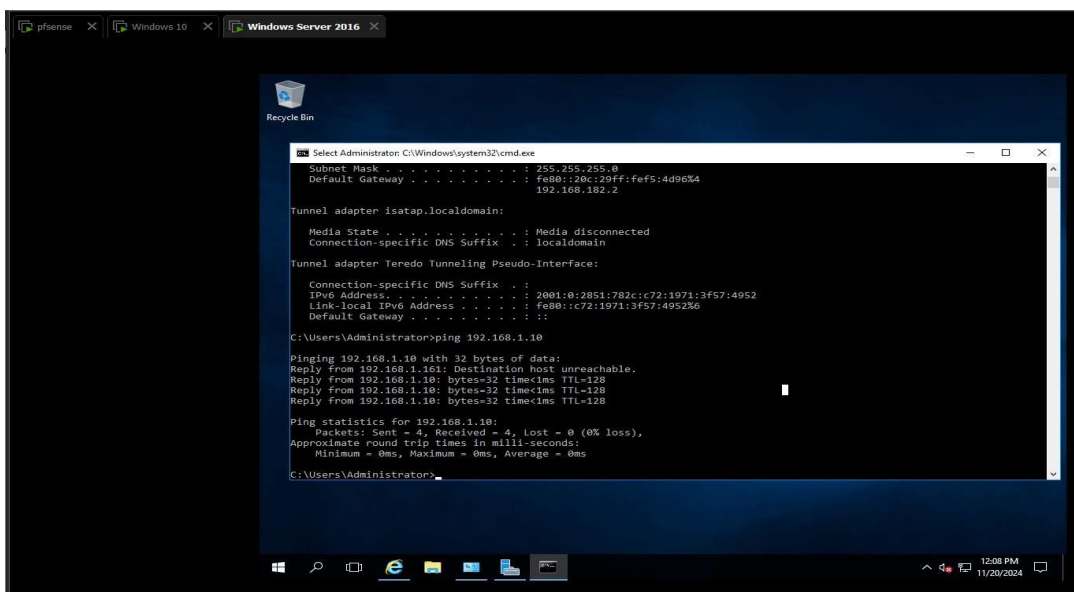
Hình 3. 25. Chọn Category Selection là custom.rules



Hình 3. 26. Tiến hành viết một số rule cơ bản và save



Hình 3. 27 Đảm bảo rằng rule đã được kích hoạt



Hình 3. 28. Ping từ máy attacker



Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

☐ Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

4 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-11-21 03:06:56	⚠	0	ICMP		192.168.182.173		192.168.1.10		1:1	ping hehehe
2024-11-21 03:06:55	⚠	0	ICMP		192.168.182.173		192.168.1.10		1:1	ping hehehe
2024-11-21 03:06:54	⚠	0	ICMP		192.168.182.173		192.168.1.10		1:1	ping hehehe
2024-11-21 03:06:51	⚠	0	ICMP		192.168.182.173		192.168.1.10		1:1	ping hehehe

Hình 3. 29. Log phát hiện ping

- Cấu hình alert trên LAN

LAN Settings

LAN Categories

LAN Rules

LAN Variables

LAN Preprocs

LAN IP Rep

LAN Logs

General Settings

Enable

☒ Enable interface

Interface

LAN (em1)

Choose the interface where this Snort instance will inspect traffic.

Description

LAN

Enter a meaningful description here for your reference.

Snap Length

1518

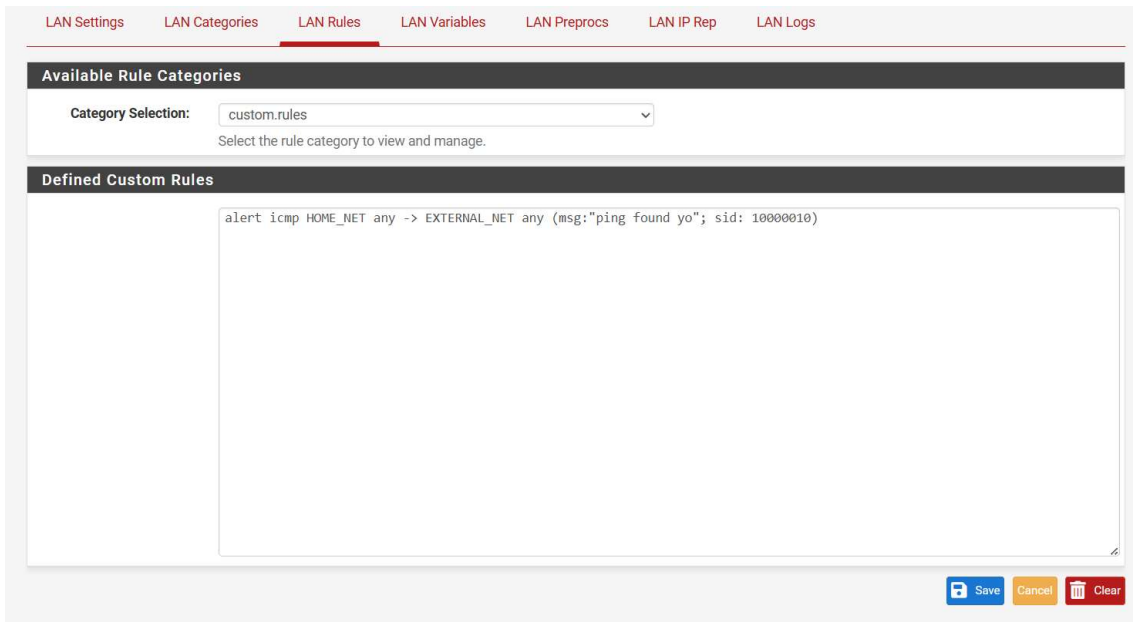
Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

Alert Settings

Send Alerts to System Log

☒ Snort will send Alerts to the firewall's system log. Default is Not Checked.

Hình 3. 30. Chọn cổng LAN và bật tính năng alert



Hình 3. 31. Viết rule custom

Interface Settings Overview						
	Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/>	WAN (em0)	 	AC-BNFA	DISABLED	WAN	 
<input type="checkbox"/>	LAN (em1)	  	AC-BNFA	DISABLED	LAN	 

Hình 3. 32. Kích hoạt rule

```
C:\Users\Ngoc Dai>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=57ms TTL=128
Reply from 8.8.8.8: bytes=32 time=56ms TTL=128
Reply from 8.8.8.8: bytes=32 time=56ms TTL=128
Reply from 8.8.8.8: bytes=32 time=57ms TTL=128

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 56ms, Maximum = 57ms, Average = 56ms

C:\Users\Ngoc Dai>
```

Hình 3. 33. Tiến hành ping

Alert Log View Settings

Interface to Inspect

LAN (em1)

Choose interface..

☐

Auto-refresh view

250

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

5 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-11-21 01:04:33	<div></div>	0			fe80::20c:29ff:fef5:4d96		ff02::1		1:10000010	ping found yo
2024-11-21 01:03:12	<div></div>	0	ICMP		192.168.1.10		8.8.8.8		1:10000010	ping found yo
2024-11-21 01:03:11	<div></div>	0	ICMP		192.168.1.10		8.8.8.8		1:10000010	ping found yo
2024-11-21 01:03:10	<div></div>	0	ICMP		192.168.1.10		8.8.8.8		1:10000010	ping found yo
2024-11-21 01:03:09	<div></div>	0	ICMP		192.168.1.10		8.8.8.8		1:10000010	ping found yo

Hình 3. 34. Phát hiện trên log

3.5. Cài đặt và sử dụng Suricata làm IPS

Trong pfSense, mục Services / Suricata / WAN - Interface Settings

Alert and Block Settings

Block Offenders

☒ Checking this option will automatically block hosts that generate a Suricata alert.

IPS Mode

Legacy Mode

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Suricata inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Suricata can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers include: bnxt, cc, cxgbe, cxl, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

Kill States

☒ Checking this option will kill firewall states for the blocked IP. Default is Checked.

Which IP to Block

BOTH

Select which IP extracted from the packet you wish to block. Choosing BOTH is suggested, and it is the default value.

Block On DROP Only

☒ Checking this option will insert blocks only when rule signatures having the DROP action are triggered. When not checked, any rule action (ALERT or DROP) will generate a block of the offending host. Default is Not Checked.

IP Pass List

default

Choose the Pass List you want this interface to use. Addresses in a Pass List are never blocked. Select "none" to prevent use of a Pass List.

The default Pass List adds Gateways, DNS servers, locally-attached networks, the WAN IP, VPNs and VIPs. Create a Pass List with an alias to customize whitelisted IP addresses. This option will only be used when block offenders is on. Choosing "none" will disable Pass List generation.

View List

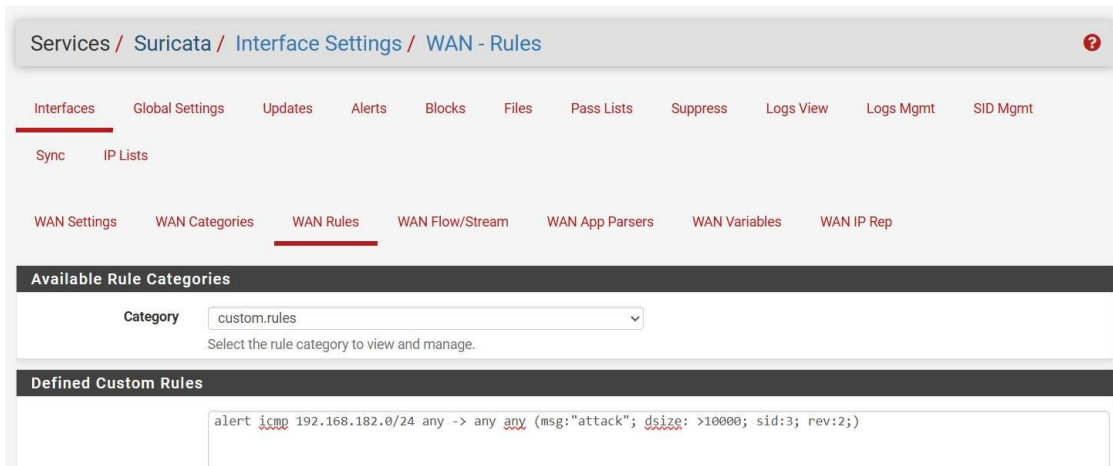
Enable Passlist Debugging Log

☐ Checking this option will enable detailed Passlist operations logging to file /var/log/suricata/suricata\_em052736/passlist\_debug.log. Default is Not Checked.

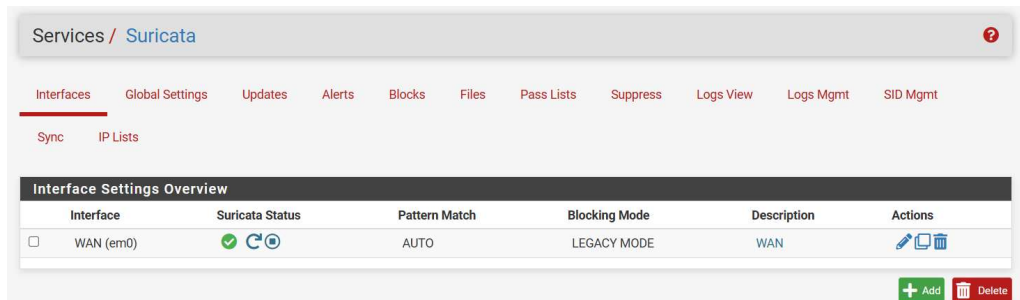
Performance and Detection Engine Settings

Hình 3. 35. Bật chế độ IPS

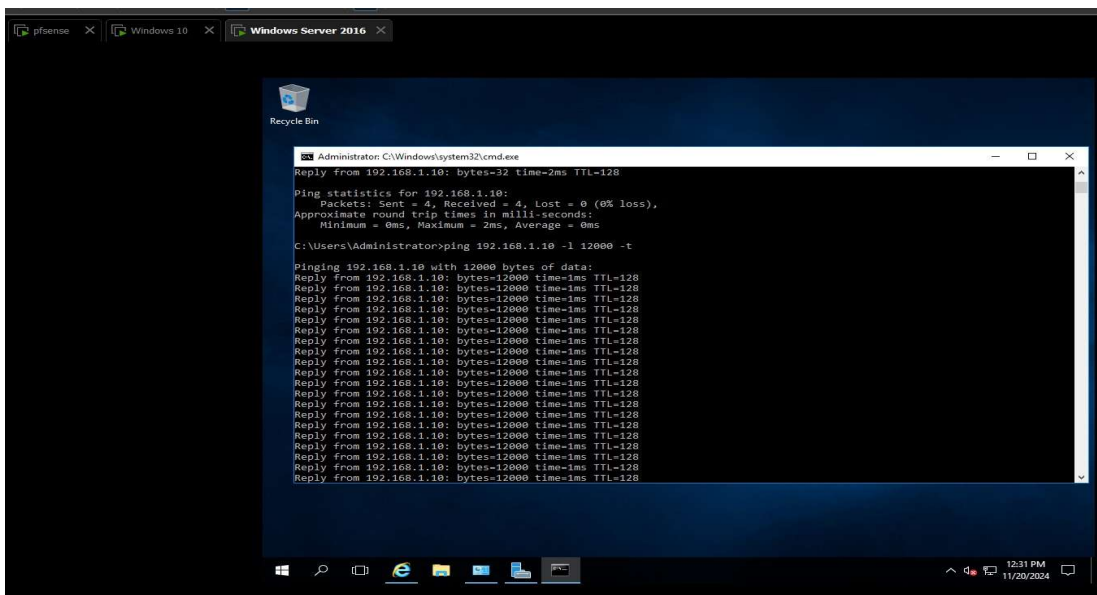
Trong Services / Suricata / Interface Settings / WAN - Rules



Hình 3. 36. Tạo 1 rule để alert các gói icmp



Hình 3. 37. Đảm bảo rule đã được kích hoạt



Hình 3. 38. Tiến hành tấn công

Services / Suricata / Alerts

Interfaces

Global Settings

Updates

Alerts

Blocks

Files

Pass Lists

Suppress

Logs View

Logs Mgmt

SID Mgmt

Sync

IP Lists

Alert Log View Settings

Instance to View

(WAN) WAN

Choose which instance alerts you want to inspect.

Save or Remove Logs

Download

All alert log files for selected interface will be downloaded

Clear

Clear the currently active Alerts log file

Save Settings

Save

Save auto-refresh and view settings

Refresh

Default is ON

250

Number of alerts to display. Default is 250

Alert Log View Filter

Last 250 Alert Entries. (Most recent entries are listed first)

Note: Alerts triggered by DROP rules that resulted in dropped (blocked) packets are shown with highlighted rows below.

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
11/21/2024 03:31:19	⚠	3	ICMP	Not Assigned	192.168.182.173	8	192.168.1.10	0	1:3	attack
11/21/2024 03:31:18	⚠	3	ICMP	Not Assigned	192.168.182.173	8	192.168.1.10	0	1:3	attack
11/21/2024 03:31:17	⚠	3	ICMP	Not Assigned	192.168.182.173	8	192.168.1.10	0	1:3	attack
11/21/2024 03:31:16	⚠	3	ICMP	Not Assigned	192.168.182.173	8	192.168.1.10	0	1:3	attack
11/21/2024 03:31:15	⚠	3	ICMP	Not Assigned	192.168.182.173	8	192.168.1.10	0	1:3	attack
11/21/2024	⚠	3	ICMP	Not Assigned	192.168.182.173	8	192.168.1.10	0	1:3	attack

Hình 3. 39. Log phát hiện tấn công

Services / Suricata / Interface Settings / WAN - Rules

Interfaces

Global Settings

Updates

Alerts

Blocks

Files

Pass Lists

Suppress

Logs View

Logs Mgmt

SID Mgmt

Sync

IP Lists

WAN Settings

WAN Categories

WAN Rules

WAN Flow/Stream

WAN App Parsers

WAN Variables

WAN IP Rep

Available Rule Categories

Category

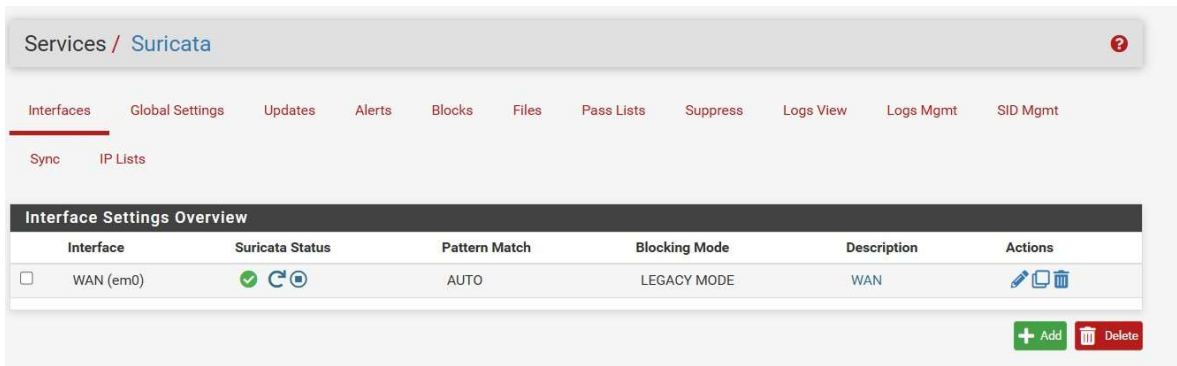
custom.rules

Select the rule category to view and manage.

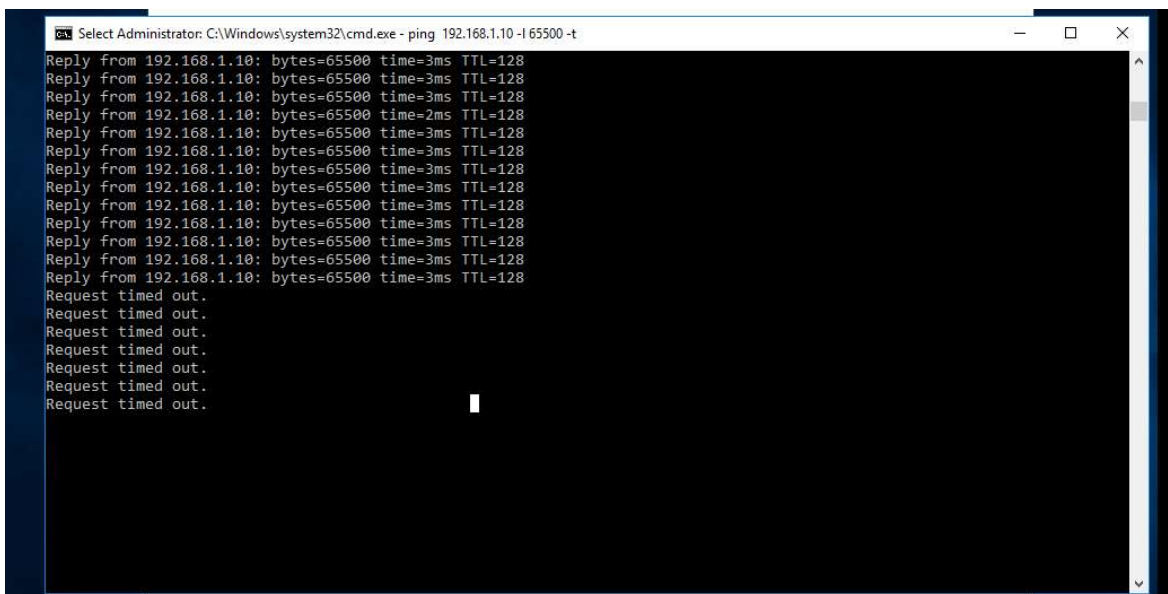
Defined Custom Rules

```
drop icmp 192.168.182.0/24 any -> any (msg:"attack"; dsize: >10000; sid:3; rev:2;)
```

Hình 3. 40. Sửa rule alert ☐ drop để chặn các gói tấn công



Hình 3. 41. Reset và đảm bảo rule đã được kích hoạt



Hình 3. 42. Lệnh tấn công xuất hiện gói bị drop

Services / Suricata / Alerts

InterfacesGlobal SettingsUpdatesAlertsBlocksFilesPass ListsSuppressLogs ViewLogs MgmtSID Mgmt

SyncIP Lists

Alert Log View Settings

Instance to View

(WAN) WAN

Choose which instance alerts you want to inspect.

Save or Remove Logs

Download

All alert log files for selected interface will be downloaded

Clear

Clear the currently active Alerts log file

Save Settings

Save

Save auto-refresh and view settings

Refresh

Default is ON

250

Number of alerts to display. Default is 250

Alert Log View Filter

Last 250 Alert Entries. (Most recent entries are listed first)

Note: Alerts triggered by DROP rules that resulted in dropped (blocked) packets are shown with highlighted rows below.

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
11/21/2024 03:37:17	🔴	3	ICMP	Not Assigned	192.168.182.173 🔍 ⛔	8	192.168.1.10 🔍 ⛔	0	1:3 🔍 ⛔	attack
11/21/2024 03:37:17	🔴	3	ICMP	Not Assigned	192.168.182.173 🔍 ⛔	8	192.168.1.10 🔍 ⛔	0	1:3 🔍 ⛔	attack
11/21/2024 03:37:16	🔴	3	ICMP	Not Assigned	192.168.182.173 🔍 ⛔	8	192.168.1.10 🔍 ⛔	0	1:3 🔍 ⛔	attack
11/21/2024 03:37:16	🔴	3	ICMP	Not Assigned	192.168.182.173 🔍 ⛔	8	192.168.1.10 🔍 ⛔	0	1:3 🔍 ⛔	attack

Hình 3. 43. Log drop

Services / Suricata / Blocked Hosts

InterfacesGlobal SettingsUpdatesAlertsBlocksFilesPass ListsSuppressLogs ViewLogs MgmtSID Mgmt

SyncIP Lists

Blocked Hosts Log View Settings

Save or Remove Hosts

Download

All blocked hosts will be saved

Clear

Clear the currently active Alerts log file

Save Settings

Save

Save auto-refresh and view settings

Refresh

Default is ON

500

Number of blocked entries to view. Default is 500

Last 500 Hosts Blocked by Suricata

Note: Only blocked IP addresses from Legacy Mode interfaces are shown! For inline IPS mode interfaces, dropped IP addresses are highlighted on the ALERTS tab.

Blocked IP	Block Date/Time	Block Alert Description	Block Rule GID:SID	Remove Block
192.168.182.173 🔍	11/21/2024 03:36:47	attack	1:3	⛔

1 host IP address is currently being blocked.

Hình 3. 44. Xuất hiện ip bị block trong Services / Suricata / Blocked Hosts

3.6. Triển khai DDNS



## Sử dụng CloudFlare để tạo 1 record mới cho tên miền pfsense.ailln.id.vn

DNS management for **ailln.id.vn**

Review, add, and edit DNS records. Edits will go into effect once saved.

DNS Setup: Full ⓘ Import and Export ▾ ⚙ Dashboard Display Settings

Search DNS Records

▼ Add filter

Search

+ Add record

<input type="checkbox"/>	Type ⓘ	Name ⓘ	Content ⓘ	Proxy status ⓘ	TTL ⓘ	Actions
<input type="checkbox"/>	A	pfsense	1.1.1.1	DNS only - reserved IP	Auto	Edit ▶

Hình 3. 45. Record mới

## Truy cập trang Cloudflare API Token để tạo 1 token mới.

### User API Tokens

API Tokens

Manage access and permissions for your accounts, sites, and products

Create Token

Token name	Permissions	Resources	Status
------------	-------------	-----------	--------

Hình 3. 46. Nhấn Create Token

### User API Tokens

[← Back to view all tokens](#)

#### Create Token

Token name: Edit zone DNS [✎](#)

#### Permissions

Select edit or read permissions to apply to your accounts or websites for this token.

Zone ▾

DNS ▾

Edit ▾

[+ Add more](#)

#### Zone Resources

Select zones to include or exclude.

Include ▾

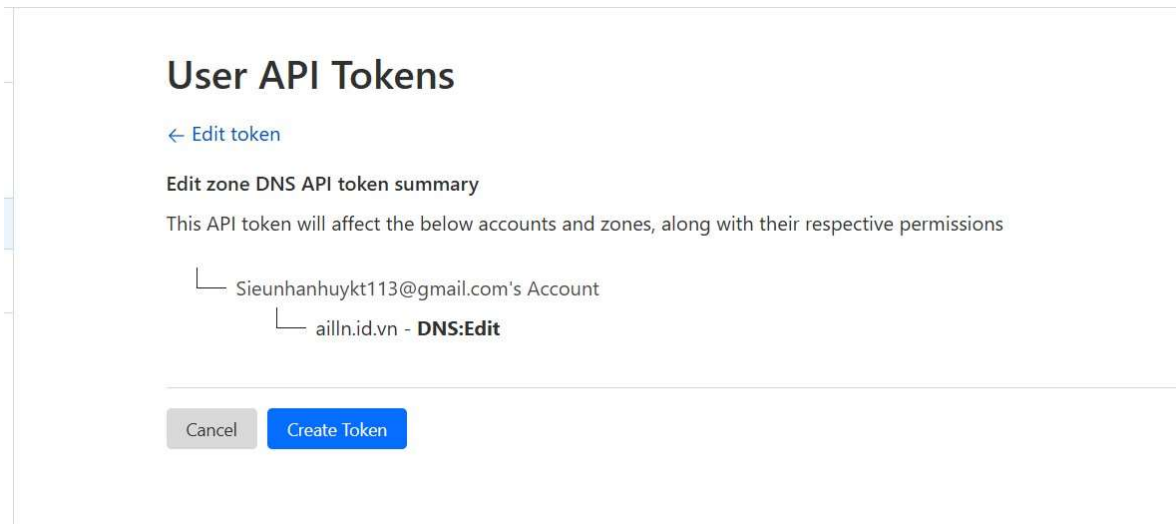
Specific zone ▾

ailln.id.vn ▾

[+ Add more](#)

Hình 3. 47. Chọn Edit zone DNS □ User API Tokens □ chọn tên miền cần dùng





Hình 3. 48. Continue to summary và chọn Create Token

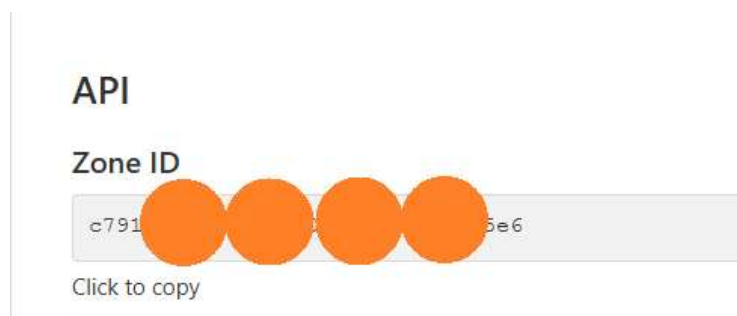
## User API Tokens

Edit zone DNS API token was successfully created

Copy this token to access the Cloudflare API. For security this will not be shown again. [learn more](#)

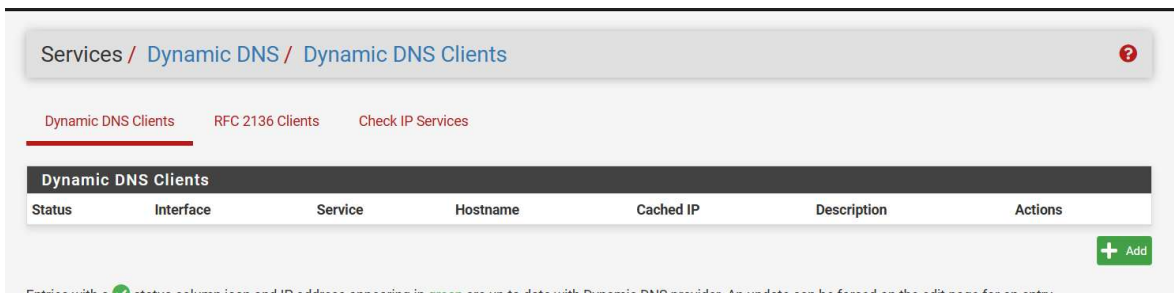


Hình 3. 49. Sau đó copy token mới và để vào một vùng khác



Hình 3. 50. Tìm kiếm thông tin Zone id

Trong Services / Dynamic DNS / Dynamic DNS Clients



Hình 3. 51. Chọn add để tạo mới DDNS





Hình 3. 52. Nhập các thông số như hình


Username: nhập Zone ID của tên miền.

Password: nhập vào API Token của


Cloudflare.

Hình 3. 53. Ấn save để lưu lại

Dynamic DNS Clients    RFC 2136 Clients    Check IP Services						
Dynamic DNS Clients						
Status	Interface	Service	Hostname	Cached IP	Description	Actions
✓	WAN	Cloudflare	pfsense.ailln.id.vn	103.38.180.246	dns	  
 Add						

Entries with a  status column icon and IP address appearing in **green** are up to date with Dynamic DNS provider. An update can be forced on the edit page for an entry.

Hình 3. 54. Xuất hiện ip mới trong pfSense

Type	Name	Content	Proxy status	TTL	Actions
<input type="checkbox"/> A	pfsense	103.38.180.246	 Proxied	Auto	<a href="#">Edit</a>

Type

Name (required)

IPv4 address (required)


Proxy status

TTL

A

pfsense

103.38.180.246

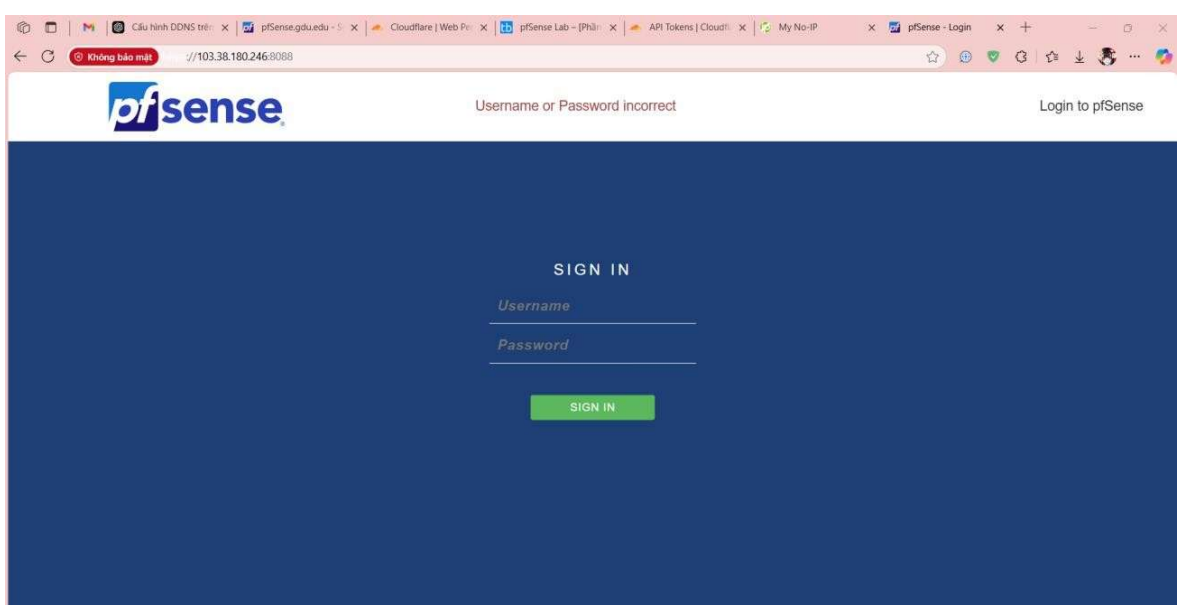
☒  Proxied

Auto

Use @ for root

This hostname is not covered by a certificate. To ensure full coverage, purchase [Advanced Certificate Manager](#) to use Total TLS for full certificate

Hình 3. 55. Xuất hiện ip mới trong CloudFlare



Hình 3. 56. Truy cập vào địa chỉ ip

## CHƯƠNG 4. KẾT LUẬN

### 4.1. Kiểm tra và phân tích hoạt động của hệ thống IDS/IPS

Trong bối cảnh an ninh mạng ngày càng trở nên phức tạp, việc kiểm tra và phân tích hoạt động của hệ thống IDS (Intrusion Detection System) và IPS (Intrusion Prevention System) đóng vai trò cực kỳ quan trọng. Hệ thống IDS/IPS được thiết kế để giám sát và phân tích lưu lượng mạng nhằm phát hiện các hành vi bất thường hoặc có thể gây hại cho hệ thống.

Quá trình kiểm tra bắt đầu bằng việc thu thập dữ liệu từ các nguồn khác nhau như nhật ký hệ thống, lưu lượng mạng và các báo cáo từ người dùng. Việc phân tích dữ liệu này giúp xác định các mẫu tấn công, xu hướng và các điểm yếu trong hệ thống. Các công cụ phân tích hiện đại sử dụng các thuật toán học máy để nhận diện các hành vi bất thường, từ đó cải thiện khả năng phát hiện và ngăn chặn các cuộc tấn công.

Một yếu tố quan trọng trong việc đánh giá hiệu quả của hệ thống IDS/IPS là tỷ lệ phát hiện (True Positive Rate) và tỷ lệ báo động giả (False Positive Rate). Tỷ lệ phát hiện cao cho thấy hệ thống có khả năng phát hiện đúng các cuộc tấn công, trong khi tỷ lệ báo động giả thấp cho thấy hệ thống không gây ra quá nhiều cảnh báo sai, giúp giảm thiểu sự can thiệp không cần thiết vào hoạt động của người dùng.

### 4.2. Đánh giá hiệu quả bảo mật trong môi trường mạng ngoài

Môi trường mạng ngoài bao gồm các yếu tố như Internet, các kết nối từ xa và các thiết bị di động, tất cả đều có thể tạo ra những lỗ hổng bảo mật nghiêm trọng. Để đánh giá hiệu quả bảo mật trong môi trường này, cần phải xem xét các biện pháp bảo vệ hiện có, chẳng hạn như tường lửa, mã hóa dữ liệu và các chính sách xác thực người dùng.

Một trong những thách thức lớn nhất trong môi trường mạng ngoài là việc bảo vệ dữ liệu nhạy cảm trong khi vẫn đảm bảo tính khả dụng và hiệu

suất của hệ thống. Các cuộc tấn công từ chối dịch vụ (DDoS) có thể làm gián đoạn hoạt động của hệ thống, trong khi các cuộc tấn công khai thác lỗ hổng phần mềm có thể dẫn

đến rõ ràng dữ liệu. Đánh giá hiệu quả bảo mật trong môi trường này đòi hỏi một cách tiếp cận toàn diện, bao gồm việc thường xuyên kiểm tra lỗ hổng, cập nhật phần mềm và đào tạo nhân viên về an ninh mạng.

#### 4.3. Kết luận và hướng phát triển

Từ những phân tích trên, có thể thấy rằng hệ thống IDS/IPS đóng vai trò quan trọng trong việc bảo vệ mạng lưới khỏi các mối đe dọa tiềm tàng. Tuy nhiên, với sự phát triển không ngừng của công nghệ và các phương thức tấn công mới, hệ thống này cần được cải tiến liên tục. Hướng phát triển trong tương lai có thể bao gồm việc tích hợp trí tuệ nhân tạo để nâng cao khả năng phát hiện và phản ứng nhanh chóng đối với các cuộc tấn công.

Ngoài ra, việc xây dựng một hệ thống bảo mật đa lớp sẽ giúp tăng cường khả năng phòng thủ, từ việc sử dụng các giải pháp bảo mật phần mềm đến việc triển khai các biện pháp bảo vệ vật lý. Sự hợp tác giữa các tổ chức và chia sẻ thông tin về các mối đe dọa cũng sẽ là yếu tố then chốt trong việc nâng cao hiệu quả bảo mật toàn diện.

#### 4.4. Đề xuất các biện pháp cải tiến bảo mật hệ thống trong tương lai

Để cải tiến bảo mật hệ thống trong tương lai, một số biện pháp có thể được đề xuất như sau:

Tăng cường đào tạo nhân viên: Nhân viên là một trong những yếu tố quan trọng nhất trong việc bảo vệ hệ thống. Việc tổ chức các khóa đào tạo thường xuyên về an ninh mạng sẽ giúp họ nhận thức rõ hơn về các mối đe dọa và cách phòng tránh.

Triển khai giải pháp bảo mật tích hợp: Sử dụng các giải pháp bảo mật tích hợp giúp giảm thiểu lỗ hổng và tối ưu hóa quy trình bảo vệ. Các công cụ như SIEM (Security Information and Event Management) có thể giúp theo dõi và phân tích các sự kiện bảo mật trong thời gian thực.

Cập nhật và vá lỗi phần mềm thường xuyên: Việc duy trì các bản cập



nhật mới nhất cho phần mềm và hệ điều hành giúp bảo vệ hệ thống khỏi các  
lỗ hổng đã biết.

Xây dựng kế hoạch ứng phó sự cố: Một kế hoạch ứng phó sự cố chi tiết sẽ giúp tổ chức phản ứng nhanh chóng và hiệu quả khi xảy ra các sự cố bảo mật, từ đó giảm thiểu thiệt hại.

Đánh giá định kỳ và kiểm tra lỗ hổng: Thực hiện các cuộc kiểm tra lỗ hổng định kỳ sẽ giúp phát hiện và khắc phục các điểm yếu trong hệ thống trước khi chúng bị khai thác bởi kẻ tấn công.

Tóm lại, việc cải thiện bảo mật hệ thống là một quá trình liên tục và cần sự chú ý từ tất cả các bên liên quan. Chỉ khi có sự đầu tư đúng mức vào công nghệ, con người và quy trình, tổ chức mới có thể đảm bảo an toàn cho dữ liệu và hệ thống của mình trong một thế giới ngày càng đầy rẫy