

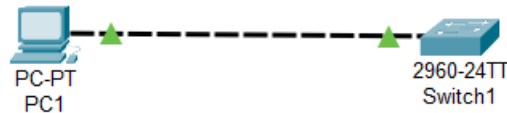
BÁO CÁO LAB 3: LAN SECURITY

1. Port Security

a. Giới thiệu

- Thông qua giới hạn và kiểm soát các thiết bị kết nối và Switch, người quản trị có thể hạn chế nhiều loại tấn công trong LAN.

b. Topology



c. Mục tiêu

- Kiểm soát các thiết bị người dùng cố định nhằm tránh sự thay đổi tự do của người dùng trong quá trình vận hành hệ thống.

d. Kịch bản

- Cấu hình sao cho chỉ có client với địa chỉ MAC của PC1 được kết nối đến port Gi0/1 của Switch1
- Nếu một client khác gắn vào port Gi0/1 của Switch1 thì port này sẽ shutdown.

e. Thực hiện

- Cấu hình port security với PC1 MAC là 00D0.9703.4E57
 - Switch(config)#interface gi0/1
 - Switch(config-if)#switchport mode access
- Gán địa chỉ MAC được phép vào port gi0/1
 - Switch(config-if)#switchport port-security mac-address 00D0.9703.4E57
- Giới hạn số lượng thiết bị mà port này cho phép là 1 (có nghĩa chỉ PC1 là được kết nối)
 - Switch(config-if)#switchport port-security maximum 1
- Nếu muốn để cho switch học tự động thì dùng câu lệnh sau
 - Switch(config-if)#switchport port-security mac-address sticky
- Cấu hình client khác gắn vào port Gi0/1 thì port này sẽ bị shutdown
 - Switch(config-if)#interface gi0/1
 - Switch(config-if)#switchport port-security violation shutdown

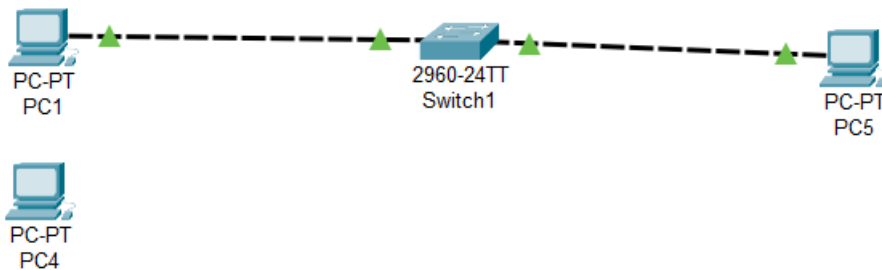
f. Kiểm tra

- Kiểm tra cấu hình port-security của gi0/1
 - Switch#show port-security interface gi0/1

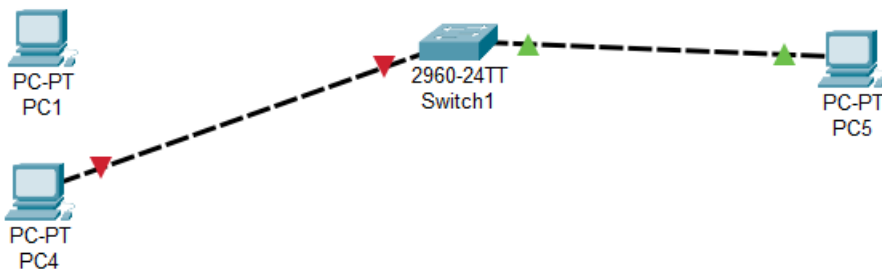
- Kết quả thu được:

```
Switch#sh port-security interface gi0/1
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
Configured MAC Addresses : 1
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

- Thử thay một client khác vào và xem kết quả, nhưng trước tiên cần đặt địa chỉ ip cho PC1 là 192.168.1.1 và PC4 (client không được cấp phép) 192.168.1.2 và một PC5 có ip là 192.168.1.3 để kiểm tra.
 - Khi PC1 kết nối với SW1, sau đó ping từ PC1 đến PC5



- Khi PC4 (client không được cấp phép) kết nối với SW1, sau đó ping từ PC4 đến PC5



g. Phân tích

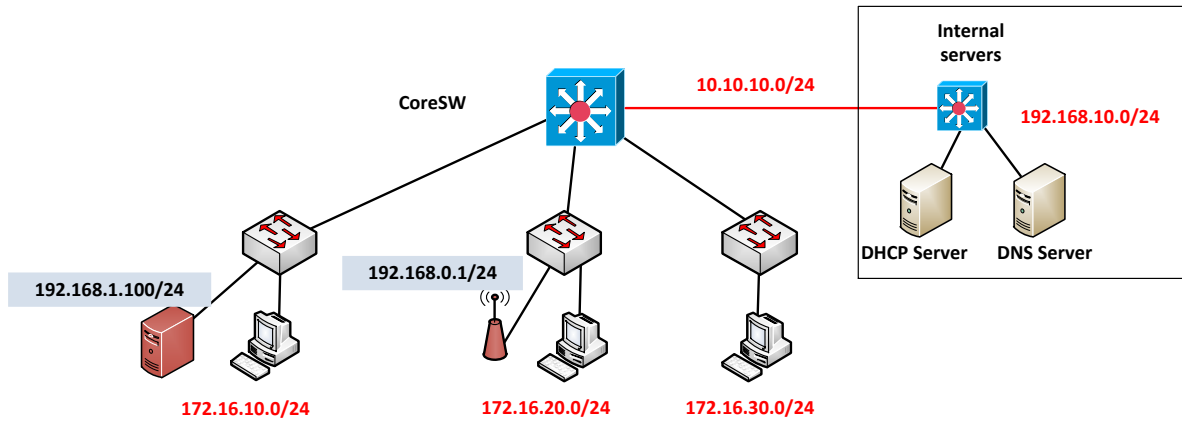
- Khi kết nối đến một client không được phép thì port đang kết nối sẽ bị tắt, việc này ngăn chặn được người dùng tự ý kết nối với các client không an toàn hoặc tự ý mở rộng mạng.
- Nếu như ta chỉ kết nối client với switch bình thường thì khi quan sát tín hiệu đèn sẽ nhận thấy là dù kết nối vào client nào thì tín hiệu vẫn là màu xanh. Vì vậy cần thực hiện trao đổi gói tin, trong trường hợp này là ping sang một client cùng mạng thì ta sẽ thấy port security hoạt động.
- Trong thực tế, trên switch ta có thể cài đặt chế độ tự hoạt động trở lại sau một khoảng thời gian trên port bị tắt của switch. Tuy nhiên trong Cisco Packet Tracer ta phải bật thủ công.

2. DHCP Snooping

a. Giới thiệu

- DHCP Snooping ngăn chặn các mối nguy cơ với hệ thống mạng tiêu biểu như man-in-the-middle.

b. Topology



c. Mục tiêu

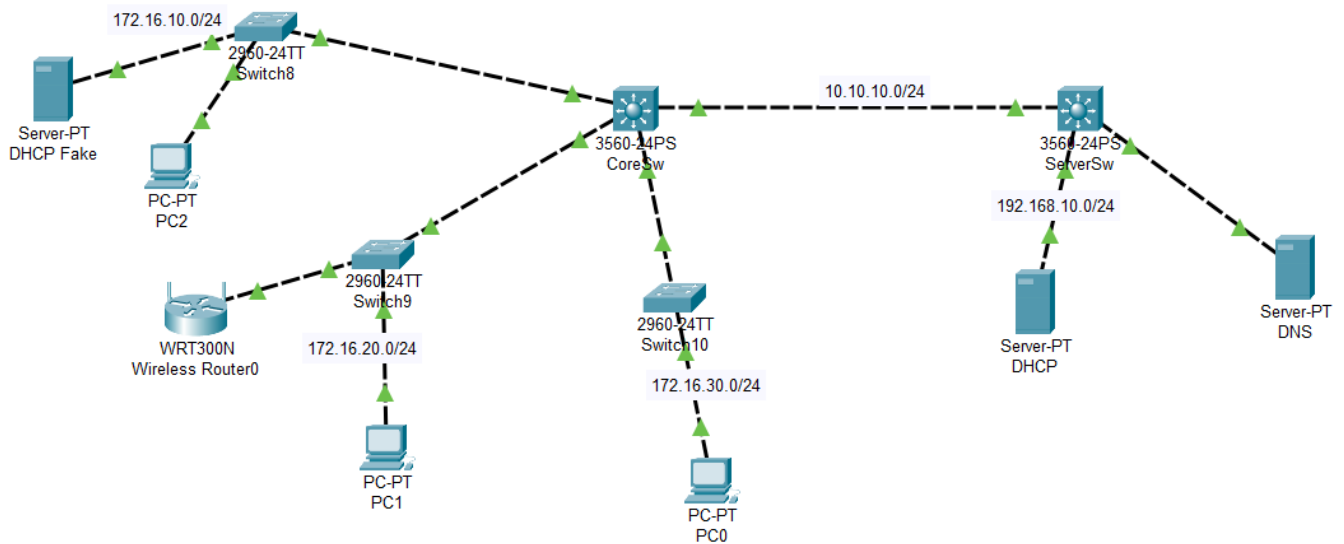
- Cho phép switch tin tưởng port được kết nối đến DHCP Server và không tin tưởng các port khác, thông qua triển khai DHCP Snooping.

d. Kịch bản

- Cấu hình theo topology trên
 - Cấu hình định tuyến
 - Cấu hình cho DHCP server cấp phát địa chỉ IP động cho các PC ở các mạng 172.16.10.0/24, 172.16.20.0/24, 172.16.30.0/24
- Thử trường hợp các DHCP server giả và AP cấp IP động
- Cấu hình DHCP snooping trên Switch, sao cho các client chỉ xin địa chỉ IP từ DHCP trên DHCP Server thật.

e. Thực hiện

- Xây dựng topology như trên:
 - Cấp địa chỉ ip theo các mạng đã đặt trên hình
 - Đặt địa chỉ ip cho các interface
 - Cấu hình định tuyến tĩnh trên CoreSw và ServerSw



- Kiểm tra định tuyến tĩnh bằng việc ping từ DHCP Server đến PC0 (PC0 ta đặt 1 địa chỉ ip tĩnh) hoặc lệnh: Switch#show ip route

- Cấu hình DHCP để cấp phát ip động.

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: Net10

Default Gateway: 172.16.10.1

DNS Server: 8.8.8.8

Start IP Address: 172 16 10 2

Subnet Mask: 255 255 255 0

Maximum Number of Users: 100

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: Net20

Default Gateway: 172.16.20.1

DNS Server: 8.8.8.8

Start IP Address: 172 16 20 2

Subnet Mask: 255 255 255 0

Maximum Number of Users: 100

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: Net30

Default Gateway: 172.16.30.1

DNS Server: 8.8.8.8

Start IP Address: 172 16 30 2

Subnet Mask: 255 255 255 0

Maximum Number of Users: 100

- Tuy nhiên, vì DHCP Server và các máy cần cấp phát ip động lại ở các broadcast domain khác nhau nên ta cần phải cấu hình Relay Agent cho CoreSw theo cú pháp:
Switch(config)# interface <port>
Switch(config-if)#ip helper-address <ip-DHCP-Server>
- Bây giờ ta thêm một DHCP Server giả mạo vào mạng 172.16.10.0/24 với ip của nó là 192.168.1.100 và cấu hình dịch vụ DHCP như sau, sau đó tiến hành kiểm tra kết quả.

DHCP Fake

Physical Config Services Desktop Programming Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

DHCP

Interface: FastEthernet0 Service: ☒ On ☐ Off

Pool Name: serverPool

Default Gateway: 192.168.1.100

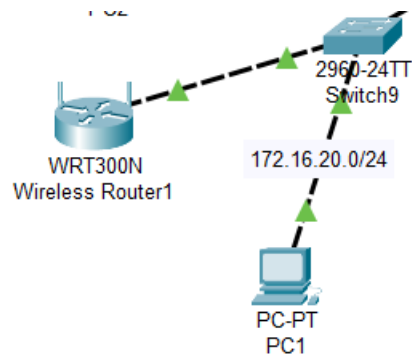
DNS Server: 192.168.1.100

Start IP Address: 192 168 1 40

Subnet Mask: 255 255 255 0

Maximum Number of Users: 100

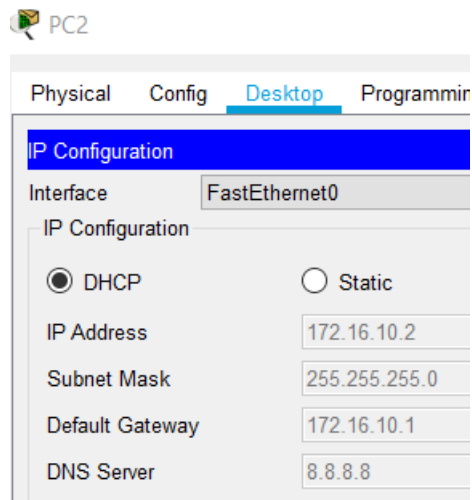
- Tiếp theo ta thêm 1 Access Point vào mạng 172.16.20.0/24, lưu ý rằng khi kết nối switch với access point thì ta nên kết nối qua cổng Ethernet để có thể cho ra kết quả thí nghiệm như mong muốn. Ngoài ra ta không cần cấu hình gì thêm lên Access Point này.



- Cấu hình DHCP Snooping cho các Switch kết nối với thiết bị cuối (end device), ta không cần phải cấu hình DHCP Snooping cho CoreSw hay ServerSw. Cụ thể ta sẽ cấu hình trên Switch8, Switch9, Switch10.
- Cú pháp
 - Switch(config)#ip dhcp snooping
 - Switch(config)#ip dhcp snooping vlan 1
 - Switch(config)#no ip dhcp snooping information option
 - Switch(config)#interface <interface> (port kết nối hoặc port hướng kết nối về DHCP thật)
 - Switch(config-if)#ip dhcp snooping trust
 - Switch(config-if)#exit
- Kiểm tra DHCP Snooping bằng cú pháp: Switch(config-if)#show ip dhcp snooping

f. Kiểm tra

- Kiểm tra cấp phát ip động khi chưa có DHCP Server giả mạo hay Access Point, ta thấy dịch vụ DHCP hoạt động bình thường.



- Sau khi đã cấu hình DHCP giả mạo trên mạng 172.16.10.2 thì ta tiến hành xin cấp ip lại cho PC2, ta thấy PC2 đã xin cấp phát ip từ DHCP Server giả mạo

PC1

Physical Config **Desktop** Programming

IP Configuration

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static

IP Address 192.168.0.100

Subnet Mask 255.255.255.0

Default Gateway 192.168.0.1

DNS Server 0.0.0.0

- Sau khi thêm Access point vào mạng 172.16.10.2, ta xin cấp địa chỉ ip động trên PC1 một lần nữa thì chúng ta thu được kết quả PC1 đã được Access Point cấp phát địa chỉ ip.

PC2

Physical Config **Desktop** Programming

IP Configuration

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static

IP Address 192.168.1.41

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.100

DNS Server 192.168.1.100

- Sau khi cấu hình DHCP Snooping , ta tiến hành xin cấp lại phát địa chỉ ip động trên PC1 và PC2. Ta thấy PC1 và PC2 đã xin cấp phát từ đúng DHCP Server thật.

Physical Config **Desktop** Programming

IP Configuration

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static

IP Address 172.16.10.36

Subnet Mask 255.255.255.0

Default Gateway 172.16.10.1

DNS Server 8.8.8.8

PC1

Physical Config **Desktop** Programming

IP Configuration

Interface FastEthernet0

IP Configuration

☒ DHCP ☐ Static

IP Address 172.16.20.7

Subnet Mask 255.255.255.0

Default Gateway 172.16.20.1

DNS Server 8.8.8.8

g. Phân tích

- Cơ chế của các giả mạo DHCP là các DHCP giả mạo sẽ trả lời thông điệp DHCPDISCOVER trước khi DHCP server thật trả lời, từ đó cấp phát cho client: IP, Subnet Mask, Default Gateway và đặc biệt là DNS server giả mạo từ đó nghe lén các thông tin truyền đi.
- Trường hợp thứ hai phổ biến hơn, khi người dùng kết nối thêm một access point vào mạng và vô tình quên tắt chức năng DHCP trên access point này thì khi một máy trong mạng xin địa chỉ IP thì có thể không nhận được địa chỉ IP từ DHCP Server thật.

h. Giải pháp

- Ngoài phương án sử dụng DHCP Snooping ra thì ta còn cần phải kết hợp với Port-Security để ngăn chặn người dùng mở rộng mạng một cách trái phép. Thêm vào đó khi lắp đặt Access Point cũng cần lưu ý yêu cầu người lắp đặt tắt chức năng DHCP trên thiết bị.

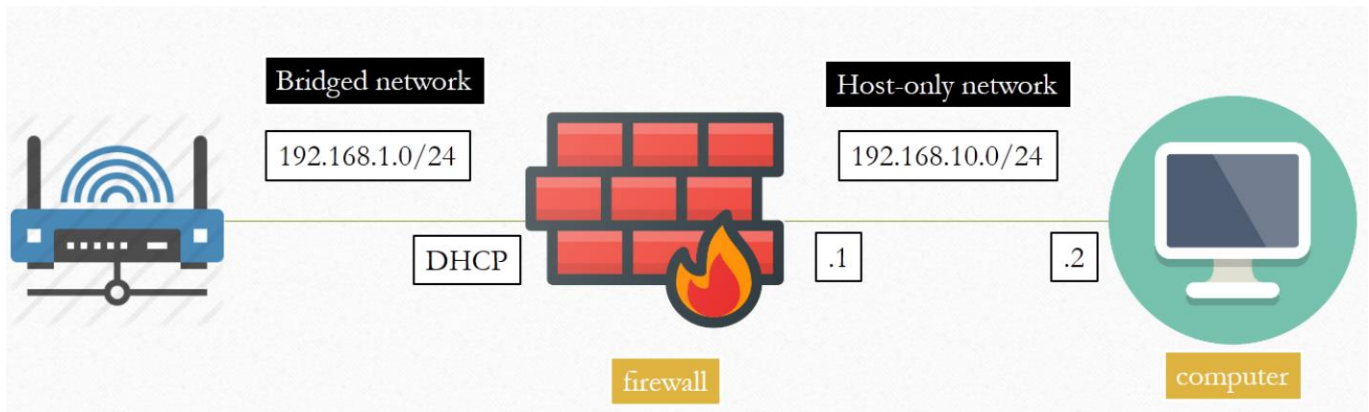
3. Firewall

a. Giới thiệu

- Không gian internet là một không gian không an toàn, mọi hoạt động trao đổi giao tiếp trên mạng đều có thể trở thành mục tiêu tấn công của hacker đặc biệt đây là mối đe dọa rất lớn đến

các hệ thống mạng nội bộ của doanh nghiệp. Vì vậy Firewall ra đời như là một công cụ giúp bảo vệ hệ thống mạng nội bộ cho thông qua việc ngăn chặn các truy cập trái phép, cho phép thiết lập các chính sách bảo mật,...

b. Toplogy



c. Mục tiêu

- Cho phép các PC bên trong mạng nội bộ ra ngoài Internet
- Kiểm soát truy cập Web
- Kiểm soát port truy cập
- Kiểm soát ứng dụng truy cập
- Thực hiện các phương thức khác

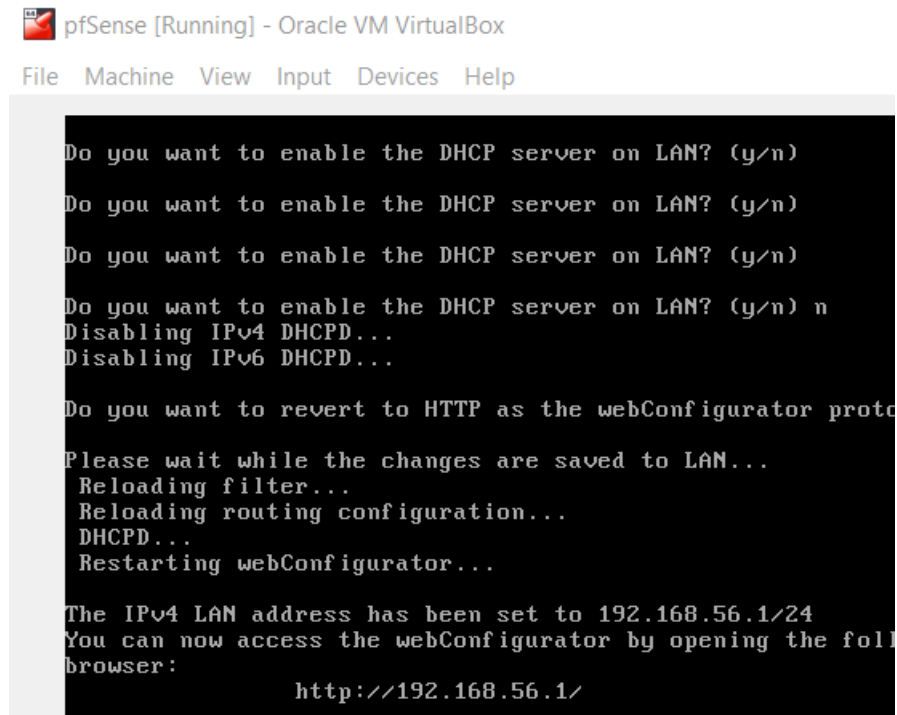
d. Kịch bản

- Cài đặt pfSense trên VirtualBox.
- Cấu hình địa chỉ ip cho 2 card mạng của Firewall.
- Thêm định tuyến tĩnh trên máy host.
- Đăng nhập vào pfSense Web Configuration, sau đó tạo rule:
 - Cho phép DNS
 - Cho phép lướt web
 - Chặn một trang web

e. Thực hiện

- Cài đặt pfSense trên VirtualBox.
- Tùy chỉnh trên máy ảo pfSense:
 - Adapter1 → Attached to: Bridged Adapter
 - Adapter2 → Attached to: Host-only Adapter
 - Nếu chưa có Host-only Adapter thì ta có thể tạo một network mới ở mục File → Host Network Manager
- Tùy chỉnh trên máy ảo đóng vai trò Host (Linux Mint)
 - Adapter1 → Attached to: Bridged Adapter
- Cấu hình LAN interface trên Firewall
 - Chọn cấu hình LAN interface
 - Đặt địa chỉ ip tĩnh cho LAN interface là 192.168.56.1/24 (Cần chú ý rằng địa chỉ ip đặt cho LAN interface phải chung đường mạng với Host-only Network)
 - Cho phép cấu hình Firewall thông qua giao thức HTTP

- Kết quả:



```

pfSense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

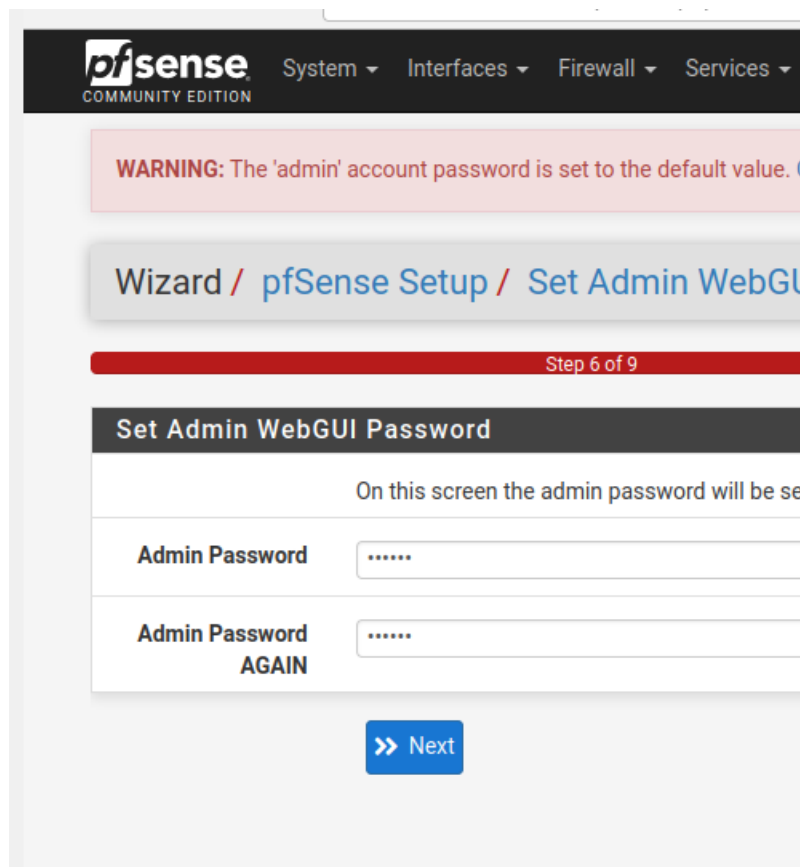
Do you want to enable the DHCP server on LAN? (y/n)
Do you want to enable the DHCP server on LAN? (y/n)
Do you want to enable the DHCP server on LAN? (y/n)
Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n)
Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
Restarting webConfigurator...

The IPv4 LAN address has been set to 192.168.56.1/24
You can now access the webConfigurator by opening the following browser:
http://192.168.56.1/

```

- Đăng nhập vào pfSense Web Configuration
- Chọn “Next” để bỏ qua các bước nhập thông tin, sau đó nhập password mới.



- Cấu hình static route cho máy bên trong Firewall bằng câu lệnh:
#sudo route add -net 0.0.0.0 netmask 0.0.0.0 gw 192.168.56.1
- Sau khi đã setup các thông số cho Firewall và máy bên trong, ta sẽ tiến hành tạo các rules như trên kịch bản đã đề ra.

- Xóa hai rules mặc định vì ngay sau khi cài đặt thành công thì pfSense tạo hai rules mặc định cho phép tất cả các gói tin đi qua nó. Lưu ý, sau khi xóa xong nhớ ấn Apply Changes để áp dụng những thay đổi vừa thực hiện.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	2 / 2.21 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/>	0 / 9 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input checked="" type="checkbox"/>	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add
 Add
 Delete
 Save
 Separator

- Tạo rule để truy cập đến DNS
 - Trước tiên cần thay đổi DNS server về DNS server của google là 8.8.8.8, ta cần thay đổi bằng cách chỉnh sửa tệp tin /etc/resolv.conf.

```
mint@mint:~$ sudo vi /etc/resolv.conf
```

```
# See man:systemd-resolved.service(8) for
# operation for /etc/resolv.conf.

nameserver 8.8.8.8
options edns0 trust-ad
```

- Chọn nút Add để thêm rule DNS, tùy chỉnh các thông tin bao gồm: loại IP là IP4 và IP6, protocol là TCP/UDP, port đích là DNS(53).

192.168.56.1/firewall_rules_edit.php?l=lan

Action

Pass

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) is returned to the sender, whereas with block the packet is dropped silently. In either case, the packet is not forwarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4+IPv6

Select the Internet Protocol version this rule applies to.

Protocol

TCP/UDP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

any

Display Advanced

The Source Port Range for a connection is typically random and almost never equal to the destination port. This setting must remain at its default value, any.

Destination

Destination

☐ Invert match

any

Destination Port Range

DNS (53)

From

Custom

Specify the destination port or port range for this rule.

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't forget to configure a remote syslog server (see the [Status: System Logs](#) page).

Description

A description may be entered here for administrative purposes and will be displayed in the firewall log.

Advanced Options

Display Advanced

Save

- Lưu rule vừa tạo và chú ý chọn Apply Changes
- Tạo rule cho phép lướt web

- Trước tiên cần tạo một alias bao bọc lấy hai port của web là 80 và 443. Chọn Firewall→Aliases→Add

Firewall / Aliases / Edit

Properties

Name web_ports
The name of the alias may only consist of the characters [a-z, 0-9, _]

Description
A description may be entered here for administrative purposes

Type Port(s)

Port(s)

Hint Enter ports as desired, with a single port or port range

Port 80
443

Save Add Port

- Tạo rule để lướt web, các thông số cơ bản cũng giống như rule trên, chỉ khác ở mục Destination Port.

Destination

Destination ☐ Invert match any

Destination Port Range (other) web_ports
From Custom

Specify the destination port or port range for this rule

- Chặn một trang web bất kì (Ví dụ ở đây là Quantrimang)
 - Thông thường 1 trang web có nhiều địa chỉ ip, nên ta cần có 1 alias để có thể đại diện cho tất cả các url có thể có.

Firewall / Aliases / Edit

Properties

Name
The name of the alias may only consist of the cha

Description
A description may be entered here for administrat

Type

Host(s)

Hint Enter as many hosts as desired. Hosts must be s
hostnames are periodically re-resolved and updat
such as 192.168.1.1-192.168.1.10 or a small subr
addresses will be generated.

IP or FQDN

- Lần này thay đổi Action là Block và thay đổi một chút ở mục Destination, còn các thông tin còn lại vẫn như các rule trước.

Destination

Destination ☒ Invert match

Destination Port

- Sau đó cần đưa rule này lên trước rule lướt web, vì rule này sẽ chặn trước khi rule lướt web cho phép Quantrimang có thể kết nối với máy bên trong. Có thể sử dụng kéo thả để thay đổi thứ tự các rule

Rules (Drag to Change Order)							
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	
<input checked="" type="checkbox"/>	2 / 2.87 MiB	*	*	*	LAN Address	80	
<input type="checkbox"/>	51 / 150 KiB	IPv4+6 TCP/UDP	*	*	*	53 (DNS)	
<input type="checkbox"/>	0 / 0 B	IPv4+6 TCP/UDP	*	*	! quantrimang_ url	*	
<input type="checkbox"/>	66 / 22.31 MiB	IPv4+6 TCP/UDP	*	*	*	web_ ports	

- Sau đó phải ấn Save và Apply Changes để áp dụng thứ tự này.

f. *Kiểm tra*

- Sau khi cấu hình static route cho máy host bên trong, ta cần đảm bảo rằng máy có thể ping ra mạng bên ngoài bằng lệnh #ping 8.8.8.8

```
File Edit View Search Terminal Help
mint@mint:~$ sudo route add -net 0.0.0.0 netmask 0.0.0.0 gw 192.168.56.1
mint@mint:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=61.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=63.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=63.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=61.5 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=114 time=60.8 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=114 time=93.4 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=114 time=65.4 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
rtt min/avg/max/mdev = 60.836/66.979/93.357/10.863 ms
mint@mint:~$
```

- Kiểm tra sau khi đã xóa hai rules mặc định bằng lệnh #ping 8.8.8.8, ta thấy rằng máy bên trong không thể liên lạc với mạng bên ngoài được nữa

```
mint@mint:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
^C
--- 8.8.8.8 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7164ms
```

- Trước khi tạo rule DNS thì máy bên trong không thể phân giải tên miền được

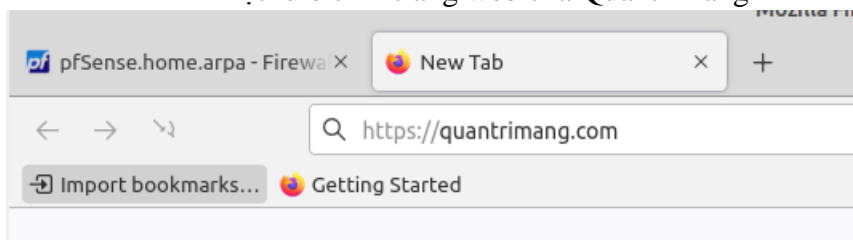
```
mint@mint:~$ nslookup google.com
;; connection timed out; no servers could be reached
```

- Kết quả sau khi tạo rule DNS

```
mint@mint:~$ nslookup google.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.194.138
Name:   google.com
Address: 172.217.194.102
Name:   google.com
Address: 172.217.194.113
```

- Kết quả sau khi tạo rule lướt Web, chúng ta đã có thể truy cập vào các trang web bình thường
- Kiểm tra sau khi đặt rule cấm trang web của Quantrimang



g. *Phân tích*

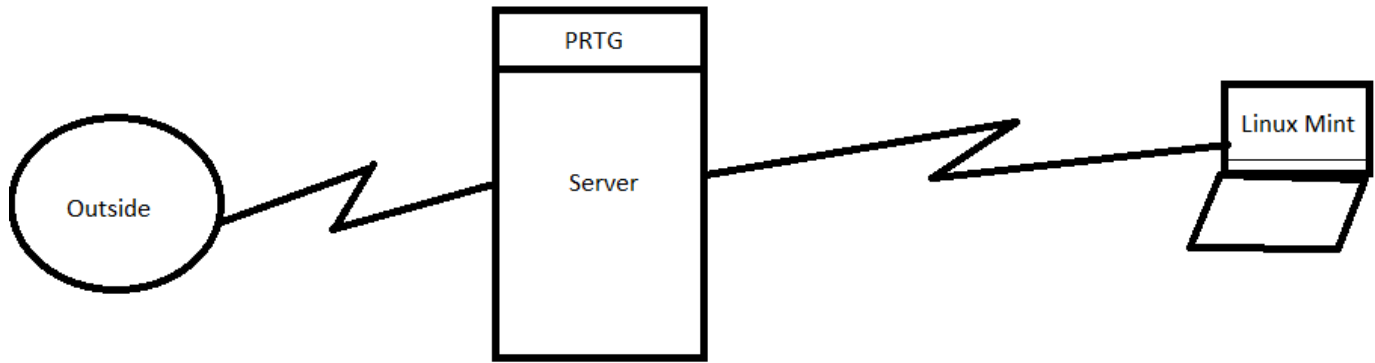
- pfSense là một firewall đơn giản và dễ sử dụng, tuy nhiên bản thân pfSense không có GUI mà chỉ có thể tương tác qua CLI, do đó ta nên sử dụng Web GUI thông qua máy Host để có thể cấu hình một cách đơn giản hơn.

4. Network Monitoring System

a. Giới thiệu

- Ngoài việc thực hiện các biện pháp an toàn trên hệ thống mạng LAN như đã được đề ra ở bên trên, chúng ta cũng cần áp dụng một hệ thống có thể cảnh báo sớm các nguy cơ về một cuộc tấn công mạng nhằm phòng ngừa các tác nhân xấu độc ảnh hưởng tới hệ thống. Network Monitoring System được xem như là một giải pháp và phần mềm được đem ra thực hành ở đây là PRTG.

b. Topology



Trong đó máy đóng vai trò theo dõi là máy Windows, máy đóng vai trò bị theo dõi là Linux Mint

c. Mục tiêu

- Thực hiện giám sát mạng với phần mềm PRTG.
- Cấu hình chức năng giám sát performance (RAM, CPU), giám sát một số dịch vụ mạng (DHCP, Web,...), giám sát dung lượng đĩa trên Server.
- Thiết lập ngưỡng cảnh báo.

d. Kịch bản

- Thêm máy cần được theo dõi vào PRTG bằng cách thêm một số thông tin
 - Địa chỉ ip
 - Username và password của máy bị theo dõi
- Thêm sensor để theo dõi thông qua SSH (cần đảm bảo rằng dịch vụ http và ssh đang chạy)
 - RAM
 - CPU
 - Dung lượng đĩa trống
 - Dịch vụ web
- Thiết lập ngưỡng cảnh báo
 - Cấu hình chuyển cảnh báo, sử dụng SMTP relay server

e. Thực hiện

- Thêm máy Linux vào làm máy bị theo dõi, nhập vào địa chỉ ip, username và password

Add a New Device

Define a device name and IP address, optional SNMP, and specific vendors, if necessary

PRTG Manual: Add a Device

Device Name and Address

Device Name ⓘ

Linux_Virtual_Machine

IP Version ⓘ

☒ IPv4

☐ IPv6

IPv4 Address/DNS Name ⓘ

192.168.1.21

Tags ⓘ

Credentials for Linux/Solaris/macOS (SSH/WBEM) Systems

☐ inherit from  Linux / macOS / Unix (User Name: <empty>, Authentication Method: 0,...)

User Name ⓘ

mint

Authentication Method ⓘ

☒ Password



☐ Private key

Password ⓘ

.....

- Thêm sensors

- Theo dõi dung lượng đĩa còn trống: chọn Target System là Linux/macOS, Technology used là SSH, sau đó chọn SSH Disk Free. Chọn đường dẫn cần theo dõi, ở đây em chọn "/" và chọn "Create"

Pos ▾	Sensor ▾	Status ▾	Message	Graph	Priority ▾	
1.	 SSH Disk Free	Up	OK	Free Bytes / 826 MB	★★★★☆	


- Làm tương tự với SSH Load Average và SSH Meminfo
- Nếu muốn theo dõi các thông tin khi lướt web, chọn Target System là Linux/macOS, Technology used là HTTP , sau đó chọn HTTP. Lưu ý, trong mục URL chuyển “https” → “http”

Pos ▼	Sensor ↕	Status ↕	Message
✚ 1.	✓ SSH Disk Free	Up	OK
✚ 2.	✓ SSH Load Average	Up	OK
✚ 3.	✓ SSH Meminfo	Up	OK

- Thiết lập ngưỡng cảnh báo
 - Đăng kí tài khoản SMTP relay server trên mailjet.
 - Cấu hình chuyển cảnh báo: Setup → Notification Delivery → Use one SMTP relay server.
 - Điền các thông tin. Chú ý rằng mục SMTP Relay Server, SMTP Relay User Name, SMTP Relay Password sẽ dựa vào thông tin tài khoản ta đã đăng kí trên mailjet.
 - Điều chỉnh Delivery Template, thêm email, điều chỉnh Access right thành Read access




Notification Templates

Object ▼

 Email and push notification to admin

- Cấu hình Trigger để khi hệ thống có sự cố thì sẽ thông báo cho chúng ta
- Chọn một sensor cần tạo trigger, chọn notification triggers
- Cấu hình bằng cách Add Trigger State

Notification Triggers

Type ^	Rule
State Trigger (ID: 1)	When sensor state is Down for at least 5 seconds, perform @ ► Email and push notification to admin 
	When sensor state is Down for at least 15 seconds, perform @ ► Email and push notification to admin  and re
	When sensor state is no longer Down, perform @ ► Email and push notification to admin 

Triggers that can be inherited from parent objects

- ☐ Inherit all triggers from parent objects and use the triggers defined above
☒ Only use the triggers defined above

f. Kiểm tra

- Kiểm tra dịch vụ ssh trên máy Linux đã được chạy hay chưa, nếu chưa có ta cần phải cài đặt bằng câu lệnh

#sudo apt-get install openssh-server

```
mint@mint:~$ sudo service sshd status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; vendor preset: enabled)
   Active: active (running) since Fri 2021-12-24 01:01:49 UTC; 1min 1s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
    Main PID: 2293 (sshd)
      Tasks: 1 (limit: 2275)
     Memory: 1.1M
    CGroup: /system.slice/ssh.service
           └─2293 sshd: /usr/sbin/sshd -D [l...
```

Dec 24 01:01:49 mint systemd[1]: Starting OpenSSH server daemon: sshd.

Dec 24 01:01:49 mint sshd[2293]: Server listening on 0.0.0.0 port 22.

- Kiểm tra dung lượng đĩa trống

- Trên máy linux

```
mint@mint:~$ sudo df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            949M   0    949M   0% /dev
tmpfs           199M  1.2M   198M   1% /run
/dev/sr0        2.0G  2.0G    0 100% /cdrom
/dev/loop0      1.9G  1.9G    0 100% /rofs
/cow            994M  169M   826M  17% /
tmpfs           994M   0    994M   0% /dev/shm
tmpfs           5.0M  4.0K   5.0M   1% /run/lock
tmpfs           994M   0    994M   0% /sys/fs/cgroup
tmpfs           994M  4.0K   994M   1% /tmp
tmpfs           199M  48K   199M   1% /run/user/999
```

- Trên PRTG



- Kiểm tra lưu lượng tải trung bình

- Trên máy Linux

```
mint@mint:~$ w
 01:57:00 up 36 min,  1 user,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
mint      tty7     :0               01:20   36:31  2.23s  0.27s mate-session
```

- Trên PRTG

Channel ▾	ID ▴	Last Value ▴	Minimum ▴	Maximum ▴
1 Minute	0	1.86	0	1.86
15 Minutes	2	0.25	0	0.25
5 Minutes	1	0.7	0	0.7
Downtime	-4			

- Kiểm tra RAM

• Trên máy Linux

```
mint@mint:~$ free
              total        used        free      shared  buff/cache   available
Mem:      2035468      425844      361256      185924      1248368      1253508
Swap:            0              0              0
```

• Trên PRTG

Channel ▾	ID ⬆	Last Value ⬆
Available Memory	1	1,215 MB
Downtime	-4	
Percent Available Memory	0	61 %

- Web service em không cài apache được nên không kiểm tra được.
- Kiểm tra xem SMTP có thành công hay không

Test SMTP Delivery Settings

Test Your SMTP Delivery Configuration

Email Address ⓘ

leenguyenlhp@gmail.com

Subject ⓘ

This is a test email from PRTG

Date Time	Parent	Type	Object	Status	Message
12/24/2021 8:27:42 AM	None	Group	Root	Notification Info	Status sending Email: OK
12/24/2021 8:26:58 AM	None	Group	Root	Notification Info	Status sending Email: OK

• Kiểm tra Delivery Contact

Notification Contacts

Description ▾	Recipient ⬆	Type ⬆
Primary Email Address	leenguyenlhp@gmail.com	Email

⏪ < 1 to 1 of 1 > ⏩

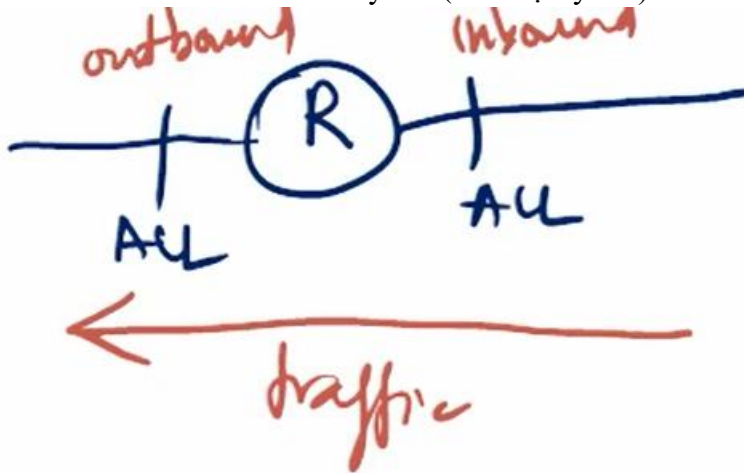
g. Phân tích

- PRTG là một ứng dụng dễ sử dụng và thao tác, thêm vào đó các sensor trên PRTG rất đa dạng.

5. Access Control List

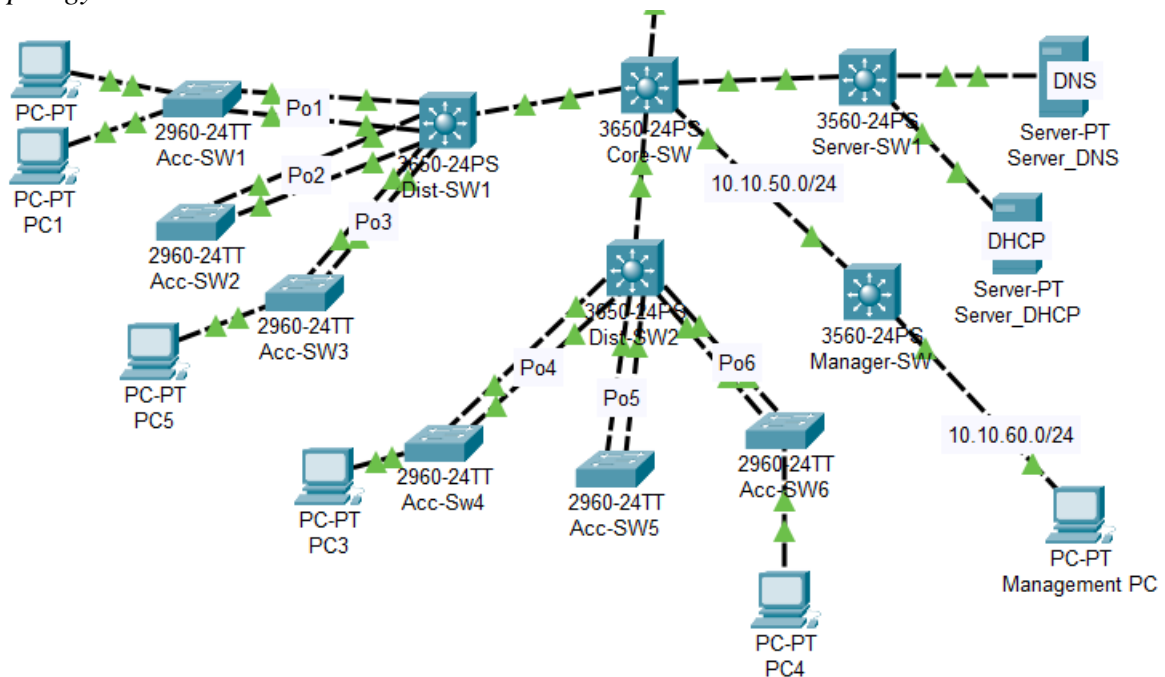
a. Giới thiệu

- Access Control List (ACL) là danh sách các điều khiển truy cập có thứ tự được áp đặt vào các interface của router/ switch layer 3 (thiết bị layer 3) để điều khiển luồng lưu lượng đi qua nó.



- Tùy vào hướng của gói tin mà quyết định port nào là inbound và port nào là outbound.

b. Topology



c. Mục tiêu

- Tạo ACL
- Sử dụng ACL để cấm các mạng.

d. Kịch bản

- Định tuyến cho khu vực Management Zone
- Mở line telnet/SSH trên các thiết bị mạng: CoreSW, Dist-SW1, Dist-SW2.
- Cấu hình ACL:
 - Cấm các PC thuộc VLAN 10 và VLAN 20 ping tới các server trong khu vực Internal Server
 - Chỉ cho phép các PC trong khu vực quản trị được phép quản trị từ xa các thiết bị mạng (CoreSW, Dist-SW1, Dist-SW2)

e. Thực hiện

- Định tuyến cho khu vực Management Zone bằng giao thức định tuyến động OSPF với area của khu vực này là 5.
- Bật telnet trên CoreSW, Dist-SW1, Dist-SW2, ví dụ ta bật Telnet/SSH trên Dist-SW2:
 - Dist-SW2(config)#enable secret cisco
 - Dist-SW2(config)#line vty 0 4
 - Dist-SW2(config)#password <mật khẩu>
 - Dist-SW2(config)#login
- Cấu hình ACL cấm các PC thuộc VLAN 10 và VLAN 20 tới các server trong khu vực Internal Server bằng cách cấu hình trên Server-SW1 theo hai bước sau:
 - Tạo ACL:


```
Server-SW1(config)#access-list 1 deny icmp 172.20.20.0 0.0.0.255 10.50.50.0 0.0.0.255
Server-SW1(config)#access-list 1 deny icmp 172.16.10.0 0.0.0.255 10.50.50.0 0.0.0.255
Server-SW1(config)#access-list 1 permit any
```
 - Áp dụng vào interface


```
Server-SW1(config)#interface fa0/18
Server-SW1(config-if)#ip access-group 1 in
```
- Để cấu hình ACL chỉ cho phép các máy bên mạng Management Zone có thể sử dụng Telnet ở CoreSW, Dist-SW1, Dist-SW2, ta có thể thực hiện như sau (giải sử ví dụ lên Core-SW, các switch khác làm tương tự, lưu ý rằng số của access-list phải lớn hơn 99):
 - Tạo ACL:


```
Core-SW(config)#access-list 101 permit tcp 10.10.60.0 0.0.0.255 any eq telnet
```

 Câu lệnh trên cho phép các gói tin từ địa chỉ ip nguồn 10.10.60.0/24 gọi dịch vụ telnet đến bất kì Switch nào cũng có thể đi qua được.


```
Core-SW(config)#access-list 101 deny tcp any any eq telnet
```

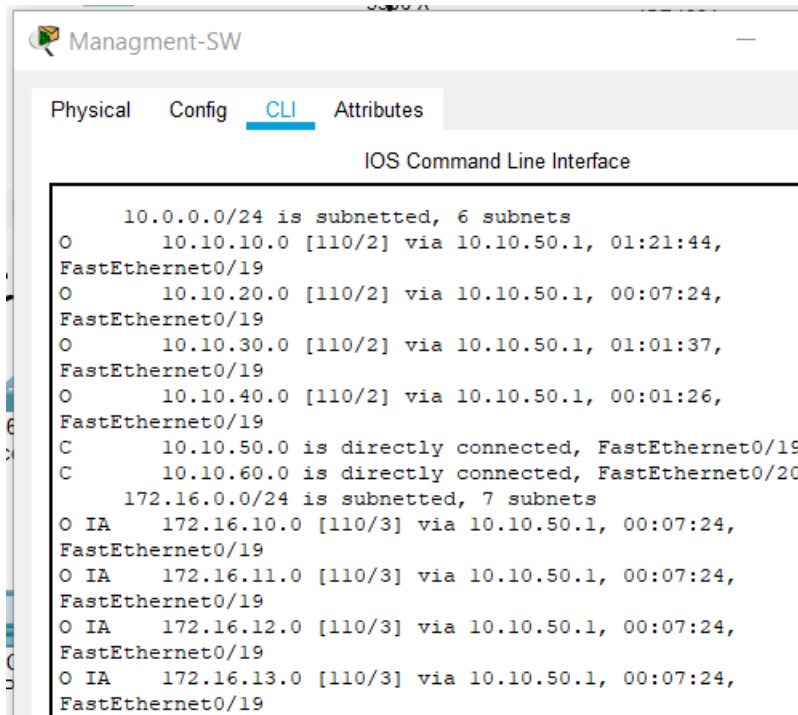
 Câu lệnh trên cấm bất kì địa chỉ ip nguồn nào gọi dịch vụ telnet đến bất kì Switch nào. Vì nếu địa chỉ ip nguồn có dạng 10.10.60.0/24 thì nó đã được permit bên trên nên câu lệnh này không ảnh hưởng đến nó, trái lại các gói tin gọi dịch vụ telnet không bắt nguồn từ mạng này sẽ không qua được.


```
Core-SW1(config)#access-list 101 permit any any
```
 - Áp dụng vào interface: Cần cài đặt nó cho tất cả các interface của Core-SW, Dist-SW1 và Dist-SW2. Ở đây, ta cài đặt trên interface gi1/0/16 của Core-SW để thử nghiệm

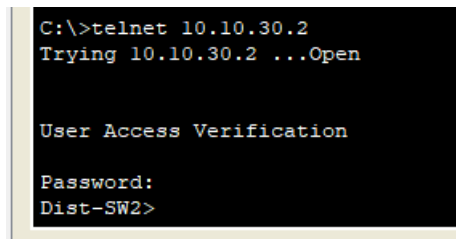

```
Core-SW(config)#interface gi1/0/16
Core-SW(config-if)#ip access-group 101 in
```

f. Kiểm tra

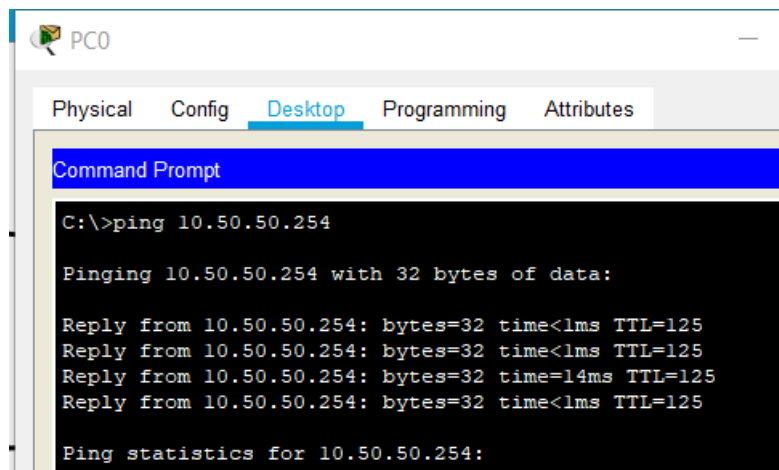
- Bảng định tuyến của Management-SW



- Kiểm tra dịch vụ Telnet/SSH đã được bật hay chưa thông qua việc gọi từ PC0 đến port gi1/0/17 của Dist-SW2



- Trước khi áp dụng ACL 1 thì máy PC0 có địa chỉ ip là 172.16.10.3 thuộc VLAN 10 có thể ping đến DHCP Server có địa chỉ ip là 10.50.50.254.



- Sau khi áp dụng ACL 1

```
C:\>ping 10.50.50.254

Pinging 10.50.50.254 with 32 bytes of data:

Reply from 10.10.40.2: Destination host unreachable.
Reply from 10.10.40.2: Destination host unreachable.
Reply from 10.10.40.2: Destination host unreachable.
Reply from 10.10.40.2: Destination host unreachable.

Ping statistics for 10.50.50.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

- Sau khi thêm ACL chỉ cho phép các máy từ mạng của Management Zone gọi Telnet/SSH ở các switc, thử gọi Telnet/SSH bằng PC0 đến Dist-SW2

```
C:\>telnet 10.10.30.2
Trying 10.10.30.2 ...
% Connection timed out; remote host not responding
C:\>
```