

Bài 5: Cấu hình Firewall

I. Mục tiêu bài lab

- Trang bị cho sinh viên kỹ năng cấu hình VPN Lan to Lan (Site to site)
- Ôn tập lại cách cấu hình Load balance cho router

II. Nội dung bài lab

- a. Chuẩn bị**
- b. Sơ đồ**
- c. Yêu cầu bài lab**
- d. Cấu hình**
- e. Cách test**
- f. Bài tập**

III. Hướng dẫn chi tiết

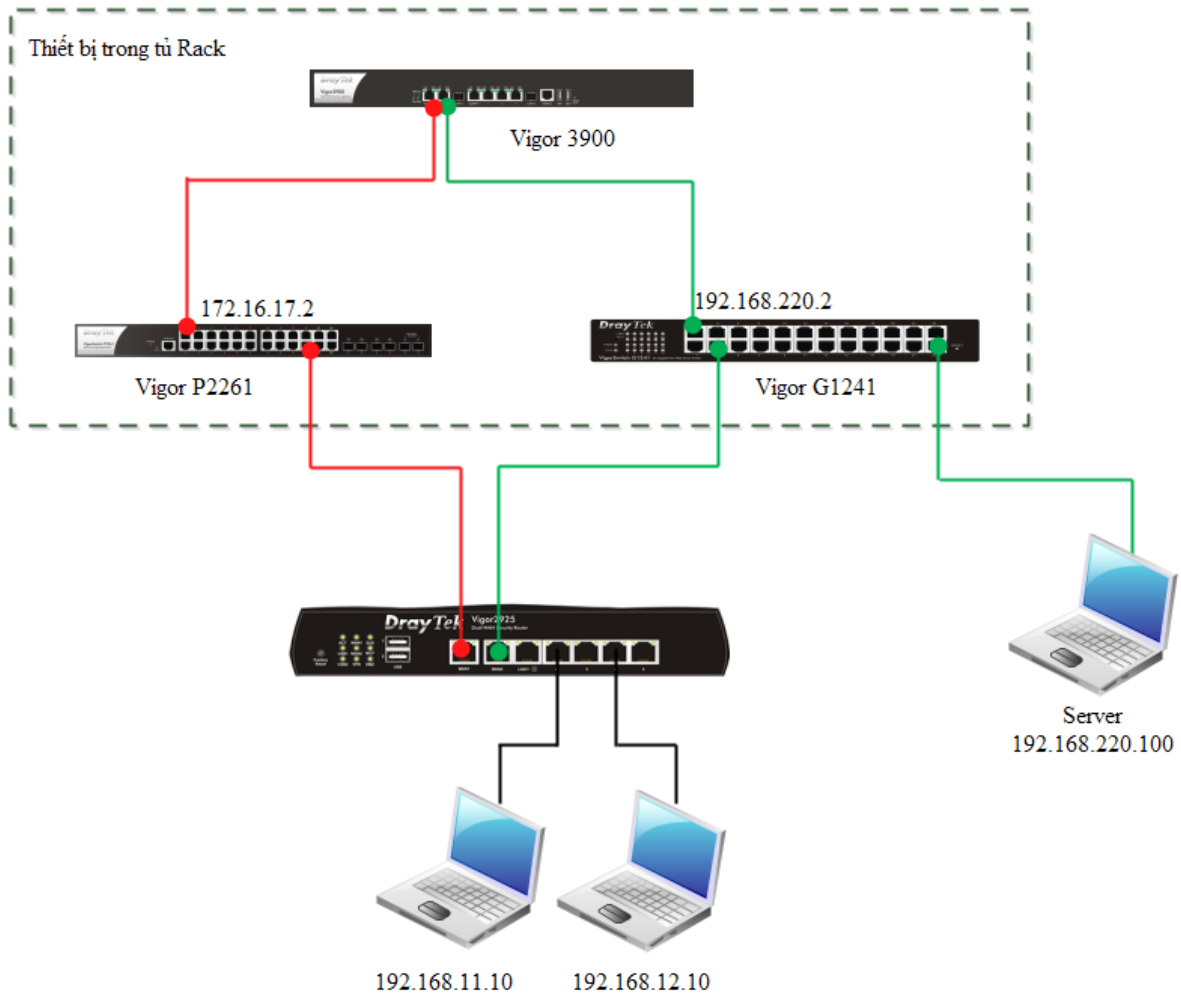
a. Chuẩn bị

- Sử dụng 1 router Vigor 2925/2912,
- 3 laptop trong đó 1 laptop nối vào switch G1241 và đặt IP tĩnh là 192.168.220.100
- Thực hiện thao tác reset default (reset cứng) router 2925/2912
- 5 sợi cáp mạng RJ45
- Nối Wan 1 của router vào cổng bất kì trên switch P2261, nối Wan 2 của router vào cổng bất kì trên switch G1241
- Cấu hình lên Load balance cho router với Wan 1 mode PPPoE, Wan 2 mode Static or Dynamic IP
- Thực hiện chia 2 VLAN
 - Lan 1: 192.168.11.x/24
 - Sử dụng vigor 2925: gán vào port 1 & 2
 - Sử dụng vigor 2912: gán vào port 1
 - Lan 2: 192.168.12.x/24
 - Sử dụng vigor 2925: gán vào port 3&4

- Sử dụng vigor 2912: gán vào port 3&4
- Cấu hình Inter-lan routing cho 2 vlan

Lưu ý: Các bạn liên hệ với giảng viên hướng dẫn để lấy thông tin Account PPPoE và IP để cấu hình Wan

b. Sơ đồ




c. Yêu cầu bài Lab

- Chặn máy 192.168.11.10 và 192.168.12.10 truy cập những dịch vụ sử dụng port 443

- Chặn IP 192.168.12.10 truy cập vào máy 192.168.11.10
- Chặn máy 192.168.11.10 truy cập vào Server ngoài internet có IP 192.168.220.100
- Chặn toàn bộ client không được đi trang web có từ khoá bongda, phim, nhạc, game, shopping, muasam

- Cấu hình

- **Lưu ý:** Firewall Draytek sẽ xét rule theo thứ tự từ trên xét xuống, rule nào thỏa thì sẽ được thực thi trước.

 Chặn máy 192.168.11.10 và 192.168.12.10 truy cập những dịch vụ sử dụng port 443

- Tạo IP object cho ip 192.168.11.10: Vào Objects setting >>> IP object >>> Chọn Index 1

Objects Setting >> IP Object

IP Object Profiles:
| [Set to Factory Default](#) |

Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

- Name: đặt tên cho profile

- Interface: chọn Any
- Address Type: chọn Single Address
- Start IP Address: điền 192.168.11.10
- Nhấn OK

Objects Setting >> IP Object

Profile Index : 1

Name:	ip_11_10
Interface:	Any
Address Type:	Single Address
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Start IP Address:	192.168.11.10
End IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Invert Selection:	<input type="checkbox"/>

OK Clear Cancel

- Tương tự ta cấu hình cho profile IP 192.168.12.10

Objects Setting >> IP Object

Profile Index : 2

Name:	ip_12_10
Interface:	Any
Address Type:	Single Address
Mac Address:	00 : 00 : 00 : 00 : 00 : 00
Start IP Address:	192.168.12.10
End IP Address:	0.0.0.0
Subnet Mask:	0.0.0.0
Invert Selection:	<input type="checkbox"/>

OK Clear Cancel


- Tạo IP group: Vào Objects setting >>> IP group >>> chọn Index 1

Objects Setting >> IP Group

IP Group Table:

| [Set to Factory Default](#) |

Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

- Name: đặt tên cho group
- Interface: Any
- Available IP Objects: chọn IP object rồi bấm nút  để add sang Selected IP Objects
- Nhấn OK

Objects Setting >> IP Group

Profile Index : 1

Name: **1**

Interface:

Available IP Objects **2**

1-ip_11_10
2-ip_12_10

Selected IP Objects

3

4

- Tao rule trong firewall: Vào Firewall >>> Filter Setup >>> chọn Filter rule 2

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2

Comments :

Filter Rule	Active	Comments	Move Up	Move Down
<input type="button" value="1"/>	<input checked="" type="checkbox"/>	xNetBios -> DNS		<u>Down</u>
<input type="button" value="2"/>	<input type="checkbox"/>		<u>UP</u>	<u>Down</u>
<input type="button" value="3"/>	<input type="checkbox"/>		<u>UP</u>	<u>Down</u>
<input type="button" value="4"/>	<input type="checkbox"/>		<u>UP</u>	<u>Down</u>
<input type="button" value="5"/>	<input type="checkbox"/>		<u>UP</u>	<u>Down</u>
<input type="button" value="6"/>	<input type="checkbox"/>		<u>UP</u>	<u>Down</u>
<input type="button" value="7"/>	<input type="checkbox"/>		<u>UP</u>	

Next Filter Set

- Chọn Enable the filter rule
- Comments: đặt tên cho rule
- Direction: LAN/RT/VPN → WAN
- Source IP: nhấn nút Edit >>> hiện ra hộp cấu hình IP Address Edit
 - Address type: chọn Group and Objects

- IP Group: chọn group IP đã tạo
- Nhấn OK
- Service Type: nhấn nút Edit >>> hiện ra hộp cấu hình Service Type Edit
 - Service Type: chọn User defined
 - Protocol: chọn TCP/UDP
 - Source Port: chọn từ 1 → 65535
 - Destination Port: chọn 443
 - Nhấn OK
- Filter: chọn Block Immediately
- Nhấn OK

Filter Set 2 Rule 2

☒ Check to enable the Filter Rule

Comments: block_https

Index(1-15) in Schedule Setup: , , ,

Clear sessions when schedule ON: ☐ Enable

Direction: LAN/RT/VPN -> WAN

Source IP: **Edit**

Destination IP: Any **Edit**

Service Type: **Edit**

Fragments: Don't Care

Application

Filter: Block Immediately **Syslog** ☐

Branch to Other Filter Set: None

Sessions Control: 0 / 60000

MAC Bind IP: Non-Strict

Quality of Service: None

Load-Balance policy: Auto-Select

User Management: None

APP Enforcement: None

URL Content Filter: None

Web Content Filter: None

Advance Setting **Edit**

OK **Clear** **Cancel**

IP Address Edit

Address Type: Group and Objects

Start IP Address: 0.0.0.0

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Invert Selection: ☐

IP Group: 1-group_1

or IP Group: None

or IP Object: None

or IP Object: None

IPv6 Group: None

or IPv6 Object: None

or IPv6 Object: None

OK **Close**

Service Type Edit

Service Type: User defined

Protocol: TCP/UDP

Source Port: = 1 ~ 65535

Destination Port: = 443 ~ 443

Service Group: None

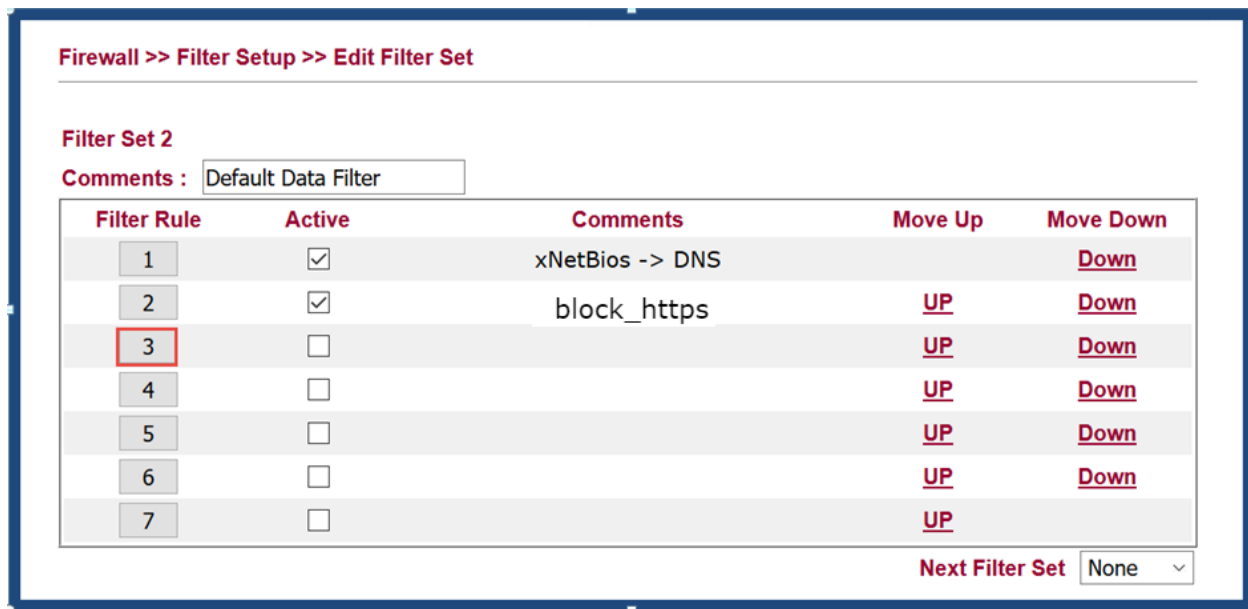
or Service Object: None

or Service Object: None

OK **Close**

✚ Chặn IP 192.168.12.10 truy cập vào máy 192.168.11.10

- Vào Firewall >>> Filter setup >>> Default data filter >>> chọn Filter rule 3



- Chọn Enable the filter rule
- Comments: đặt tên cho rule
- Direction: LAN/RT/VPN → LAN/RT/VPN
- Source IP: nhấn nút Edit >>> hiện ra hộp cấu hình IP Address Edit
 - Address type: chọn Single address
 - Start IP address: điền 192.168.12.10
 - Nhấn OK
- Destination IP: nhấn nút Edit >>> hiện ra hộp cấu hình IP Address Edit
 - Address type: chọn Single address
 - Start IP address: điền 192.168.11.10
 - Nhấn OK
- Filter: chọn Block Immediately
- Nhấn OK

Filter Set 2 Rule 3

☒ Check to enable the Filter Rule

Comments: rule_2

Index(1-15) in **Schedule** Setup: , , ,

Clear sessions when schedule ON: ☐ Enable

Direction: LAN/RT/VPN -> LAN/RT/VPN

Source IP: Any Edit

Destination IP: Any Edit

Service Type: Any Edit

Fragments: Don't Care

Application

Filter: Block Immediately Syslog ☐

Branch to Other Filter Set: None

Sessions Control: 0 / 60000 ☐

MAC Bind IP: Non-Strict ☐

Quality of Service: None ☐

Load-Balance policy: Auto-Select ☐

User Management: None ☐

APP Enforcement: None ☐

URL Content Filter: None ☐

Web Content Filter: None ☐

Advance Setting Edit

OK Clear Cancel

IP Address Edit

Address Type: Single Address

Start IP Address: 192.168.12.10

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

IP Address Edit

Address Type: Single Address

Start IP Address: 192.168.11.10

End IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

✚ Chặn máy 192.168.11.10 truy cập vào Server ngoài internet có IP 192.168.220.100

- Vào Firewall >>> Filter setup >>> Default data filter >>> chọn Filter rule 4

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2

Comments: Default Data Filter

Filter Rule	Active	Comments	Move Up	Move Down
1	<input checked="" type="checkbox"/>	xNetBios -> DNS		Down
2	<input checked="" type="checkbox"/>	block_https	UP	Down
3	<input checked="" type="checkbox"/>	rule_2	UP	Down
4	<input type="checkbox"/>		UP	Down
5	<input type="checkbox"/>		UP	Down
6	<input type="checkbox"/>		UP	Down
7	<input type="checkbox"/>		UP	

Next Filter Set: None

- Chọn Enable the filter rule

- Comments: đặt tên cho rule
- Direction: LAN/RT/VPN → WAN
- Source IP: nhấn nút Edit >>> hiện ra hộp cấu hình IP Address Edit
 - Address type: chọn Single address
 - Start IP address: điền 192.168.11.10
 - Nhấn OK
- Destination IP: nhấn nút Edit >>> hiện ra hộp cấu hình IP Address Edit
 - Address type: chọn Single address
 - Start IP address: điền 192.168.220.100
 - Nhấn OK
- Filter: chọn Block Immediately
- Nhấn OK

✚ Chặn toàn bộ client không được đi trang web có từ khoá bongda, phim, nhạc, game, shopping, muasam (Sử dụng URL content filter để chặn)

- Tạo keyword object:

- Vào Objects Setting >>> Keyword Object >>> chọn Index 1

Keyword Object Profiles:

| [Set to Factory Default](#) |

Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

<< [1-32](#) | [33-64](#) | [65-96](#) | [97-128](#) | [129-160](#) | [161-192](#) | [193-200](#) >>

[Next](#) >>

- Name: đặt tên profile
- Contents: điền keyword muốn chặn
- Nhấn OK

- Lưu ý: Mỗi profile chỉ cho phép tạo 3 keyword, mỗi keyword cách nhau khoảng trắng, tổng số ký tự cho phép là 63

Objects Setting >> Keyword Object Setup

Profile Index : 1

Name	keyword_1
Contents	bongda phim nhac

Limit of Contents: Max 3 Words and 63 Characters.
Each word should be separated by a single space.

You can replace a character with %HEX.
Example:
Contents: backdoo%72 virus keep%20out

Result:

1. backdoor
2. virus
3. keep out

OK Clear Cancel

- Vào Objects Setting >>> Keyword Object >>> chọn Index 2
 - Name: đặt tên profile
 - Contents: điền keyword muốn chặn

Objects Setting >> Keyword Object Setup

Profile Index : 2

Name	keyword_2
Contents	game shopping muasam

Limit of Contents: Max 3 Words and 63 Characters.
Each word should be separated by a single space.

You can replace a character with %HEX.
Example:
Contents: backdoo%72 virus keep%20out

Result:

1. backdoor
2. virus
3. keep out


OK Clear Cancel

- Tạo keyword group: Vào Objects setting >>> Keyword Group >>> chọn Index 1

Keyword Group Table:

[Set to Factory Default](#)

Index	Name	Index	Name
<u>1.</u>		<u>17.</u>	
<u>2.</u>		<u>18.</u>	
<u>3.</u>		<u>19.</u>	
<u>4.</u>		<u>20.</u>	
<u>5.</u>		<u>21.</u>	
<u>6.</u>		<u>22.</u>	
<u>7.</u>		<u>23.</u>	
<u>8.</u>		<u>24.</u>	
<u>9.</u>		<u>25.</u>	
<u>10.</u>		<u>26.</u>	
<u>11.</u>		<u>27.</u>	
<u>12.</u>		<u>28.</u>	
<u>13.</u>		<u>29.</u>	
<u>14.</u>		<u>30.</u>	
<u>15.</u>		<u>31.</u>	
<u>16.</u>		<u>32.</u>	

- Name: đặt tên cho profile
- Chọn keyword object và lịch nút 
- Nhấn OK

Objects Setting >> Keyword Group Setup

Profile Index : 1

1

Name:

group_1

2

Available Keyword Objects

1-keyword_1

2-keyword_2

3

>>

<<

4

OK

Clear

Cancel

Selected Keyword Objects(Max 16 Objects)

- Tạo profile CSM: Vào CSM >>> URL content filter profile

CSM >> URL Content Filter Profile

URL Content Filter Profile Table:

[Set to Factory Default](#)

Profile	Name	Profile	Name
1.		5.	
2.		6.	
3.		7.	
4.		8.	

Administration Message (Max 255 characters)

Default Message

<body><center>
<p>The requested Web page has been blocked by URL Content Filter.<p>Please contact your system administrator for further information.</center></body>

OK

- Profile name: đặt tên cho profile
- Priority: chọn Either: URL Access Control Frist
- 1.URL Access Control
 - Chọn Enable URL Access Control
 - Action: Chọn Block
 - Nhấn Edit

CSM >> URL Content Filter Profile

Profile Index: 1

Profile Name:

Priority: Log:

1.URL Access Control

☒ Enable URL Access Control ☐ Prevent web access from IP address

Action: Group/Object Selections

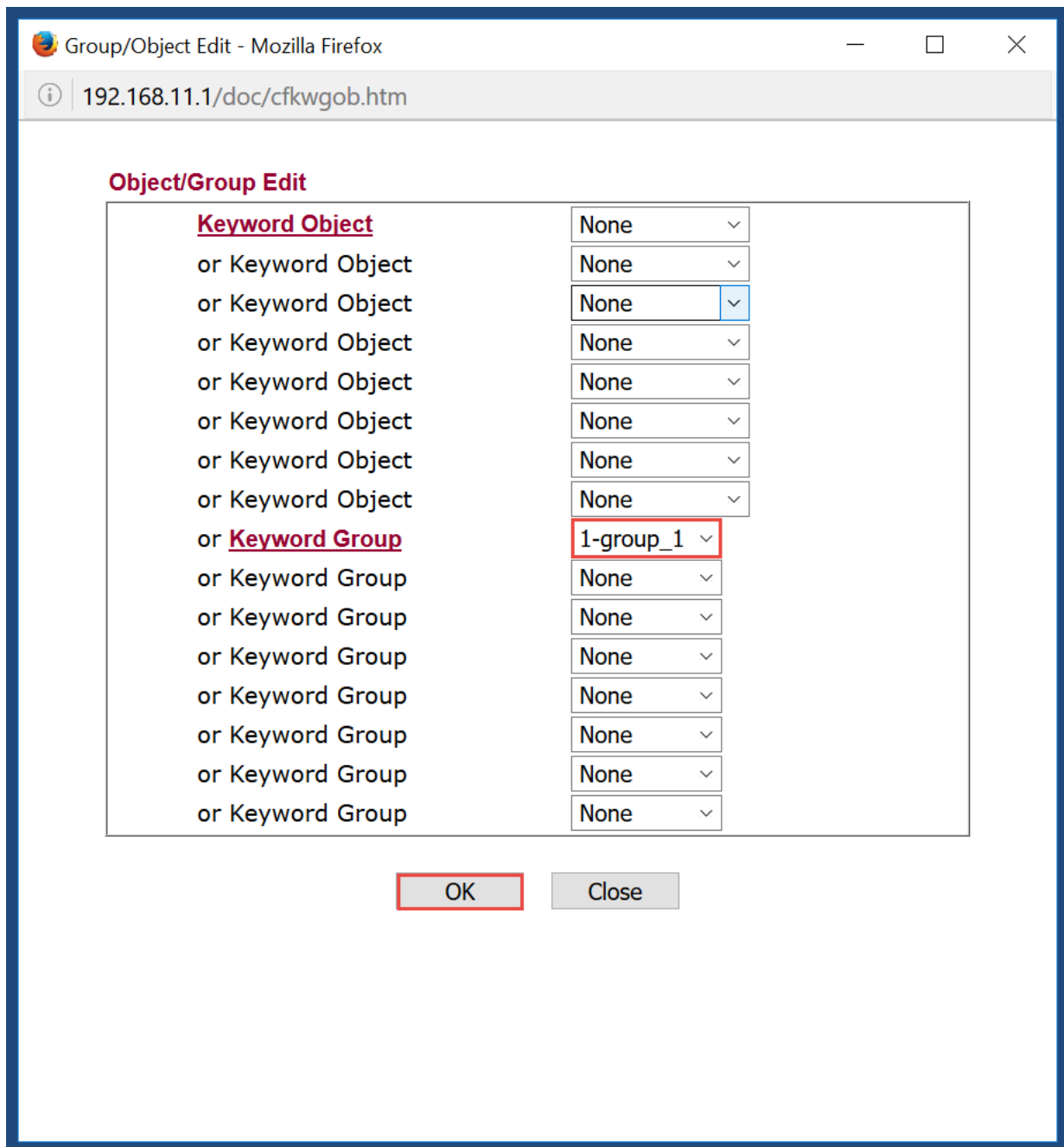
☐ Exception List

2.Web Feature

☐ Enable Restrict Web Feature

Action: ☐ Cookie ☐ Proxy ☐ Upload File Extension Profile:

- Keyword group: chọn key group đã được tạo ở bước trên
- Nhấn OK



- Nhấn OK

Profile Index: 1

Profile Name:

Priority: **Log:**

1.URL Access Control

☒ Enable URL Access Control ☐ Prevent web access from IP address

Action: Group/Object Selections: [Edit](#)

2.Web Feature


☐ Enable Restrict Web Feature

Action: ☐ Cookie ☐ Proxy ☐ Upload **File Extension Profile:**

[OK](#) [Clear](#) [Cancel](#)

- Nếu bạn muốn thay đổi nội dung thông báo khi truy cập vào trang web bị cấm thì vào CSM >>> URL content filter >>> Administration Message >>> thay đổi nội dung những dòng tô vàng

Lưu ý: Nội dung thông báo được viết bằng code HTML và số lượng ký tự tối đa là 255 ký tự

CSM >> URL Content Filter Profile 

URL Content Filter Profile Table: [Set to Factory Default](#)


Profile	Name	Profile	Name
1.	csm_1	5.	
2.		6.	
3.		7.	
4.		8.	

Administration Message (Max 255 characters) [Default Message](#)

```
<body><center><br><p>The requested Web page has been blocked by URL Content Filter.
<p>Please contact your system administrator for further information.</center></body>
```

[OK](#)

Ví dụ: Viết thông báo như sau “Bạn đã truy cập trang web bị cam. Vui lòng truy cập trang web khác hoặc liên hệ với IT”

CSM >> URL Content Filter Profile 

URL Content Filter Profile Table: | [Set to Factory Default](#) |

Profile	Name	Profile	Name
<u>1.</u>	csm_1	<u>5.</u>	
<u>2.</u>		<u>6.</u>	
<u>3.</u>		<u>7.</u>	
<u>4.</u>		<u>8.</u>	

Administration Message (Max 255 characters) Default Message

```
<body><center><br><p>Bạn đã truy cập trang web bị cam.<p>Vui lòng truy cập trang web khác hoặc liên hệ với IT.</center></body>
```

OK

- Vào Firewall >>> Filter setup >>> Default data filter >>> chọn Filter rule 5

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2

Comments :

Filter Rule	Active	Comments	Move Up	Move Down
<input type="checkbox"/> 1	<input checked="" type="checkbox"/>	xNetBios -> DNS		Down
<input type="checkbox"/> 2	<input checked="" type="checkbox"/>	block_https	UP	Down
<input type="checkbox"/> 3	<input checked="" type="checkbox"/>	rule_2	UP	Down
<input type="checkbox"/> 4	<input checked="" type="checkbox"/>	rule_3	UP	Down
<input checked="" type="checkbox"/> 5	<input type="checkbox"/>		UP	Down
<input type="checkbox"/> 6	<input type="checkbox"/>		UP	Down
<input type="checkbox"/> 7	<input type="checkbox"/>		UP	

Next Filter Set

- Chọn Enable the Filter rule
- Comments: đặt tên cho rule
- Direction: chọn từ LAN/RT/VPN → WAN

- Filter: chọn Pass Immediately
- URL content filter: chọn profile CMS đã tạo ở trên
- Nhấn OK

Firewall >> Edit Filter Set >> Edit Filter Rule

Filter Set 2 Rule 5

☒ Check to enable the Filter Rule

Comments:

Index(1-15) in **Schedule** Setup: , , ,

Clear sessions when schedule ON: ☐ Enable

Direction:

Source IP:

Destination IP:

Service Type:

Fragments:

Application	Action/Profile	Syslog
Filter:	<input type="text" value="Pass Immediately"/>	<input type="checkbox"/>
Branch to Other Filter Set:	<input type="text" value="None"/>	
Sessions Control	<input type="text" value="0 / 60000"/>	<input type="checkbox"/>
MAC Bind IP	<input type="text" value="Non-Strict"/>	<input type="checkbox"/>
Quality of Service	<input type="text" value="None"/>	<input type="checkbox"/>
Load-Balance policy	<input type="text" value="Auto-Select"/>	<input type="checkbox"/>
User Management	<input type="text" value="None"/>	<input type="checkbox"/>
APP Enforcement:	<input type="text" value="None"/>	<input type="checkbox"/>
URL Content Filter:	<input type="text" value="1-csm_1"/>	<input type="checkbox"/>
Web Content Filter:	<input type="text" value="None"/>	<input type="checkbox"/>

Advance Setting

- Cách test

- Chặn máy 192.168.11.10 và 192.168.12.10 truy cập những dịch vụ sử dụng port 443

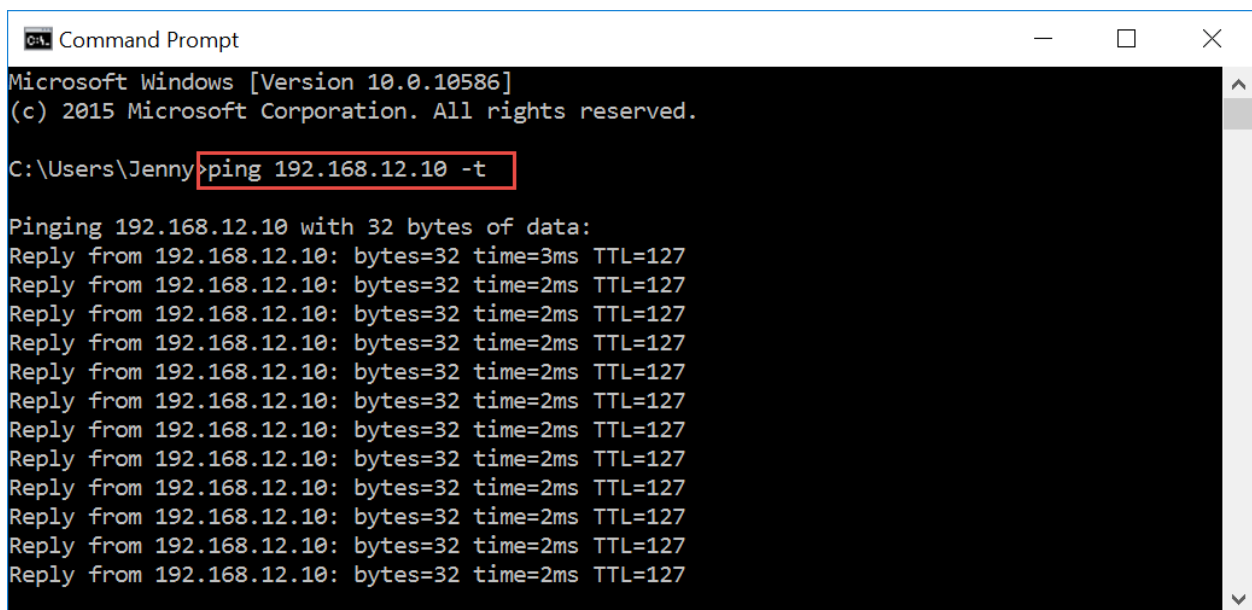
- Trên máy 192.168.11.10 và 192.168.12.10 truy cập vào những trang web chạy https. Ví dụ: <https://facebook.com>, <https://youtube.com>, <https://mail.google.com> hoặc các trang web ngân hàng → sẽ không truy cập được

✚ Chặn IP 192.168.12.10 truy cập vào máy 192.168.11.10

- Dùng 2 laptop gắn vào port 1 và port 3 trên router gắn IP tĩnh như sau:

- Máy gắn vào port 1 đặt IP 192.168.11.10
- Máy gắn vào port 3 đặt IP 192.168.12.10

- Thực hiện lệnh ping từ máy 192.168.11.10 sang máy 192.168.12.10 → ping thành công



```
Command Prompt
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Jenny>ping 192.168.12.10 -t

Pinging 192.168.12.10 with 32 bytes of data:
Reply from 192.168.12.10: bytes=32 time=3ms TTL=127
Reply from 192.168.12.10: bytes=32 time=2ms TTL=127
Reply from 192.168.12.10: bytes=32 time=2ms TTL=127
Reply from 192.168.12.10: bytes=32 time=2ms TTL=127
Reply from 192.168.12.10: bytes=32 time=2ms TTL=127
Reply from 192.168.12.10: bytes=32 time=2ms TTL=127
Reply from 192.168.12.10: bytes=32 time=2ms TTL=127
Reply from 192.168.12.10: bytes=32 time=2ms TTL=127
Reply from 192.168.12.10: bytes=32 time=2ms TTL=127
Reply from 192.168.12.10: bytes=32 time=2ms TTL=127
Reply from 192.168.12.10: bytes=32 time=2ms TTL=127
```

- Thực hiện lệnh ping từ máy 192.168.12.10 sang máy 192.168.11.10 → ping không thành công

d. Bài Tập

- Cấu hình load balance cho router

- Cấu hình chia Vlan

- Vigor 2925: chia 2 vlan
 - Vlan 1: 192.168.100.x/24 gắn vào port 1 và 3
 - Vlan 2: 192.168.101.x/24 gắn vào port 2 và 4
- Vigor 2912: chia 2 vlan
 - Vlan 1: 192.168.100.x/24 gắn vào port 2 và 3
 - Vlan 2: 192.168.101.x/24 gắn port 4

- Cấu hình inter-vlan routing cho các vlan (tất cả các vlan thấy nhau)

- Cấu hình Firewall

- Vlan 1 có range IP từ 192.168.100.200→192.168.100.254 (ban GĐ) không bị giới hạn truy cập
- Rule 1: Block range IP 192.168.100→192.168.100.150 và 192.168.101.50→192.168.101.60 không được truy cập các dịch vụ ftp, mail sử dụng port 25, 110
- Rule 2: Cấm các máy bên trong không được sử dụng tất cả các dịch vụ của yahoo (web, chat, email)
- Rule 3:
 - Vlan 1 được phép truy cập các trang web đã được qui định như: facebook, youtube, raovat, 5s, chotot, baochi, marketing. Còn lại trang web khác thì cấm hết
 - ➔ Gợi ý: chỉ cần tạo URL content filter chọn Pass thì router sẽ cho phép truy cập trang web đã được cấu hình, còn lại thì sẽ cấm hết.
 - Vlan 2: chỉ được truy cập các trang web về thuế và ngân hàng, luật pháp
 - Thay đổi nội dung thông báo khi truy cập vào trang web bị cấm

