

# NASA hw6

Author: B12705014陳泊華

## OPNSense

### Question 1

- Block：阻止封包通過，但不會向來源發送任何回應
- Reject：拒絕封包通過，並向發送源地址發送一個拒絕回應

Block對於不想讓攻擊者知道防火牆的存在或詳細信息的情況下更為適合。但是，這也可能導致來源主機不知道封包被阻止，而進行不必要的重試，可能會導致一些網絡延遲或重試負擔；Reject可以更及時地通知來源主機並確保它們不會進一步重試相同的封包。這在一些情況下可能更加合適，特別是當你希望來源主機知道防火牆的存在並採取相應的措施時。

### Question 2

- Interface Net：適用於整個子網的範圍且不能被assign給interface
- Interface Address：適用於單個IP地址的範圍

當希望規則適用於整個子網時，可以選擇Interface Net；希望規則僅適用於特定IP地址時，可以選擇Interface Address

reference: <https://forum.netgate.com/topic/99227/net-verses-address>  
(<https://forum.netgate.com/topic/99227/net-verses-address>).

### Question 3

- Stateful firewall：能夠記住先前的網絡通信狀態，並根據這些記錄對數據包進行過濾和識別。
- Stateless firewall：僅僅根據單個數據包的屬性來進行過濾，它不記住先前的通信狀態，不需要保存通信狀態表，因此通常更加簡單和輕量，但在某些場景下可能無法提供足夠的安全性。

OPNsense屬於有狀態防火牆，它可以跟踪網絡連接的狀態並根據連接狀態進行智能過濾和阻止。這使得OPNsense能夠提供更全面的安全性，並能夠更好地防止各種網絡攻擊。

reference: <https://www.fortinet.com/resources/cyberglossary/stateful-vs-stateless-firewall> (<https://www.fortinet.com/resources/cyberglossary/stateful-vs-stateless-firewall>).

### Question 4

## 1. 授權和商業模式

pfSense是一個基於商業模式的開源項目，它的背後是Netgate公司。pfSense提供了一個基於捐贈的模式，同時也提供了付費的商業支持和特性。OPNsense則是完全的開源項目，並且不依賴於商業公司。它的發展主要由社區成員和志願者共同推動，因此它更加注重用戶社區的參與和開發。

## 2. 使用者介面

pfSense提供了一個穩定和成熟的用戶界面，其設計旨在提供易於使用的操作和配置。它的功能豐富，包括VPN、防火牆、路由、代理等。OPNsense也有類似的功能，並且努力提供一個直觀且現代的用戶界面。在某些方面，OPNsense可能提供了更多的自定義和高級功能，同時也更加注重安全性和開放性。











reference: <https://www.wundertech.net/pfsense-vs-opnsense/>  
(<https://www.wundertech.net/pfsense-vs-opnsense/>).


## OPNSense

\*本大題我延用Lab6的VM進行設定，使用Mac M1電腦的UTM開啟OPNSense VM，再用Arch Linux做為Client

- 連上OPNSense之後至Interface -> Other Types新增VLAN8
- 接著至Interface -> Assignments新增此Device
- 在三台Client上分別設定hostname、VLAN、mtu

Interfaces: Assignments

Interface	Identifier ⓘ	Device	
[LAN]	lan	 em1 (a6:39:08:53:4b:b4) ▼	
[OPT1]	opt1	 vlan01 (Parent: em1, Tag: 5) ▼	
[OPT2]	opt2	 vlan02 (Parent: em1, Tag: 99) ▼	
[OPT3]	opt3	 vlan03 (Parent: em1, Tag: 8) ▼	
[WAN]	wan	 em0 (5e:bd:53:91:80:25) ▼	



在三台Client上分別執行：

```
$ ip link add link enp0s1 name enp0s1.[number] type vlan id [number]
$ ifconfig enp0s1.[number] mtu 1496 避免後面的VLAN tag因mtu限制遭丟棄
```

\$ ip a 檢查 (以Client5為例)

```
[root@Client5 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1496 qdisc fq_codel state UP group default qlen 1000
    link/ether d2:f5:ee:1a:f7:92 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.16/24 metric 1024 brd 192.168.1.255 scope global dynamic enp0s1
        valid_lft 4739sec preferred_lft 4739sec
    inet6 fe80::d0f5:eeff:fe1a:f792/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
3: enp0s1.5@enp0s1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1496 qdisc noqueue state UP group default qlen 1000
    link/ether d2:f5:ee:1a:f7:92 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::d0f5:eeff:fe1a:f792/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
[root@Client5 ~]#
```


reference:

- (i) [https://wiki.archlinux.org/title/Network\\_configuration#Set\\_the\\_hostname](https://wiki.archlinux.org/title/Network_configuration#Set_the_hostname)  
([https://wiki.archlinux.org/title/Network\\_configuration#Set\\_the\\_hostname](https://wiki.archlinux.org/title/Network_configuration#Set_the_hostname)).
- (ii) [https://linux.vbird.org/linux\\_server/centos6/0140networkcommand.php#ip\\_cmd](https://linux.vbird.org/linux_server/centos6/0140networkcommand.php#ip_cmd)  
([https://linux.vbird.org/linux\\_server/centos6/0140networkcommand.php#ip\\_cmd](https://linux.vbird.org/linux_server/centos6/0140networkcommand.php#ip_cmd)).
- (iii) <https://www.ifconfig.it/hugo/2014/08/mtu/> (<https://www.ifconfig.it/hugo/2014/08/mtu/>).

## Question 5










- 分別至Interfaces -> OPT1、OPT2、OPT3設定IPv4

- 下面以VLAN5的設定截圖為例

 Description	<input type="text" value="OPT1"/>	
---	-----------------------------------	--


---

**Generic configuration**

 Block private networks	<input type="checkbox"/>	
 Block bogon networks	<input type="checkbox"/>	
 IPv4 Configuration Type	<input type="text" value="Static IPv4"/>	
 IPv6 Configuration Type	<input type="text" value="None"/>	
 MAC address	<input type="text"/>	
 Promiscuous mode	<input type="checkbox"/>	
 MTU	<input type="text"/>	
 MSS	<input type="text"/>	
 Dynamic gateway policy	<input type="checkbox"/> This interface does not require an intermediate system to act as a gateway	

---

**Static IPv4 configuration**

 IPv4 address	<input type="text" value="10.5.0.254"/>	<input type="text" value="24"/>
--	---	---------------------------------

- 設定 DHCP 伺服器8.8.8.8、8.8.4.4

- 按下右上角啟動服務

Enable

☒ Enable DHCP server on the OPT1 interface

Deny unknown clients

☐

Ignore Client UIDs

☐

Subnet

10.5.0.0

Subnet mask

255.255.255.0

Available range

10.5.0.1 - 10.5.0.254

Range

from

10.5.0.1

to

10.5.0.254

Additional Pools

Pool Start	Pool End	Description

WINS servers

DNS servers

8.8.8.8

8.8.4.4

Question 6

至Firewall -> Aliases設定Alias

選擇type，在contents的地方設定相對應得Alias

Aliases

GeoIP settings

Search

Filter type

Categories

7

Enabled	Name	Type	Description	Content	Loaded#	Last updated	Commands
<input type="checkbox"/>	<input checked="" type="checkbox"/>	GOOGLE_DNS	Host(s)	8.8.8.8,8.8.4.4			<div></div>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ADMIN_PORTS	Port(s)	22,80,443			<div></div>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	CSIE_WORKSTATIONS	URL (IPs)	ws1.csie.org,ws2...			<div></div>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	bogons	External (advanced)	bogon networks ...	10		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	bogonsv6	External (advanced)	bogon networks ...			
<input type="checkbox"/>	<input checked="" type="checkbox"/>	virusprot	External (advanced)	overload table fo...	0		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	sshlockout	External (advanced)	abuse lockout ta...	0		

Showing 1 to 7 of 13 entries

Question 7

至VLAN99的介面設定：

Source OPT2 address

Source port range只允許ADMIN\_PORTS

Destination為this firewall

Interfaces

Firewall

Aliases

Automation

Categories

Groups

NAT

Rules

Floating

LAN

Loopback

OPT1

OPT2

OPT3

WAN

Shaper

Settings

Log Files

Diagnostics

Edit Firewall rule

Action

Pass

Disabled

☐ Disable this rule

Quick

☒ Apply the action immediately on match.

Interface

OPT2

Direction

in

TCP/IP Version

IPv4

Protocol

TCP

Source / Invert

☐ Use this option to invert the sense of the match.

Source

OPT2 address

Source port range

from:ADMIN\_PORTSto:ADMIN\_PORTS

Firewall: Rules: OPT2

Select category

Inspect

The changes have been applied successfully.

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	
	Automatically generated rules								
	IPv4 TCP	OPT2 address	ADMIN_PORTS	This Firewall	any - 22	*	*		
	pass	block		reject	log			in	first match
	pass (disabled)	block (disabled)		reject (disabled)	log (disabled)			out	last match
Active/Inactive Schedule (click to view/edit)									
Alias (click to view/edit)									
OPT2 rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.									

在VLAN99上確認有回傳資料，在VLAN5、8上則沒有

```
$ curl 192.168.64.2
[root@Client99 ~]# curl 192.168.64.2
<!doctype html>
<html lang="en" class="no-js">
  <head>
    <meta charset="UTF-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge">

    <meta name="robots" content="noindex, nofollow" />
    <meta name="keywords" content="" />
    <meta name="description" content="" />
    <meta name="copyright" content="" />
    <meta name="viewport" content="width=device-width, initial-scale=1, minimum-scale=1" />
    <meta name="mobile-web-app-capable" content="yes">
    <meta name="apple-mobile-web-app-capable" content="yes">

    <title>Login | OPNsense</title>

    <link href="/ui/themes/opnsense/build/css/main.css?v=d8a056033ee9b6ed" rel="stylesheet">
    <link href="/ui/themes/opnsense/build/images/favicon.png?v=d8a056033ee9b6ed" rel="shortcut icon">

    <script src="/ui/js/jquery-3.5.1.min.js"></script>
```

Question 8

以下截圖為VLAN99根據題目要求的Firewall rules設定：

Firewall: Rules: vlan99

Select category

Inspect

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description	
Automatically generated rules									
	IPv4 TCP	vlan99 net	*	This Firewall	ADMIN_PORTS	*	*		
	IPv4 *	*	*	GOOGLE_DNS	*	*	*		
	IPv4 *	*	*	CSIE_WORKSTATIONS	*	*	*		
pass		block		reject		log		in	first match
pass (disabled)		block (disabled)		reject (disabled)		log (disabled)		out	last match
Active/Inactive Schedule (click to view/edit)									
Alias (click to view/edit)									
vlan99 rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.									

\$ traceroute ws1-5.csie.org

```
[root@Client99 ~]# traceroute ws1.csie.org
traceroute to ws1.csie.org (140.112.30.186), 30 hops max, 60 byte packets
 1 _gateway (10.99.0.254) 2.910 ms 2.882 ms 2.871 ms
 2 192.168.64.1 (192.168.64.1) 7.018 ms 7.007 ms 6.999 ms
 3 192.168.3.99 (192.168.3.99) 9.314 ms 9.268 ms 9.472 ms
 4 192.168.202.1 (192.168.202.1) 9.412 ms 9.366 ms 9.061 ms
 5 * * *
 6 tp-e4-c76r2.router.hinet.net (168.95.85.162) 11.062 ms 33.182 ms 33.142 ms
 7 220-128-4-14.tpdt-3032.hinet.net (220.128.4.14) 31.391 ms 9.502 ms 11.813 ms
 8 220-128-2-49.tpdt-3307.hinet.net (220.128.2.49) 11.934 ms 220-128-27-25.tpdt-3307.hinet.net (220.128.27.25) 14.843 ms 14.836 ms
 9 211-22-226-201.hinet-ip.hinet.net (211.22.226.201) 11.780 ms 11.898 ms 11.890 ms
10 core_wan_0201.cc.ntu.edu.tw (140.112.0.201) 11.939 ms 12.118 ms 11.908 ms
11 140.112.0.237 (140.112.0.237) 12.100 ms 12.091 ms 7.903 ms
12 140.112.149.122 (140.112.149.122) 10.766 ms 10.833 ms 39.908 ms
13 ws1.csie.ntu.edu.tw (140.112.30.186) 35.915 ms 35.888 ms 36.730 ms
```

```
[root@Client99 ~]# traceroute ws2.csie.org
traceroute to ws2.csie.org (140.112.30.187), 30 hops max, 60 byte packets
 1 _gateway (10.99.0.254) 1.756 ms 1.670 ms 1.657 ms
 2 192.168.64.1 (192.168.64.1) 3.990 ms 4.063 ms 4.055 ms
 3 192.168.3.99 (192.168.3.99) 7.788 ms 7.781 ms 7.834 ms
 4 192.168.202.1 (192.168.202.1) 7.803 ms 7.849 ms 7.934 ms
 5 * * *
 6 168-95-84-130.tpe4-3331.hinet.net (168.95.84.130) 9.368 ms 23.342 ms 23.399 ms
 7 220-128-5-65.tpe4-3301.hinet.net (220.128.5.65) 23.295 ms 220-128-5-9.tpe4-3301.hinet.net (220.128.5.9) 20.187 ms 20.138 ms
 8 * 220-128-3-134.tpdb-3031.hinet.net (220.128.3.134) 20.025 ms 20.012 ms
 9 220-128-26-93.tpdt-3307.hinet.net (220.128.26.93) 19.745 ms 220-128-26-13.tpdt-3307.hinet.net (220.128.26.13) 19.735 ms 220-128-26-93.tpdt-3307.hinet.net (220.128.26.93) 19.977 ms
10 211-22-226-201.hinet-ip.hinet.net (211.22.226.201) 20.079 ms 19.874 ms 19.774 ms
11 core_wan_0201.cc.ntu.edu.tw (140.112.0.201) 28.979 ms 28.968 ms 8.298 ms
12 140.112.0.237 (140.112.0.237) 8.188 ms 140.112.0.217 (140.112.0.217) 8.150 ms 10.733 ms
13 140.112.149.122 (140.112.149.122) 11.218 ms 12.452 ms 11.205 ms
14 ws2.csie.ntu.edu.tw (140.112.30.187) 10.951 ms 10.946 ms 10.679 ms
```

```
[root@Client99 ~]# traceroute ws3.csie.org
traceroute to ws3.csie.org (140.112.30.188), 30 hops max, 60 byte packets
 1 _gateway (10.99.0.254) 1.313 ms 1.958 ms 1.947 ms
 2 192.168.64.1 (192.168.64.1) 3.950 ms 3.942 ms 4.030 ms
 3 192.168.3.99 (192.168.3.99) 11.773 ms 13.014 ms 12.996 ms
 4 192.168.202.1 (192.168.202.1) 14.494 ms 14.422 ms 14.391 ms
 5 * * *
 6 tp-e4-c76r1.router.hinet.net (168.95.84.162) 18.879 ms 21.328 ms 15.075 ms
 7 220-128-5-65.tpe4-3301.hinet.net (220.128.5.65) 20.150 ms 220-128-5-9.tpe4-3301.hinet.net (220.128.5.9) 20.528 ms 220-128-5-65.tpe4-3301.hinet.net (220.128.5.65) 20.518 ms
 8 220-128-3-134.tpdb-3031.hinet.net (220.128.3.134) 19.907 ms 19.893 ms 20.091 ms
 9 220-128-26-93.tpd-3307.hinet.net (220.128.26.93) 26.651 ms 26.641 ms 220-128-26-13.tpd-3307.hinet.net (220.128.26.13) 14.941 ms
10 211-22-226-201.hinet-ip.hinet.net (211.22.226.201) 20.051 ms 20.039 ms 20.028 ms
11 core_wan_0201.cc.ntu.edu.tw (140.112.0.201) 20.632 ms 20.621 ms 19.759 ms
12 140.112.0.237 (140.112.0.237) 8.427 ms 140.112.0.217 (140.112.0.217) 11.207 ms 64.912 ms
13 140.112.149.122 (140.112.149.122) 69.504 ms 69.496 ms 69.488 ms
14 ws3.csie.ntu.edu.tw (140.112.30.188) 64.875 ms 66.273 ms 66.182 ms
```

```
[root@Client99 ~]# traceroute ws4.csie.org
traceroute to ws4.csie.org (140.112.30.189), 30 hops max, 60 byte packets
 1 _gateway (10.99.0.254) 3.026 ms 3.001 ms 3.584 ms
 2 192.168.64.1 (192.168.64.1) 5.018 ms 5.010 ms 5.004 ms
 3 192.168.3.99 (192.168.3.99) 7.669 ms 7.664 ms 7.834 ms
 4 192.168.202.1 (192.168.202.1) 14.092 ms 14.239 ms 14.235 ms
 5 * * *
 6 168-95-85-130.tpe4-3332.hinet.net (168.95.85.130) 15.853 ms 14.149 ms 14.013 ms
 7 220-128-4-14.tpd-3032.hinet.net (220.128.4.14) 12.571 ms 18.859 ms 18.846 ms
 8 220-128-2-49.tpd-3307.hinet.net (220.128.2.49) 18.871 ms 18.862 ms 18.852 ms
 9 211-22-226-201.hinet-ip.hinet.net (211.22.226.201) 18.805 ms 18.795 ms 18.784 ms
10 core_wan_0201.cc.ntu.edu.tw (140.112.0.201) 18.774 ms 18.765 ms 18.755 ms
11 140.112.0.217 (140.112.0.217) 18.782 ms 18.771 ms 140.112.0.237 (140.112.0.237) 16.646 ms
12 140.112.149.122 (140.112.149.122) 16.477 ms 10.319 ms 29.328 ms
13 ws4.csie.ntu.edu.tw (140.112.30.189) 29.117 ms 29.094 ms 24.290 ms
```

```
[root@Client99 ~]# traceroute ws5.csie.org
traceroute to ws5.csie.org (140.112.30.190), 30 hops max, 60 byte packets
 1 _gateway (10.99.0.254) 1.158 ms 1.123 ms 1.357 ms
 2 192.168.64.1 (192.168.64.1) 3.057 ms 3.029 ms 3.196 ms
 3 192.168.3.99 (192.168.3.99) 11.702 ms 11.686 ms 11.630 ms
 4 192.168.202.1 (192.168.202.1) 11.609 ms 11.598 ms 11.666 ms
 5 * * *
 6 168-95-85-134.tpe4-3332.hinet.net (168.95.85.134) 13.560 ms 24.100 ms 24.004 ms
 7 220-128-4-14.tpd-3032.hinet.net (220.128.4.14) 13.731 ms 14.568 ms 14.452 ms
 8 220-128-2-49.tpd-3307.hinet.net (220.128.2.49) 13.163 ms 220-128-27-25.tpd-3307.hinet.net (220.128.27.25) 17.877 ms 220-128-2-49.tpd-3307.hinet.net (220.128.2.49) 18.146 ms
 9 211-22-226-201.hinet-ip.hinet.net (211.22.226.201) 14.413 ms 14.706 ms 14.698 ms
10 core_wan_0201.cc.ntu.edu.tw (140.112.0.201) 14.690 ms 19.336 ms 19.328 ms
11 140.112.0.217 (140.112.0.217) 18.581 ms 19.283 ms 140.112.0.237 (140.112.0.237) 17.470 ms
12 140.112.149.122 (140.112.149.122) 20.347 ms 15.295 ms 15.269 ms
13 ws5.csie.ntu.edu.tw (140.112.30.190) 11.034 ms 9.912 ms 9.841 ms
```



至System -> Settings -> Administrations將ssh password login打開（或自行生成ssh-key）

Lobby

Reporting

System

Access

Configuration

Firmware

Gateways

High Availability

Routes

Settings

Administration

Cron

General

Logging

Logging / targets

Miscellaneous

Tunables

Trust

Wizard

Log Files

Diagnostics

Alternate Hostnames for DNS Rebinding and HTTP\_REFERER Checks

HTTP Compression

Off

Access log

☐ Enable access log

Listen Interfaces

All (recommended)

HTTP\_REFERER enforcement

☐ Disable HTTP\_REFERER enforcement check

Secure Shell

Secure Shell Server

☐ Enable Secure Shell

Login Group

wheel, admins

Root Login

☒ Permit root user login

Authentication Method

☒ Permit password login

SSH port

22

Listen Interfaces

All (recommended)

Advanced

Show cryptographic overrides

```
[root@Client99 ~]# ssh 10.99.0.254

[root@Client99 ~]# ssh 10.99.0.254
The authenticity of host '10.99.0.254 (10.99.0.254)' can't be established.
ED25519 key fingerprint is SHA256:dddeEFPFmLYZj09l+WP0adXkxJ8ZDJJvDPVKNmZ1t6E.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.99.0.254' (ED25519) to the list of known hosts.
(root@10.99.0.254) Password:
Last login: Sun Mar 31 02:28:41 2024

-----
|               Hello, this is OPNsense 24.1               |
|-----|-----|
| Website:      https://opnsense.org/                      |
| Handbook:    https://docs.opnsense.org/                  |
| Forums:      https://forum.opnsense.org/                 |
| Code:        https://github.com/opnsense                  |
| Twitter:     https://twitter.com/opnsense                 |
|-----|-----|
|               @@@@@@@@@@@@@@@@@@                        |
|               @@@@                                     @@@@ |
|               @@@\\      ///@@@                        |
|               ))))))      ((((((                       |
|               @@@//      \\@@@                         |
|               @@@@                                     @@@@ |
|               @@@@@@@@@@@@@@@@@@                        |
|-----|-----|

*** OPNsense.localdomain: OPNsense 24.1 ***

LAN (em1)      -> v4: 192.168.1.1/24
WAN (em0)      -> v4/DHCP4: 192.168.64.2/24
                v6/DHCP6: fd70:70a3:a6a8:38c8:5cbd:53ff:fe91:8025/64
vlan5 (vlan01) -> v4: 10.5.0.254/24
vlan8 (vlan03) -> v4: 10.8.0.254/24
vlan99 (vlan02) -> v4: 10.99.0.254/24

SSH:  SHA256 BvJ0kWHvgvItWi1Q+KRS7sa/XK6+LLXCbGuTHhStr88 (ECDSA)
SSH:  SHA256 dddeEFPFmLYZj09l+WP0adXkxJ8ZDJJvDPVKNmZ1t6E (ED25519)
SSH:  SHA256 YdCCUx6bekSjwnCLikr25clR+/wZcer0YNM/3PFL5cE (RSA)

0) Logout                7) Ping host
1) Assign interfaces      8) Shell
2) Set interface IP address  9) pfTop
3) Reset the root password 10) Firewall log
4) Reset to factory defaults 11) Reload all services
5) Power off system        12) Update from console
6) Reboot system           13) Restore a backup

Enter an option: █
```

分別至Firewall -> Rules -> VLAN5, VLAN8進行設定

### Firewall: Rules: vlan5

Select category Inspect

<input type="checkbox"/>	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description ?					
	Automatically generated rules  19												
<input type="checkbox"/>		IPv4 TCP	vlan5 net	*	This Firewall	*	*	*					
<input type="checkbox"/>		IPv4 ICMP	*	*	vlan8 net	*	*	*					
<input type="checkbox"/>		IPv4 *	*	*	*	*	block_VLAN5_all_day						
	pass	block		reject		log	in	first match					
	pass (disabled)	block (disabled)		reject (disabled)		log (disabled)	out	last match					

Active/Inactive Schedule (click to view/edit)

Alias (click to view/edit)

vlan5 rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

VLAN8

Firewall: Rules: vlan8

Select category

Inspect

The changes have been applied successfully.

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
Automatically generated rules								
	IPv4 *	vlan8 net	*	This Firewall	*	*	*	
	IPv4 *	*	*	vlan5 net	*	*	*	
pass	block	reject	log	in	first match			
pass (disabled)	block (disabled)	reject (disabled)	log (disabled)	out	last match			
Active/Inactive Schedule (click to view/edit)								
Alias (click to view/edit)								
vlan8 rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.								

請見以下分割畫面ping測試截圖：

```
[root@Client5 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether d2:f5:ee:1a:f7:92 brd ff:ff:ff:ff:ff:ff scope global dynamic enp0s1
    inet 10.37.129.4/24 metric 1024 brd 10.37.129.255 scope global dynamic enp0s1
        valid_lft 86080sec preferred_lft 86080sec
    inet6 fe80::d0f5:eeff:fe1a:f792/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
3: enp0s1.5@enp0s1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1496 qdisc noqueue state UP group default qlen 1000
    link/ether d2:f5:ee:1a:f7:92 brd ff:ff:ff:ff:ff:ff scope global dynamic enp0s1.5
    inet 10.5.0.1/24 metric 1024 brd 10.5.0.255 scope global dynamic enp0s1.5
        valid_lft 6924sec preferred_lft 6924sec
    inet6 fe80::d0f5:eeff:fe1a:f792/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
[root@Client5 ~]# ping 10.8.0.1
PING 10.8.0.1 (10.8.0.1) 56(84) bytes of data.
64 bytes from 10.8.0.1: icmp_seq=1 ttl=63 time=3.18 ms
64 bytes from 10.8.0.1: icmp_seq=2 ttl=63 time=4.68 ms
64 bytes from 10.8.0.1: icmp_seq=3 ttl=63 time=4.43 ms
64 bytes from 10.8.0.1: icmp_seq=4 ttl=63 time=4.89 ms
--- 10.8.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3009ms
rtt min/avg/max/mdev = 3.184/4.296/4.890/0.662 ms
[root@Client5 ~]#
```

```
[root@Client8 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1496 qdisc fq_codel state UP group default qlen 1000
    link/ether 6a:be:38:e4:13:40 brd ff:ff:ff:ff:ff:ff
    inet 10.37.129.3/24 metric 1024 brd 10.37.129.255 scope global dynamic enp0s1
        valid_lft 79591sec preferred_lft 79591sec
    inet6 fe80::68be:38ff:fee4:1340/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
3: enp0s1.8@enp0s1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1496 qdisc noqueue state UP group default qlen 1000
    link/ether 6a:be:38:e4:13:40 brd ff:ff:ff:ff:ff:ff
    inet 10.8.0.1/24 metric 1024 brd 10.8.0.255 scope global dynamic enp0s1.8
        valid_lft 5608sec preferred_lft 5608sec
    inet6 fe80::68be:38ff:fee4:1340/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
[root@Client8 ~]# ping 10.5.0.1
PING 10.5.0.1 (10.5.0.1) 56(84) bytes of data.
--- 10.5.0.1 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3073ms
[root@Client8 ~]#
```

Question 10

- 至Firewall -> Settings -> Schedules設定指定的schedule

Firewall: Settings: Schedules

Name	Time Range(s)	Description
block_VLAN5_all_day	March 14 0:00-23:59	

- 回到Firewall -> Rules新增VLAN5的Block schedule規則

Firewall: Rules: vlan5

Select category

Inspect

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
Automatically generated rules								
	IPv4 TCP	vlan5 net	*	This Firewall	*	*	*	
	IPv4 ICMP	*	*	vlan8 net	*	*	*	
	IPv4 *	*	*	*	*	*	block_VLAN5_all_day	
pass	block	reject	log	in	first match			
pass (disabled)	block (disabled)	reject (disabled)	log (disabled)	out	last match			
Active/Inactive Schedule (click to view/edit)								
Alias (click to view/edit)								
vlan5 rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.								

reference: <https://docs.opnsense.org/manual/firewall.html>

(<https://docs.opnsense.org/manual/firewall.html>)

## Question 11

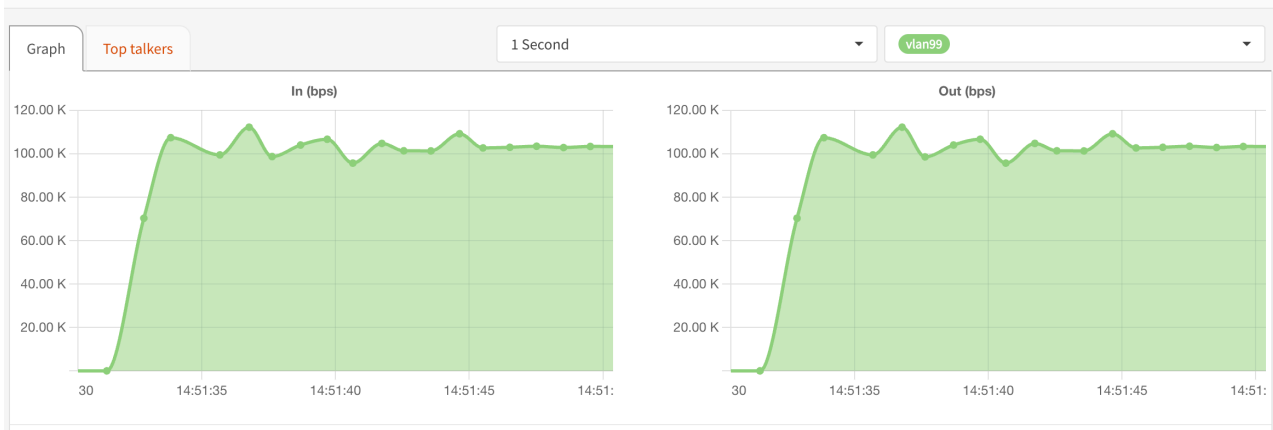
\*本題我選擇先在Client99上安裝hping，然後到Firewall -> 以利hping測試

- 計算網路流量時，封包大小和發送頻率共同決定了總體流量
- 使用hping指令，-1代表使用ICMP模式，-d後面定義資料傳輸量（bytes）；又手冊上有寫道u（waiting）代表hping傳送資料的等待時間，故經換算後有以下指令：

- 0.1Mb

```
$ hping -1 -i u100000 -d 1250 10.99.0.254 >/dev/null
```

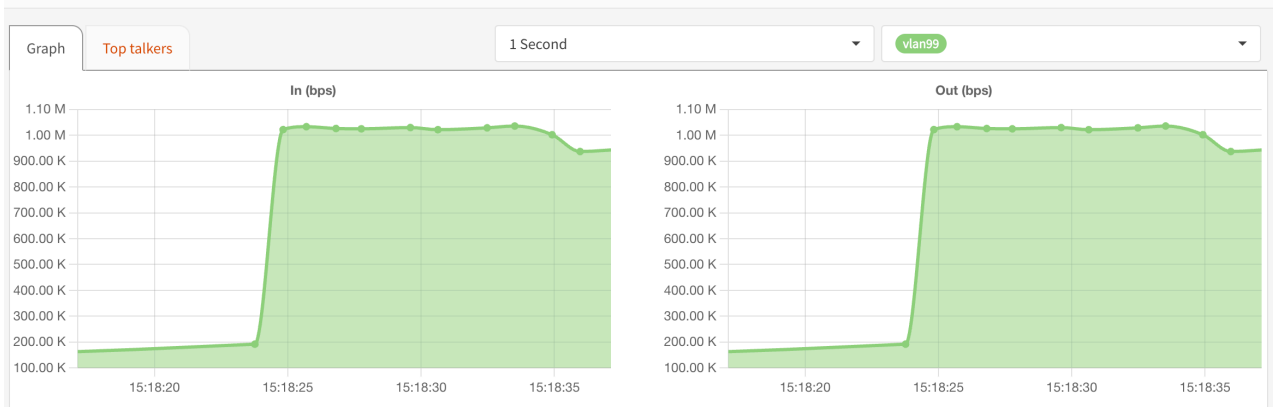
### Reporting: Traffic



- 1Mb

```
$ hping -1 -i u10000 -d 1250 10.99.0.254 >/dev/null
```

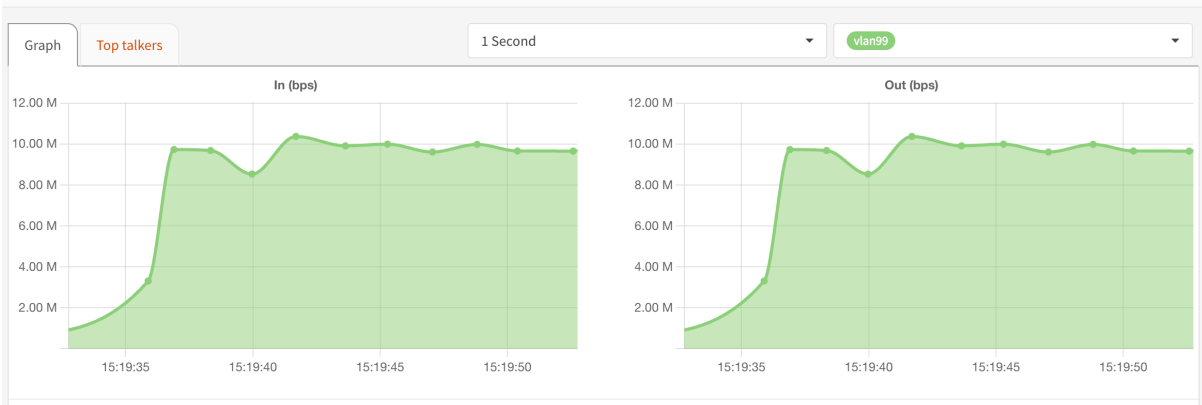
### Reporting: Traffic



- 10Mb

```
$ hping -1 -i u1000 -d 1250 10.99.0.254 >/dev/null
```

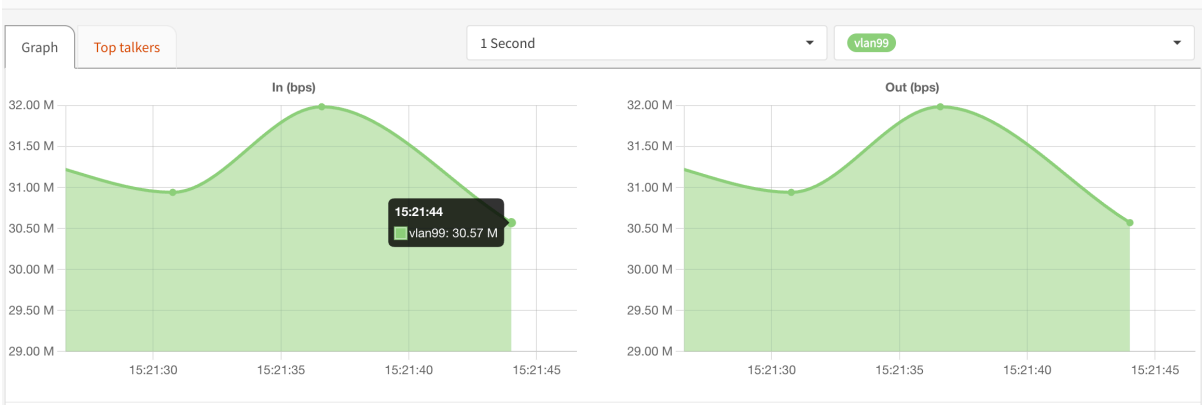
Reporting: Traffic



- 50Mb

```
$ hping -1 -i u200 -d 1250 10.99.0.254 >/dev/null
```

Reporting: Traffic

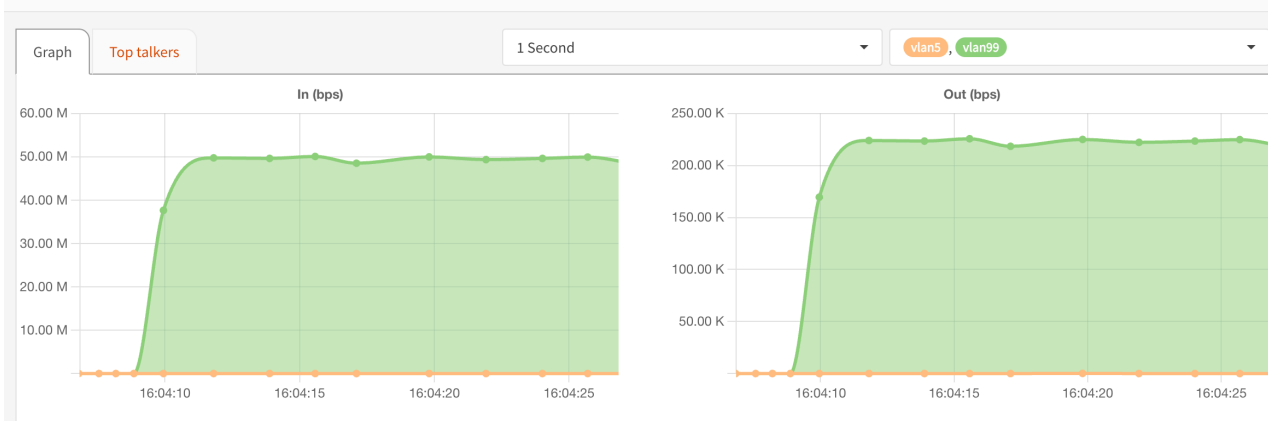


觀察：流量卡在30Mb上下，推論可能是流量達到上限

解決：試著將指令改為以下，由於ACK echo的回應量較小，可以節省流量

```
$ hping3 -S -p 80 -i u2000 -d 12500 10.99.0.254 >/dev/null
```

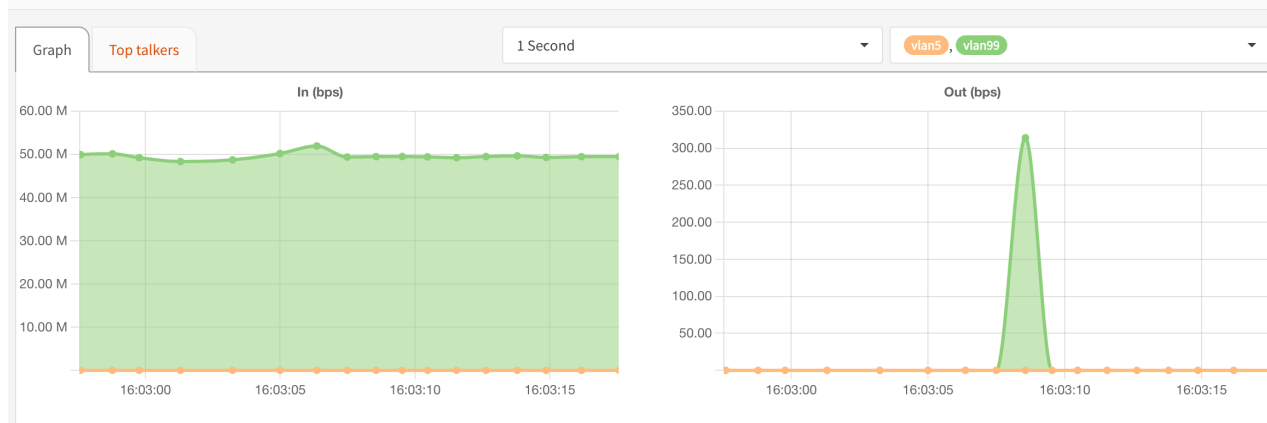
Reporting: Traffic



或嘗試將-d參數設為12500，讓Client99依照mtu狀況拆解封包

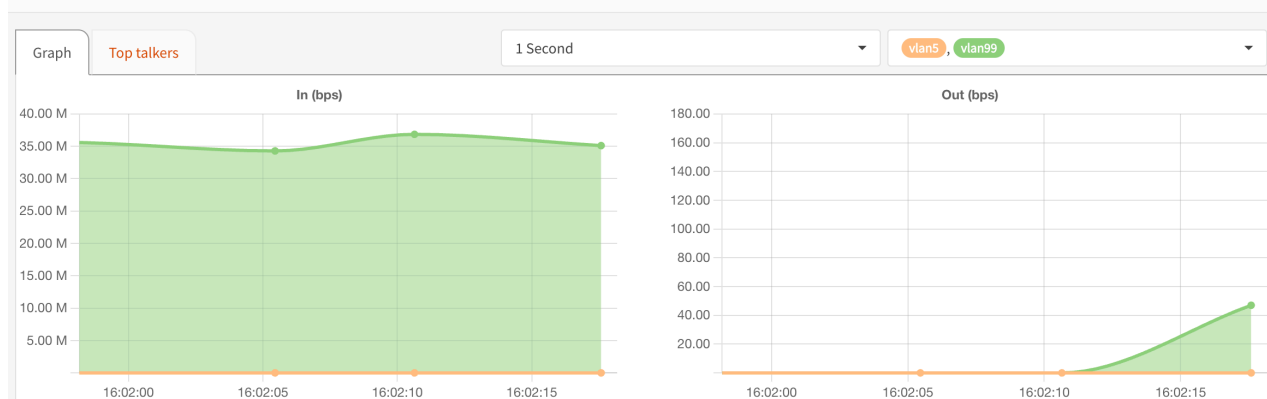
```
$ hping -1 -i u2000 -d 12500 10.99.0.254 >/dev/null
```

Reporting: Traffic



或嘗試新增firewall rule block掉ICMP的echo後重新執行

Reporting: Traffic



reference: <https://linux.die.net/man/8/hping3> (<https://linux.die.net/man/8/hping3>).

## Question 12

至System -> Configurations -> Backups下載，如附檔