

Network Administration/System Administration

Homework #4

B10202012 劉仲楷

Short Answers

1. Block 不會告知 client 的封包被 dropped；但 reject 會告知（TCP 透過 RST、UDP 透過 ICMP 的 Unreachable）。通常內網會用 reject，外網（不信任的來源）用 block。
來源：<https://docs.opnsense.org/manual/firewall.html#action>
2. Source $\xrightarrow{\text{in}}$ firewall $\xrightarrow{\text{out}}$ Destination。通常都直接限制 in 流量，out 只會在限制防火牆本身發出封包才會使用。
來源：<https://docs.opnsense.org/manual/firewall.html#direction>
3. Network 用所有來自那個介面的所有網段；address 是只有那個介面的單一 IP。Network 常用來允許該介面對外上網或封鎖整個子網等；address 常用來允許連線到防火牆的服務等。
來源：https://docs.opnsense.org/manual/firewall_generic.html#address-types

OPNsense

網路架構與環境設定

WAN 使用與 Lab 相同的 NAT 方式（預設 DHCP）

1 安裝 OPNsense

1. 新增虛擬機：
 - Name: opnsense
 - ISO: 剛剛載的 OPNsense ISO 檔
 - OS: FreeBSD 64-bit
 - RAM: 4GB
 - CPU: 2 cores
 - Disk size: 8G
2. 設定網卡：
 - Adapter 1: Host-only Adapter、vboxnet0、Intel PRO/1000 MT Desktop

-
- Adapter 2: NAT

3. 開機，登入 username: installer、password: opnsense，點選
 - (a) Continue with default keymap > Install UFS > VBox Harddisk 10 (7G) > Yes
 - (b) 安裝好後 Complete install > Reboot Now
4. 完成後即可 Shutdown，拔掉 ISO：
 - (a) Setting > Storage > Devices > OPNsense.*.iso > Remove attachment
5. 開機登入 username: root、password: opnsense，點選 3) Reset the root password 輸入新密碼（學號：b10202012）

2 設定 VLAN

1. 預設第一張網卡是 LAN，第二張網卡是 WAN。如果沒有自動識別請按 1 分配介面
2. WAN有DHCP，所以應該已經拿到 10.0.2.0/24 的 IP 了，點選
 - 2) Set interface IP address > LAN 設定LAN IP
 - (a) IPv4 address: 192.168.56.1
 - (b) Subnet bit count: 24
 - (c) 其他選項都用預設值
3. 連上 <https://192.168.56.1/>，登入 username: root、password: b10202012，setup wizard 的 Timezone 選 Asia/Taipei，剩下 Next 到底，最後 Apply。
4. 設定 VLAN 介面 Interfaces > Devices > VLAN
 - (a) 點 +
 - Device: vlan0.11
 - Parent: em0 [LAN]
 - VLAN tag: 11
 - Priority: Best Effort
 - Description: VLAN 11
 - (b) Save 後再加入 VLAN 12 和 VLAN 99，同樣設定換掉 11，最後按 Apply
5. Interfaces > Assignments
 - (a) 到 Assign a new interface，Description 各填 VLAN 11 後按 Add
 - (b) 同樣操作 VLAN 12、VLAN 99，最後按 Save
6. Interfaces > [VLAN11]
 - (a) 打勾 Enable interface
 - (b) IPv4 configuration type: Static IPv4

-
- (c) IPv4 address: 10.30.11.1/24
 - (d) 按 Save 和 Apply changes
 7. 同樣操作在 VLAN 12、VLAN 99，IP: 10.30.12.1/24、10.30.99.1/24
 8. WAN 預設 NAT，DHCP，不需要更動

3 DHCP

1. 設定 DHCP : **Services** > **ISC DHCPv4** > **[VLAN11]**
 - (a) 打勾 Enable
 - (b) Range From: 10.30.11.100，To: 10.30.11.199
 - (c) DNS Server: 8.8.8.8、8.8.4.4
 - (d) Save
2. 同樣操作 VLAN 12、VLAN 99，Range : 10.30.12.100 ~ 10.30.12.199、10.30.99.100 ~ 10.30.99.199
3. 設定防火牆 : **Firewall** > **Rules** > **[VLAN 11]** > +
 - Action: Pass
 - Interface: VLAN 11
 - Direction: in
 - Protocol: UDP
 - Destination port: (other) 67 ~ 68 (見 [EnWiki: DHCP#Operation](#))
 - Description: Allow DHCP traffic
4. Save 後 Apply changes，同樣設定在 VLAN 12，VLAN 99

4 Alias

1. 點選 **Firewall** > **Aliases**
2. 設定 **GOOGLE_DNS**
 - 點 +
 - 打勾 Enable
 - Name: **GOOGLE_DNS**
 - Type: Hosts
 - Content: 8.8.8.8, 8.8.4.4 (每打完一個按一次 tab)
 - Description: Google DNS
3. 設定 **GOOGLE_DNS**

-
- 點 +
 - 打勾 Enable
 - Type: Ports
 - Name: ADMIN_PORTS
 - Content: 20, 80, 443
 - Description: Admin ports

4. 設定 GOOGLE_DNS

- 點 +
- 打勾 Enable
- Type: Hosts
- Name: CSIE_WS
- Content: ws1.csie.org, ..., ws7.csie.org
- Description: CSIE workstation

5. Apply

5 SSH 和 VLAN 99

1. 設定 SSH：選單點選 System > Settings > Administration > Secure Shell (參考 [OPNSense forum: ssh access #2](#))

- 打勾 Enable Secure Shell
- 打勾 Permit root user login
- 打勾 Permit password login
- Save

2. 設定 VLAN 99 規則：選單 Firewall > Rules > [VLAN 99] > +

- Action: Pass
- Interface: VLAN 99
- Direction: in
- Protocol: any
- Source: VLAN 99 net
- Destination: GOOGLE_DNS, CSIE_WS
- Description: Allow VLAN99 to access Google DNS, CSIE

3. 點 Save，再新增一條規則：+

- Action: Pass
- Interface: VLAN 99
- Direction: in

- Protocol: TCP/UDP
- Source: VLAN 99 net
- Destination: This Firewall
- Description: Allow VLAN99 to access Google DNS, CSIE

4. 點 Apply Changes

結果：

`ip r & traceroute ws1.csie.org`

```
localhost:~# ip r & traceroute ws1.csie.org
default via 10.30.99.1 dev eth0.99
10.30.99.0/24 dev eth0.99 scope link src 10.30.99.10
traceroute to ws1.csie.org (140.112.30.182), 30 hops max, 46 byte packets
 1 10.30.99.1 (10.30.99.1) 1.232 ms 0.820 ms 1.517 ms
 2 10.0.3.2 (10.0.3.2) 1.373 ms 1.131 ms 1.366 ms
 3 gateway243.m3.ntu.edu.tw (140.112.243.254) 1.898 ms 1.255 ms 1.502 ms
 4 140.112.0.98 (140.112.0.98) 3.962 ms 1.768 ms 1.419 ms
 5 core_dorm_0230.cc.ntu.edu.tw (140.112.0.230) 1.609 ms 1.452 ms 1.869 ms
 6 140.112.0.237 (140.112.0.237) 3.228 ms 140.112.0.217 (140.112.0.217) 1.336 ms 1.384 ms
 7 140.112.149.122 (140.112.149.122) 3.731 ms 2.713 ms 4.043 ms
 8 ws7.csie.ntu.edu.tw (140.112.30.182) 1.598 ms 1.683 ms 1.391 ms
[11]+  Done                  ip r
localhost:~#
```

`ssh root@10.30.99.1`

```

localhost:~# ssh root@10.30.99.1
The authenticity of host '10.30.99.1 (10.30.99.1)' can't be established.
ED25519 key fingerprint is SHA256:F0lgI0j693jIFJEFwXU+dE9HrBGJf2ycdZQAxTAynvI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.30.99.1' (ED25519) to the list of known hosts.
(root@10.30.99.1) Password:
Last login: Wed Oct  8 01:26:28 2025

-----
|      Hello, this is OPNsense 25.7      |
|                                         |
| Website:    https://opnsense.org/      |
| Handbook:   https://docs.opnsense.org/ |
| Forums:     https://forum.opnsense.org/ |
| Code:       https://github.com/opnsense |
| Reddit:     https://reddit.com/r/opnsense |
|                                         |
-----

*** OPNsense.internal: OPNsense 25.7 (amd64) ***

LAN (em0)      -> v4: 192.168.56.1/24
VLAN11 (vlan0.11) -> v4: 10.30.11.1/24
VLAN12 (vlan0.12) -> v4: 10.30.12.1/24
VLAN99 (vlan0.99) -> v4: 10.30.99.1/24
WAN (em1)      -> v4/DHCP4: 10.0.3.15/24
                v6/DHCP6: fd17:625c:f037:3:a00:27ff:fec1:cdec/64

HTTPS: sha256 C2 FD 42 AE 21 73 00 8C AA 16 B8 8B 7B D4 13 30
        A6 F8 25 97 7C B5 09 B7 29 27 61 24 AC 73 90 07
SSH:   SHA256 QqEDF1ku4kkhhnLupuU8qbhEqc5/PAQnE1EEmr21VR0 (ECDSA)
SSH:   SHA256 F0lgI0j693jIFJEFwXU+dE9HrBGJf2ycdZQAxTAynvI (ED25519)
SSH:   SHA256 Zn8DKLZIJF7YnGmMkxg80SDdTjquVpN+NzBlyipjst4 (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: _

```

6 VLAN 11 和 VLAN 12

- 設定自動抓取：點選 Firewall > Aliases > + (參考 [OPNSense docs: aliases#url-tables](#))
 - 打勾 Enable
 - Name: BLOCK_SITES
 - Type: URL Table (IPs)
 - Content: https://www.csie.ntu.edu.tw/~euom/colorful_websites.txt
 - Description: Block Sites
- 設定 Schedule：點選 Firewall > Settings > Schedules > +

-
- Name: Mon_AM
 - Description: Every Mon 9-12
 - Month 下面點選 Mon
 - Time: Start time 選 09:00 ; Stop time 選 12:00
 - 點 Add time > Save
3. 設定阻擋早上 traffic 規則：選單 Firewall > Rules > [VLAN 11] > + (以下沒寫都是預設，寫完規則都要點 Save)
- Action: Block
 - Description: Block all traffic every Mon 9-12
 - Schedule: Mon_AM
4. 設定阻擋 VLAN 99、防火牆 規則：選單 Firewall > Rules > [VLAN 11] > +
- Action: Block
 - Source: VLAN 11 net
 - Destination: This Firewall, VLAN 99 net
 - Description: Block access to Firewall, VLAN99
5. 設定阻擋給定網址：再點 +
- Action: Block
 - Source: VLAN 11 net
 - Destination: BLOCK_SITES
 - Description: Block access to given sites
6. 重複在 VLAN 12 設定這三條規則
7. 允許 VLAN 11 連線到 VLAN 12 : Firewall > Rules > [VLAN 11] > +
- Action: Pass
 - Source: VLAN 11 net
 - Destination: VLAN 12 net
 - Description: Allow VLAN11 to VLAN12
8. 阻擋 VLAN 12 連線到 VLAN 12 : Firewall > Rules > [VLAN 12] > +
- Action: Block
 - Source: VLAN 12 net
 - Destination: VLAN 11 net
 - Description: Block VLAN12 to VLAN11
9. 允許所有 traffic (VLAN 11、12 都要) : Firewall > Rules > [VLAN 1?] > +
- Action: Pass
 - Description: Allow all traffic
10. 注意照上面順序建立會得到 rules 的順序是 allow DHCP > block Mon 9-12 > 剩下的 > Allow all traffic。並且都是 first match 規則。最後要 Apply changes。

7 下載 Backup

略過