NASA HW4

B11901164 陳秉緯

Short Answers

1.
   - Block: 拒絕流量並且不讓client端知道它已被丟棄，通常適用於不受信任的網路
   - Reject: 拒絕流量並讓client端知道，當不允許存取時，client端不必等待time-out
   - 連結：https://docs.opnsense.org/manual/firewall.html#action

2.
   - Direction "in"：表示規則適用於進入防火牆介面的流量。使用時機：想控制從外部網路進入防火牆的流量時，例如允許或拒絕特定來源 IP 的連線，適用於保護內部網路，防止未經授權的外部訪問。
   - Direction "out"：表示規則適用於從防火牆介面出去的流量。使用時機：想控制從內部網路流向外部網路的流量時，例如限制內部用戶訪問特定網站或服務，適用於管理內部用戶的對外訪問，防止資料外洩或限制不必要的流量。
   - 連結：https://docs.opnsense.org/manual/firewall.html#direction

3.
   - interface net：與該 interface 相關的整個subnet，它會自動包含該介面所屬網段的所有 IP addresses。
   - interface address：該 interface 本身的 IP address，而不是整個子網。
   - 連結：https://docs.opnsense.org/manual/firewall.html#basic-settings

OPNsense

1. ref: https://hackmd.io/@FHVirus/nasa2025-fw-lab#/
   步驟：
   1. 下載 OPNsense qcow2 檔
   2. 使用下列指令把 .qcow2 轉成 .vdi 檔：
      ```
      qemu-img convert -f qcow2 -O vdi <qcow2 檔名>.qcow2 <output 檔名>.vdi
      ```

2. ref: https://hackmd.io/@FHVirus/nasa2025-fw-lab#/
   步驟：
   1. 打開Oracle VirtualBox，點擊 New
   2. Name: [HW4] OPNsense, Type: BSD, Base Memory: 4096 MB, 點擊Use an Existing Virtual Hard Disk File，選擇剛剛的 .vdi 檔，好了後按 Finish

3. 點 Tools > Create 一個 Host-only Networks vboxnet0，底下 IPV4 Address: 192.168.56.10, IPV4 Network Mask: 255.255.255.0
4. 點剛剛新增的 [HW4] OPNsense，點 Settings > Network，Adapter 1 的 Attached to: Host-only Adapter，然後enable Adapter 2，Attached to: NAT，如果後來發現網路有問題，就去Tools > NAT Networks 點擊 Create 新增 NatNetwork，並更換 Attached to 成NatNetwork
5. 開機
6. root 登入
7. 2
8. 1
9. Enter
10. LAN IPV4 Address: 192.168.56.1
11. 24
12. Enter到底，看到
    - LAN (em0) -> v4: 192.168.56.1/24
    - WAN (em1) -> v4/DHCP4: 10.0.2.15/24
13. 3. Reset the root password
14. 更改密碼成 b11901164
15. 在瀏覽器打開 192.168.56.1
16. 帳號：root，密碼：b11901164
17. setup wizard 取消 取消 "Block private networks..." 與 "Block non-Internet routed networks..."，其他就一直點Next
18. 在 Interfaces > Devices > VLAN 新增 vlan0.11, vlan0.12, and vlan0.99
19. 在 Interfaces > Assignments 新增 [VLAN11], [VLAN12], and [VLAN99]
20. 分別點擊 [VLAN11], [VLAN12], and [VLAN99]，進去按Enable， IPv4 Configuration Type 改成 Static IPv4，IPv4 address分別是 10.30.11.1/24, 10.30.12.1/24, and 10.30.99.1/24，最後點 Save

3. ref: https://docs.opnsense.org/manual/dhcp.html#using-dhcpv4
步驟：
    1. 在 Services > ISC DHCPv4 > [VLAN 11]
        - 點 Enable DHCP server on VLAN11 Interface
        - from: 10.30.11.100
        - to: 10.30.11.199
        - DNS servers: 8.8.8.8, 8.8.4.4
        - 點 Save

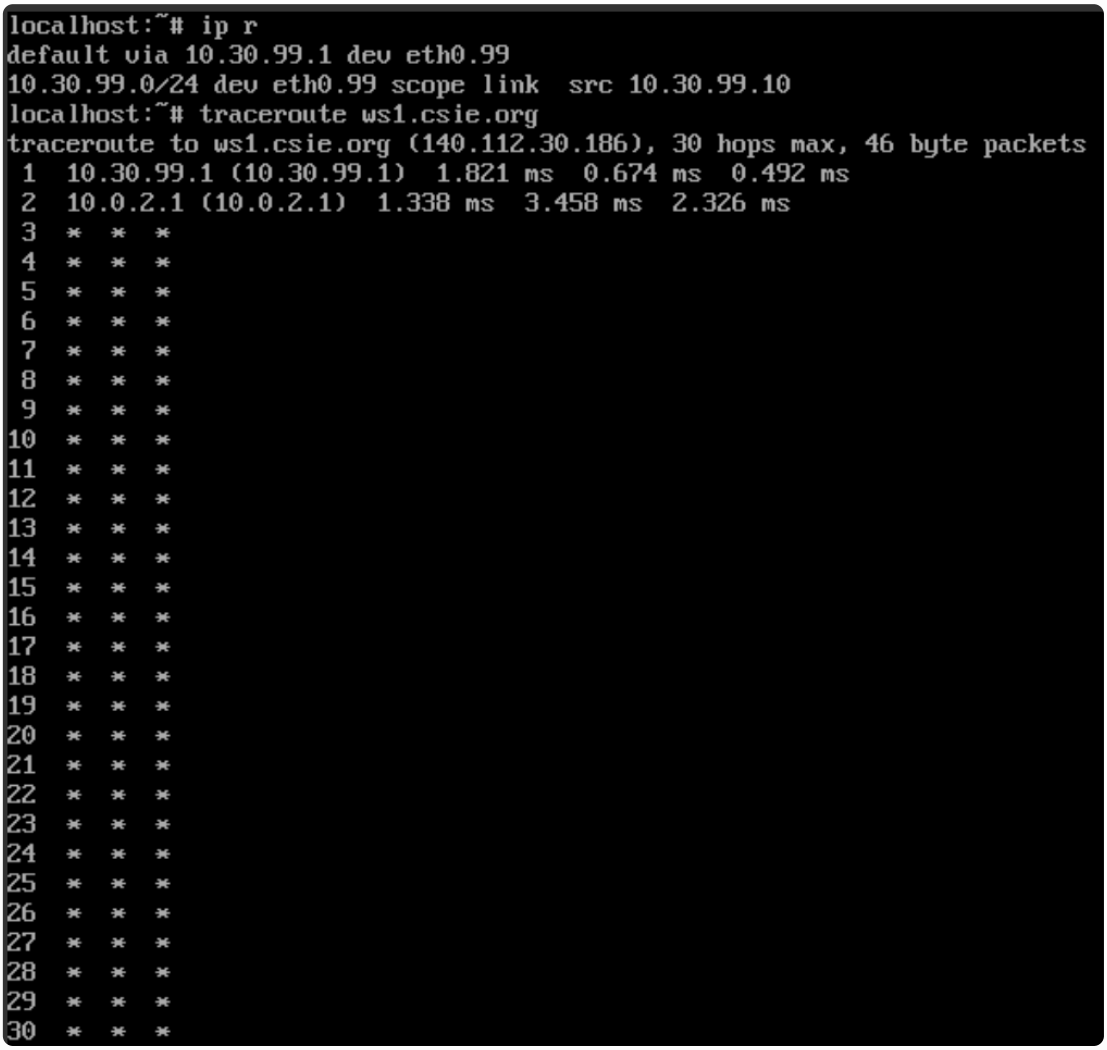
2. [VLAN 12] 與 [VLAN99] 也做一樣的操作，只是 11 改成 12 或 99
3. 在 Firewall > Rules > VLAN11 新增規則
    - 允許 DHCP 流量
        - Action: Pass
        - Protocol: UDP
        - Source: VLAN11 net
        - Destination: This Firewall
        - Destination port range: from 67 to 68
    - 允許 Google DNS 流量
        - Action: Pass
        - Protocol: UDP/TCP
        - Source: VLAN11 net
        - Destination: any
        - Destination Port: DNS
4. Save & Apply
5. 在 Firewall > Rules > VLAN12 重複步驟 3 - 4
6. 在 Firewall > Rules > VLAN99 重複步驟 3 - 4

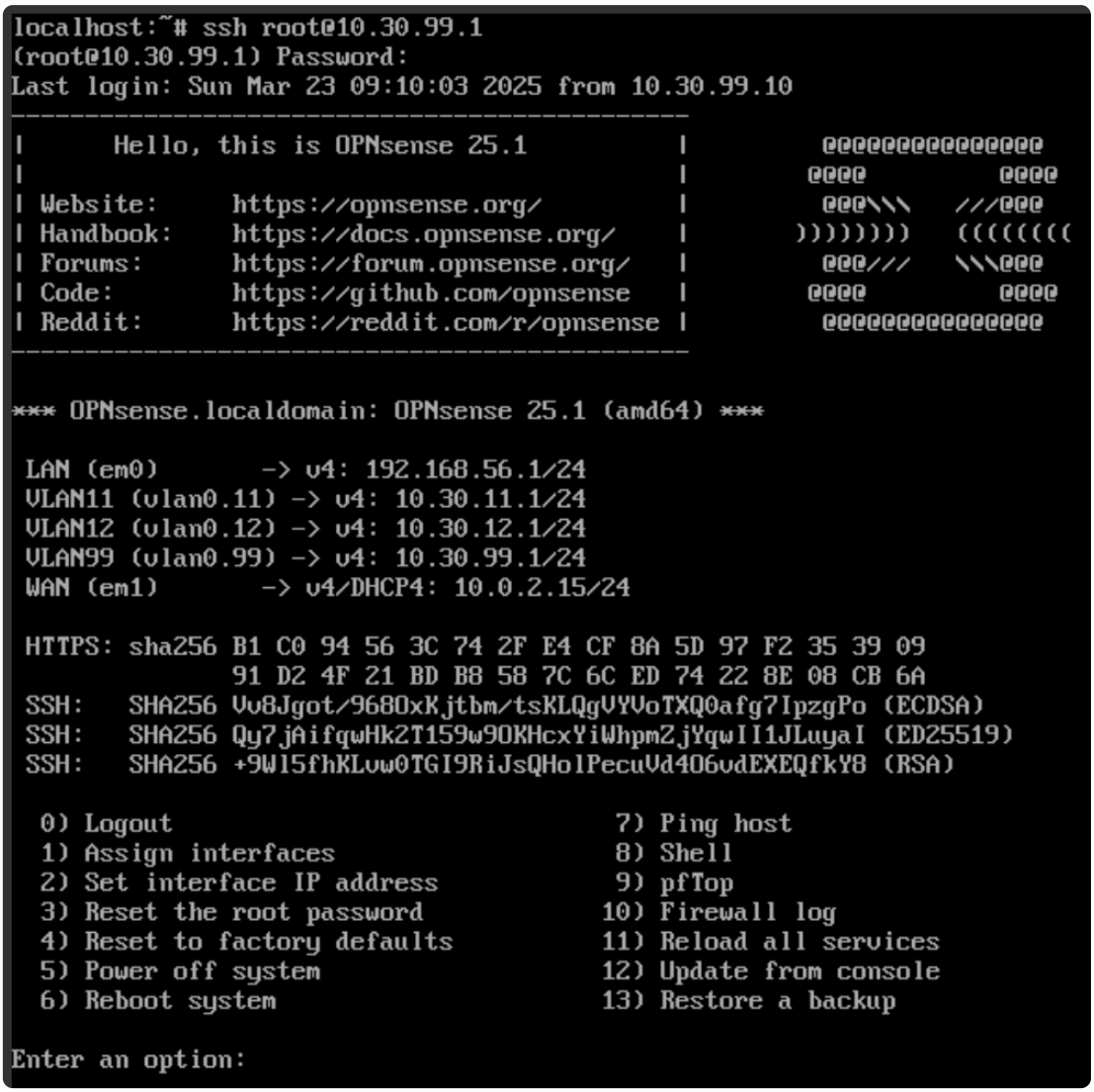
4. ref: https://docs.opnsense.org/manual/aliases.html#aliases
步驟：
    1. 去 Firewall > Aliases
    2. 點擊 +
    3.
        - Name: GOOGLE_DNS
        - Type: Host(s)
        - Content: 8.8.8.8, 8.8.4.4
    4. 點擊 Save & Apply
    5. 點擊 +
    6.
        - Name: ADMIN_PORTS
        - Type: Port(s)
        - Content: 22, 80, 443
    7. 點擊 Save & Apply
    8. 點擊 +
    9.
        - Name: CSIE_WS
        - Type: Host(s)

        - Content: ws1.csie.org, ws2.csie.org, ws3.csie.org, ws4.csie.org, ws5.csie.org, ws6.csie.org, ws7.csie.org
    10. 點擊 Save & Apply
5. ref: https://docs.opnsense.org/manual/settingsmenu.html#secure-shell
   步驟：
    1. 去 System > Settings > Administration
    2. 在 Secure Shell 將以下打勾
        - Enable Secure Shell
        - Permit root user login
        - Permit password login
    3. 點擊 Save
    4. 去 Firewall > Rules > VLAN99
    5. 點擊 + 新增：允許 VLAN99 透過 ADMIN_PORTS 連到防火牆
        - Action: Pass
        - Protocol: TCP
        - Source: VLAN99 net
        - Destination: This Firewall
        - Destination port range: from ADMIN_PORTS to ADMIN_PORTS
    6. 點擊 Save & Apply
    7. 點擊 + 新增：允許 VLAN 99 存取 GOOGLE_DNS
        - Action: Pass
        - Protocol: TCP/UDP
        - Source: VLAN99 net
        - Destination: GOOGLE_DNS
        - Destination Port: DNS
    8. 點擊 Save & Apply
    9. 點擊 + 新增：允許 VLAN 99 存取 CSIE_WS
        - Action: Pass
        - Protocol: TCP/UDP
        - Source: VLAN99 net
        - Destination: CSIE_WS
    10. 點擊 Save & Apply
    11. 點擊 + 新增：阻擋所有其他流量
        - Action: Block

- Protocol: any
- Source: VLAN99 net
- Destination: any

12. 點擊 Save & Apply
13. 截圖：





6. ref: https://pfsensesetup.com/opnsenseinstall.com/how-to-schedule-a-rule-in-opnsense/

   步驟：

   1. 去 Firewall > Rules > VLAN11
   2. 點擊 + 新增：阻擋 VLAN 11 存取防火牆
      - Action: Block
      - Protocol: any
      - Source: VLAN11 net
      - Destination: This Firewall
   3. 點擊 Save & Apply
   4. 點擊 + 新增：阻擋 VLAN 11 存取 VLAN 99
      - Action: Block
      - Protocol: any
      - Source: VLAN11 net
      - Destination: VLAN99 net

5. 點擊 Save & Apply
6. 去 Firewall > Rules > VLAN12
7. 點擊 + 新增：阻擋 VLAN 12 存取防火牆
    - Action: Block
    - Protocol: any
    - Source: VLAN12 net
    - Destination: This Firewall
8. 點擊 Save & Apply
9. 點擊 + 新增：阻擋 VLAN 12 存取 VLAN 99
    - Action: Block
    - Protocol: any
    - Source: VLAN12 net
    - Destination: VLAN99 net
10. 點擊 Save & Apply
11. 去 Firewall > Aliases
12. 點擊 +
13.
    - Name: BLOCKED_SITES
    - Type: URL Table (IPs)
    - Content: https://www.csie.ntu.edu.tw/~euom/colorful_websites.txt
    - Refresh Frequency: Days: 1, Hours: 0
14. 點擊 Save & Apply
15. 去 Firewall > Rules > VLAN11
16. 點擊 + 新增：阻擋 VLAN 11 存取 這個網址
    - Action: Block
    - Protocol: any
    - Source: VLAN11 net
    - Destination: BLOCKED_SITES
17. 點擊 Save & Apply
18. 去 Firewall > Rules > VLAN12
19. 點擊 + 新增：阻擋 VLAN 12 存取 這個網址
    - Action: Block
    - Protocol: any
    - Source: VLAN12 net
    - Destination: BLOCKED_SITES

20. 點擊 Save & Apply
21. 去 Firewall > Rules > VLAN11
22. 點擊 + 新增： VLAN 11 可以建立連線到 VLAN 12
    - Action: Pass
    - Protocol: any
    - Source: VLAN11 net
    - Destination: VLAN12 net
23. 點擊 Save & Apply
24. 去 Firewall > Rules > VLAN12
25. 點擊 + 新增： VLAN 12 不可以建立連線到 VLAN 11
    - Action: Block
    - Protocol: any
    - Source: VLAN12 net
    - Destination: VLAN11 net
26. 點擊 Save & Apply
27. 去 Firewall > Settings > Schedules
28. 點擊 +
29.
    - Name: Monday_Block
    - Month 點 Mon
    - Time: Start Time: 9:00, Stop Time: 12:00
30. 點擊 Add Time & Save
31. 去 Firewall > Rules > VLAN11
32. 點擊 + 新增： 每個禮拜一的早上 09:00 到 12:00，VLAN 11 不可以通過除了對防火牆的 DHCP 請求及回應之外的任何封包
    - Action: Block
    - Protocol: any
    - Source: VLAN11 net
    - Destination: any
    - Schedule: Monday_Block
33. 點擊 Save & Apply
34. 點擊 + 新增： 允許 VLAN 11 可以自由和其他機器建立連線
    - Action: Pass
    - Protocol: any
    - Source: VLAN11 net

    - Destination: any
35. 點擊 Save & Apply
36. 去 Firewall > Rules > VLAN12
37. 點擊 + 新增： 每個禮拜一的早上 09:00 到 12:00，VLAN 12 不可以通過除了對防火牆的 DHCP 請求及回應之外的任何封包
    - Action: Block
    - Protocol: any
    - Source: VLAN12 net
    - Destination: any
    - Schedule: Monday_Block
38. 點擊 Save & Apply
39. 點擊 + 新增： 允許 VLAN 12 可以自由和其他機器建立連線
    - Action: Pass
    - Protocol: any
    - Source: VLAN12 net
    - Destination: any
40. 點擊 Save & Apply

7. ref: https://docs.opnsense.org/manual/backups.html#backup
   步驟：
   1. 點擊 System > Configuration > Backups
   2. 確保Download下兩個勾勾都沒勾
   3. 點擊按鈕 Download configuration
   4. 更改檔名成 b11901164.xml