

## Homework #4

Due Time: 2025/03/23 (Sun.) 21:59

Red Correction Date: 2025/03/19

Contact TAs: vegetable@csie.ntu.edu.tw

### Instructions and Announcements

- **NO LATE SUBMISSION OR PLAGIARISM IS ALLOWED.**
- Discussions with others are encouraged. However, you should write down your solutions **in your own words**. In addition, for **each and every** problem you have to specify the references (the URL of the web page you consulted or the people you discussed with) on the first page of your solution to that problem.
- Some problems below may not have standard solutions. We will give you the points if your answer is followed by reasonable explanations.

### Submission

- Please place your answers in the same order as the problem sheet and do not repeat problem descriptions, just organize them by problem number in a tidy manner.
- Please zip the pdf file and xml file, name the zip file “{your\_student\_id}.zip”, and submit it via NTU COOL. The directory layout should be the same as listed below:

```
{your_student_id}/  
+-- {your_student_id}.pdf  
+-- {your_student_id}.xml
```

### Grading

- The total score for the correctness and completeness of your answer is 100 points.
- It's possible you don't get full credits even if you have the correct answer. You should show how you get the answers step by step and list the references.
- Tidiness score: 3 bonus points, graded by TA.
- Final score = correctness score + tidiness score.

## Short Answers (15 pt)

為了練習看文件，以下的簡答題請在最後附上在 OPNsense 的[官方文件](#)中可以找到答案的頁面連結（請直接寫出連結，不要使用 \href 等指令）。

1. (5 pt) 請說明 OPNsense 的 Rules 設定中，“Block” 和 “Reject” 兩個選項的差別以及使用時機。
2. (5 pt) 請說明 OPNsense 的 Rules 設定中，Direction 的 “in” 和 “out” 兩個選項的差別以及使用時機。
3. (5 pt) 請說明 OPNsense 的 Rules 設定中，Source 和 Destination 選擇 “interface net” 和 “interface address” 兩個選項的差別。



## OPNsense<sup>1</sup> (85 pt)

這次的作業的主要目標為：

1. 模擬系上部份網路架構
2. 安裝並架設完整的 OPNsense 服務
3. 練習寫文件 (Document)

### 網路架構與環境設定 (0 pt 但要看一下)

#### 網路架構

本次的網路架構模擬架構說明以 Oracle VirtualBox 為主。以下標注  HINT  的說明皆為建議而非硬性規定，你可以自行選擇喜歡的設定方式。若使用其他的 VM hypervisor (VMware, Hyper-V, QEMU 等)，請自行找尋適合的設定方式。

這次要模擬的網路架構如圖 1：

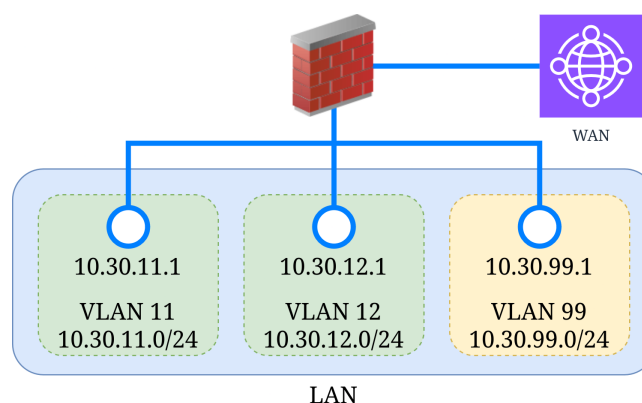










Figure 1: 要模擬的網路架構圖





- 有一個 WAN，防火牆透過一個獨立的介面 (interface) 接上 WAN。
  - 此 WAN 需要能連上網際網路。

<sup>1</sup>是 OPNsense，不是 OPNSense 也不是 OpenSense

- 請在你的作業中註明防火牆的 WAN 設定方式(如：使用 DHCP 或 Static IP)和 IP/subnet。
-  HINT  在模擬環境中，建議使用 VirtualBox 的 NAT 或 NAT 等來模擬 WAN。
- 有一個 Network 當作 LAN，此 LAN 被數個 VLAN 共用；防火牆則透過一個介面連接 LAN，再將此介面分割為子介面（如 Lab 操作內容）後接上所有 VLAN。
  - 防火牆 VM 對 LAN 只能有一個實體介面。
  - 此 LAN 中要有三個 VLAN，分別是：
    - \* VLAN 11: 10.30.11.0/24（模擬教室一）
    - \* VLAN 12: 10.30.12.0/24（模擬教室二）
    - \* VLAN 99: 10.30.99.0/24（模擬管理專用 VLAN）
  -  HINT  在模擬環境中，建議使用 VirtualBox 的 Host-only Network 或 Internal Network 來模擬 LAN。
  -  HINT  VirtualBox 的 Host-only Network 雖然有指定 Host (你的電腦) 的 IP 和 subnet，但其實不在此 subnet 裡的 VM 們也可以互相溝通（只是 Host 戳不到）；VM 們接上同一個 Host-only Network 就會像接上同一臺 switch 一樣。
  -  HINT  VirtualBox 的 Host-only Network 預設會限制可以指定的 subnet，可以透過修改設定檔來更改或取消限制。詳見[這裡](#)。

## VM 設定

OPNsense 的 VM 規格可以仿照 Lab 時的設定，給 4GB 記憶體、單核 CPU。

-  HINT  如果你是用 ISO 安裝，建議給 8GB 硬碟；使用.qcow2/.vdi 開機的話不需更改。
-  HINT  如果跑不起來，可以試試在 VirtualBox 的設定指定作業系統版本（FreeBSD）或是給雙核 CPU（在某些 Windows 機器上似乎有差）。

AMD64 架構的 OPNsense ISO 檔可以到 [OPNsense 官方下載區](#) 下載；AMD64 和 ARM 架構都可到 [這個非官方的版本](#) 下載 qcow2 檔，並使用 `qemu-img convert -f qcow2 -o vdi <qcow2 檔名>.qcow2 <output 檔名>.vdi`，便可使用 VirtualBox 正常開啟 VM。請注意不要照 release 頁面所說的 **resize 硬碟**，否則可能會發生不可預期的錯誤。

本次作業涉及較複雜的網路架構模擬，不建議使用 QEMU 操作；又因作業會需要架設 DHCP server，請不要使用 bridge 網路模擬 LAN；請避免讓 OPNsense 的 DHCP server 發送 IP 給你架設的 VM 以外的任何機器。

## 防火牆安裝 (85 pt)

### 作答說明

在設定好環境之後，終於要來設定防火牆了！對於每一題，請條列式寫下你詳細的設定步驟，如：

1. 用瀏覽器到 <https://10.30.99.1/> 登入，帳號：root，密碼：<fw\_passwd>
2. 進入 Firewall > Rules > WAN 頁面，點右上角加號新增一條 rule：
  - (列出每個需要改的選項，若保持預設值可以省略、都選是或否可以簡略說明)
  - (如果夠短的話也可以寫成一句、不用條列，以清楚為原則)
3. 按 Save 並在回到 Rules 頁面後按 Apply

請特別注意防火牆 rule 的順序，若未特別註明將依作答順序做判斷。

💡HINT💡 你可以自己開其他虛擬機（Alpine 等）來做測試，但不需附上測試步驟及結果。

💡HINT💡 以上只是示範，不用每題都寫怎麼登入。

## 題目

- (15 pt) 有別於 Lab 的操作，請安裝 OPNsense（VM 關機、拔掉 ISO、開機後可以正常使用 OPNsense）或是使用 .qcow2/.vdi 硬碟開機，並從 console 設定防火牆的各個介面和 root 密碼。
  - root 的密碼須設為你的學號，英文字母小寫。
  - 因為安全性因素，在安裝過程中不可以把 pfctl 關掉（所以你可能想 Host-only Network 來模擬 LAN）
  - 本題只需要安裝 OPNsense，其他的設定（e.g., 指定 IP、使用 setup wizard 等）請寫在下一題。
- (15 pt) 防火牆的 VM 最多只可以有兩個介面。其中，LAN 介面要像 trunk 一樣跑 tagged VLAN traffic，而三個連接 VLAN 的介面要是從同一個 LAN 介面分出來的（如 Lab 操作）。IP 要求：

介面	VLAN Tag	防火牆 IP
WAN	none	自行選擇
LAN		
VLAN 11: 10.30.11.0/24	11	10.30.11.1
VLAN 12: 10.30.12.0/24	12	10.30.12.1
VLAN 99: 10.30.99.0/24	99	10.30.99.1

請簡述你的 VM 的介面設定、你的 WAN / LAN 是哪種 Network，以及你選擇的 IP 和 subnet。

- VirtualBox 網路預設就是 trunk mode、可以讓所有 VLAN 的封包通過。
  - 💡HINT💡 VLAN 預設和 WAN 一樣會 block 所有的 connection，測試時請注意。
- (10 pt) 請以 ISC DHCP service 設定防火牆做為 VLAN 11、VLAN 12、VLAN 99 的 DHCP server
    - DHCP lease 中的 DNS server 要有 8.8.8.8 和 8.8.4.4
    - DHCP 只能發放尾數為 .100 ~ .199 的 IP
    - 記得要設定防火牆的 rule 讓 DHCP 會通！
    - 再次提醒，**請勿讓 OPNsense 的 DHCP server 發送 IP 給外面的設備。**
  - (5 pt) 請設定以下 alias：

Alias Name	Value
GOOGLE_DNS	8.8.8.8, 8.8.4.4
ADMIN_PORTS	22, 80, 443
CSIE_WS	ws1.csie.org, ws2.csie.org, ..., ws7.csie.org



- (15 pt) 打開防火牆的 SSH 功能，並設定讓使用者 root 可以用密碼登入。設定 VLAN 99 的機器可以透過 ADMIN\_PORTS 連到防火牆，且 VLAN 99 的機器只能存取以下位址或機器：

- GOOGLE\_DNS
- CSIE\_WS
- 防火牆本身。

設定的過程中，請記得要設定 rule 的 source IP。完成本題後請：

- 請提供由 VLAN 99 中的機器 ip r 和 traceroute 到 CSIE\_WS 中任一機器的截圖，需含有指令本身。如果你擔心個資，你可以讓 VM Hypervisor（你的電腦）連上 CSIE VPN。
- 請提供由 VLAN 99 中的機器 ssh 到防火牆的截圖，需含有指令本身。

6. (15 pt) 請替教室的網路設定以下規則：

- VLAN 11、VLAN 12 中的任何機器皆不可與防火牆本身或 VLAN 99 中任何機器連線。但對防火牆的 DHCP 請求及回應除外。
- VLAN 11 和 VLAN 12 中的任何機器皆不可連線到 [這個網址](#) 裡列出的網址對應的 IP 位址。
  - 請設定防火牆每天自動抓取這個網址的最新內容，並更新取得的 IP 位址列表。
  -  HINT  請善用 alias 功能。
- VLAN 11 的機器可以建立連線到 VLAN 12 的機器，反之則不行。
- 每個禮拜一的早上 09:00 到 12:00，VLAN 11 和 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。
- 除上述規定外，VLAN 11 和 VLAN 12 的機器可以自由和其他機器建立連線。

7. (10 pt) 備份設定是很重要的！請到 System > Configuration > Backups 下載備份設定檔 config.xml，將檔名改為你的學號（英文字母小寫，如 b11902030.xml）連同作業 PDF 一起繳交。