PFSENSE 設定

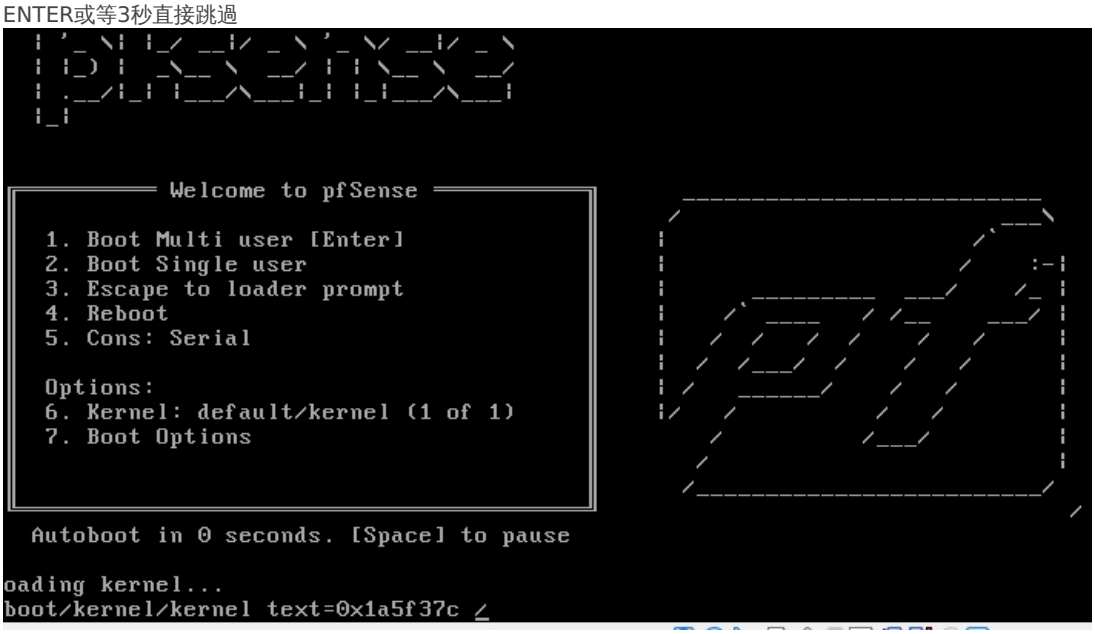
PFSENSE 設定

目錄

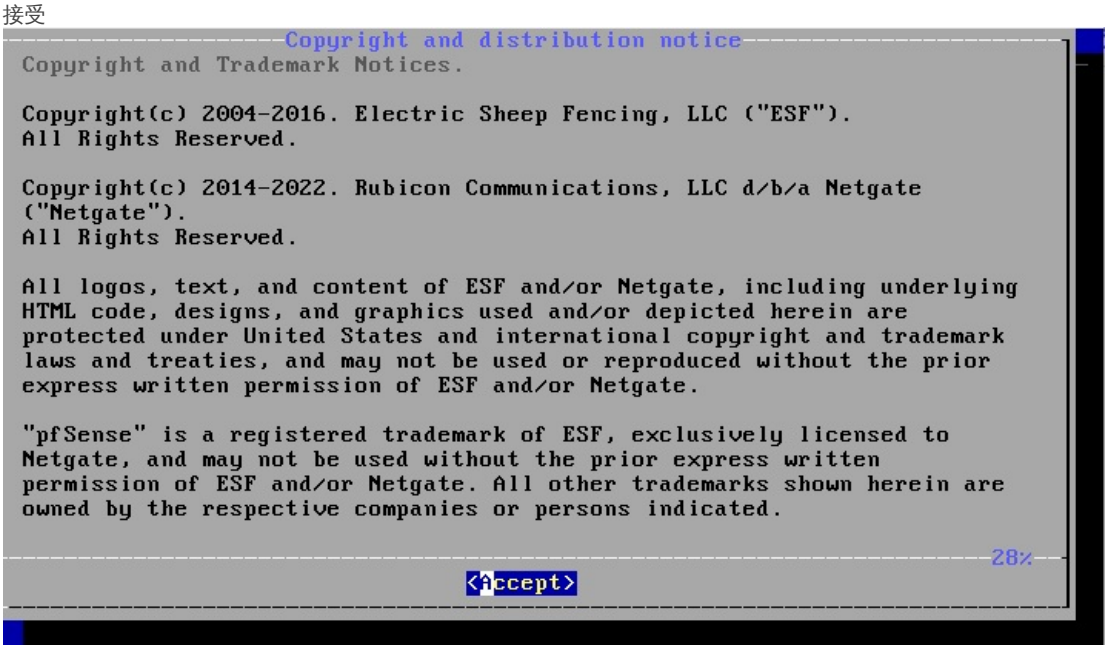
安裝及初次設定

1. 安裝
   1 安裝環境可以是X64 PC 或 VM
   2 首先到官方網頁先下載安裝檔 https://www.pfsense.org/download/，下載光碟ISO 或是 IMG檔都可以，ISO燒錄成光碟，或使用ISO 或 IMG檔，寫入USB隨身碟，推薦軟體 IMGNURN，balenaEtcher。
   3 使用ISO或USB開機，

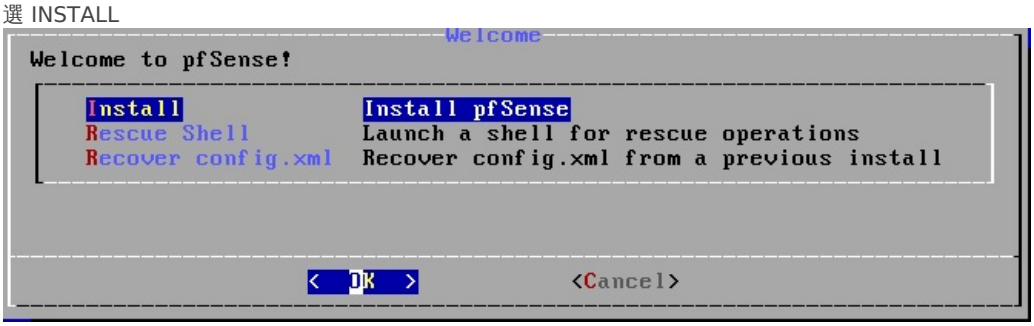
   ENTER或等3秒直接跳過



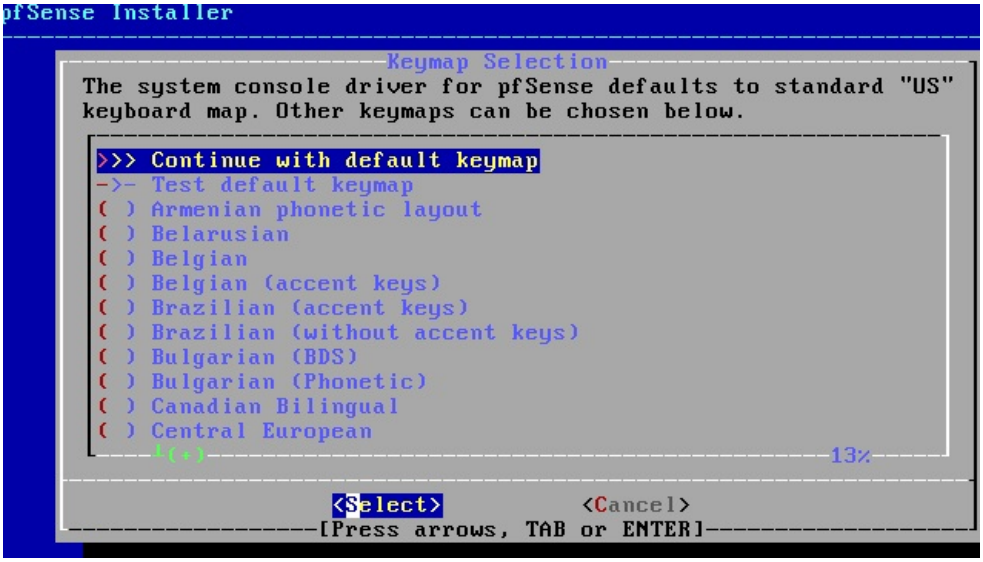
   接受



   選 INSTALL

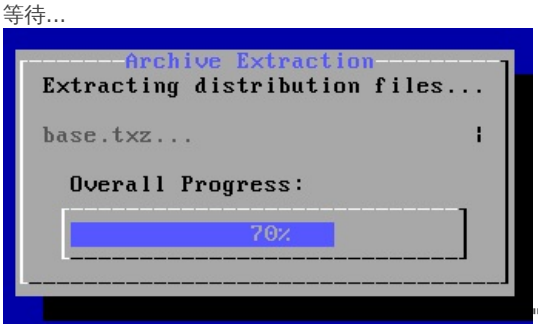


   選預設鍵盤

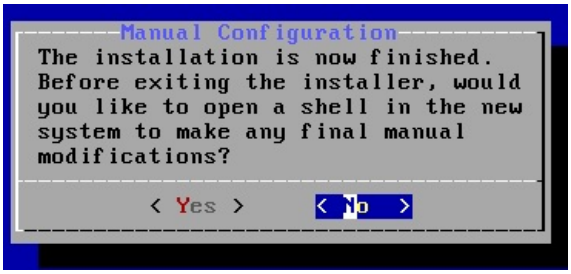


選UFS BIOS，新機可選 UFS-UEFI

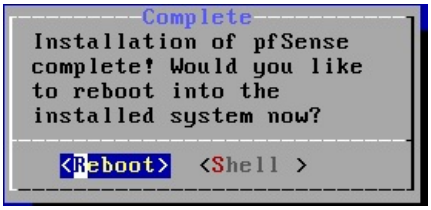
等待...



NO



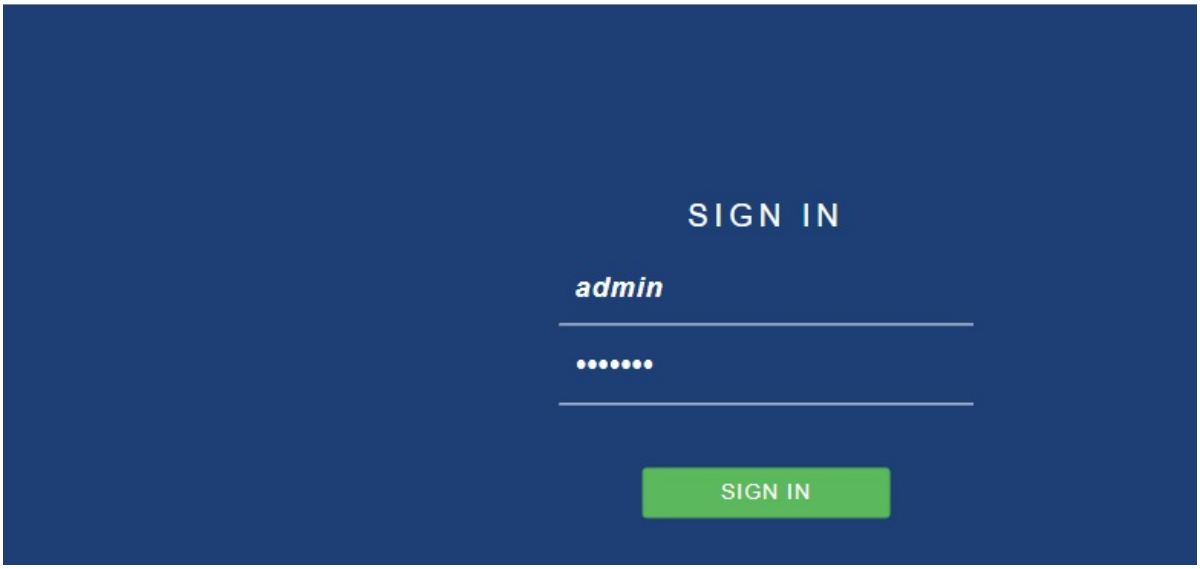
REBOOT



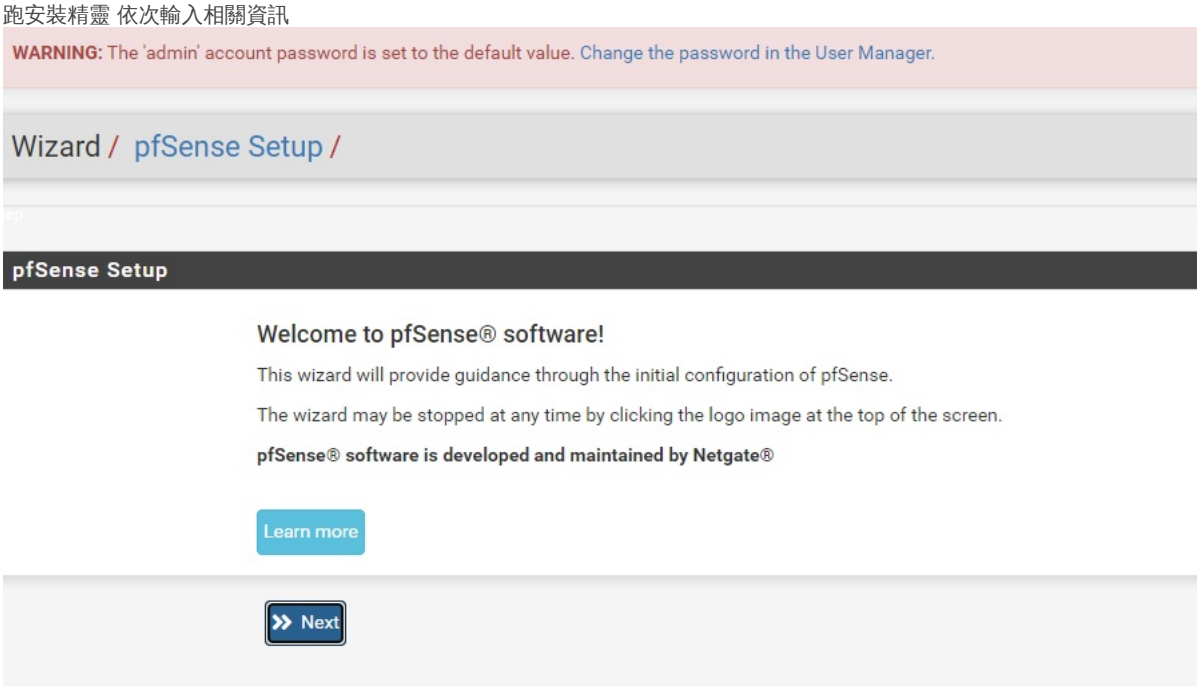
移出光碟後重新開機，會開到初始畫面

2. 初次設定
可以選擇本機畫面安裝，或網頁直接輸入IP 192.168.1.1(通常是第二個網路孔，第一孔DHCP，連不到先用本機安裝) 帳密 admin/pfsense 登入後進行安裝精靈。

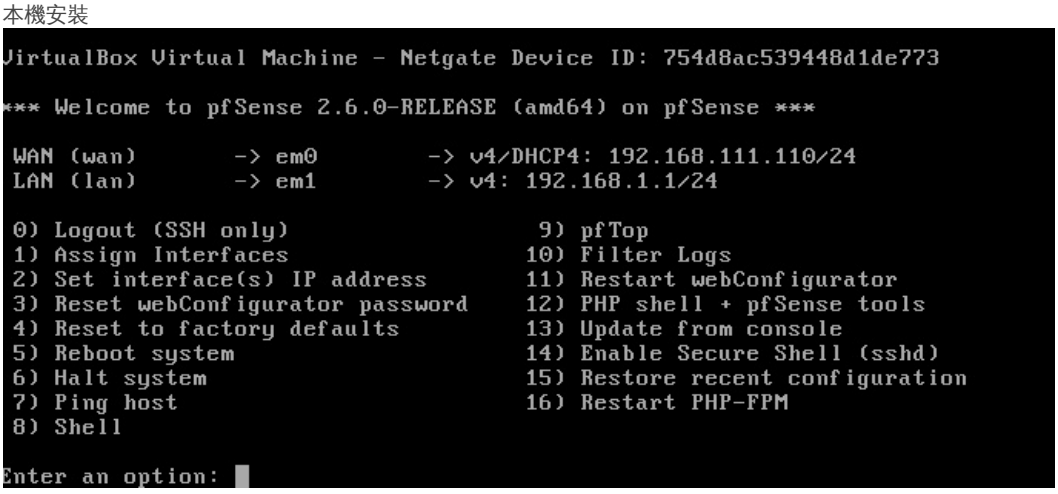
網頁安裝 192.168.1.1



跑安裝精靈 依次輸入相關資訊

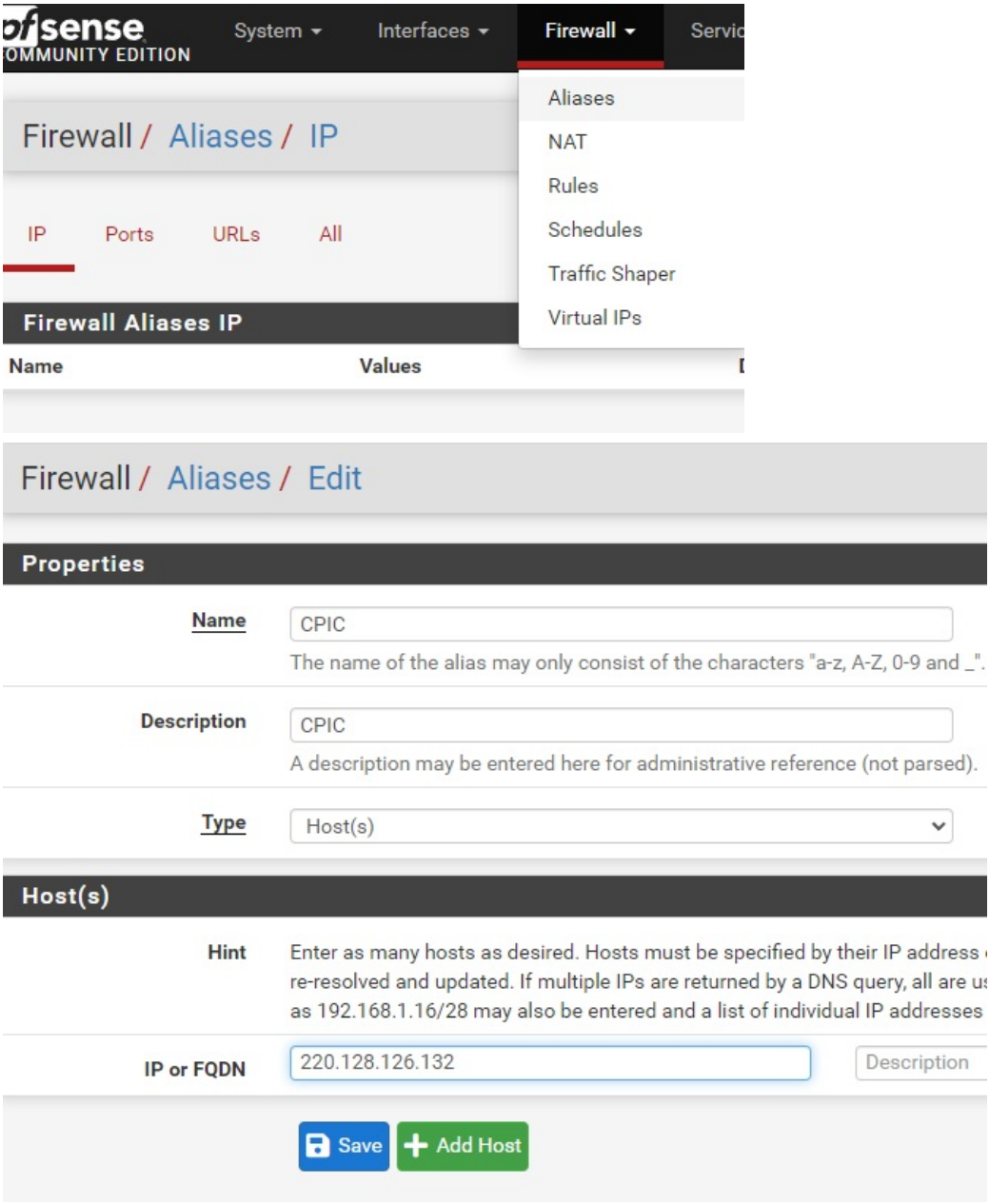


本機安裝

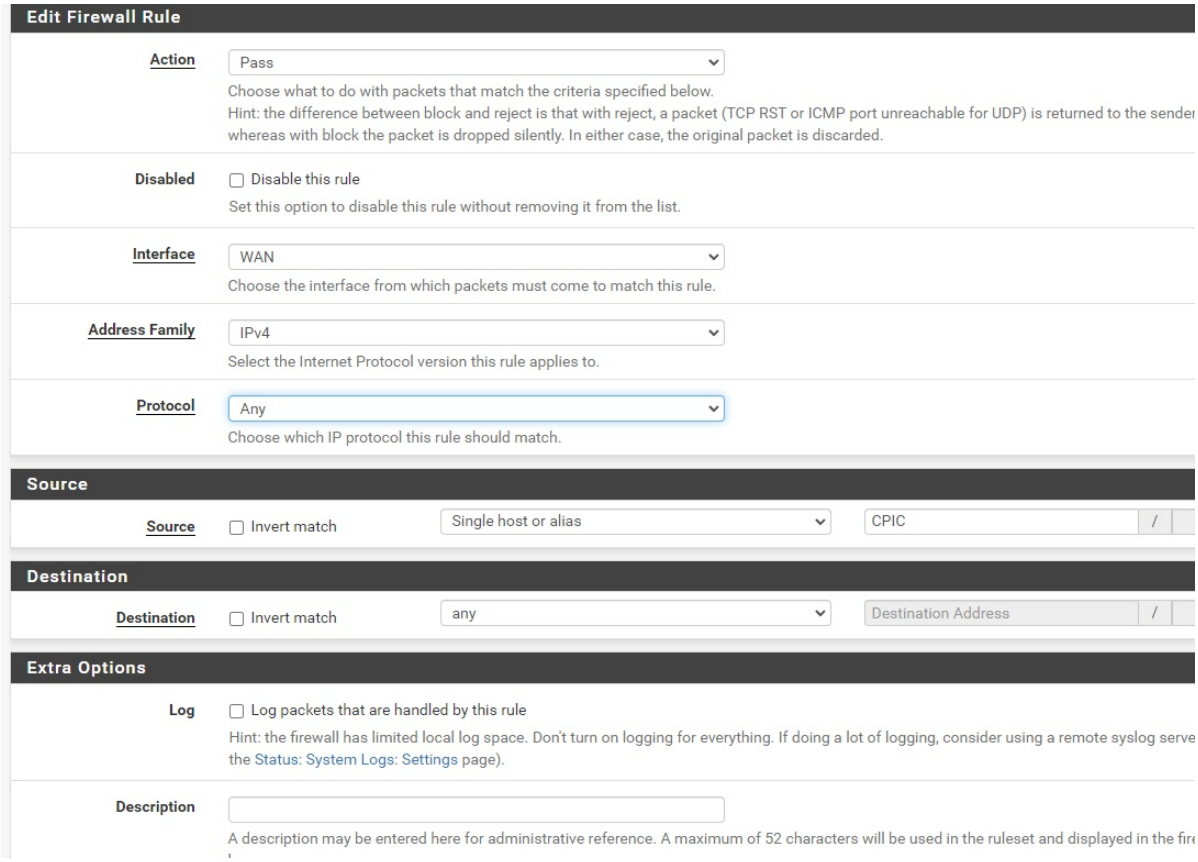


創勁基本設定
Hostname:pfs
domain:對方網域 或隨便
密碼:

Firewall\Aliases 新增創勁IP



Firewall\Rules 增加信任IP (CPIC)



3. 參考資料
英文
中文 https://ithelp.ithome.com.tw/articles/10246505
https://docs.netgate.com/pfsense/en/latest/install/download-installer-image.html

CPFS基本設定

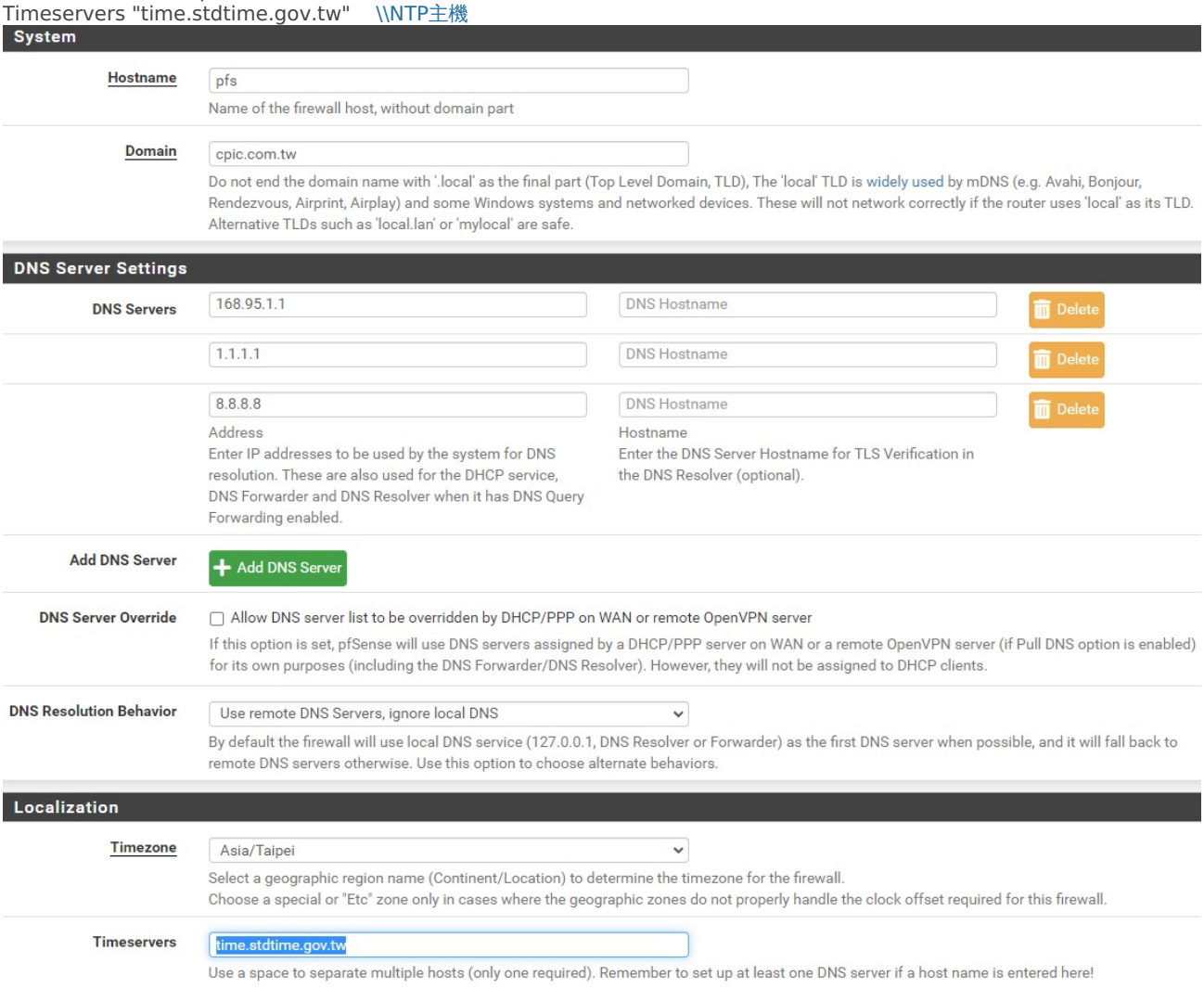
基本設定

- 一般設定
- 進階設定
- WAN IP 設定
- LAN IP 設定
- DHCP 設定
- 存取限制設定開放WAN ADDRESS 給CPIC
-

一般設定

System \ General Setup

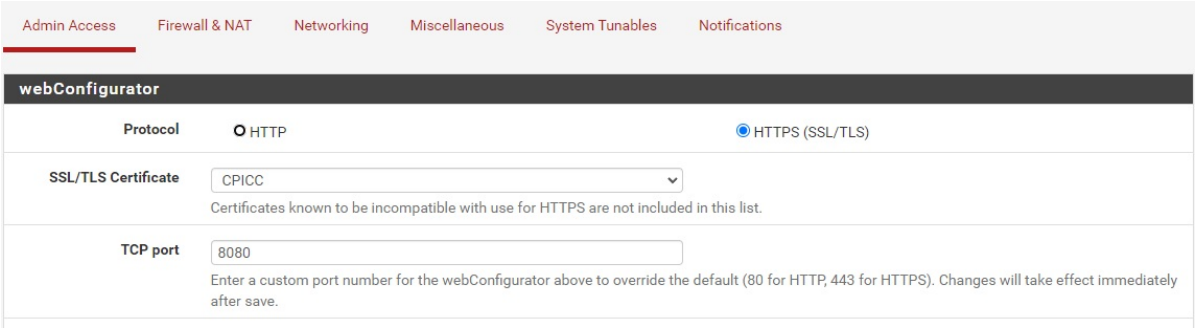
Hostname "客戶英文網域或拼音" \\主機名稱
Domain "cpic.local" \\ 網域
DNS Servers "1.1.1.1" "8.8.8.8" "168.95.1.1" \\DNS 可輸入多個
Timezone "Asia\Taipei" \\時區
Timeservers "time.stdtime.gov.tw" \\NTP主機



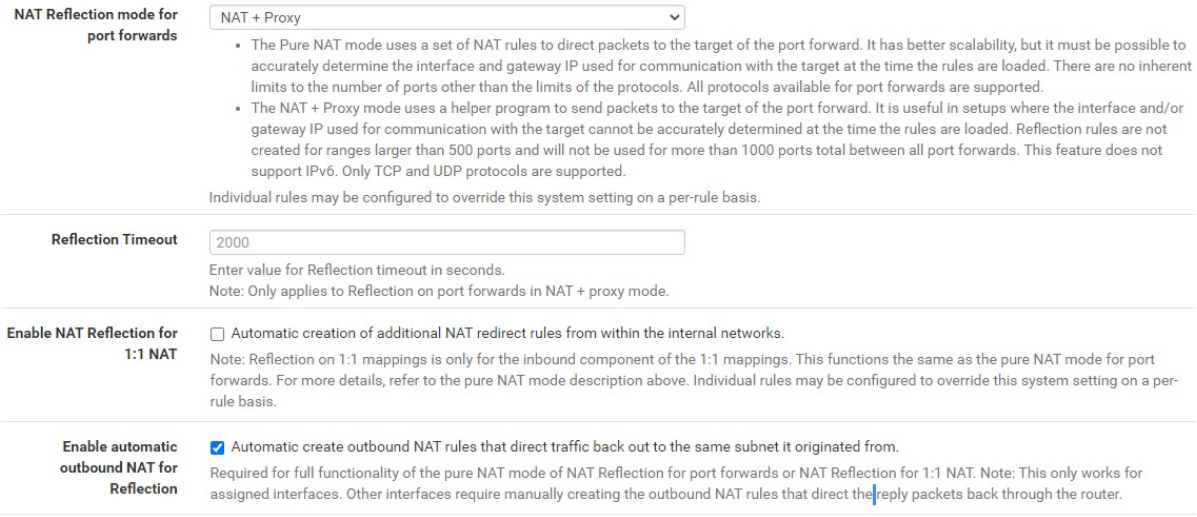
進階設定

System \ Advanced

1. Admin Access
   Protocol "https" \\
   TCP port "8080" \\不佔用 80 443

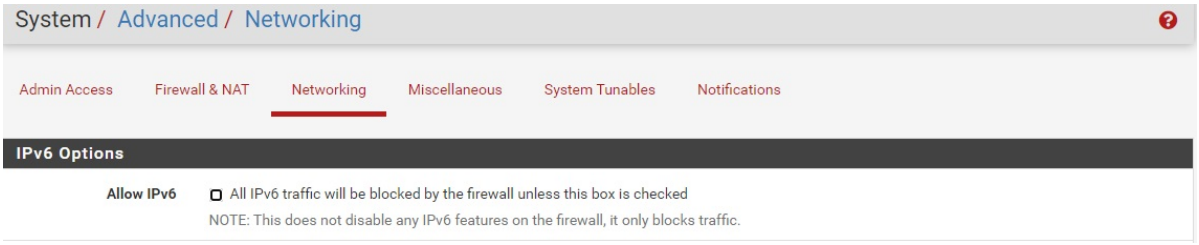


2. Firewall & NAT
   NAT Reflection mode for port forwards "NAT+PROXY" \\內網可存取內網NAT主機
   Enable automatic outbound NAT for Reflection "勾選" \\自動建立NAT 防火牆RULES

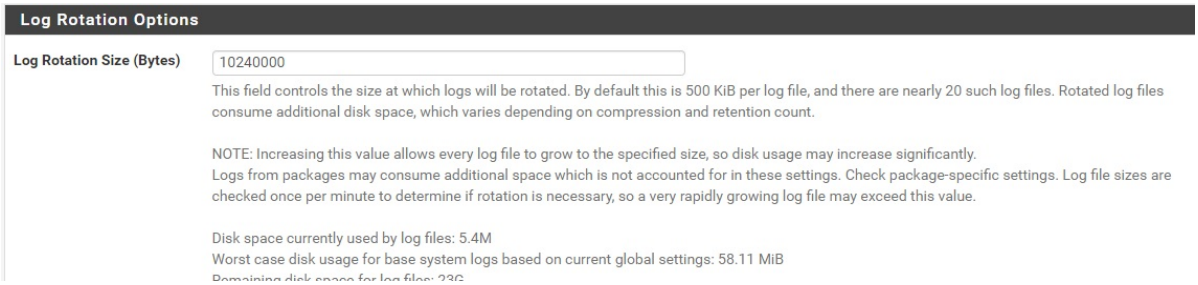


3. Notifications
   Disable SMTP "不勾選"
   E-Mail server "msa.hinet.net"
   From e-mail address "xxx.yyy@msa.hinet.net"
   Notification E-Mail address "alarm@cpic.com.tw"

4. Networking
   Allow IPv6 "不勾選" \\取消IPv6



5. Status \ System Logs \ Settings
Log Rotation Size (Bytes) "10240000" \\設定log檔案大小為 10MB



WAN IP 設定

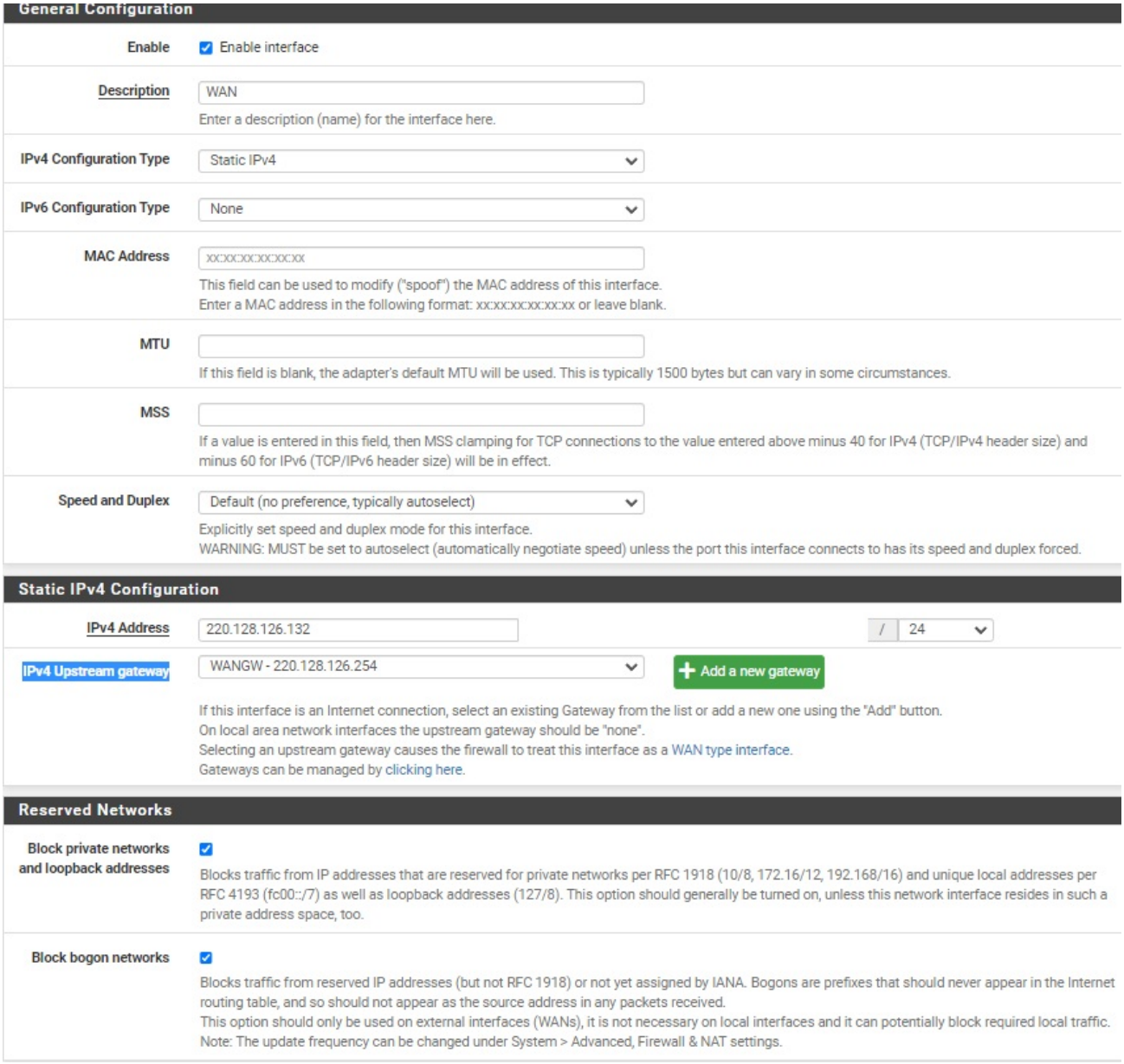
Interfaces \ WAN

IPv4 ：DHCP/PPPOE/STATIC

IPv6 ：Disable

Gateway: 有固定靜態-IP 要新增

Add a new gateway > 輸入 GW IP。



ENABLE 勾選

IPv4 Configuration Type > STATIC PPPOE DHCP

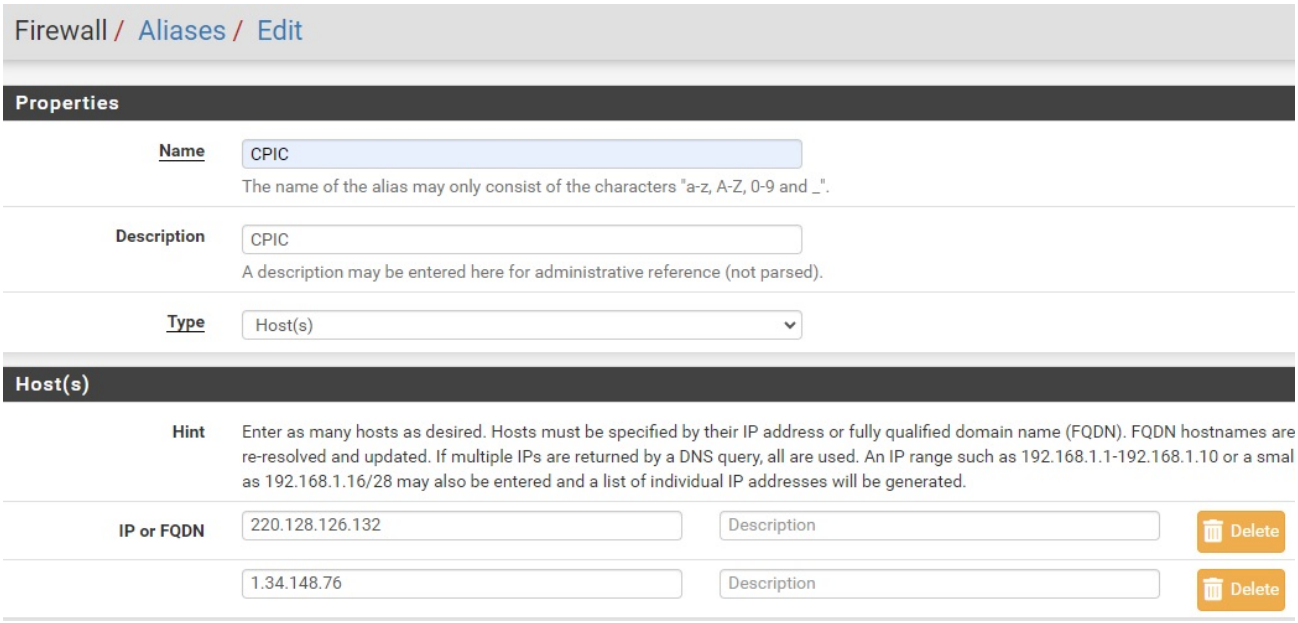
IPv4 Address Mask IPv4 Upstream gateway

開放WAN ADDRESS 給CPIC

LAN IP 設定

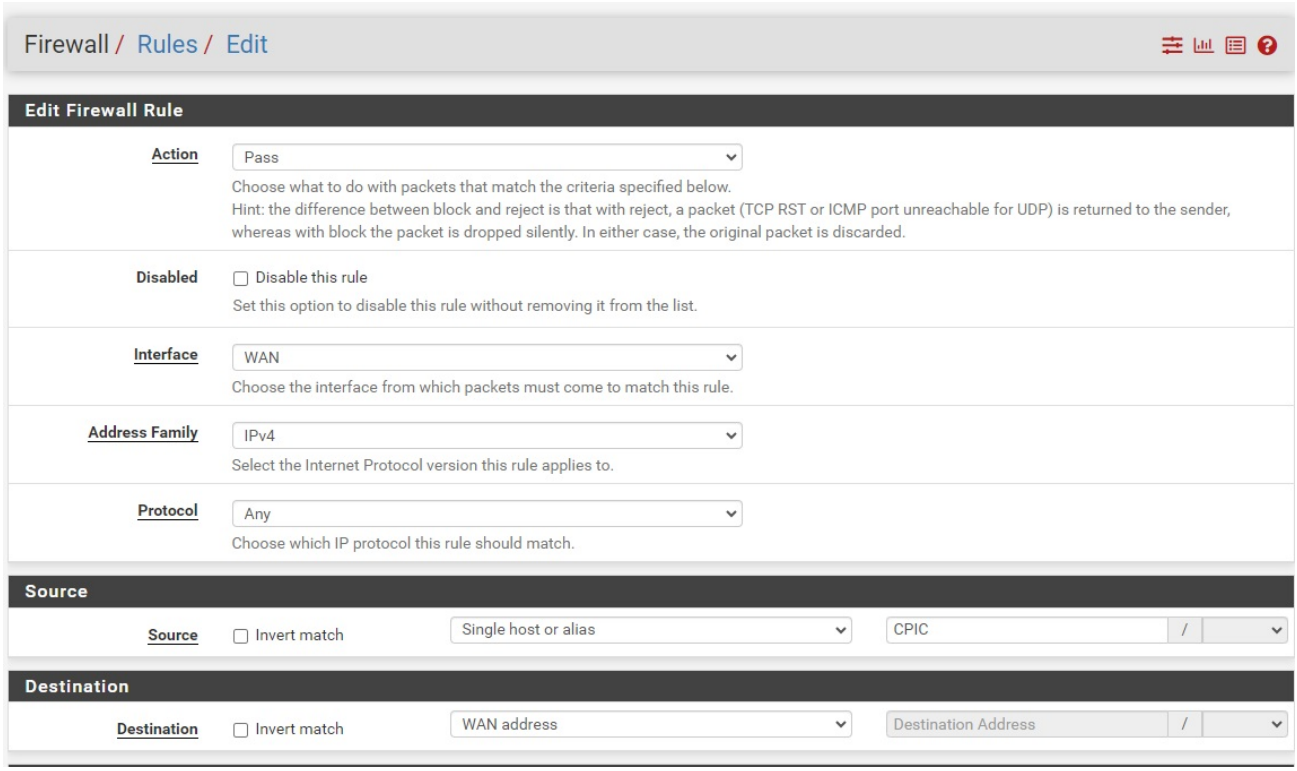
DHCP 設定

設定Firewall Aliases， 將公司IP 將公司IP 加入



防火牆規則設定允許CPIC

Firewall \ Rules \ WAN 允許所有:IPV4 **Protocol:ANY**



進階設定

進階設定

阻擋網頁功能

阻擋網頁功能

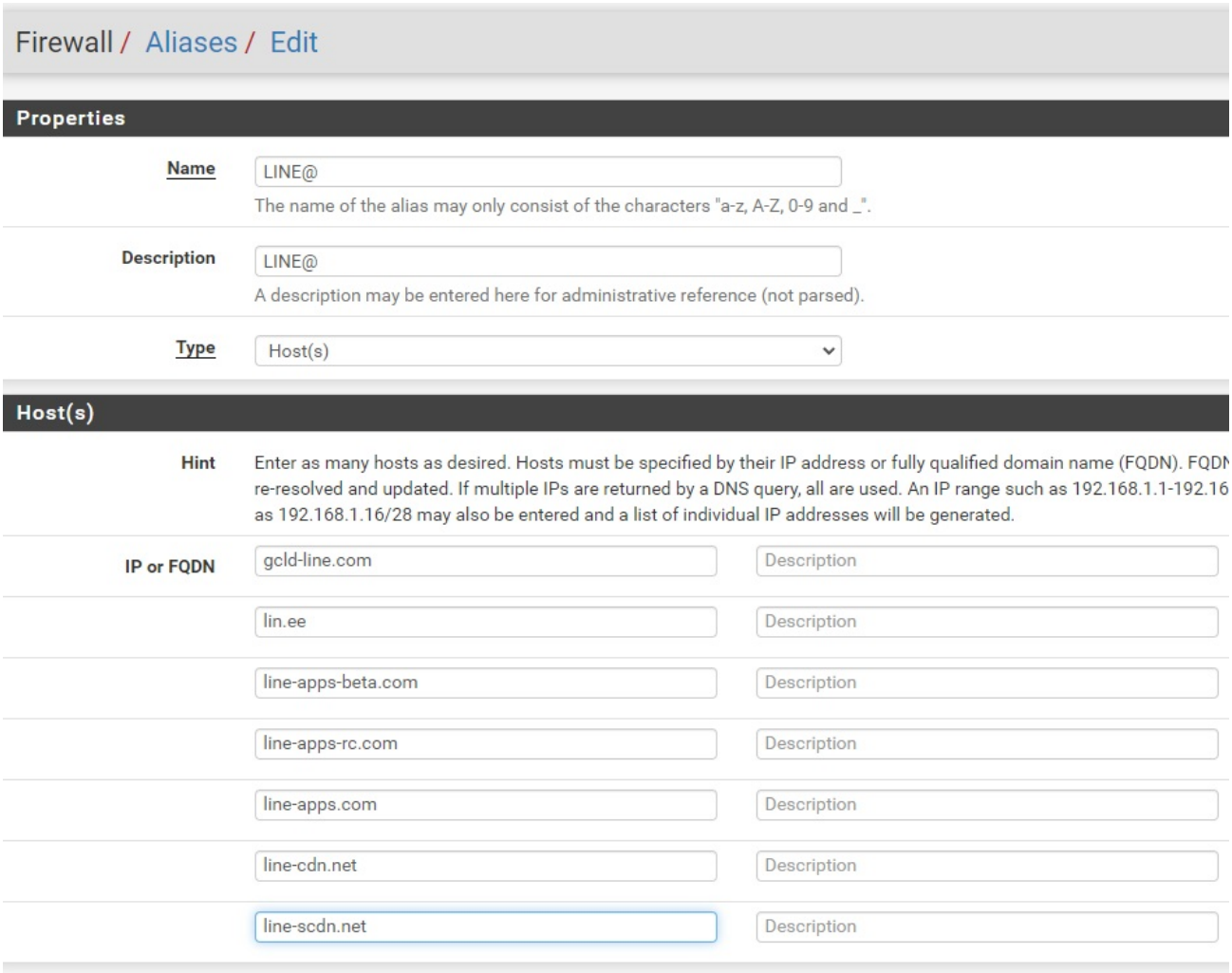
以往Pfsense防火牆要設定封鎖某網站，要使用SQUID PROXY過濾或是透過套件pfBlockerNG封鎖DNS來達成，現在可用相對簡單方式。

查出要封鎖網站的所有相關網址
建議使用https://www.netify.ai/
例如 line

PRIMARY DOMAINS

- gcld-line.com
- lin.ee
- line-apps-beta.com
- line-apps-rc.com
- line-apps.com
- line-cdn.net
- line-scdn.net
- line.me
- line.naver.jp
- linecorp.com
- linemyshop.com
- lineshoppingseller.com

在aliase裡面新增所有網址



在規則封鎖

Firewall / Rules / Edit

Edit Firewall Rule

Action
Reject
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled
☑ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface
LAN
Choose the interface from which packets must come to match this rule.

Address Family
IPv4+IPv6
Select the Internet Protocol version this rule applies to.

Protocol
Any
Choose which IP protocol this rule should match.

Source

Source
☐ Invert match
LAN net
Source Address /

Destination

Destination
☐ Invert match
Single host or alias
LINE /

進階設定

OPENVPN

新增PACKAGE OPENVPN

初次使用精靈

建立本機使用者

使用外部驗證

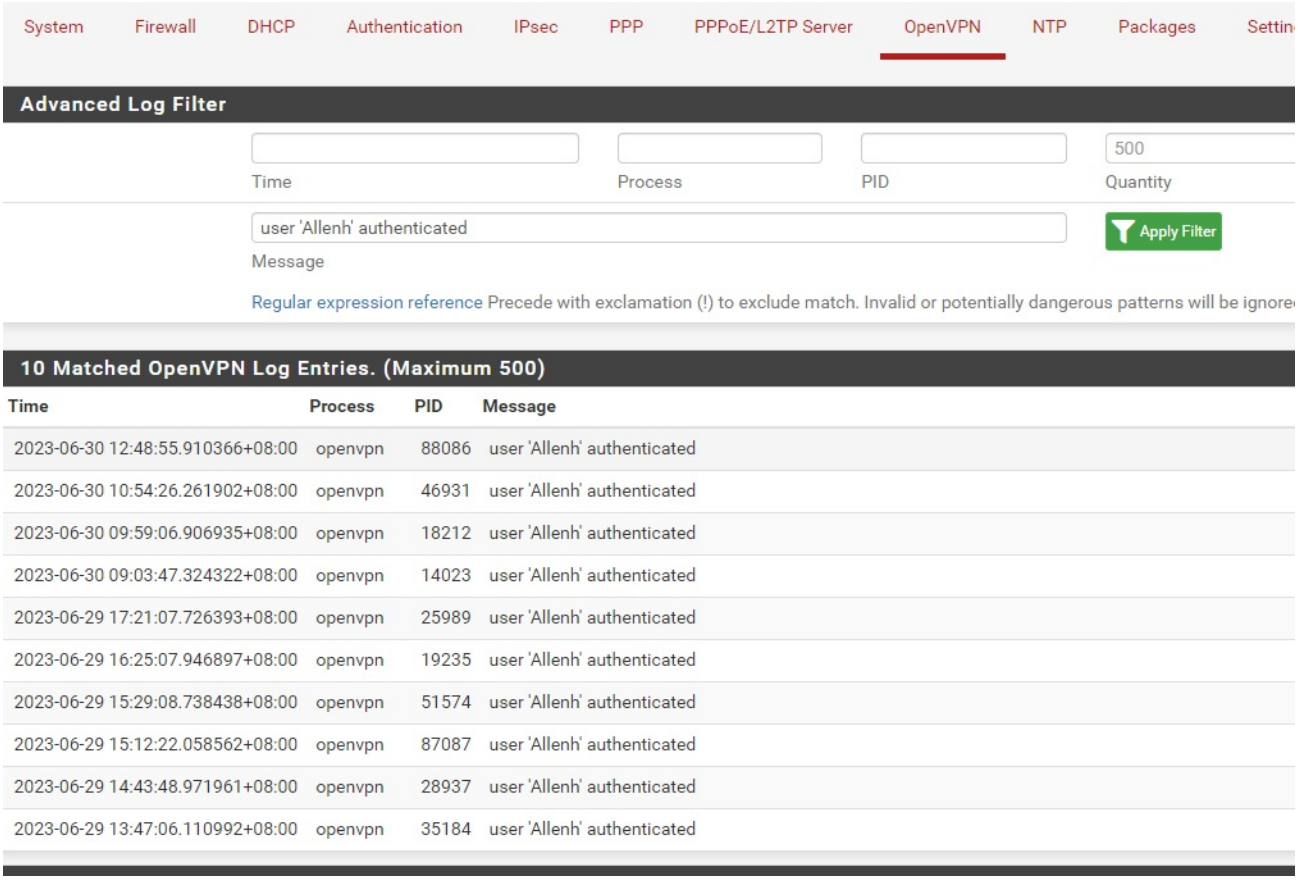
查詢登入紀錄

查詢登入紀錄

到 Status \ System Logs \ OpenVPN 處

使用FILTER功能,搜尋user登入紀錄

Message 輸入 `user 'username' authenticated`



阻擋網頁功能-2

阻擋網頁功能-2

方法1如果失敗嘗試用方法2，方法1可能阻擋網頁有多個對外IP，可能就會失效。

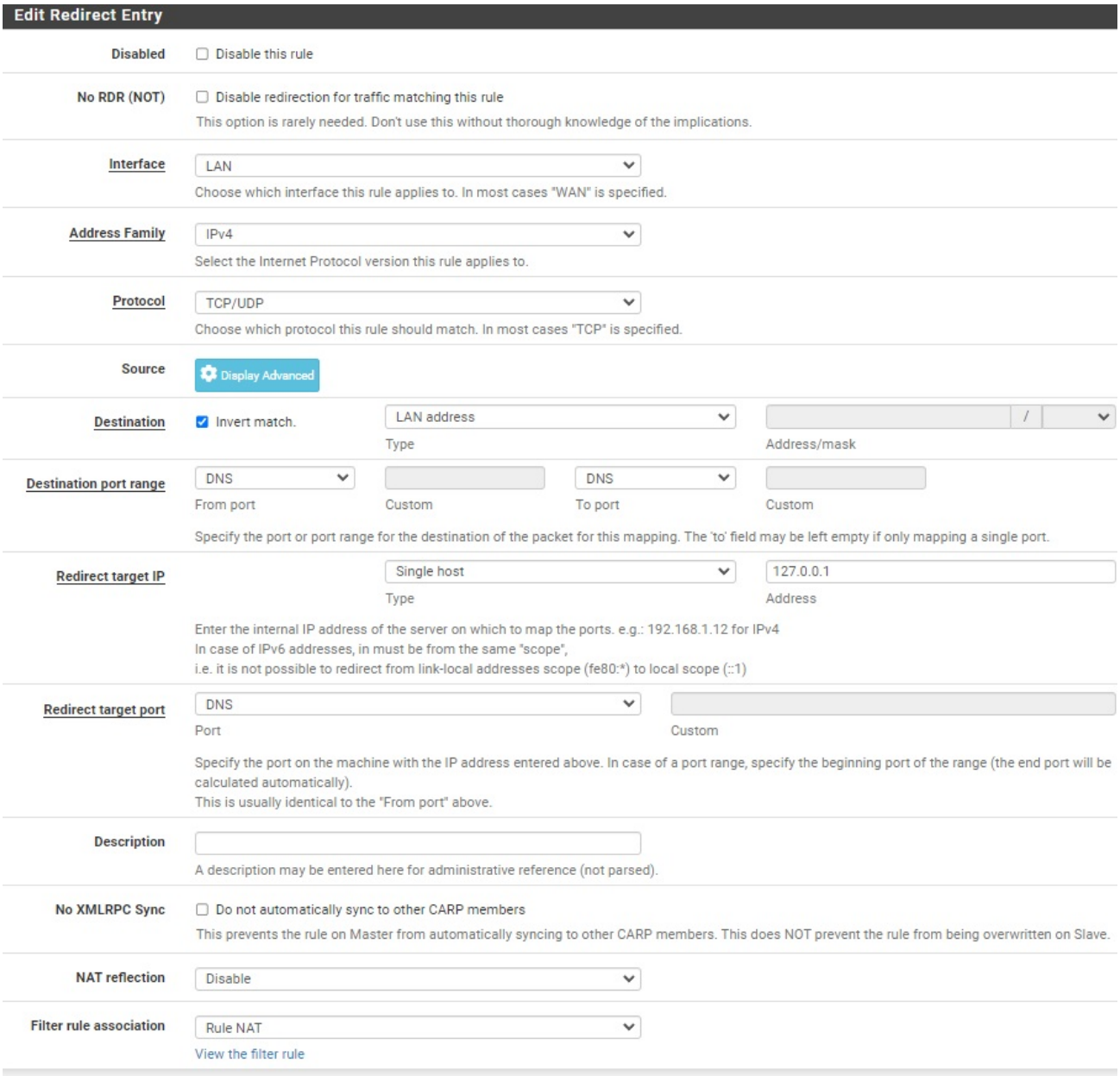
- **重導向DNS到 防火牆本身
- 利用防火牆DNS做阻擋。
- 或利用 PFBLOCK套件阻擋。

重導向DNS到 防火牆本身

讓CLIENT端查詢DNS 只能用防火牆IP

參考原廠說明

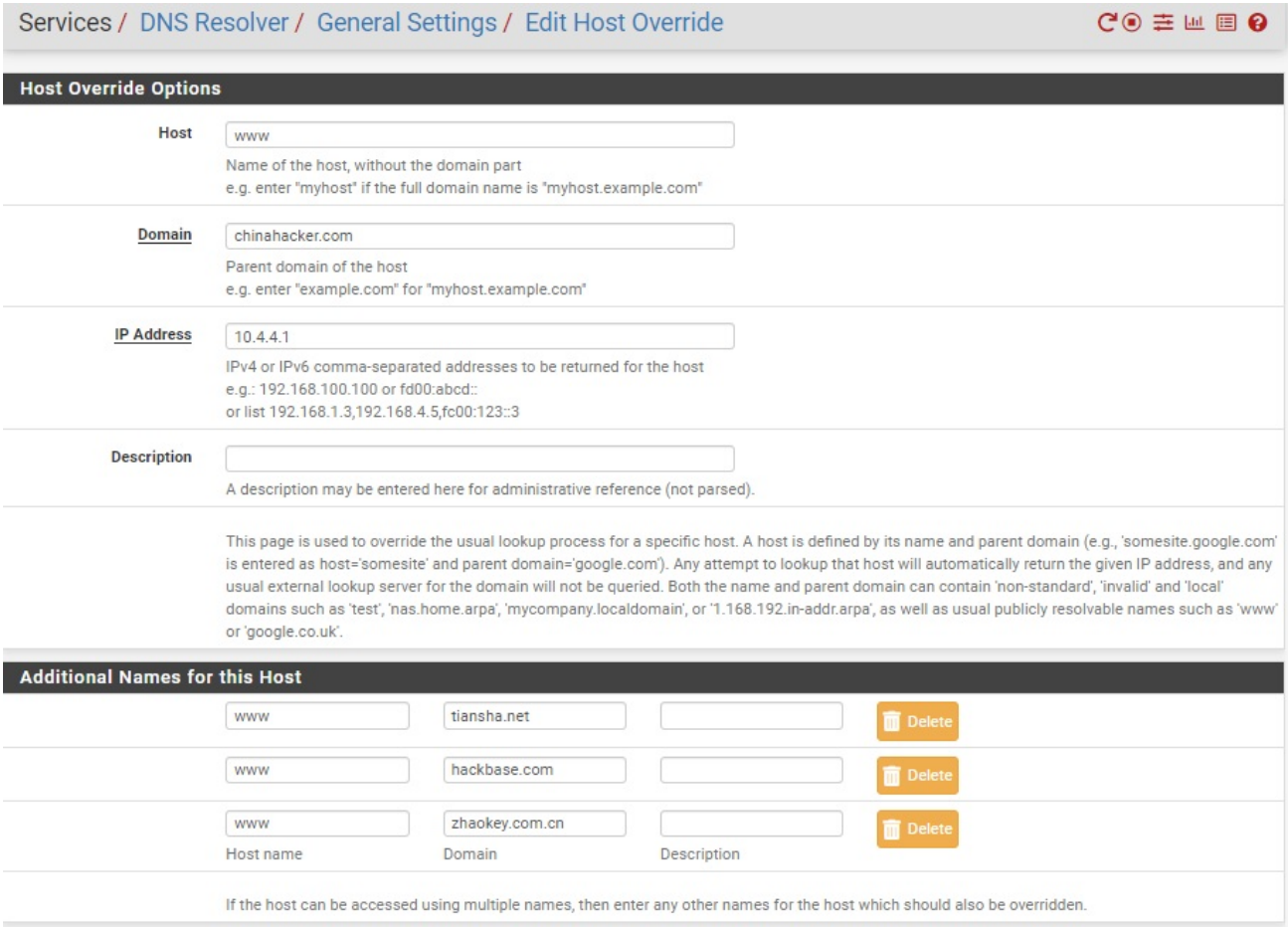
到 Firewall \ NAT \ Port Forward 建立規則



利用防火牆DNS做阻擋

到 Services \ DNS Resolver 最底下 Host Overrides 新增主機

IP ADDRESS 隨意輸入



百里助專案

客戶需求

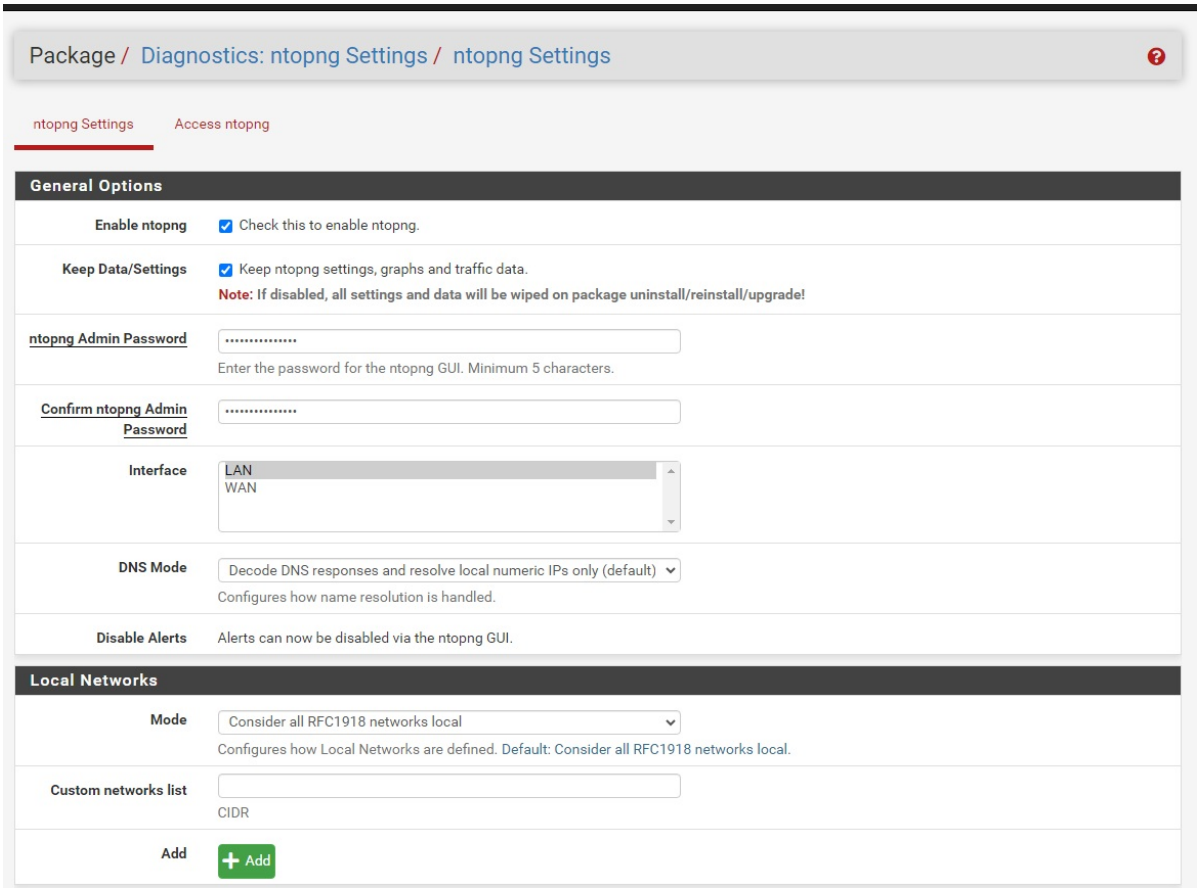
- 觀看連線資訊
- 利用防火牆做阻擋。
- 或利用防火牆限速。

解決方案

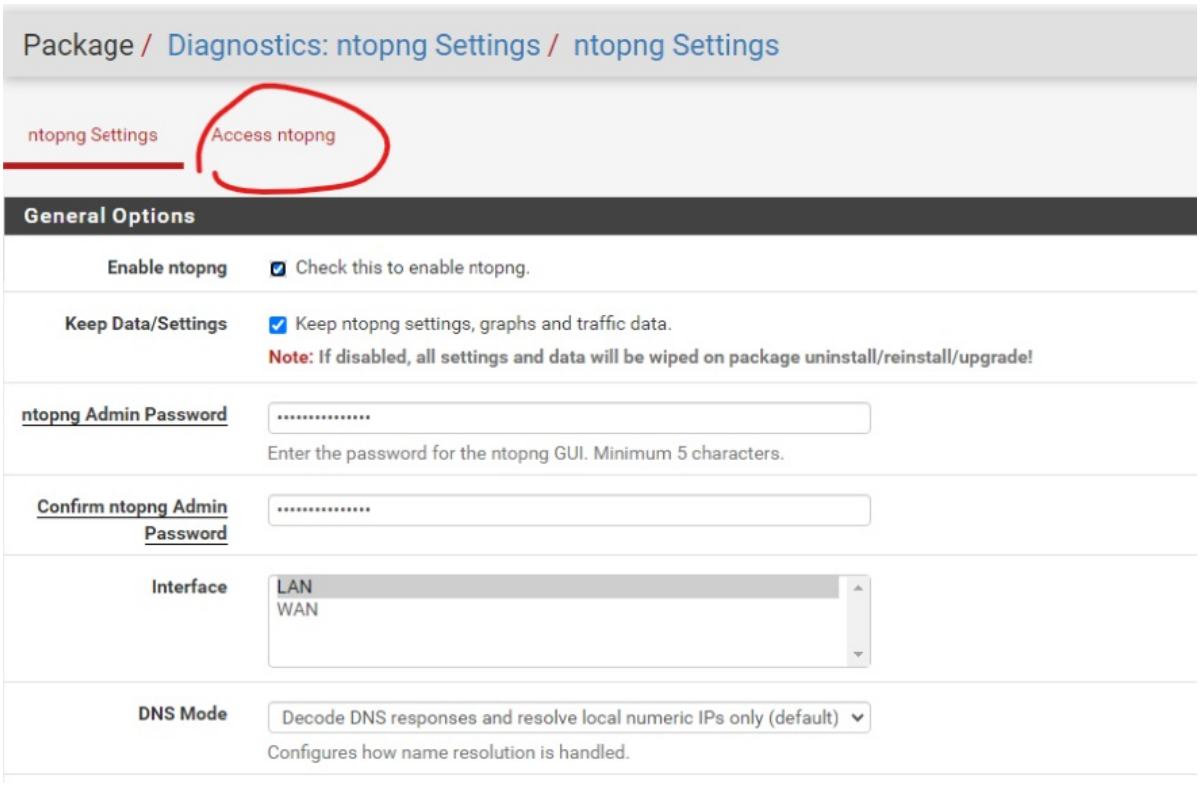
- 觀看連線資訊
  使用套件 ntopng安裝:
  1 到 System \ Package Manager \ Available Packages 搜尋 ntopng，點選安裝。

  2 到 Diagnostics \ ntopng Settings \ ntopng Settings進行設定

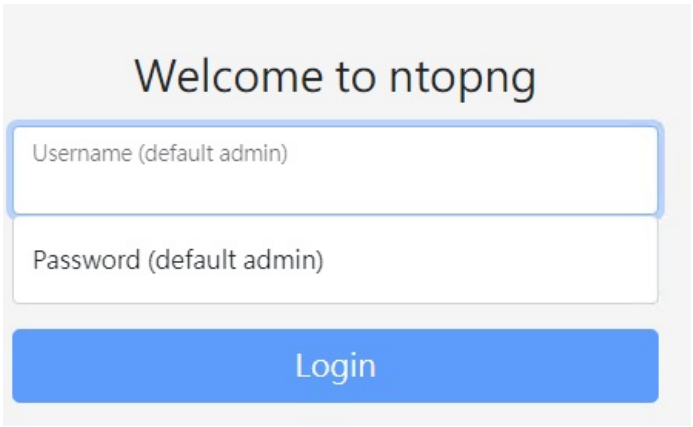
  勾選 Enable ntopng，Keep Data/Settings
  再設定 ntopng 網頁密碼，等下登入會用到。



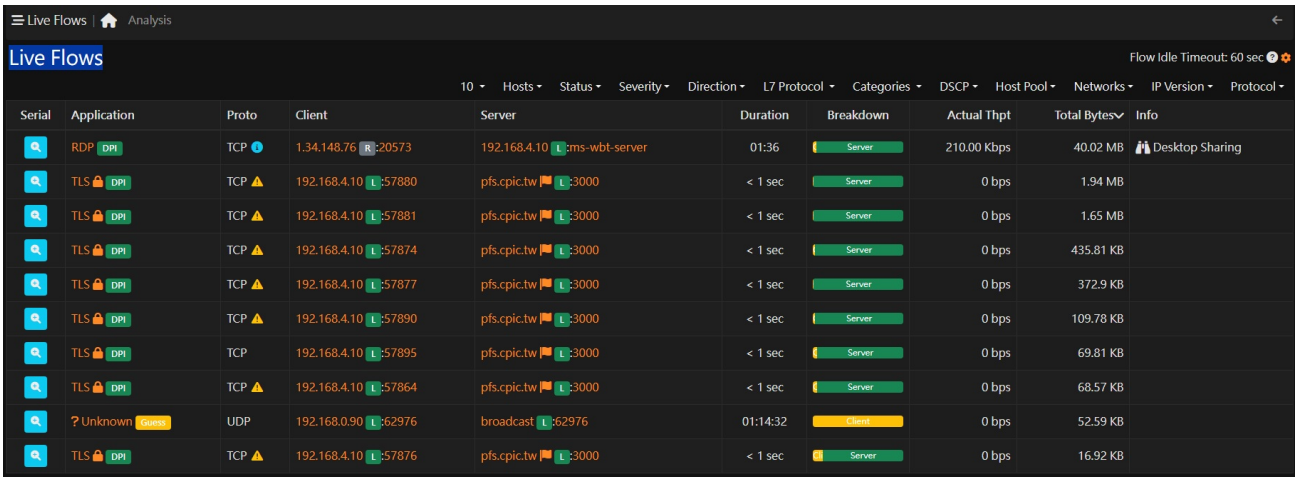
3 網頁登入 點選設定旁 Access ntopng



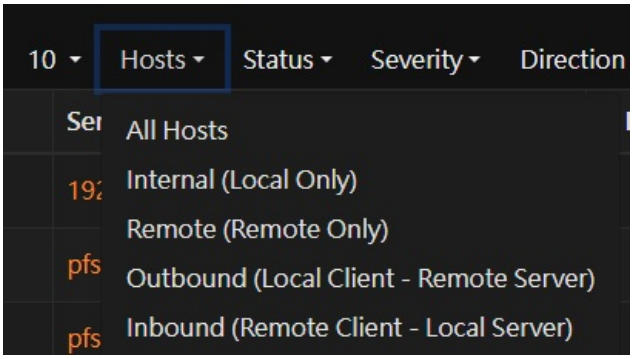
畫面如下
輸入帳密 admin/剛剛設定的密碼



到 flow \ live 看及時流量



篩選區網IP Local Only，選出高流量IP 點入可以看CLIENT細項。



Router/AccessPoint MAC Address	A2:4D:16:79:D5:B6	
Host MAC Address	DE:99:0B:70:9C:00	Unknown Device Ty
IP Address	192.168.4.10 [192.168.4.0/24]	Host Pool: Default
Name	192.168.4.10 L P	
Active Monitoring	Add ICMP Monitor +	
Active Alerted Flows	7	
Behavioural Counter Anomalies	1	
First / Last Seen	2023/08/01 14:57:34 [01:18:43 ago]	2023/08/01 16:16:1
Sent vs Received Traffic Breakdown	Sent	
Traffic Sent / Received	78,714 Pkts / 54.23 MB	61,770 Pkts / 18.79
	As Client	As Server
Flows: Active / Total / Alerted / Port Unreach	10 / 597 / 218 / 0	1 / 5 / 4 / 0
Total Flows with Blacklisted Hosts	0	0
Total Unidirectional TCP Flows	0	0
Peers: Active	11	1
TCP Unresponsive Flows (Peer IP and Server Port)	0	0
Contacted Servers	DNS: 1 / SMTP: 0 / POP: 0 / IMAP: 0 / NTP: 0	

- 利用防火牆做阻擋。

1. 到 Firewall \ Aliases \ IP 新增群組
   分別新增 black flowcontrol

WIREGUARD Site to Site

WIREGUARD Site to Site

参考

https://docs.netgate.com/pfsense/en/latest/recipes/wireguard-s2s.html