進階設定

進階設定

阻擋網頁功能

阻擋網頁功能

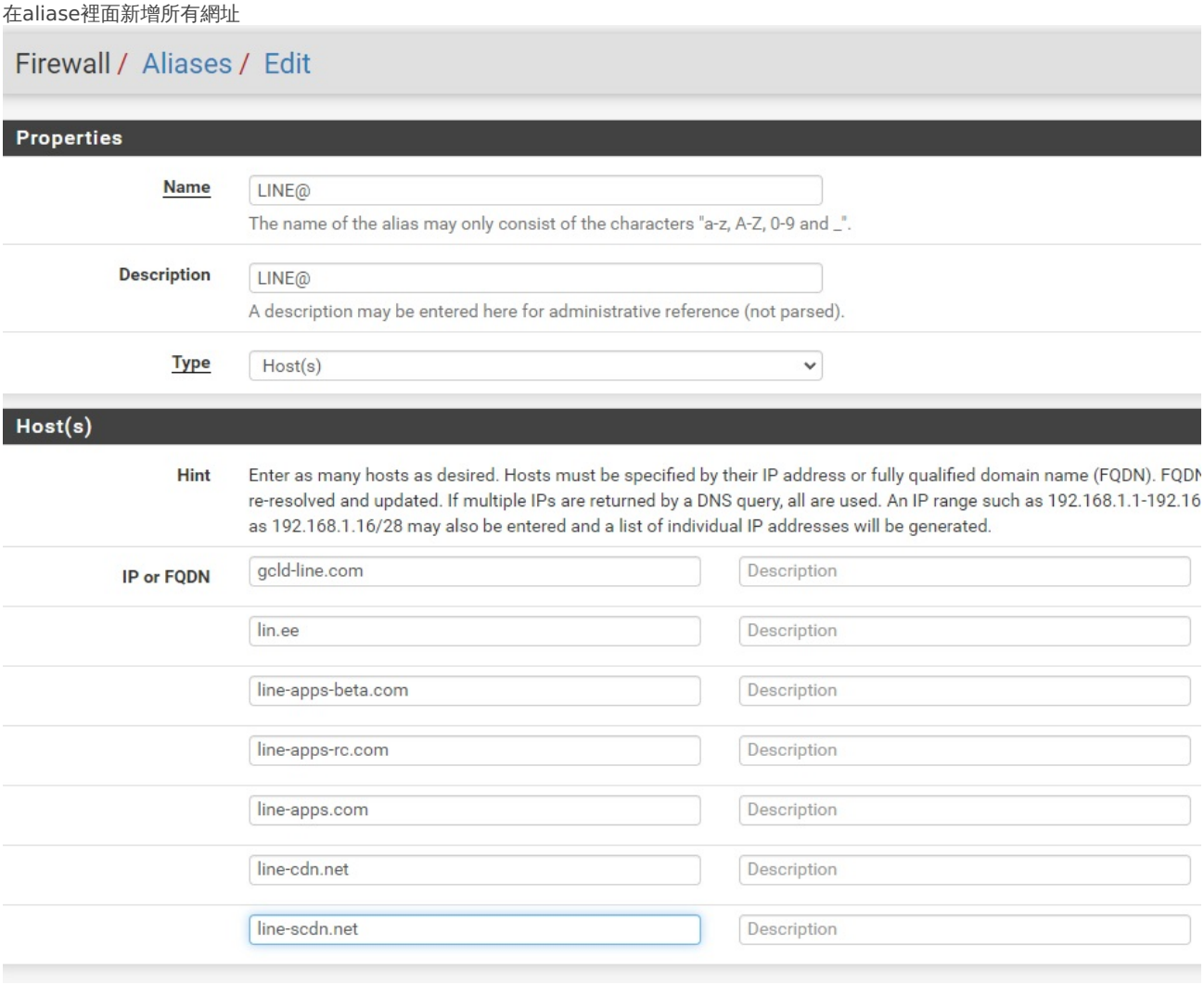
以往Pfsense防火牆要設定封鎖某網站，要使用SQUID PROXY過濾或是透過套件pfBlockerNG封鎖DNS來達成，現在可用相對簡單方式。

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 /

OPENVPN

新增PACKAGE OPENVPN

初次使用精靈

建立本機使用者

使用外部驗證

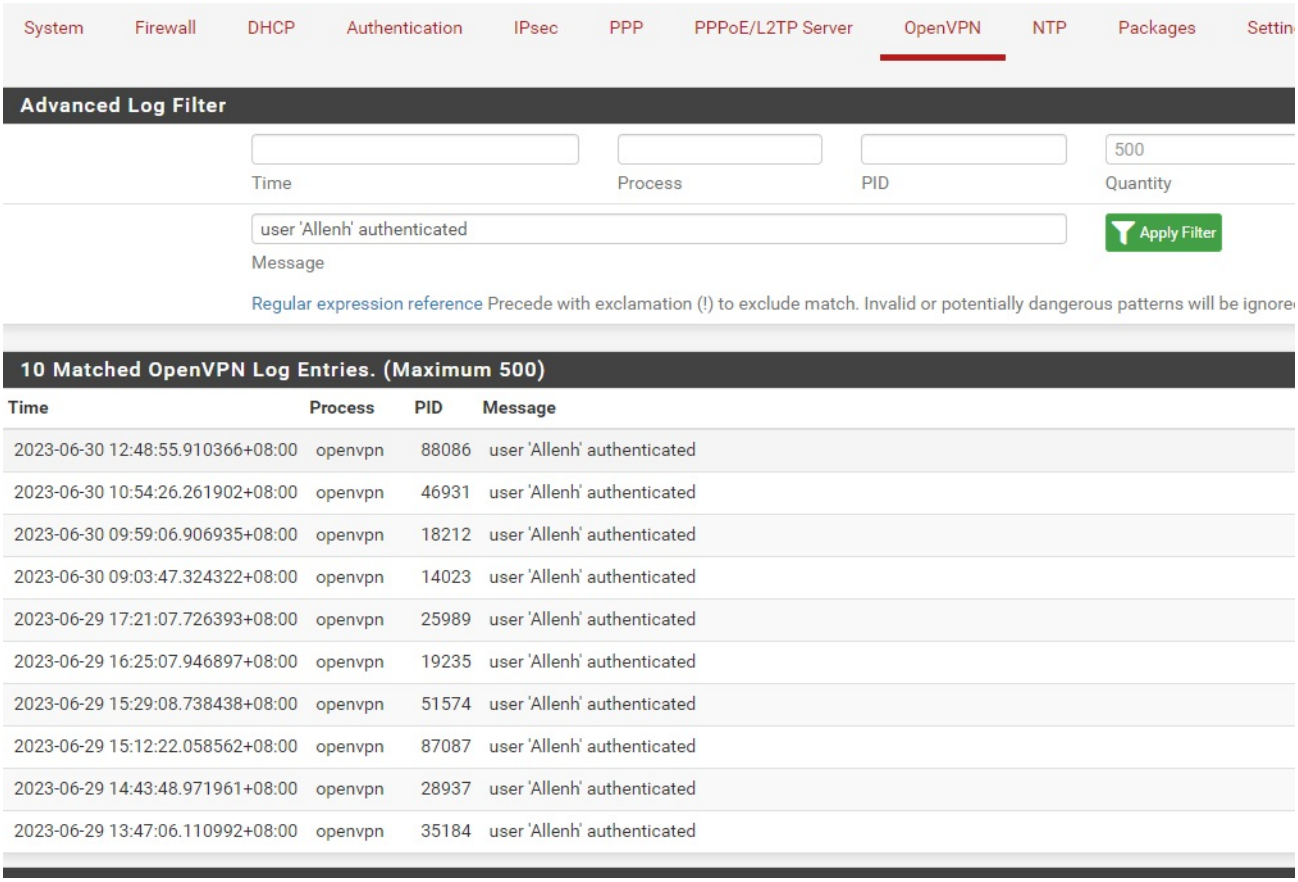
查詢登入紀錄

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。

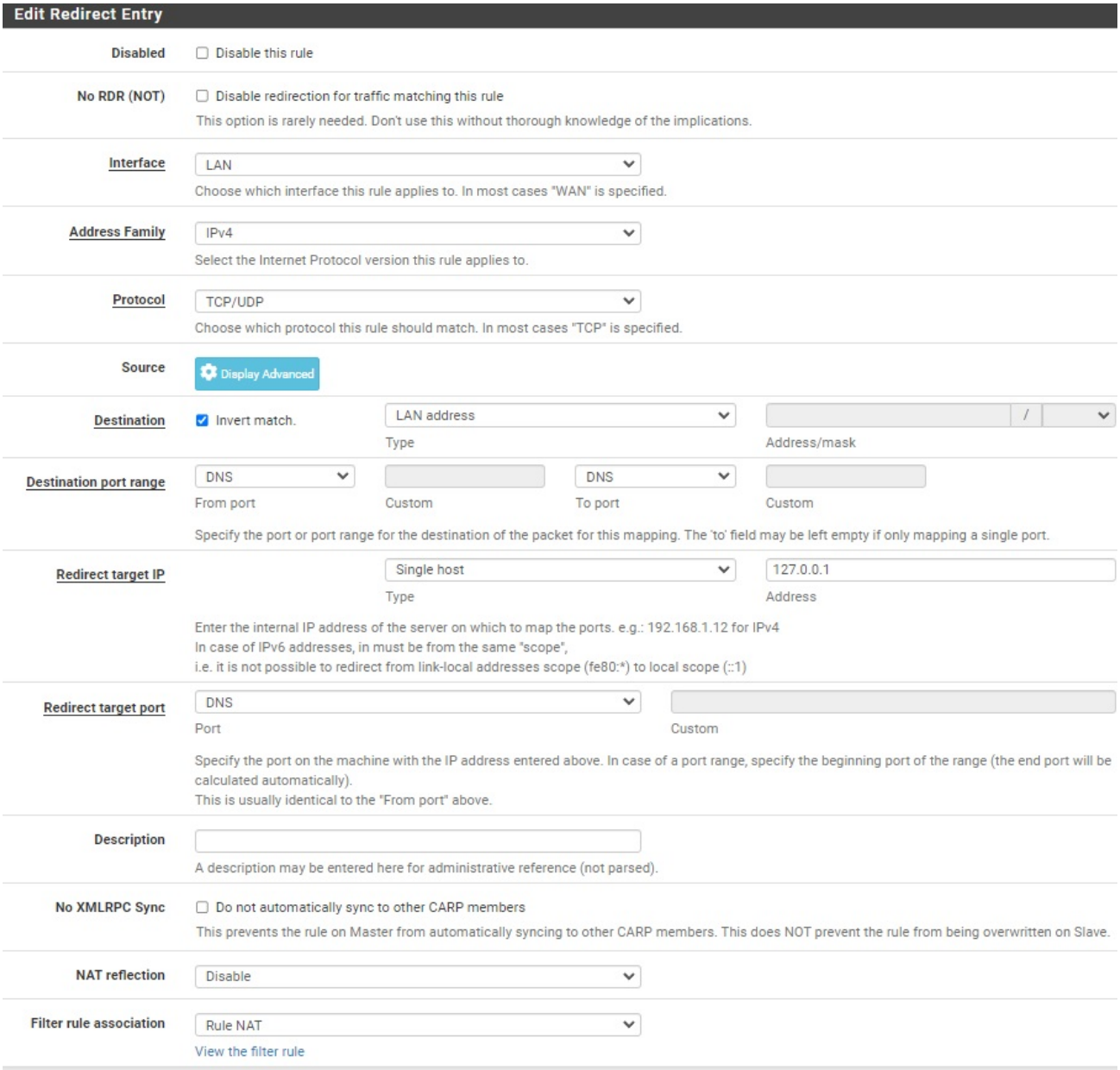
- **重導向DNS到 防火牆本身
- 利用防火牆DNS做阻擋。
- 或利用 PFBLOCK套件阻擋。

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

Services / DNS Resolver / General Settings / Edit Host Override

Host Override Options

Host

www

Name of the host, without the domain part
e.g. enter "myhost" if the full domain name is "myhost.example.com"

Domain

chinahacker.com

Parent domain of the host
e.g. enter "example.com" for "myhost.example.com"

IP Address

10.4.4.1

IPv4 or IPv6 comma-separated addresses to be returned for the host
e.g.: 192.168.100.100 or fd00:abcd::
or list 192.168.1.3,192.168.4.5,fc00:123::3

Description

A description may be entered here for administrative reference (not parsed).

This page is used to override the usual lookup process for a specific host. A host is defined by its name and parent domain (e.g., 'somesite.google.com' is entered as host='somesite' and parent domain='google.com'). Any attempt to lookup that host will automatically return the given IP address, and any usual external lookup server for the domain will not be queried. Both the name and parent domain can contain 'non-standard', 'invalid' and 'local' domains such as 'test', 'nas.home.arpa', 'mycompany.localdomain', or '1.168.192.in-addr.arpa', as well as usual publicly resolvable names such as 'www' or 'google.co.uk'.

Additional Names for this Host

Host name	Domain	Description	
www	tiansha.net		Delete
www	hackbase.com		Delete
www	zhaokey.com.cn		Delete

If the host can be accessed using multiple names, then enter any other names for the host which should also be overridden.

百里助專案

客戶需求

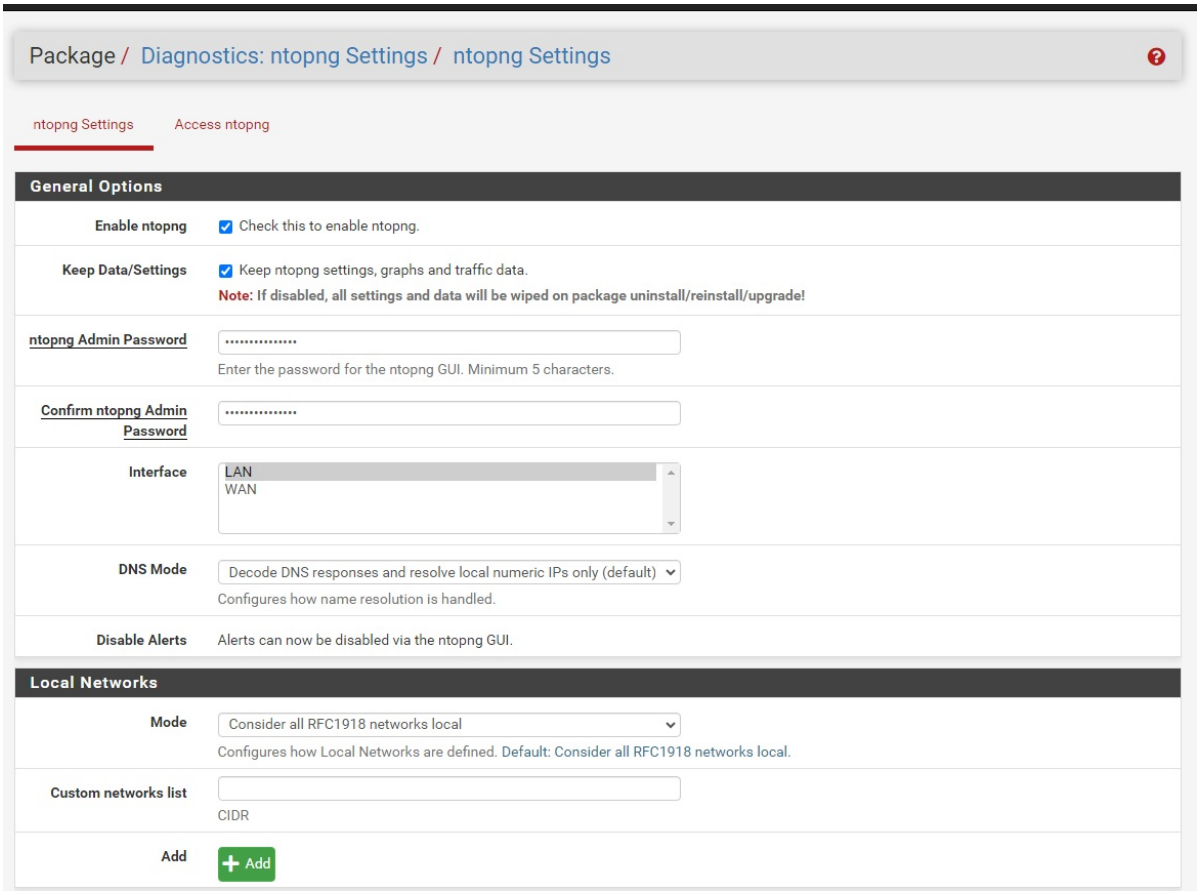
- 觀看連線資訊
- 利用防火牆做阻擋。
- 或利用防火牆限速。

解決方案

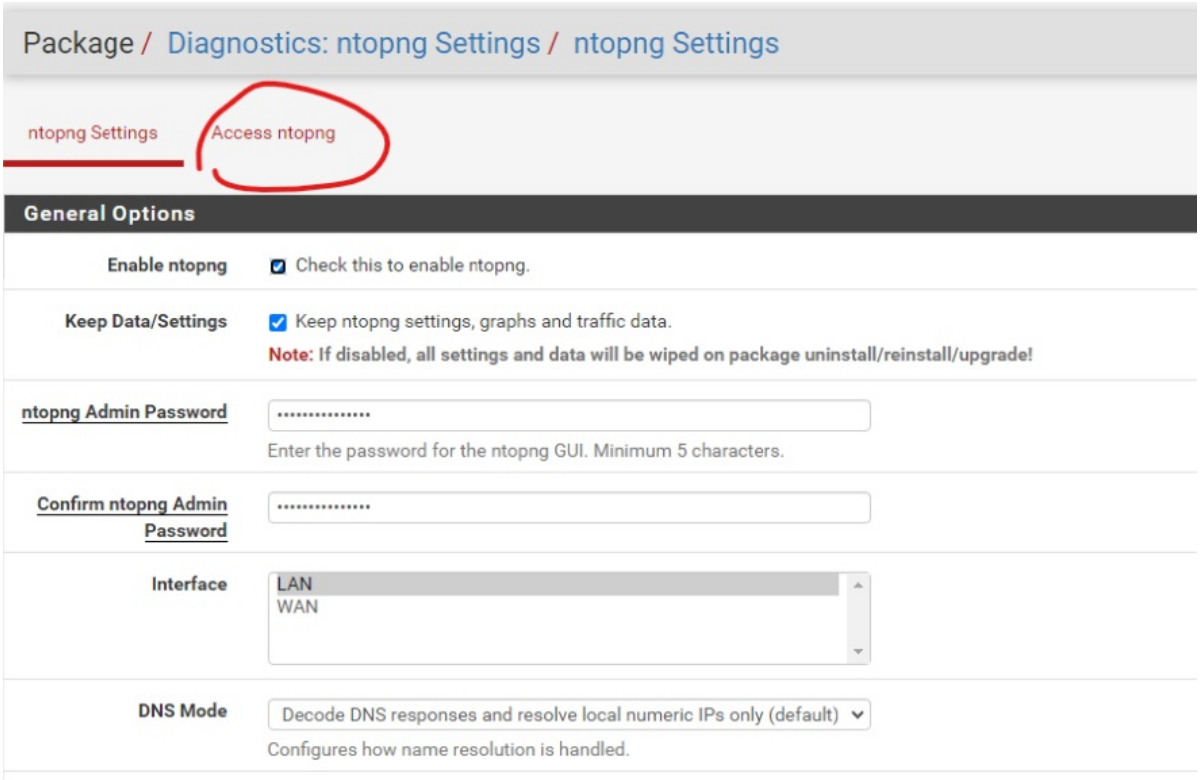
- 觀看連線資訊
  使用套件 ntopng安裝:
  1 到 System \ Package Manager \ Available Packages 搜尋 ntopng，點選安裝。

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

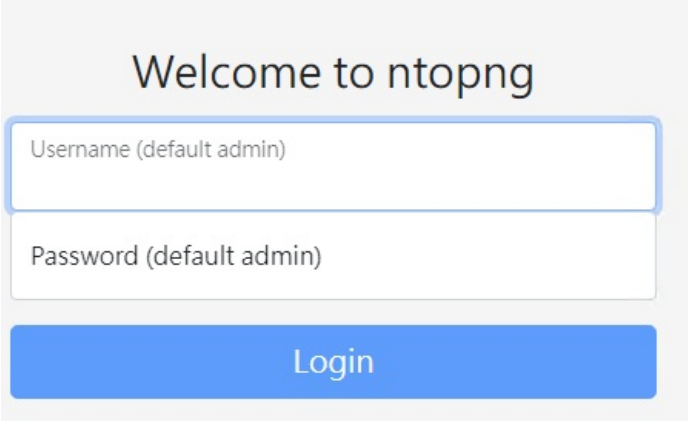
  勾選 Enable ntopng , Keep Data/Settings
  再設定 ntopng 網頁密碼，等下登入會用到。



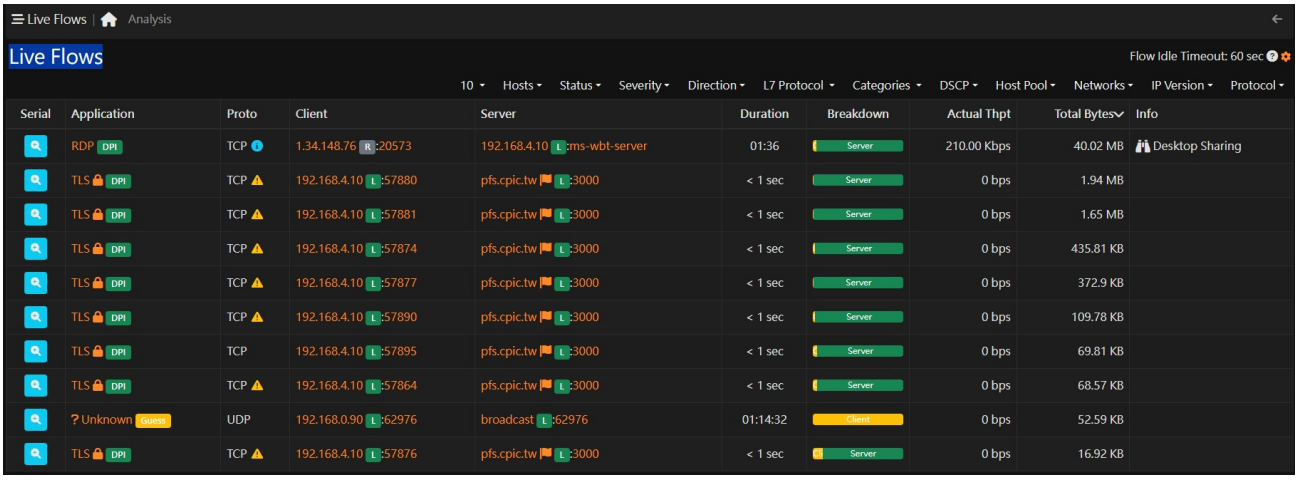
3 網頁登入 點選設定旁 Access ntopng



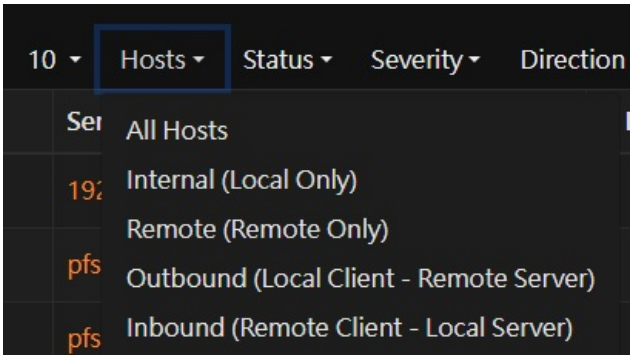
畫面如下
輸入帳密 admin/剛剛設定的密碼



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