

# 百里助專案

## 客戶需求

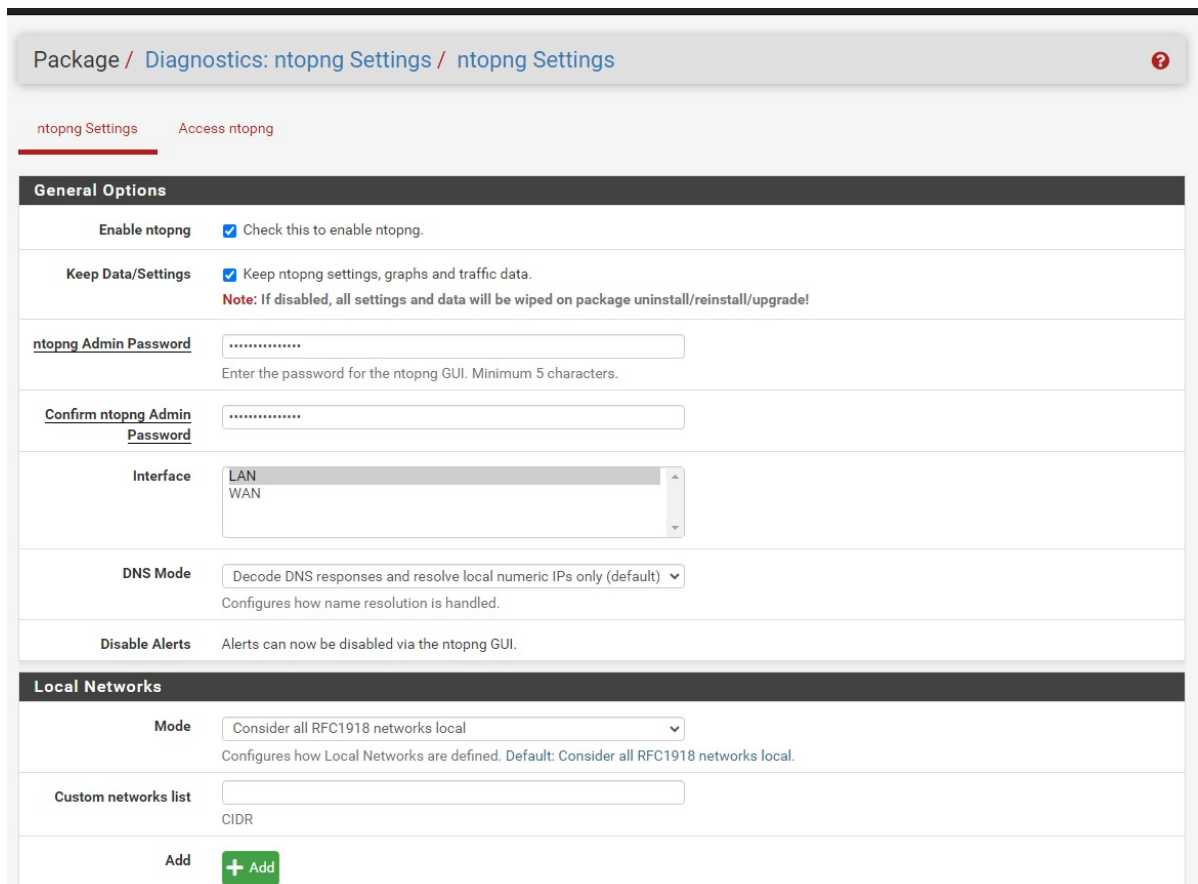
- 觀看連線資訊
- 利用防火牆做阻擋。
- 或利用防火牆限速。

## 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。



The screenshot shows the ntopng Settings page in a web interface. The breadcrumb path is Package / Diagnostics: ntopng Settings / ntopng Settings. The page has two tabs: ntopng Settings (selected) and Access ntopng. The main content is divided into two sections: General Options and Local Networks.

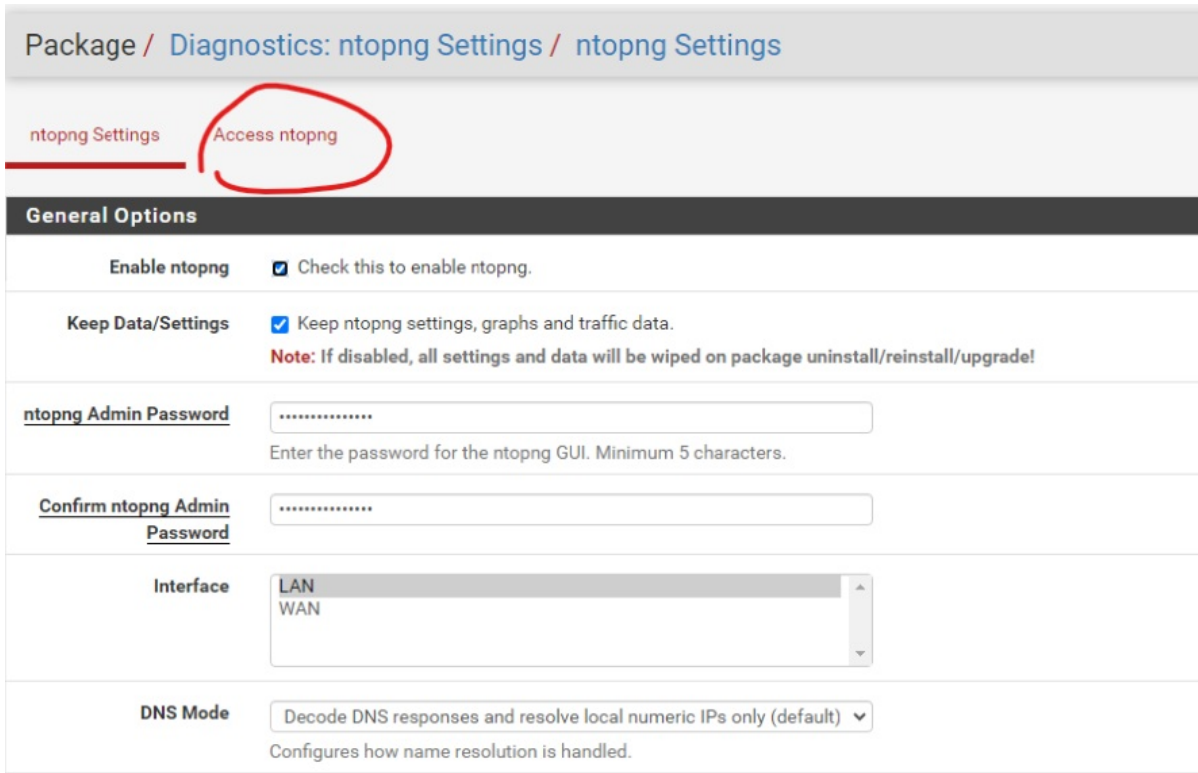
**General Options**

- Enable ntopng**:  Check this to enable ntopng.
- Keep Data/Settings**:  Keep ntopng settings, graphs and traffic data.  
**Note:** If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade!
- ntopng Admin Password**:  Enter the password for the ntopng GUI. Minimum 5 characters.
- Confirm ntopng Admin Password**:
- Interface**: LAN (selected), WAN
- DNS Mode**: Decode DNS responses and resolve local numeric IPs only (default) (selected). Configures how name resolution is handled.
- Disable Alerts**: Alerts can now be disabled via the ntopng GUI.

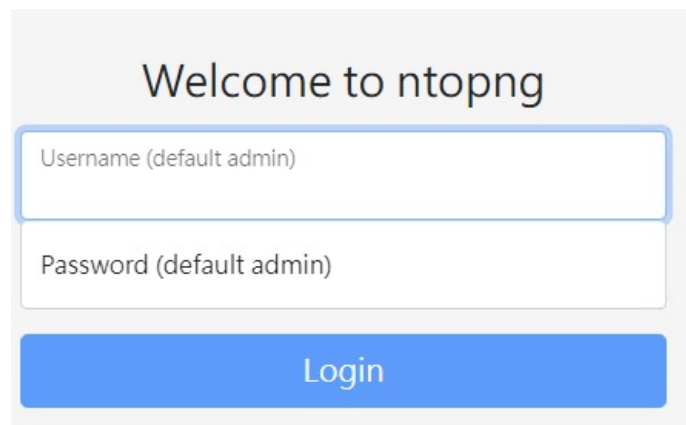
**Local Networks**

- Mode**: Consider all RFC1918 networks local (selected). Configures how Local Networks are defined. Default: Consider all RFC1918 networks local.
- Custom networks list**:  CIDR
- Add**:

3 網頁登入 點選設定旁 Access ntopng



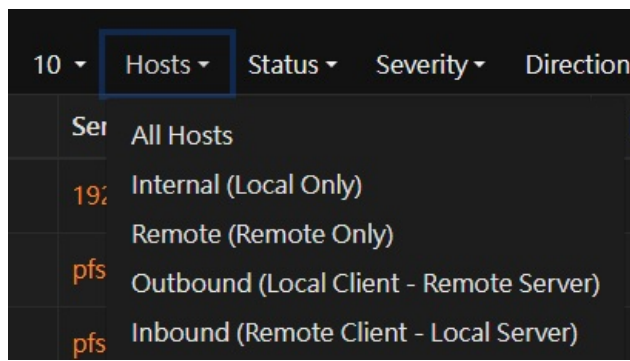
畫面如下  
輸入帳密 admin/剛剛設定的密碼




到 flow \ live 看及時流量

Serial	Application	Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
	RDP <span>DPI</span>	TCP	1.34.148.76 <span>R</span> :20573	192.168.4.10 <span>L</span> :ms-wbt-server	01:36	<span>Server</span>	210.00 Kbps	40.02 MB	<span>Desktop Sharing</span>
	TLS <span>DPI</span>	TCP	192.168.4.10 <span>L</span> :57880	pfs.cpictw <span>L</span> :3000	< 1 sec	<span>Server</span>	0 bps	1.94 MB	
	TLS <span>DPI</span>	TCP	192.168.4.10 <span>L</span> :57881	pfs.cpictw <span>L</span> :3000	< 1 sec	<span>Server</span>	0 bps	1.65 MB	
	TLS <span>DPI</span>	TCP	192.168.4.10 <span>L</span> :57874	pfs.cpictw <span>L</span> :3000	< 1 sec	<span>Server</span>	0 bps	435.81 KB	
	TLS <span>DPI</span>	TCP	192.168.4.10 <span>L</span> :57877	pfs.cpictw <span>L</span> :3000	< 1 sec	<span>Server</span>	0 bps	372.9 KB	
	TLS <span>DPI</span>	TCP	192.168.4.10 <span>L</span> :57890	pfs.cpictw <span>L</span> :3000	< 1 sec	<span>Server</span>	0 bps	109.78 KB	
	TLS <span>DPI</span>	TCP	192.168.4.10 <span>L</span> :57895	pfs.cpictw <span>L</span> :3000	< 1 sec	<span>Server</span>	0 bps	69.81 KB	
	TLS <span>DPI</span>	TCP	192.168.4.10 <span>L</span> :57864	pfs.cpictw <span>L</span> :3000	< 1 sec	<span>Server</span>	0 bps	68.57 KB	
	? Unknown <span>Queue</span>	UDP	192.168.0.90 <span>L</span> :62976	broadcast <span>L</span> :62976	01:14:32	<span>Client</span>	0 bps	52.59 KB	
	TLS <span>DPI</span>	TCP	192.168.4.10 <span>L</span> :57876	pfs.cpictw <span>L</span> :3000	< 1 sec	<span>Server</span>	0 bps	16.92 KB	

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:99:08:70:9C:00	Unknown Device Ty
IP Address	192.168.4.10 [ 192.168.4.0/24 ]	Host Pool: Default #
Name	🌙 192.168.4.10 🔄 ⚙️ 📡 📄 📌	
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		
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

🔄 修訂版本 #5

★ 由 brianlin 建立於 1 August 2023 06:53:16

🔧 由 brianlin 更新於 1 August 2023 08:28:54