

進階設定

進階設定

- [阻擋網頁功能](#)
- [OPENVPN](#)
- [阻擋網頁功能-2](#)
- [百里助專案](#)
- [WIREGUARD Site to Site](#)

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

- gclid-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alias裡面新增所有網址

Firewall / Aliases / Edit

Properties

Name
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

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

Type

Host(s)

Hint Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.16 as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN	Description
<input type="text" value="gclid-line.com"/>	<input type="text" value="Description"/>
<input type="text" value="lin.ee"/>	<input type="text" value="Description"/>
<input type="text" value="line-apps-beta.com"/>	<input type="text" value="Description"/>
<input type="text" value="line-apps-rc.com"/>	<input type="text" value="Description"/>
<input type="text" value="line-apps.com"/>	<input type="text" value="Description"/>
<input type="text" value="line-cdn.net"/>	<input type="text" value="Description"/>
<input type="text" value="line-scdn.net"/>	<input type="text" value="Description"/>

在規則封鎖

Edit Firewall Rule

Action

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

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

Protocol
Choose which IP protocol this rule should match.

Source

Source Invert match /

Destination

Destination Invert match /

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

System Firewall DHCP Authentication IPsec PPP PPPoE/L2TP Server **OpenVPN** NTP Packages Settings

Advanced Log Filter

Time Process PID Quantity

Message

[Regular expression reference](#) Precede with exclamation (!) to exclude match. Invalid or potentially dangerous patterns will be ignored.

10 Matched OpenVPN Log Entries. (Maximum 500)

Time	Process	PID	Message
2023-06-30 12:48:55.910366+08:00	openvpn	88086	user 'Allenh' authenticated
2023-06-30 10:54:26.261902+08:00	openvpn	46931	user 'Allenh' authenticated
2023-06-30 09:59:06.906935+08:00	openvpn	18212	user 'Allenh' authenticated
2023-06-30 09:03:47.324322+08:00	openvpn	14023	user 'Allenh' authenticated
2023-06-29 17:21:07.726393+08:00	openvpn	25989	user 'Allenh' authenticated
2023-06-29 16:25:07.946897+08:00	openvpn	19235	user 'Allenh' authenticated
2023-06-29 15:29:08.738438+08:00	openvpn	51574	user 'Allenh' authenticated
2023-06-29 15:12:22.058562+08:00	openvpn	87087	user 'Allenh' authenticated
2023-06-29 14:43:48.971961+08:00	openvpn	28937	user 'Allenh' authenticated
2023-06-29 13:47:06.110992+08:00	openvpn	35184	user 'Allenh' 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

Edit Redirect Entry

Disabled Disable this rule

No RDR (NOT) Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface
Choose which interface this rule applies to. In most cases "WAN" is specified.

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

Protocol
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Destination Invert match. /
Type Address/mask

Destination port range
From port Custom To port Custom
Specify the port or port range for the destination of the packet for this mapping. The "to" field may be left empty if only mapping a single port.

Redirect target IP
Type Address
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, in must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Redirect target port
Port Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

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

No XMLRPC Sync Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection
View the filter rule

Filter rule association
View the filter rule

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

Host Override Options

Host

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

Domain

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

IP Address

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', 'has.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

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。

Package / Diagnostics: ntopng Settings / ntopng Settings

ntopng Settings Access ntopng

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
WAN

DNS Mode Decode DNS responses and resolve local numeric IPs only (default) ▾
Configures how name resolution is handled.

Disable Alerts Alerts can now be disabled via the ntopng GUI.

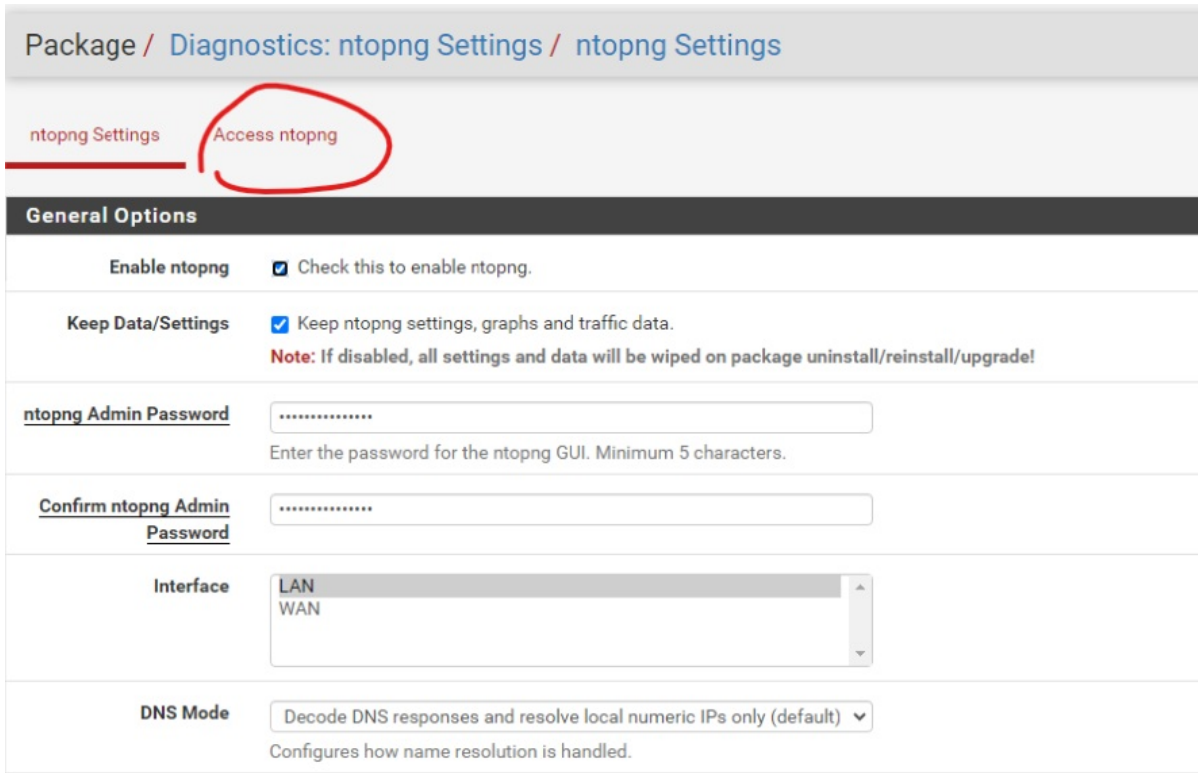
Local Networks

Mode Consider all RFC1918 networks local ▾
Configures how Local Networks are defined. Default: Consider all RFC1918 networks local.

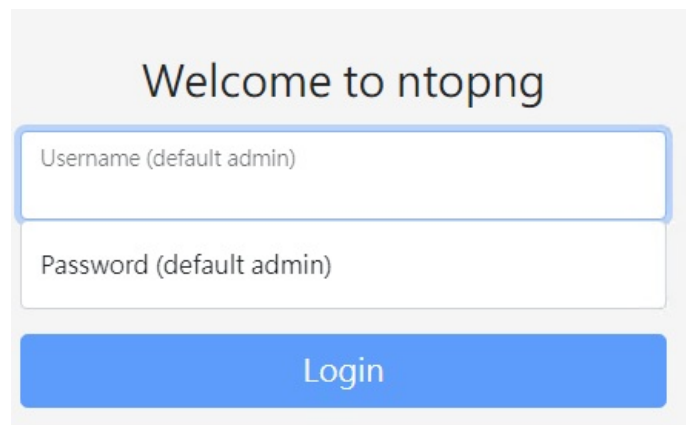
Custom networks list
CIDR

Add

3 網頁登入 點選設定旁 Access ntopng



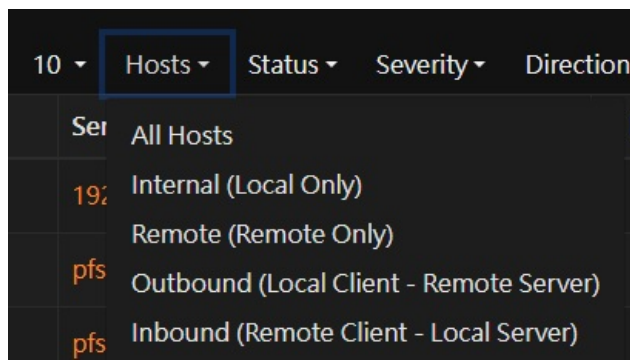
畫面如下
輸入帳密 admin/剛剛設定的密碼




到 flow \ live 看及時流量

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

WIREGUARD Site to Site

WIREGUARD Site to Site

参考

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