

PFSENSE 設定

PFSENSE 設定

- [目錄](#)
- [安裝及初次設定](#)
- [CPFS基本設定](#)
- [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](#)

目錄

- 安裝
 - 基本安裝
- 基本設定
 - 初次設定
- 進階設定
 - 阻擋網頁功能
 - OPENVPN
- 特殊功能

安裝及初次設定

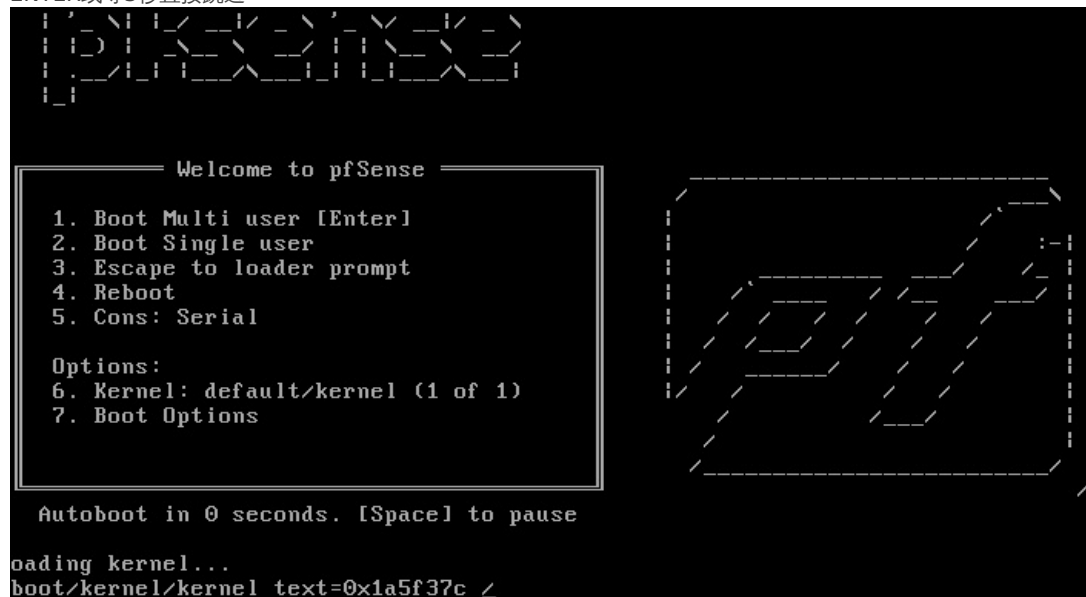
1. 安裝

1 安裝環境可以是X64 PC 或 VM

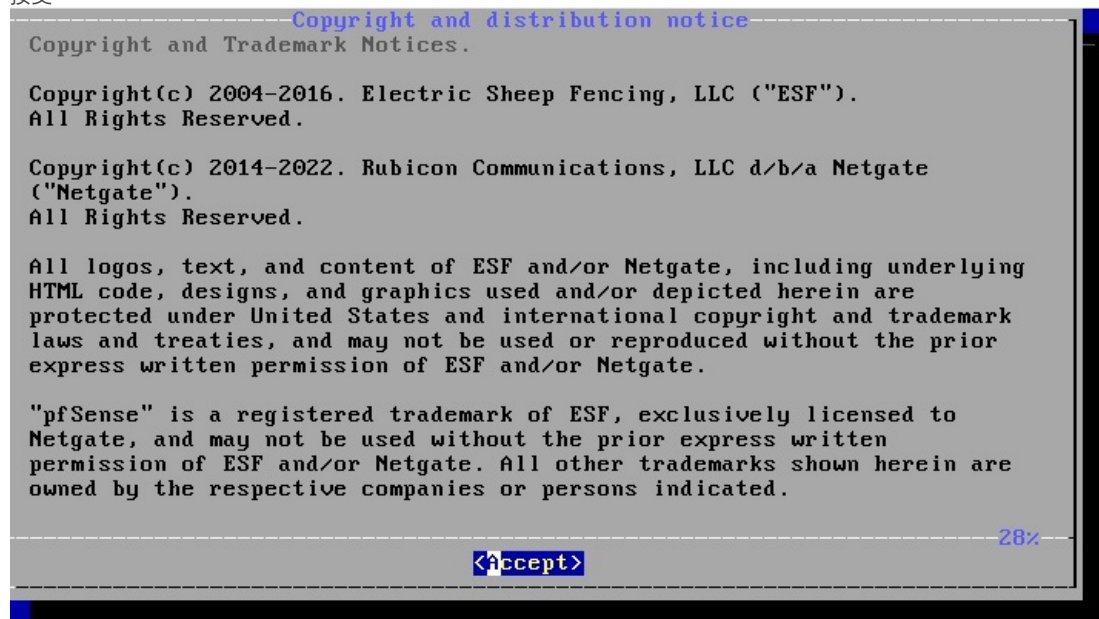
2 首先到官方網頁先下載安裝檔 <https://www.pfsense.org/download/>，下載光碟ISO 或是 IMG檔都可以，ISO燒錄成光碟，或使用ISO 或 IMG檔，寫入USB隨身碟，推薦軟體 IMGURN，balenaEtcher。

3 使用ISO或USB開機，

ENTER或等3秒直接跳過



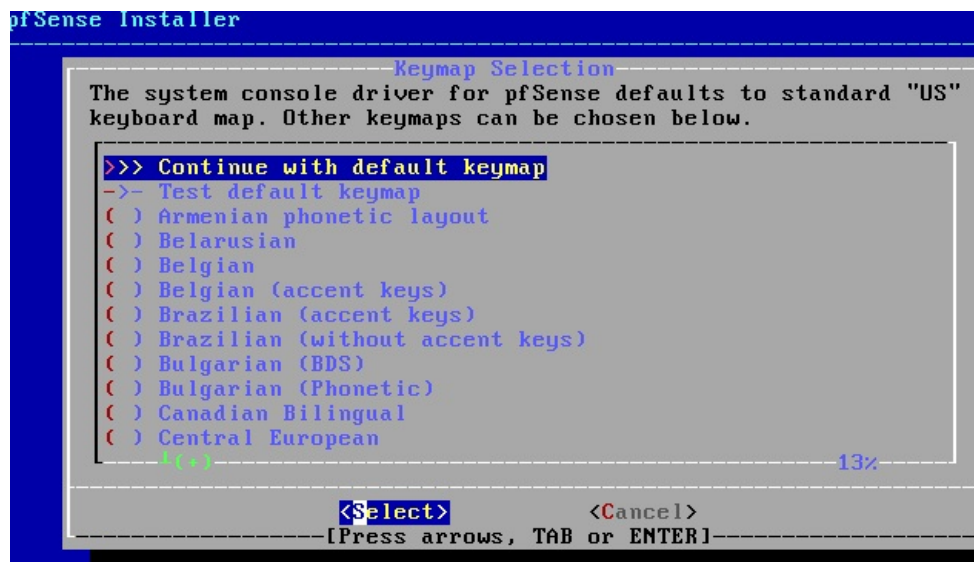
接受



選 INSTALL



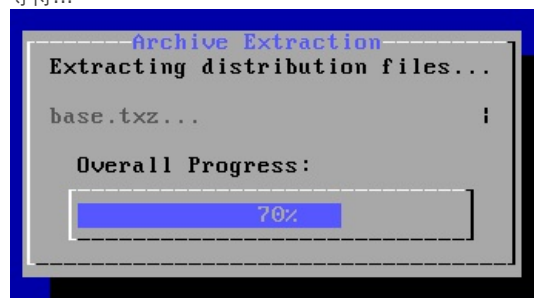
選預設鍵盤



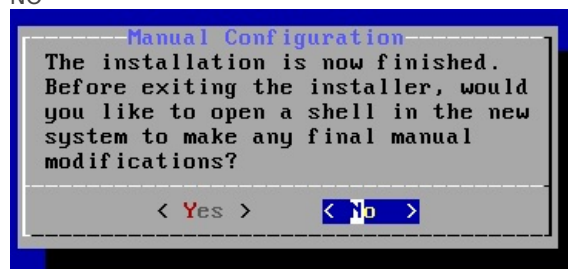
選UFS BIOS，新機可選 UFS-UEFI



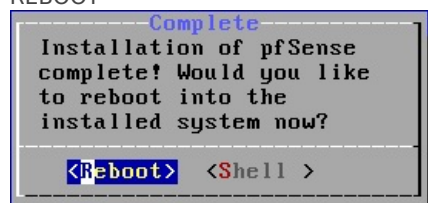
等待...



NO



REBOOT

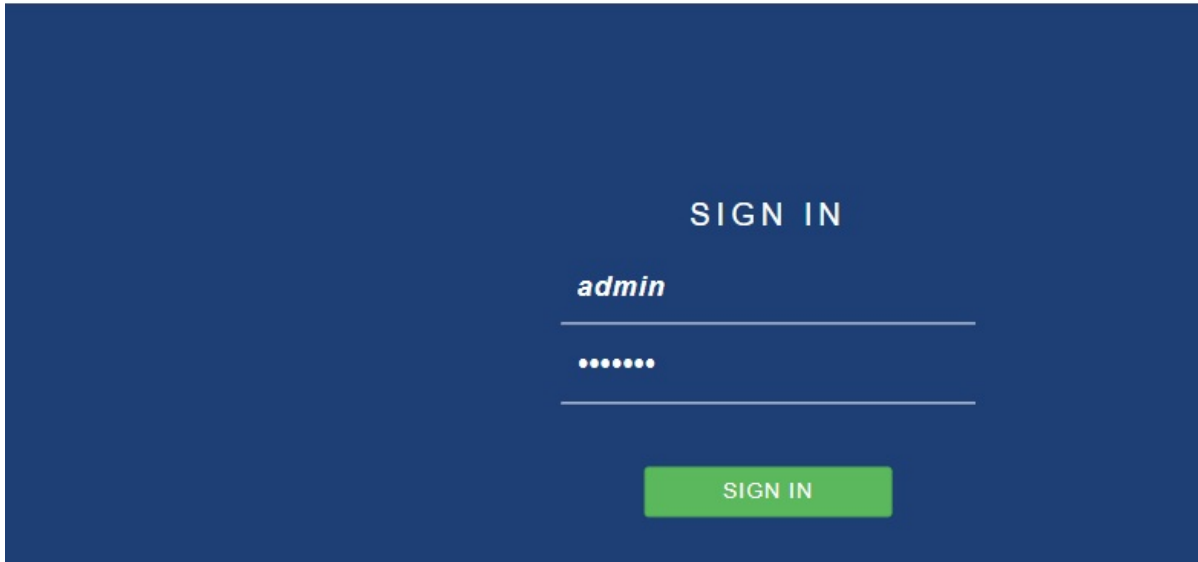


移出光碟後重新開機，會開到初始畫面

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) 帳號 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

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup /

pfSense Setup

Welcome to pfSense® software!

This wizard will provide guidance through the initial configuration of pfSense.

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

pfSense® software is developed and maintained by Netgate®

[Learn more](#)

[» Next](#)

本機安裝

```
VirtualBox Virtual Machine - Netgate Device ID: 754d8ac539448d1de773
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.111.110/24
LAN (lan)      -> em1          -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

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 / Aliases / IP

IP Ports URLs All

- Aliases
- NAT
- Rules
- Schedules
- Traffic Shaper
- Virtual IPs

Firewall Aliases IP

Name	Values
------	--------

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 FQDN. Hosts are re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. For example, as 192.168.1.16/28 may also be entered and a list of individual IP addresses

IP or FQDN

Firewall\Rules 增加信任IP (CPIC)

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 /

Extra Options

Log Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (the Status: System Logs: Settings page).

Description
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the fir

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

System										
Hostname	<input type="text" value="pfs"/> Name of the firewall host, without domain part									
Domain	<input type="text" value="cpic.com.tw"/> Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternative TLDs such as 'local.lan' or 'mylocal' are safe.									
DNS Server Settings										
DNS Servers	<table><tbody><tr><td><input type="text" value="168.95.1.1"/></td><td><input type="text" value="DNS Hostname"/></td><td><input type="button" value="Delete"/></td></tr><tr><td><input type="text" value="1.1.1.1"/></td><td><input type="text" value="DNS Hostname"/></td><td><input type="button" value="Delete"/></td></tr><tr><td><input type="text" value="8.8.8.8"/></td><td><input type="text" value="DNS Hostname"/></td><td><input type="button" value="Delete"/></td></tr></tbody></table> <p>Address Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.</p> <p>Hostname Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).</p>	<input type="text" value="168.95.1.1"/>	<input type="text" value="DNS Hostname"/>	<input type="button" value="Delete"/>	<input type="text" value="1.1.1.1"/>	<input type="text" value="DNS Hostname"/>	<input type="button" value="Delete"/>	<input type="text" value="8.8.8.8"/>	<input type="text" value="DNS Hostname"/>	<input type="button" value="Delete"/>
<input type="text" value="168.95.1.1"/>	<input type="text" value="DNS Hostname"/>	<input type="button" value="Delete"/>								
<input type="text" value="1.1.1.1"/>	<input type="text" value="DNS Hostname"/>	<input type="button" value="Delete"/>								
<input type="text" value="8.8.8.8"/>	<input type="text" value="DNS Hostname"/>	<input type="button" value="Delete"/>								
Add DNS Server	<input type="button" value="+ Add DNS Server"/>									
DNS Server Override	<input type="checkbox"/> Allow DNS server list to be overridden by DHCP/PPP on WAN or remote OpenVPN server If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN or a remote OpenVPN server (if Pull DNS option is enabled) for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.									
DNS Resolution Behavior	<input type="text" value="Use remote DNS Servers, ignore local DNS"/> By default the firewall will use local DNS service (127.0.0.1, DNS Resolver or Forwarder) as the first DNS server when possible, and it will fall back to remote DNS servers otherwise. Use this option to choose alternate behaviors.									
Localization										
Timezone	<input type="text" value="Asia/Taipei"/> Select a geographic region name (Continent/Location) to determine the timezone for the firewall. Choose a special or "Etc" zone only in cases where the geographic zones do not properly handle the clock offset required for this firewall.									
Timeservers	<input type="text" value="time.stdtime.gov.tw"/> Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if a host name is entered here!									

進階設定

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

Admin Access	Firewall & NAT	Networking	Miscellaneous	System Tunables	Notifications
--------------	----------------	------------	---------------	-----------------	---------------

webConfigurator

Protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS (SSL/TLS)
SSL/TLS Certificate	<input type="text" value="CPICC"/> <small>Certificates known to be incompatible with use for HTTPS are not included in this list.</small>
TCP port	<input type="text" value="8080"/> <small>Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.</small>

- 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

NAT Reflection mode for port forwards	<input type="text" value="NAT + Proxy"/> <ul style="list-style-type: none"> The Pure NAT mode uses a set of NAT rules to direct packets to the target of the port forward. It has better scalability, but it must be possible to accurately determine the interface and gateway IP used for communication with the target at the time the rules are loaded. There are no inherent limits to the number of ports other than the limits of the protocols. All protocols available for port forwards are supported. The NAT + Proxy mode uses a helper program to send packets to the target of the port forward. It is useful in setups where the interface and/or gateway IP used for communication with the target cannot be accurately determined at the time the rules are loaded. Reflection rules are not created for ranges larger than 500 ports and will not be used for more than 1000 ports total between all port forwards. This feature does not support IPv6. Only TCP and UDP protocols are supported. <small>Individual rules may be configured to override this system setting on a per-rule basis.</small>
Reflection Timeout	<input type="text" value="2000"/> <small>Enter value for Reflection timeout in seconds. Note: Only applies to Reflection on port forwards in NAT + proxy mode.</small>
Enable NAT Reflection for 1:1 NAT	<input type="checkbox"/> Automatic creation of additional NAT redirect rules from within the internal networks. <small>Note: Reflection on 1:1 mappings is only for the inbound component of the 1:1 mappings. This functions the same as the pure NAT mode for port forwards. For more details, refer to the pure NAT mode description above. Individual rules may be configured to override this system setting on a per-rule basis.</small>
Enable automatic outbound NAT for Reflection	<input checked="" type="checkbox"/> Automatic create outbound NAT rules that direct traffic back out to the same subnet it originated from. <small>Required for full functionality of the pure NAT mode of NAT Reflection for port forwards or NAT Reflection for 1:1 NAT. Note: This only works for assigned interfaces. Other interfaces require manually creating the outbound NAT rules that direct the reply packets back through the router.</small>

- 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"

E-Mail

Disable SMTP	<input type="checkbox"/> Disable SMTP Notifications <small>Check this option to disable SMTP notifications but preserve the settings below. Some other mechanisms, such as packages, may need these settings in place to function.</small>
E-Mail server	<input type="text" value="msa.hinet.net"/> <small>This is the FQDN or IP address of the SMTP E-Mail server to which notifications will be sent.</small>
SMTP Port of E-Mail server	<input type="text" value="25"/> <small>This is the port of the SMTP E-Mail server, typically 25, 587 (submission) or 465 (smtps).</small>
Connection timeout to E-Mail server	<input type="text"/> <small>This is how many seconds it will wait for the SMTP server to connect. Default is 20s.</small>
Secure SMTP Connection	<input type="checkbox"/> Enable SMTP over SSL/TLS
Validate SSL/TLS	<input type="checkbox"/> Validate the SSL/TLS certificate presented by the server <small>When disabled, the server certificate will not be validated. Encryption will still be used if available, but the identity of the server will not be confirmed.</small>
From e-mail address	<input type="text" value="test.cpic@msa.hinet.net"/> <small>This is the e-mail address that will appear in the from field.</small>
Notification E-Mail address	<input type="text" value="alarm@cpic.com.tw"/> <small>Enter the e-mail address to send email notifications to.</small>
Notification E-Mail auth username (optional)	<input type="text"/> <small>Enter the e-mail address username for SMTP authentication.</small>
Notification E-Mail auth password	<input type="text" value="Notification E-Mail auth password"/> <input type="text" value="Notification E-Mail auth password"/> <small>Enter the e-mail account password for SMTP authentication. Confirm</small>
Notification E-Mail auth mechanism	<input type="text" value="PLAIN"/> <small>Select the authentication mechanism used by the SMTP server. Most work with PLAIN, some servers like Exchange or Office365 might require LOGIN.</small>

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

IPv6 Options**Allow IPv6** All IPv6 traffic will be blocked by the firewall unless this box is checked

NOTE: This does not disable any IPv6 features on the firewall, it only blocks traffic.

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

Log Rotation Options**Log Rotation Size (Bytes)**

This field controls the size at which logs will be rotated. By default this is 500 KiB per log file, and there are nearly 20 such log files. Rotated log files consume additional disk space, which varies depending on compression and retention count.

NOTE: Increasing this value allows every log file to grow to the specified size, so disk usage may increase significantly. Logs from packages may consume additional space which is not accounted for in these settings. Check package-specific settings. Log file sizes are checked once per minute to determine if rotation is necessary, so a very rapidly growing log file may exceed this value.

Disk space currently used by log files: 5.4M

Worst case disk usage for base system logs based on current global settings: 58.11 MiB

Remaining disk space for log files: 236

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。

General Configuration

Enable Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address /

IPv4 Upstream gateway + Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by [clicking here](#).

Reserved Networks

Block private networks and loopback addresses
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

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

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 hostnames are re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN

防火牆規則設定允許CPIC

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

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 /

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

- 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

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

Delete

Delete

Delete

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。

The screenshot shows the ntopng Settings page. The breadcrumb trail is Package / Diagnostics: ntopng Settings / ntopng Settings. There are two tabs: ntopng Settings (active) and Access ntopng. The page is divided into two main 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**: [password field]
Enter the password for the ntopng GUI. Minimum 5 characters.
- Confirm ntopng Admin Password**: [password field]
- Interface**: LAN (selected), WAN
- DNS Mode**: Decode DNS responses and resolve local numeric IPs only (default) [dropdown]
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 [dropdown]
Configures how Local Networks are defined. Default: Consider all RFC1918 networks local.
- Custom networks list**: [text field]
CIDR
- Add**:

3 網頁登入 點選設定旁 Access ntopng

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.

畫面如下
輸入帳密 admin/剛剛設定的密碼

Welcome to ntopng

Username (default admin)

Password (default admin)

Login

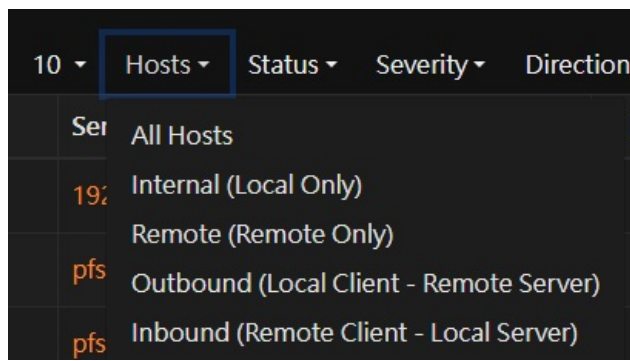
到 flow \ live 看及時流量

Live Flows Analysis

Flow Idle Timeout: 60 sec

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:57873 sms-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 Counts	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 [192.168.4.0/24]	
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

進階設定

WIREGUARD Site to Site

WIREGUARD Site to Site

參考

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