

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	<input type="text" value="168.95.1.1"/>	DNS Hostname	<input type="text"/>	<input type="button" value="Delete"/>
	<input type="text" value="1.1.1.1"/>	DNS Hostname	<input type="text"/>	<input type="button" value="Delete"/>
	<input type="text" value="8.8.8.8"/>	DNS Hostname	<input type="text"/>	<input type="button" value="Delete"/>
	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.		Hostname Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).	
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	<input type="text" value="220.128.126.132"/>	<input type="text" value="Description"/>	 Delete
	<input type="text" value="1.34.148.76"/>	<input type="text" value="Description"/>	 Delete

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 /

🔄 修訂版本 #11

★ 由 brianlin 建立於 19 June 2023 07:22:43

🔧 由 brianlin 更新於 9 July 2023 17:43:20