

Configuration Certilab

Table des matières

1. Configuration IP et paramètres généraux	2
2. Administration sur l'interface Web	3
3. Création des Certificat d'autorité et Certificats Serveur	5
1. Certificat Autorité	5
2. Certificats de Serveurs	6
3. Liste des certificats :	7
4. Mise en place du Certificat SSL sur le WebConfigurator du Certilab	8
5. Test de la connexion en https :	8
6. Contenu des certificats	9

1. Configuration IP et paramètres généraux

On va devoir mettre une adresse IP à l'interface principale de notre OS PfSense.

```
Message from syslogd@certilab at Dec  3 21:17:19 ...
php-fpm[396]: /index.php: Successful login for user 'admin' from: 172.16.0.58 (Local Database)

FreeBSD/amd64 (certilab.galaxy-swiss.local) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: 940a04eb54ef7a29878c
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on certilab ***

WAN (wan)      -> em0      -> v4: 172.16.0.40/17

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
```

Ici on doit taper sur le 2, afin de mettre une adresse IP à l'interface em0 qui sera notre accès à l'interface Web pour continuer à l'administration de manière plus graphique et plus simple.

```
Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 172.16.0.40

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 17

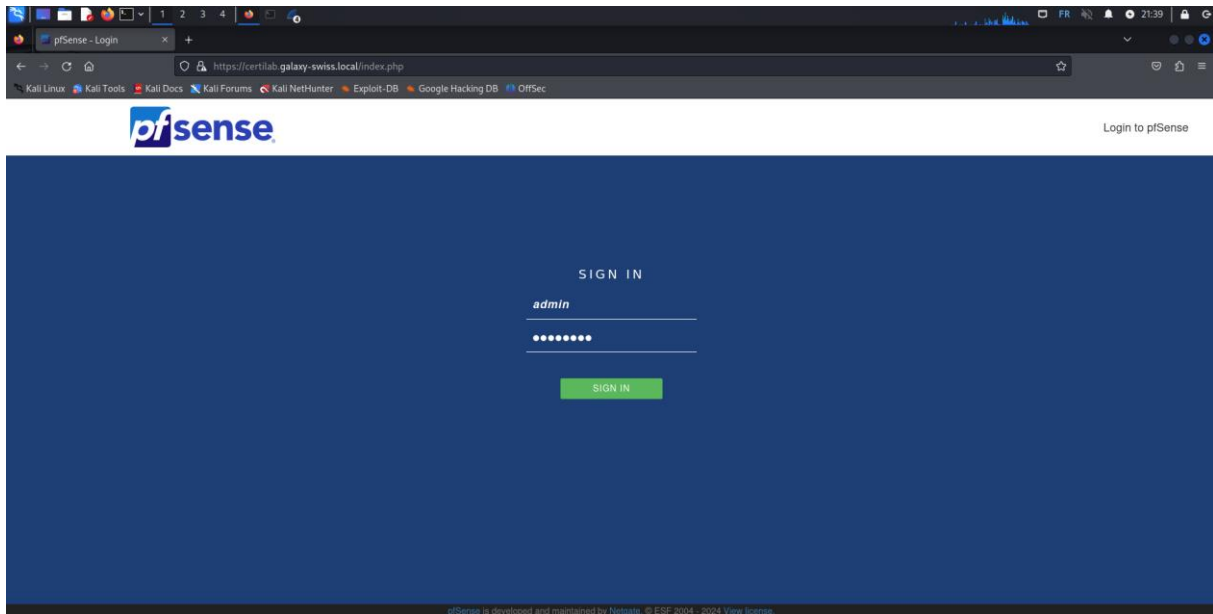
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address WAN interface via DHCP6? (y/n) n

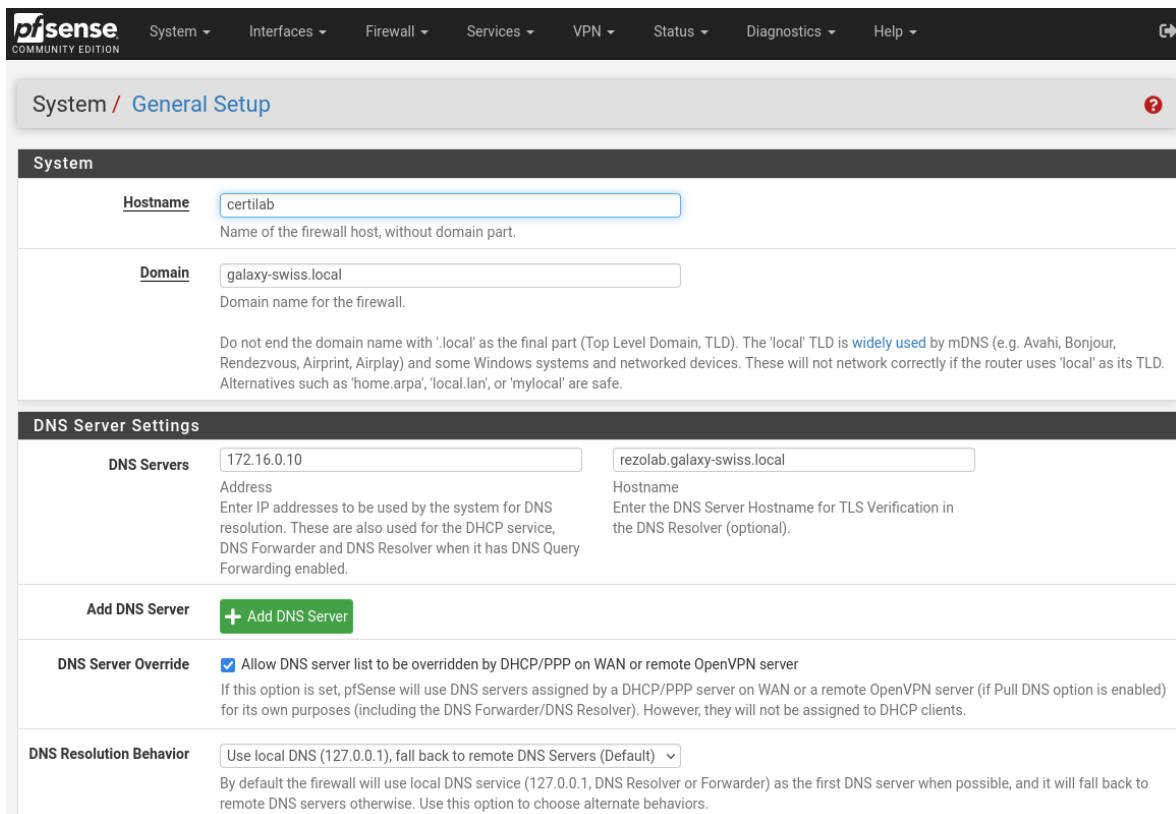
Enter the new WAN IPv6 address. Press <ENTER> for none:
>
```

2. Administration sur l'interface Web

On va passer sur l'interface Web, on peut s'y connecter avec son FQDN grâce a son nom DNS :



On va continuer la configuration IP Notamment en lui affectant notre serveur DNS qui est Rezolab



Et lui mettre une adresse de passerelle pour qu'elle puisse communiquer avec les autres réseaux :

Static IPv4 Configuration

IPv4 Address

172.16.0.40

/ 17

IPv4 Upstream gateway

gateway - 172.16.0.1

+ 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](#).

On peut voir les informations générales du PFSense actuel

Status / Dashboard

System Information

Name	certilab.galaxy-swiss.local
User	admin@172.16.0.58 (Local Database)
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 21:10:00 CET 2023 FreeBSD 14.0-CURRENT Unable to check for updates
Uptime	00 Hour 41 Minutes 21 Seconds
Current date/time	Tue Dec 3 21:51:10 CET 2024
DNS server(s)	• 172.16.0.10
Last config change	Tue Dec 3 21:46:22 CET 2024
State table size	0% (3/96000) Show states
MBUF Usage	0% (3302/1000000)
CPU usage	Retrieving CPU data
Memory usage	26% of 962 MiB
SWAP usage	0% of 1024 MiB

Interfaces

LAN

1000baseT <full-duplex>

172.16.0.40

Gateways

Name	RTT	RTTsd	Loss	Status
gateway 172.16.0.1	0.0ms	0.0ms	100%	Offline, Packetloss

Services Status

Service	Description	Action
dnsmasq	DNS Forwarder	
dpinger	Gateway Monitoring Daemon	
syslogd	System Logger Daemon	

Douchez Tao

Configuration Certilab – AP Navajo

4

3. Création des Certificat d'autorité et Certificats Serveur

1. Certificat Autorité

Tout d'abord, nous devons créer un Certificat d'autorité autosigné afin de fournir aux différentes interfaces web une sécurisation en https.

On va créer une zone d'autorité appelée « zoneautorite » qu'on va déclarer comme un « Trust Store » qui va permettre à l'OS de faire confiance au certificat créé.

The screenshot shows the 'Create / Edit CA' form in the 'System / Certificate / Authorities / Edit' interface. The form has three tabs: 'Authorities' (selected), 'Certificates', and 'Revocation'. The form fields are as follows:

- Descriptive name:** zoneautorite. The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '.
- Method:** Create an internal Certificate Authority.
- Trust Store:** ☒ Add this Certificate Authority to the Operating System Trust Store. When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.
- Randomize Serial:** ☒ Use random serial numbers when signing certificates. When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Ici on va définir les algos de chiffrement avec le type de clé, plus les bits sont élevés plus les échanges vont être difficiles à déchiffrer. Ensuite on a les informations facultatives telles que la région etc...que nous allons pas remplir. Notre Certification d'Autorité est bien créée.

The screenshot shows the 'Internal Certificate Authority' form. The form fields are as follows:

- Key type:** RSA.
- Key length (bits):** 8192. The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
- Digest Algorithm:** sha512. The digest method used when the CA is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.
- Lifetime (days):** 3650.
- Common Name:** ca-interne.
- Optional components:** The following certificate authority subject components are optional and may be left blank.
 - Country Code:** FR.
 - State or Province:** e.g. Texas.
 - City:** e.g. Austin.
 - Organization:** e.g. My Company Inc.
 - Organizational Unit:** e.g. My Department Name (optional).

2. Certificats de Serveurs

Ensuite nous allons créer les Certificats de Serveurs, ici je déclare son nom et pour que cela soit explicite je mets le nom du serveur en question « Certilab ».

The screenshot shows the 'Add/Sign a New Certificate' form. At the top, there is a breadcrumb trail: 'System / Certificates / Certificates / Edit'. Below this, there are three tabs: 'Authorities', 'Certificates' (which is selected and underlined in red), and 'Certificate Revocation'. The form itself has a dark header bar with the text 'Add/Sign a New Certificate'. Below the header, there are two main sections. The first section is labeled 'Method' and contains a dropdown menu with the option 'Create an internal Certificate'. The second section is labeled 'Descriptive name' and contains a text input field with the value 'certilab'. Below the input field, there is a small text block that reads: 'The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", \''.

Ces Certificats doivent s'appuyer sur le Certificat d'autorité défini juste avant, alors nous déclarons donc que « zoneautorite » est le certificat qui sert d'autorité au certificat Certilab. On ne rentre pas les informations facultatives.

The screenshot shows the 'Internal Certificate' form. It has a dark header bar with the text 'Internal Certificate'. Below the header, there are several sections. The first section is labeled 'Certificate authority' and contains a dropdown menu with the value 'zoneautorite'. The second section is labeled 'Key type' and contains a dropdown menu with the value 'RSA'. Below this, there is a text input field with the value '8192'. Below the input field, there is a small text block that reads: 'The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.' The third section is labeled 'Digest Algorithm' and contains a dropdown menu with the value 'sha512'. Below the dropdown menu, there is a small text block that reads: 'The digest method used when the certificate is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.' The fourth section is labeled 'Lifetime (days)' and contains a text input field with the value '3650'. Below the input field, there is a small text block that reads: 'The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.' The fifth section is labeled 'Common Name' and contains a text input field with the value 'e.g. www.example.com'. Below the input field, there is a small text block that reads: 'The following certificate subject components are optional and may be left blank.' The sixth section is labeled 'Country Code' and contains a dropdown menu with the value 'FR'. The seventh section is labeled 'State or Province' and contains a text input field with the value 'e.g. Texas'. The eighth section is labeled 'City' and contains a text input field with the value 'e.g. Austin'. The ninth section is labeled 'Organization' and contains a text input field with the value 'e.g. My Company Inc'. The tenth section is labeled 'Organizational Unit' and contains a text input field with the value 'e.g. My Department Name (optional)'.

Ici, on veille à faire bien attention que ce soit un type de certificat « Server certificate » pour qu'on puisse les implanter dans les configurations de nos serveurs.

Après cela, le premier certificat de serveur est créé, on peut cliquer sur « save » et faire la même chose avec les autres :

Certificate Attributes

Attribute Notes

The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type

Server Certificate

Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

3. Liste des certificats :

Certificat D'autorité :

System / Certificate / Authorities

Authorities Certificates Revocation

Search

Search term

Both

Search

Clear

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
zoneautorite	✓	self-signed	3	CN=certilab.galaxy-swiss.local, C=FR Valid From: Wed, 13 Nov 2024 15:26:55 +0100 Valid Until: Sat, 11 Nov 2034 15:26:55 +0100		   

+ Add

Certificats Serveurs :

System / Certificates / Certificates				
Authorities Certificates Certificate Revocation				
Search				
Search term Both Search Clear				
Enter a search string or *nix regular expression to search certificate names and distinguished names.				
Certificates				
Name	Issuer	Distinguished Name	In Use	Actions
certilab Server Certificate CA: No Server: Yes	zoneautorite	CN=certilab.galaxy-swiss.local, C=FR Valid From: Wed, 13 Nov 2024 15:28:20 +0100 Valid Until: Thu, 13 Nov 2025 15:28:20 +0100	webConfigurator	
extralab Server Certificate CA: No Server: Yes	zoneautorite	CN=extralab.galaxy-swiss.local, C=FR Valid From: Wed, 13 Nov 2024 15:51:46 +0100 Valid Until: Thu, 13 Nov 2025 15:51:46 +0100		
proxylab Server Certificate CA: No Server: Yes	zoneautorite	CN=proxylab.galaxy-swiss.local, C=FR Valid From: Wed, 13 Nov 2024 16:01:12 +0100 Valid Until: Thu, 13 Nov 2025 16:01:12 +0100		
+ Add/Sign				

4. Mise en place du Certificat SSL sur le WebConfigurator du Certilab

Pour que l'interface Web sécurisée soit opérationnelle, nous devons sélectionner le protocole HTTPS dans les paramètres avancés et sélectionner le certificat correspondant au Certilab.

System / Advanced / Admin Access

Admin Access Firewall & NAT Networking Miscellaneous System Tunables Notifications

webConfigurator

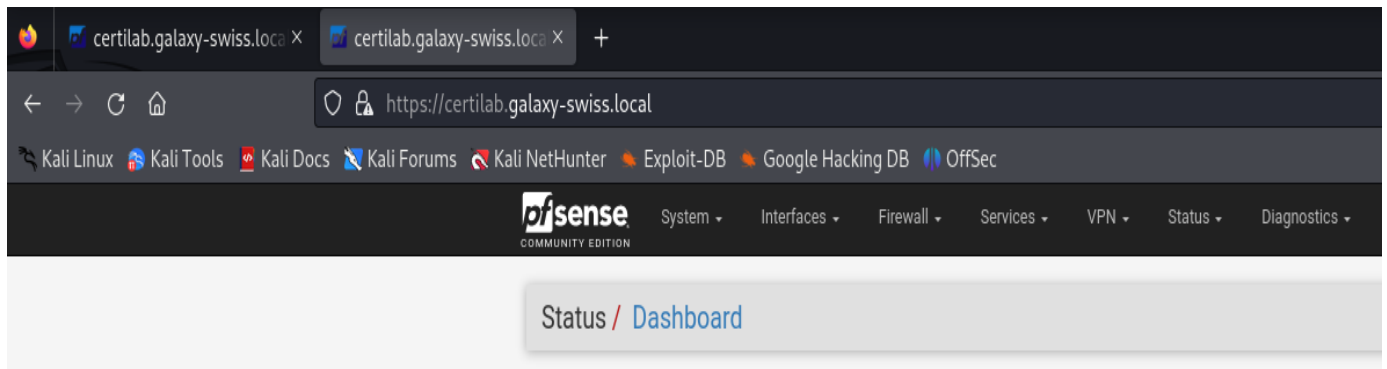
Protocol ☐ HTTP ☒ HTTPS (SSL/TLS)

SSL/TLS Certificate certilab

TCP port proxylab

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.

5. Test de la connexion en https :

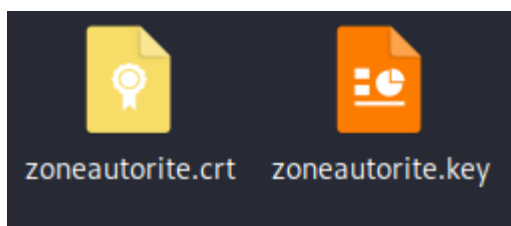


On peut voir que nous sommes connectés en https et qu'on ne peut pas nous connecter en http, ce qui sécurise donc les échanges entre ce serveur et les autres services.

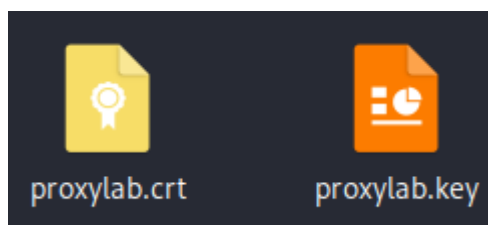
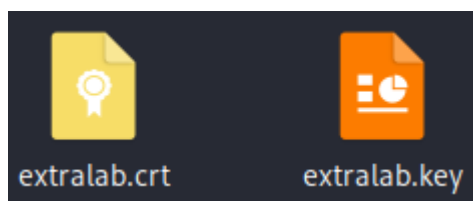
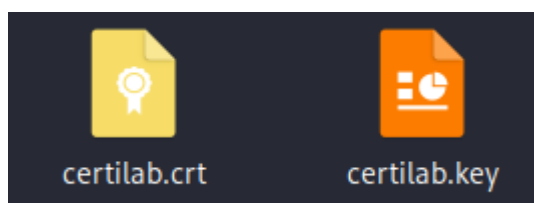
Nous allons évidemment faire la même chose sur les autres serveurs disposant d'une interface Web à sécuriser

6. Contenu des certificats

Certificat d'autorité



Certificats Serveurs



4. Dossier Technique de Configuration de Certilab

Screenshot Dashboard :

The screenshot shows the pfSense Dashboard. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is divided into two columns. The left column, titled 'System Information', displays details about the system, including the name (certilab.galaxy-swiss.local), user (admin@172.16.0.58), version (2.7.2-RELEASE), uptime (01 Hour 36 Minutes 12 Seconds), current date/time (Tue Dec 3 22:46:01 CET 2024), DNS server(s) (172.16.0.10), last config change (Tue Dec 3 21:46:22 CET 2024), state table size (0% (2/96000)), MBUF Usage (0% (3556/1000000)), CPU usage (2%), memory usage (25% of 962 MiB), and SWAP usage (0% of 1024 MiB). The right column, titled 'Interfaces', shows the LAN interface (1000baseT <full-duplex>) with IP address 172.16.0.40. Below this, the 'Gateways' section shows a single gateway (gateway 172.16.0.1) with RTT (0.0ms), RTTsd (0.0ms), Loss (100%), and Status (Offline, Packetloss). The 'Services Status' section shows three services: dnsmasq (DNS Forwarder), dpinger (Gateway Monitoring Daemon), and syslogd (System Logger Daemon), all with status icons and action buttons.

Name	RTT	RTTsd	Loss	Status
gateway 172.16.0.1	0.0ms	0.0ms	100%	Offline, Packetloss

Service	Description	Action
dnsmasq	DNS Forwarder	⌂ ⌂
dpinger	Gateway Monitoring Daemon	⌂ ⌂
syslogd	System Logger Daemon	⌂ ⌂

Screenshot Status Interfaces :

The screenshot shows the pfSense Status Interfaces page. The top navigation bar includes links for Status, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is titled 'LAN Interface (wan, em0)'. It displays a list of interface details, including Status (up), MAC Address (08:00:27:d9:e9:d1), IPv4 Address (172.16.0.40), Subnet mask IPv4 (255.255.128.0), Gateway IPv4 (172.16.0.1), IPv6 Link Local (fe80::a00:27ff:fed9:e9d1%em0), MTU (1500), Media (1000baseT <full-duplex>), In/out packets (4962/13327 (573 KiB/3.56 MiB)), In/out packets (pass) (4962/13327 (573 KiB/3.56 MiB)), In/out packets (block) (0/3 (0 B/284 B)), In/out errors (0/0), Collisions (0), and Interrupts (9784 (2/s)). A yellow warning box at the bottom states: 'Using dial-on-demand will bring the connection up again if any packet triggers it. To substantiate this point: disconnecting manually will not prevent dial-on-demand from making connections to the outside! Don't use dial-on-demand if the line is to be kept disconnected.'

Using dial-on-demand will bring the connection up again if any packet triggers it. To substantiate this point: disconnecting manually will not prevent dial-on-demand from making connections to the outside! Don't use dial-on-demand if the line is to be kept disconnected.

Screenshot Firewall/rules :

Firewall / Rules / LAN

Floating LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☒	✓ 2/3.79 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
☒	✗ 0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Add
 Add
 Delete
 Toggle
 Copy
 Save
 Separator

Screenshot Routing-Table :

Diagnostics / Routes

Routing Table Display Options

Resolve names ☐ Enable
Enabling name resolution may cause the query to take longer. It can be stopped at any time by clicking the Stop button in the browser.

Rows to display

Filter
Use a regular expression to filter the tables. Invalid or potentially dangerous patterns will be ignored.

Update

IPv4 Routes

Destination	Gateway	Flags	Uses	MTU	Interface	Expire
default	172.16.0.1	UGS	5	1500	em0	
127.0.0.1	link#3	UH	2	16384	lo0	
172.16.0.0/17	link#1	U	1	1500	em0	
172.16.0.40	link#3	UHS	4	16384	lo0	