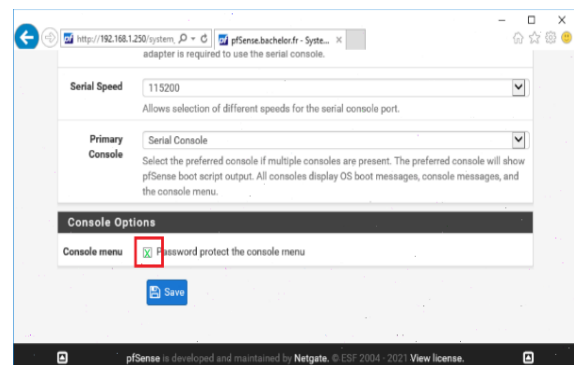
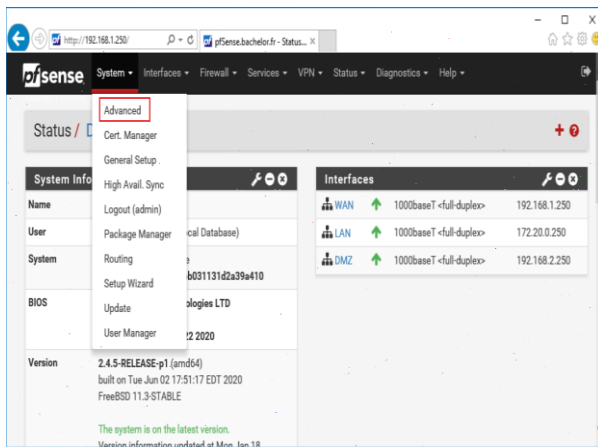




- A- Sécurisez la console par mot de passe
- B- Sécurisez l'accès par ssh
- C- Sécurisez L'interface web par https
 - a- Créer une autorité de certification interne
 - b- Générer un certificat web
 - c- Injecter le certificat web dans mon serveur pfsense

A- Sécuriser la console Pfsense

vous cochez la case console menu et vous Sauvegardez



On constate que ma console à un login

```
WAN (wan)      -> em0      -> v4: 192.168.1.250/24
LAN (lan)      -> em1      -> v4: 172.20.0.250/24
OPT1 (opt1)   -> em2      -> v4: 192.168.2.250/24

0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

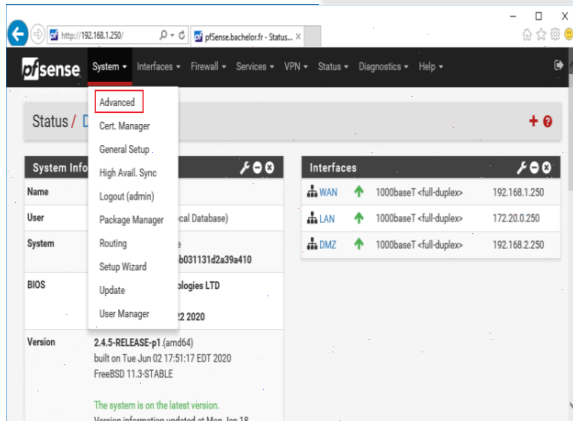
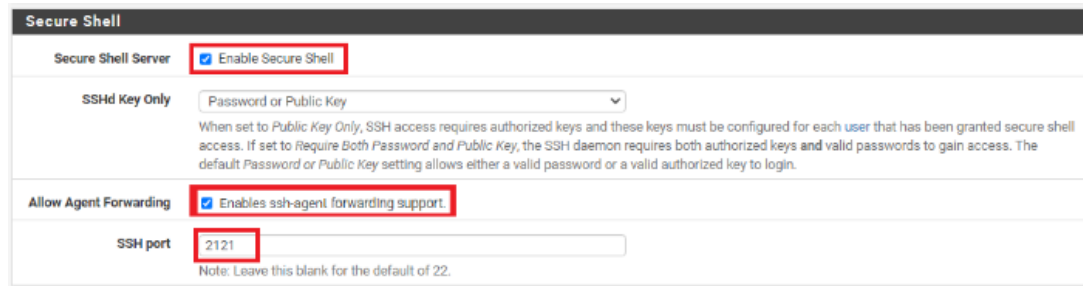
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Disable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM

Enter an option:

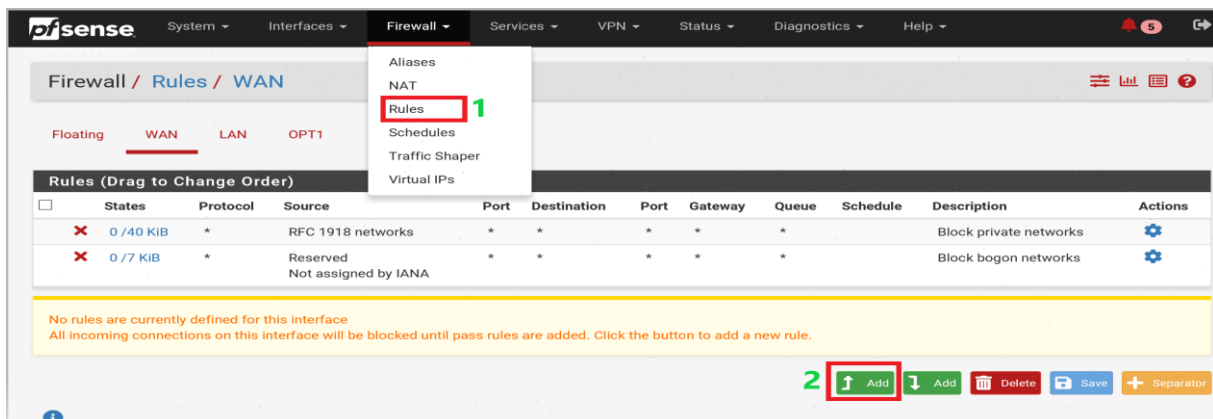
FreeBSD/amd64 (Heimdall.sitka.local) (ttyv0)
login: █
```

B- Sécurisez l'accès par ssh

On active ssh pour accéder à la console de manière sécurisée on change le port par défaut en (2121) en terme de sécurité il est toujours conseillé de changer les port par défaut; on peut aussi faire une authentification avec clé **privé/public** au lieu d'une authentification par mot de passe



Maintenant il faut une **règle** autorisant ssh sur l'interface **Wan** on va dans le menu **interface +rule + ad**



On rentre les choix ci-dessous après il ne faut pas oublier d'enregistrer et d'appliquer les changements comme indiqué dans ces captures d'écran.

Firewall / Rules / Edit

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 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
 Source Address

[Display Advanced](#)
 The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this is its default value, any.

Destination

Destination Invert match
 Destination Address

Destination Port Range
 From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering.

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, see the Status: System Logs: Settings page).

Description
 A description may be entered here for administrative reference. A maximum of 52 characters will be logged.

Advanced Options [Display Advanced](#)

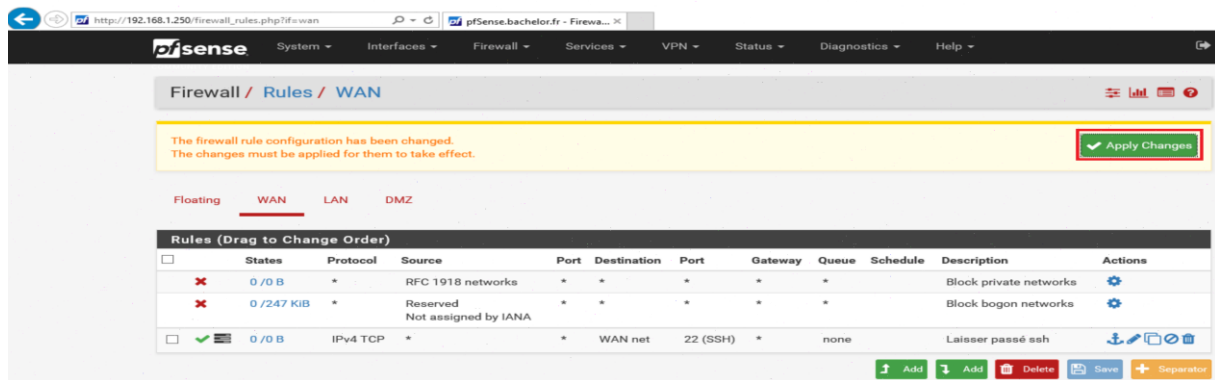
Rule Information

| | |
|--------------------|---|
| Tracking ID | 1640165746 |
| Created | 12/22/21 10:35:46 by admin@172.20.0.14 (Local Database) |
| Updated | 12/22/21 10:39:53 by admin@172.20.0.14 (Local Database) |

[Save](#)

Après avoir enregistré  on applique les changements





Attention sur Windows 2016 ssh n'est pas installé nativement contrairement à Windows 2019 ou Windows 10 sur ces deux dernière version ssh est parmi les fonctionnalités qu'on peut installer. Donc pour Windows 2016 suivre la procédure du fichier ssh_2016.docx pour installer ssh

On teste la connexion à l'intérieure de notre périmètre j'utilise une des machines dans un Lan : Je prends la machine AD je démarre le PowerShell et je me connecte sur une des interfaces de pfsense :

Le serveur pfsense m'envoie l'empreinte numérique de sa clé publique :

```
PS C:\Users\Administrateur> ssh admin@172.20.0.250 -p 2121
The authenticity of host '[172.20.0.250]:2121 ([172.20.0.250]:2121)' can't be established.
ED25519 key fingerprint is SHA256:riqHfD03Z9fhNsyAM1TC2shBu9F6+qSnpoKCTL/0dT0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[172.20.0.250]:2121' (ED25519) to the list of known hosts.
Password for admin@heimdall.sitka.local:
VMware Virtual Machine - Netgate Device ID: 7c7777e1ee8ed9111e66

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on heimdall ***

WAN (wan)      -> em0      -> v4: 192.168.1.250/24
LAN (lan)     -> em1      -> v4: 172.20.0.250/24
OPT1 (opt1)   -> em2      -> v4: 192.168.2.250/24

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) Disable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option:
```

On peut vérifier si l'empreinte numérique sur le serveur ssh est la même que celle envoyée par le serveur j'affiche le contenu détaillé du répertoire /etc/ssh après je génère l'empreinte numérique de la clé publique **ssh_host_ed25519_key.pub** en suivant les étapes 1+2+3+4 En fin je compare les deux empreintes on constate qu'elles sont identiques

```
Enter an option: 8
[2.5.2-RELEASE][admin@heimdall.sitka.local]/root: su root
# cd /etc/ssh
# ls
moduli          ssh_host_ed25519_key.pub  sshd_config
ssh_config      ssh_host_rsa_key
ssh_host_ed25519_key  ssh_host_rsa_key.pub
# ssh-keygen -lvf ssh_host_ed25519_key.pub
256 SHA256:FiqHfD03Z9fhNsvAM1TC2shBu9F6+qSnpokCTL/0dTo root@heimdall.sitka.local
(ED25519)
+--[ED25519 256]--+
. . .
.oo.
. o=.o
++o
o..S.
oo..
=.o..+..*
=. .B++E= . B
..B=O+=..
+-----[SHA256]-----+
```

Maintenant on va tester la connexion en dehors de notre périmètre Wan, sitka_Lan et opt_lan
On va essayer une connexion de notre machine physique qui est en dehors de ce périmètre

```
Windows PowerShell
PS C:\> ssh admin@192.168.1.250
ssh: connect to host 192.168.1.250 port 22: Connection timed out
PS C:\>
```

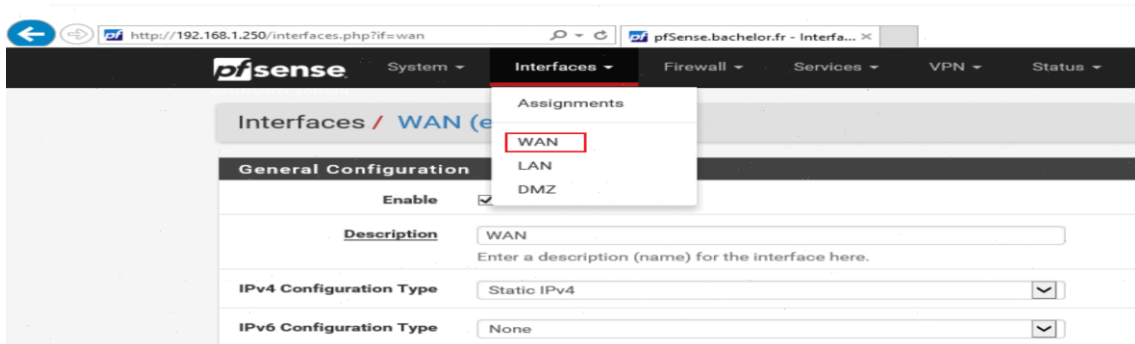
On remarque qu'il y'a échec de connexion ; on essaye de faire un ping sur cette interface, même constat

```
Windows PowerShell
PS C:\> ping 192.168.1.250

Envoi d'une requête 'Ping' 192.168.1.250 avec 32 octets de données :
Réponse de 192.168.1.156 : Impossible de joindre l'hôte de destination.
Réponse de 192.168.1.156 : Impossible de joindre l'hôte de destination.
Réponse de 192.168.1.156 : Impossible de joindre l'hôte de destination.
Réponse de 192.168.1.156 : Impossible de joindre l'hôte de destination.

Statistiques Ping pour 192.168.1.250:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
PS C:\>
```

Cet échec est normal car PfSense bloque toutes requêtes venant d'une adresse privée en dehors de son périmètre Wan, sitka_lan et opt_lan, on peut vérifier ceci aisément en allant dans le menu Interface + Wan tout en bas de la page on trouve deux cases cochées ce qui explique ce blocage



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.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

[Save](#)

On trouve la même chose dans les règles par défaut de l'interface wan

Firewall / Rules / WAN

Floating **WAN** LAN DMZ

Rules (Drag to Change Order)

| States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions |
|----------------|----------|----------------------------------|------|-------------|----------|---------|-------|----------|------------------------|---------|
| ✗ 0 / 0 B | * | RFC 1918 networks | * | * | * | * | * | | Block private networks | ⚙️ |
| ✗ 0 / 138 K B | * | Reserved Not assigned by IANA | * | * | * | * | * | | Block bogon networks | ⚙️ |
| ☑️ 0 / 326 K B | IPv4 TCP | * | * | WAN net | 22 (SSH) | * | none | | | 📌 🗑️ 🔄 |

les deux règles qui nous bloques

[Add](#) [Add](#) [Delete](#) [Save](#) [Separator](#)


Maintenant on va essayer d'accéder à notre serveur PfSense à partir de l'extérieur en utilisant notre adresse publique.

Tout d'abord :

- 1- Il faut accéder à la boîte internet et ouvrir le port 22 en créant une redirection de port

| Service | Adresse IP du serveur | Protocole | Ports externes | Ports internes | Activer la règle |
|---------|-----------------------|-----------|----------------|----------------|-------------------------------------|
| SSH | 192.168.1.250 | TCP/UDP | 22 * 22 | 22 * 22 | <input checked="" type="checkbox"/> |

- 2- Ensuite il faut déterminer notre adresse publique soit à partir de la boîte ou un site internet <http://www.whatismyip.com>

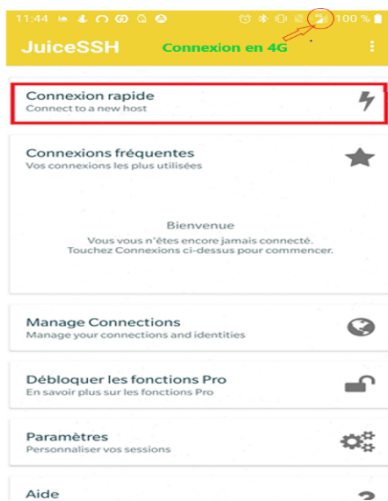
- 3- Après sur notre smartphone on télécharge un client ssh sur  google store **Juicessh**



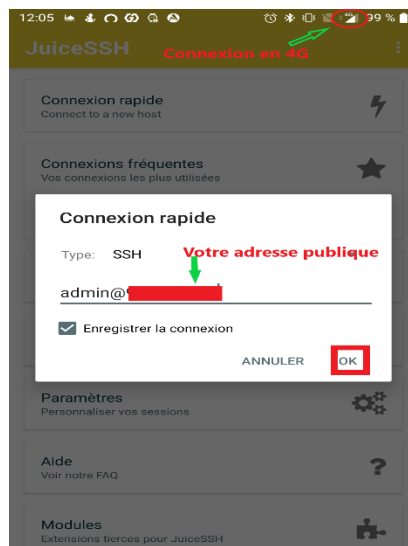
JuiceSSH - SSH Client

- 4- Sur notre smartphone il faut qu'on se mette en 4G et non en wifi car il ne faut pas oublier que PfSense bloque les connexions provenant d'adresse IP en dehors de son périmètre.
- 5- On ouvre l'application et on commence à établir notre connexion ssh

On sélectionne connexion rapide



ssh admin@ adresse publique

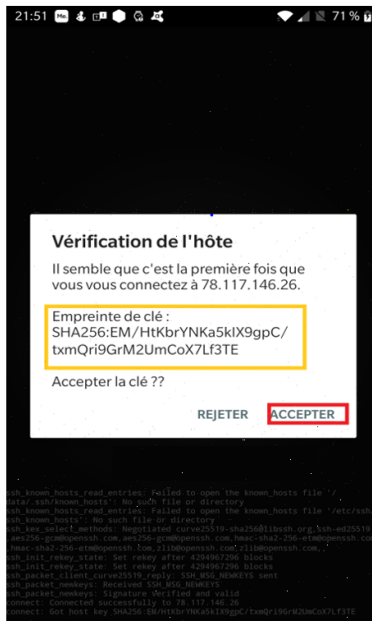


Le serveur nous envoie l'empreinte de sa clé publique

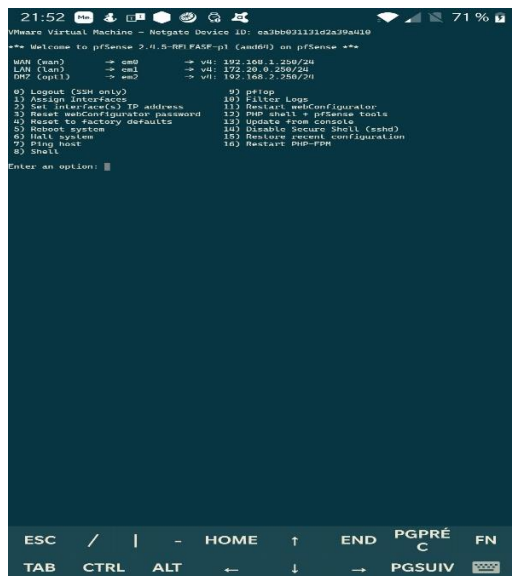
On constate que c'est la même que celle qu'on a calculé

Sur le serveur

EM/HtKbrYNKa5kIX9gpC/txmQri9GrM2UmCoX7Lf3TE rentre le mot de passe admin



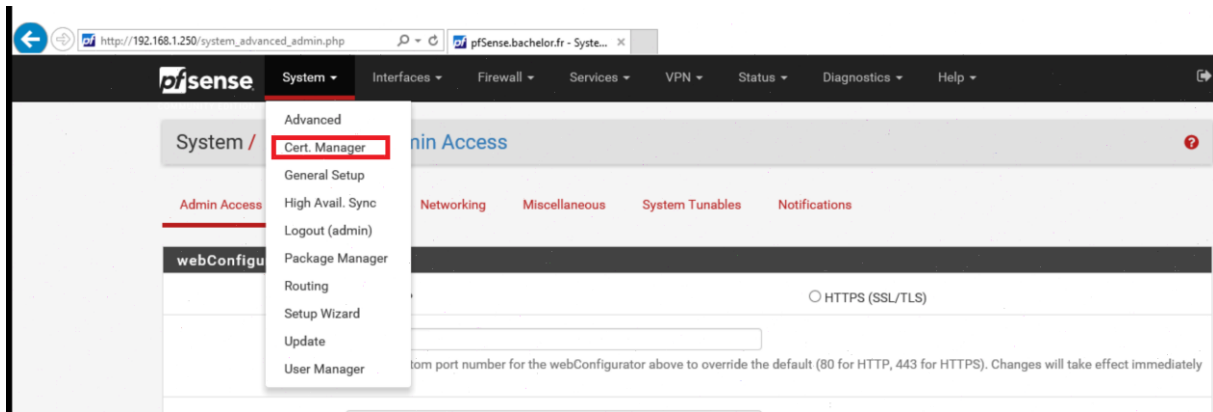
Après on tombe sur notre console PfSense



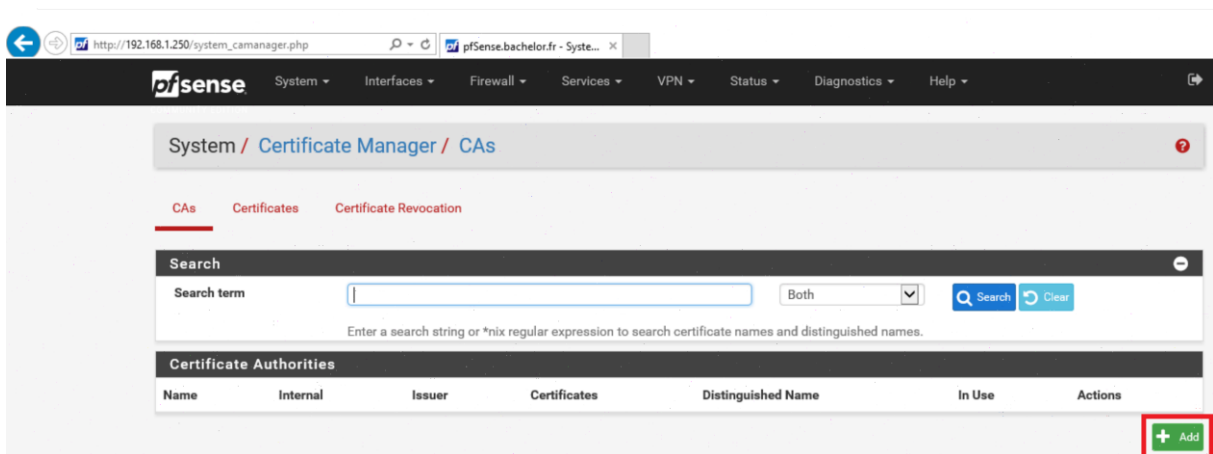
D- Sécurisez L'interface web par https

1- Créer une autorité de certification interne

On va dans le menu **système + CertManager**



On commence à créer une autorité de certification interne



On remplit les champs suivants

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Certificate Manager / CAs / Edit

CA's Certificates Certificate Revocation

Create / Edit CA

Descriptive name

Method

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.

Internal Certificate Authority

Key type

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
The digest method used when the CA is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Lifetime (days)

Common Name

The following certificate authority subject components are optional and may be left blank.

Country Code

State or Province

City

Organization

Organizational Unit

Une fois qu'on enregistre nos paramètres notre autorité de certification apparaît, on appuie sur le crayon pour éditer notre CA

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

System / Certificate Manager / CAs

CA Certificates Certificate Revocation

Search

Search term Both

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 |
|---------------------------------|-------------------------------------|-------------|--------------|--|--------------------------|---------|
| Autorité de certification Sitka | <input checked="" type="checkbox"/> | self-signed | 0 | ST=IDF, OU=SK, O=sitka, L=Paris, CN=internal-ca-sitka, C=FR Valid From: Sat, 27 Nov 2021 21:31:04 +0100 Valid Until: Tue, 25 Nov 2031 21:31:04 +0100 | <input type="checkbox"/> | |

On affiche notre certificat et la clé publique qui lui est associé

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

System / Certificate Manager / CAs / Edit

CA Certificates Certificate Revocation

Create / Edit CA

Descriptive name

Method

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.

Existing Certificate Authority

Certificate data

```
-----BEGIN CERTIFICATE-----
MIIEIDCCAwIqAwIBAgIIPmg7cGMSa8swDQYJKoZIhvcNAQELBQAwZD
EalMBgGA1UE
AxIMRab150ZXJ1YWwtY2EtY210a2ExCzAJBgNVBAYTAkZSMQwwCgYDVQ
QIEwNjREYx
Paste a certificate in X.509 PEM format here.
```

Certificate Private Key (optional)

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBAwggSjAgEAAoIBAQC70e
kVixgQcd/7
FiH4jAa0qAii45sMX5P9T56INa7J2Qd88szCh2CUBvggG9V9VX2T8r
h1ebXA+BwH
Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).
```

Next Certificate Serial
Enter a decimal number to be used as a sequential serial number for the next certificate to be signed by this CA.

2- Générer un certificat web

Maintenant on va créer notre certificat web délivrer par la CA **autorité de certification sitka** qu'on a mis en place dans l'étape précédente il suffit de cliquer sur add et remplir les champs nécessaires

The screenshot shows the pfSense web interface for the Certificate Manager. The breadcrumb navigation is 'System / Certificate Manager / Certificates'. The 'Certificates' tab is highlighted with a red box. Below the search bar, there is a table with the following data:

| Name | Issuer | Distinguished Name | In Use | Actions |
|--|-------------|--|--------|---------|
| webConfigurator default (6001f6f281597) Server Certificate CA: No Server: Yes | self-signed | O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-6001f6f281597 Valid From: Fri, 15 Jan 2021 21:11:30 +0100 Valid Until: Thu, 17 Feb 2022 21:11:30 +0100 | | |

The '+ Add/Sign' button at the bottom right is highlighted with a red box.

ci-dessous les champs remplie pour créer notre certificat

CA's Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create an internal Certificate ▾

Descriptive name Certificat SSL pour le serveur web Heimdall

Internal Certificate

Certificate authority Autorité de certification Sitka ▾

Key type RSA ▾

2048 ▾

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 sha256 ▾

The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Lifetime (days) 3650

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.

Common Name heimdall.sitka.local

The following certificate subject components are optional and may be left blank.

Country Code FR ▾

State or Province IDF

City Paris

Organization sitka

Organizational Unit SK

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.

Alternative Names

| Type | Value | Action |
|------------------|----------------------|--------|
| FQDN or Hostname | heimdall.sitka.local | Delete |
| FQDN or Hostname | pfsense.sitka.local | Delete |
| IP address | 172.20.0.250 | Delete |
| IP address | 192.168.1.250 | Delete |
| IP address | 192.168.2.250 | Delete |
| URI | www.heimdall.local | Delete |

Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add + Add

Save

Une fois qu'on enregistre notre certificat apparait

System / Certificate Manager / Certificates

Created internal certificate Certificat SSL pour le serveur web Heimdall

CA's 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 |
|--|---------------------------------|--|--------|---------|
| webConfigurator default (61a2591ac0fff) Server Certificate CA: No Server: Yes | self-signed | O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-61a2591ac0fff ⓘ Valid From: Sat, 27 Nov 2021 17:13:14 +0100 Valid Until: Fri, 30 Dec 2022 17:13:14 +0100 | | |
| Certificat SSL pour le serveur web Heimdall Server Certificate CA: No Server: Yes | Autorité de certification Sitka | ST=IDF, OU=SK, O=sitka, L=Paris, CN=heimdall.sitka.local, C=FR ⓘ Valid From: Sat, 27 Nov 2021 22:21:01 +0100 Valid Until: Tue, 25 Nov 2031 22:21:01 +0100 | | |

+ Add/Sign

3- Injecter le certificat web dans mon serveur PfSense

Maintenant on va injecter notre certificat dans notre serveur web PfSense, donc on va dans **système + Avanced**

- On sélectionne notre certificat créé
- On laisse le port par défaut
- On laisse 2 en nombre de connexion simultanée c'est-à-dire 2 personnes max peuvent se connecter sur l'interface web PfSense
- On refuse la connexion en http
- On refuse que le navigateur enregistre les données de connexion

Admin Access Firewall & NAT Networking Miscellaneous System Tunables Notifications

webConfigurator

Protocol HTTP **HTTPS (SSL/TLS)**

SSL/TLS Certificate **Certificat SSL pour le serveur web Heimdall**
Certificates known to be incompatible with use for HTTPS are not included in this list.

TCP port
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.

Max Processes
Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.

WebGUI redirect **Disable webConfigurator redirect rule**
When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.

HSTS **Disable HTTP Strict Transport Security**
When this is unchecked, Strict-Transport-Security HTTPS response header is sent by the webConfigurator to the browser. This will force the browser to use only HTTPS for future requests to the firewall FQDN. Check this box to disable HSTS. (NOTE: Browser-specific steps are required for disabling to take effect when the browser already visited the FQDN while HSTS was enabled.)

OCSP Must-Staple **Force OCSP Stapling in nginx**
When this is checked, OCSP Stapling is forced on in nginx. Remember to upload your certificate as a full chain, not just the certificate, or this option will be ignored by nginx.

WebGUI Login Autocomplete **Enable webConfigurator login autocomplete**
When this is checked, login credentials for the webConfigurator may be saved by the browser. While convenient, some security standards require this to be disabled. Check this box to enable autocomplete on the login form so that browsers will prompt to save credentials (NOTE: Some browsers do not respect this option).

Après on sauvegarde notre navigateur va démarrer automatiquement
On se connecte sur l'interface <https://172.20.0.250>

Heimdall.sitka.local - Status: Dashi

Non sécurisé | <https://172.20.0.250>

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Status / Dashboard

System Information

| | |
|---------|---|
| Name | Heimdall.sitka.local |
| User | admin@172.20.0.14 (Local Database) |
| System | VMware Virtual Machine Netgate Device ID: 74a1573f04e3a4d71064 |
| BIOS | Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020 |
| Version | 2.5.2-RELEASE (amd64) built on Fri Jul 02 15:33:00 EDT 2021 FreeBSD 12.2-STABLE |

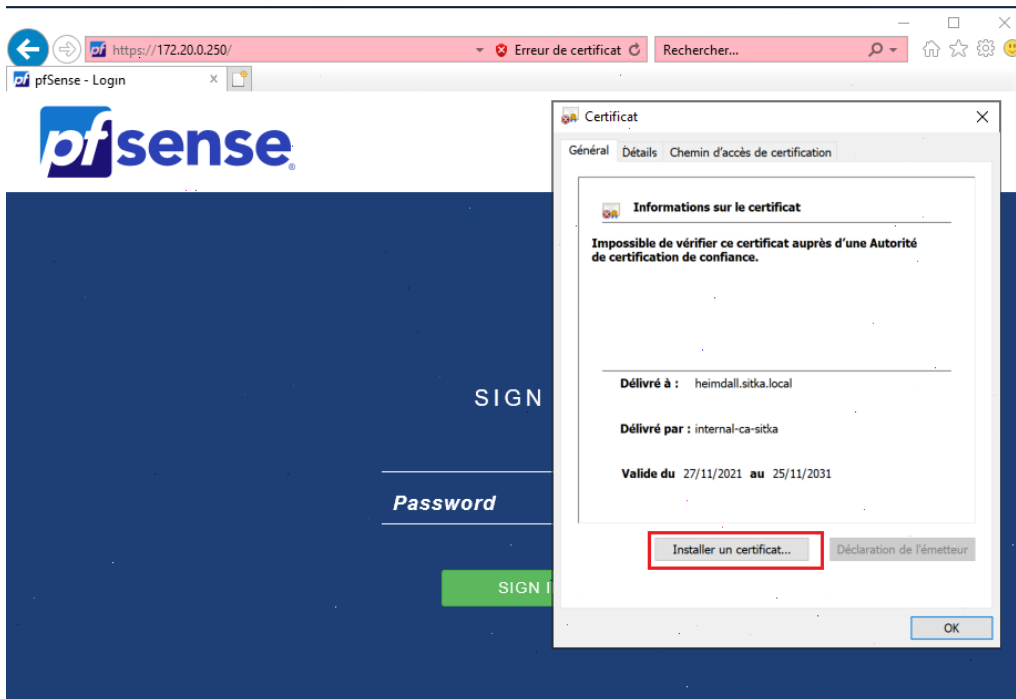
Netgate Services And Support

Contract type: Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

Le certificat représente des erreurs car notre autorité de certification n'est pas de confiance donc il faut l'intégrer dans le magasin des autorités de certification de confiance en installant le certificat de l'autorité racine



Protection de la connexion

The image shows the 'Login Protection' configuration page. The following settings are highlighted with red boxes:

- Threshold:** 8
- Blocktime:** 180
- Detection time:** 259200

The page also includes a 'Whitelist' section with an 'Add address' button and a '128' limit indicator. A note states: 'Addresses added to the whitelist will bypass login protection.'