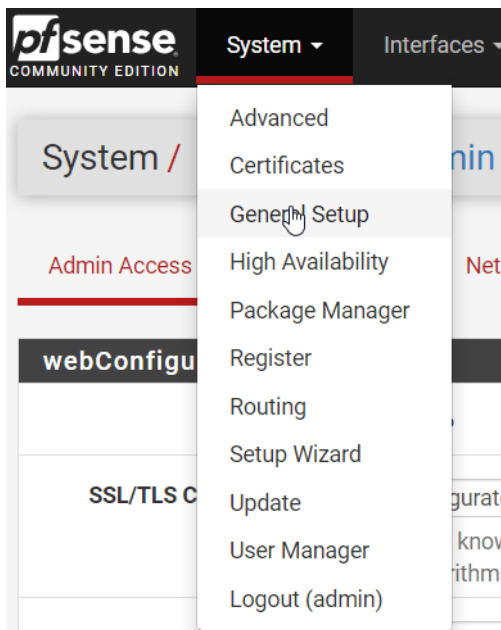


Création autorité de certification -PFSENSE

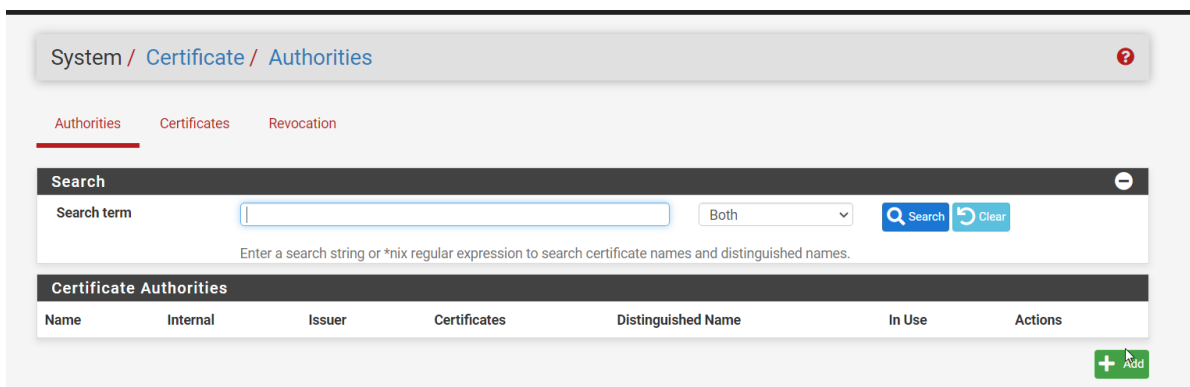
Prérequis :

- Avoir un routeur pfSense installé.

Se rendre dans **System>Certificates>Authorities**.



Cliquer sur **+Add**



Renseigner :

- Descriptive name
- State or Province
- City
- Organization
- Organizational Unit

Cliquer sur **Save**.

Descriptive name

PRT-autorite-certification

State or Province

vaulcuse

City

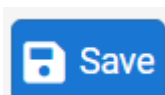
pertuis

Organization





nextech

Organizational Unit

informatique



Votre Autorité de Certification est maintenant créée.

Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
PRT-autorite-certification	✓	self-signed	0	ST=vaulcuse, OU=informatique, O=nextech, L=pertuis, CN=internal-ca Valid From: Wed, 14 Feb 2024 08:16:31 +0000 Valid Until: Sat, 11 Feb 2034 08:16:31 +0000		  

FIN.

Création de certificat serveur

Nous allons créer un certificat pour le serveur que l'on souhaite.

Cela permettra d'obtenir un chiffrement.

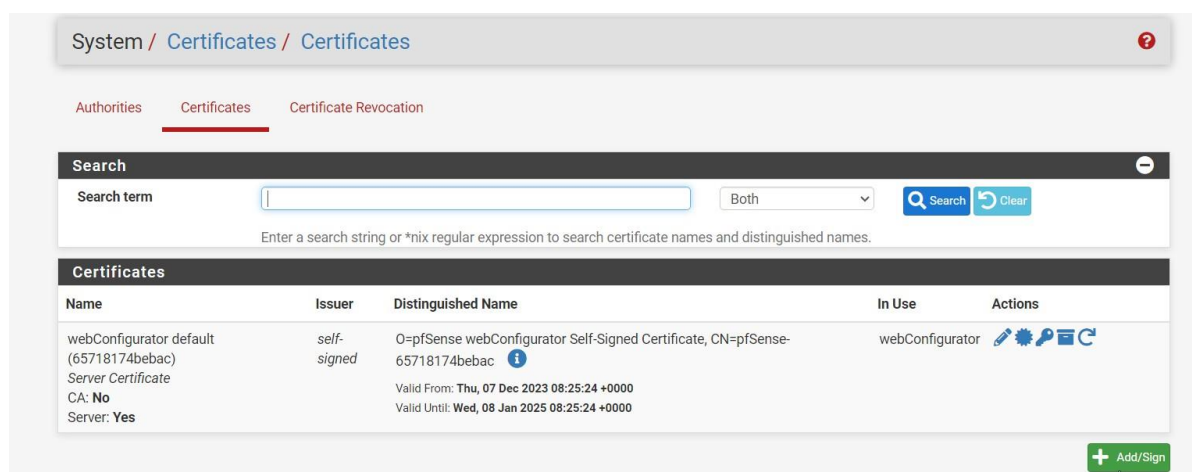
Prérequis :

- Avoir un routeur pfSense
- Avoir créée une autorité de certification

Se rendre dans **System>Certificates>Certificates**



Cliquer sur **+ Add/Sign**.



Renseigner les champs :

- Descriptive name (une description)
- Common Name (l'adresse IP du serveur pour lequel on émet le certificat)
- Certificat type (« Server Certificate» si vous émettez pour un serveur)
- Alternative Names (le nom DNS du serveur)

Descriptive name

Common Name

Certificate Type

Alternative Names
Type Value

On clique sur **Save**.



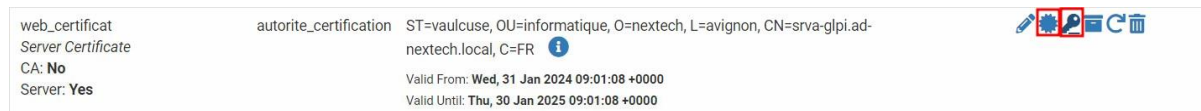
FIN.

Déploiement du certificat serveur sur un serveur web (Debian, Apache)


Prérequis :


- Avoir un routeur pfSense
- Avoir créer une autorité de certification
- Avoir créer un certificat serveur
- Être root

Récupérer le certificat serveur et la clé privé sur Pfsense.



Vous avez deux fichiers.

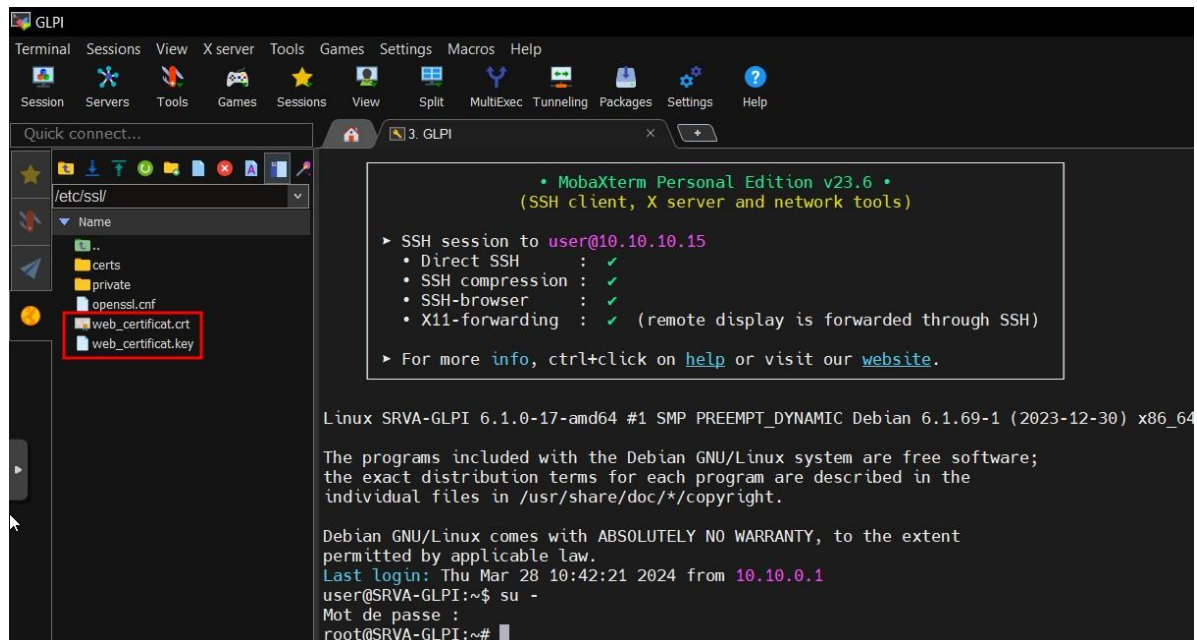
 web_certificat.key

 web_certificat (1).crt

Transférer les documents via SFTP sur votre serveur (avec MobaXTerm) dans le dossier **/tmp/**

Déplacer les dans le répertoire **/etc/ssl/**

```
mv /tmp/web_certificat.crt /etc/ssl/
```



Vérifier qu'ils y sont bien.

```
root@SRVA-GLPI:/etc/ssl# ls
certs  openssl.cnf  private  web_certificat.crt  web_certificat.key
root@SRVA-GLPI:/etc/ssl#
```

Exécuter la commande suivante, afin d'activer le chiffrement.

```
a2enmod ssl
```

Modifier maintenant le Virtualhost **/etc/apache2/sites-available/*.conf**

```
root@SRVA-GLPI:/etc/apache2/sites-available# ls
000-default.conf  ad-nextech.local.conf  default-ssl.conf
root@SRVA-GLPI:/etc/apache2/sites-available# nano ad-nextech.local.conf
```

Rediriger le trafic HTTP vers HTTPS et ajouter les lignes SSL.

```
<VirtualHost *:80>
    ServerName srva-glpi.ad-nextech.local
    Redirect permanent / https://srva-glpi.ad-nextech.local
</VirtualHost>

<VirtualHost *:443>
    ServerName srva-glpi.ad-nextech.local
    DocumentRoot /var/www/glpi/public

    SSLEngine on
    SSLCertificateFile /etc/ssl/web_certificat.crt
    SSLCertificateKeyFile /etc/ssl/web_certificat.key

    <Directory /var/www/glpi/public>
        Require all granted

        RewriteEngine On

        RewriteCond %{REQUEST_FILENAME} !-f
        RewriteRule ^(.*)$ index.php [QSA,L]
    </Directory>

    <FilesMatch \.php$>
        SetHandler "proxy:unix:/run/php/php8.2-fpm.sock|fcgi://localhost/"
    </FilesMatch>
</VirtualHost>
```

Redirection HTTP vers HTTPS

Ajout SSL et certificats

Redémarrer les services apache

```
sudo systemctl restart apache2
```

FIN.

Ajout du certificat de l'Autorité de Certification sur une machine Windows 10

Prérequis :

- Avoir un routeur pfSense.
- Avoir créée une autorité de certification.

Si après avoir émis un certificat serveur, vous disposez de cette erreur lors de l'accès au serveur, c'est que votre machine cliente ne dispose pas de certificat de l'autorité de certification qui a émis le certificat serveur.

Il va donc falloir déployer le certificat de l'autorité de certification sur le PC client.



Votre connexion n'est pas privée

Des individus malveillants tentent peut-être de subtiliser vos informations personnelles sur le site **10.20.0.254** (mots de passe, messages ou numéros de carte de crédit, par exemple).

[En savoir plus](#)

NET::ERR_CERT_AUTHORITY_INVALID



Pour bénéficier du niveau de sécurité le plus élevé de Chrome, [activez la protection renforcée](#)

Paramètres avancés

Revenir en lieu sûr

Pour cela, se rendre sous System>Certificate>Authorities.

Télécharger le certificat de l'autorité de certification en cliquant sur ce logo.



System / Certificate / Authorities

Authorities

Certificates

Revocation

Search

Search term





Both

Search

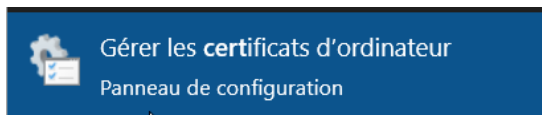
Clear

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

Certificate Authorities

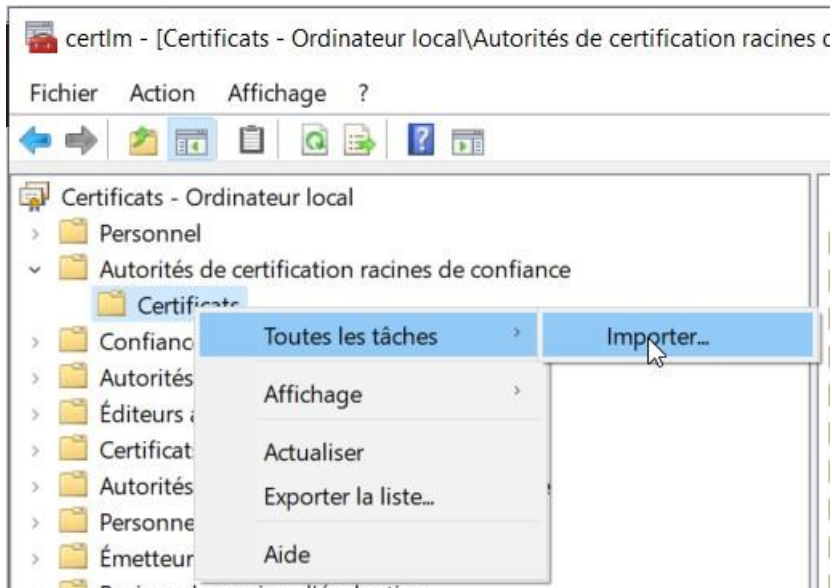
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
PRT-autorite-certification	✓	self-signed	1	ST=vaulcuse, OU=informatique, O=nextech, L=pertuis, CN=internal-ca Valid From: Wed, 14 Feb 2024 08:16:31 +0000 Valid Until: Sat, 11 Feb 2034 08:16:31 +0000		   

Ouvrir « Gérer les certificats d'ordinateur » sur votre machine Windows.

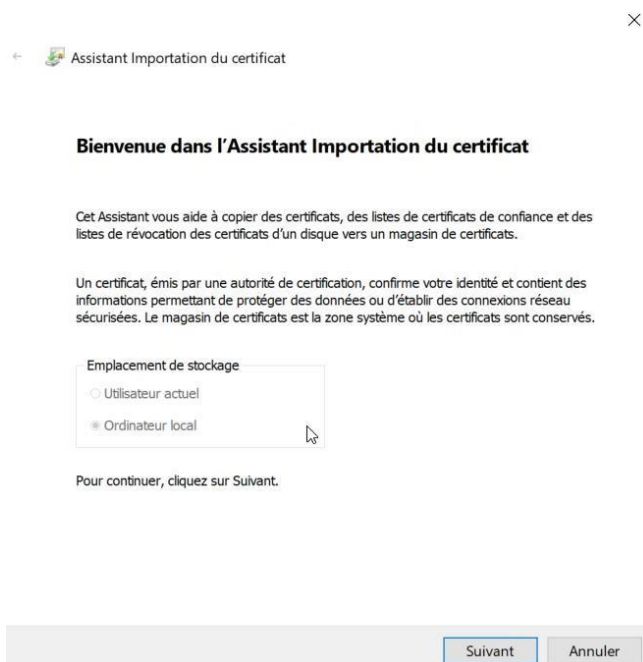


Dans la console se rendre sous Certificats – Ordinateur local > Autorités de certification racines de confiance>Certificats.

Effectuer un clic droit sur le dossier et sélectionner « Toutes les tâches>Importer »



Cliquer sur Suivant.



Cliquer sur « Parcourir »

← Assistant Importation du certificat

Fichier à importer

Spécifiez le fichier à importer.

Nom du fichier :

Parcourir...

Remarque : plusieurs certificats peuvent être stockés dans un même fichier aux formats suivants :

Échange d'informations personnelles- PKCS #12 (.PFX,.P12)

Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.P7B)

Magasin de certificats sérialisés Microsoft (.SST)

Sélectionner votre certificat télécharger au préalable.

▼ Aujourd'hui (1)

PRT-autorite-certification

▼ Plus tôt dans la semaine (1)

Cliquer sur Suivant.

← Assistant Importation du certificat

Magasin de certificats

Les magasins de certificats sont des zones système où les certificats sont conservés.

Windows peut sélectionner automatiquement un magasin de certificats, ou vous pouvez spécifier un emplacement pour le certificat.

☐ Sélectionner automatiquement le magasin de certificats en fonction du type de certificat

☒ Placer tous les certificats dans le magasin suivant

Magasin de certificats :

Autorités de certification racines de confiance

Parcourir...

Suivant

Annuler

Vous pouvez « Terminer ».



← Assistant Importation du certificat

Fin de l'Assistant Importation du certificat

Le certificat sera importé après avoir cliqué sur Terminer.

Vous avez spécifié les paramètres suivants :

Magasin de certificats sélectionné par l'utilisateur	Autorités de certification racines de co
Contenu	Certificat
Nom du fichier	C:\Users\user\Downloads\PRT-autori

Terminer

Annuler

FIN.

GPO distribution de certificat

Prérequis :

- Avoir un routeur pfSense.
- Avoir créée une autorité de certification.

Ouvrir la console de « Gestion des stratégies de groupe »

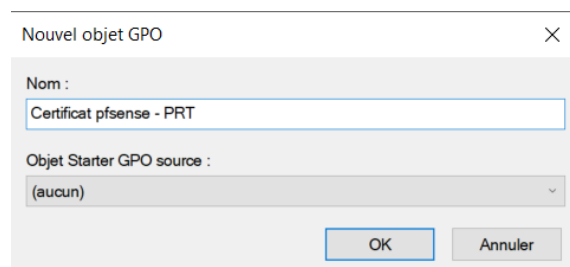
Applications

Gestion des stratégies de groupe

Créer un objet GPO dans votre domaine.



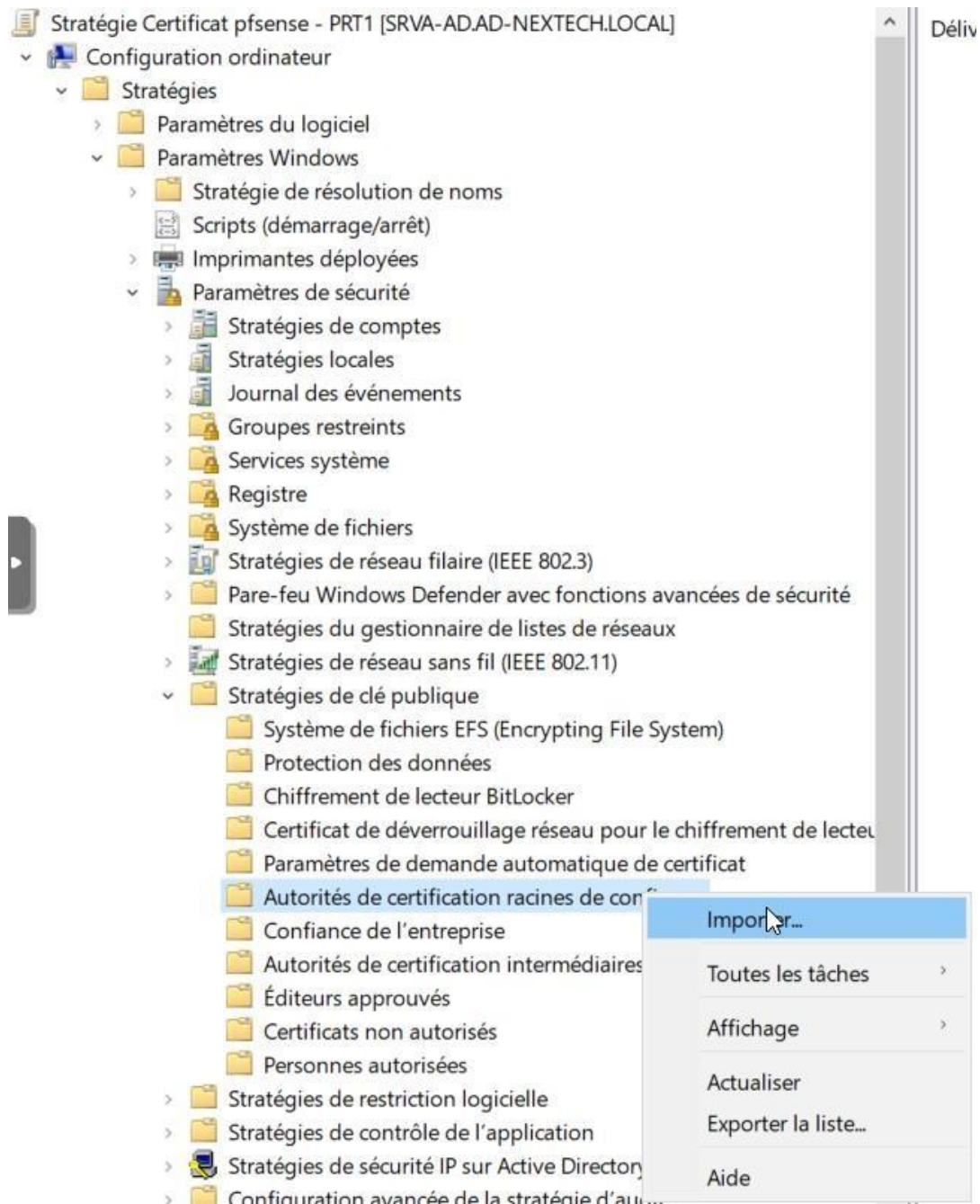
Le nommer.



Effectuer un clic droit sur la GPO nouvellement créée et **modifier** là.



Importer votre certificat sous **Configuration ordinateur>Stratégies>Paramètres Windows>Paramètres de sécurité>Stratégies de clé publique>Autorités de certification racines de confiance**.



Cliquer sur **Suivant**.

←  Assistant Importation du certificat

Bienvenue dans l'Assistant Importation du certificat

Cet Assistant vous aide à copier des certificats, des listes de certificats de confiance et des listes de révocation des certificats d'un disque vers un magasin de certificats.

Un certificat, émis par une autorité de certification, confirme votre identité et contient des informations permettant de protéger des données ou d'établir des connexions réseau sécurisées. Le magasin de certificats est la zone système où les certificats sont conservés.

Emplacement de stockage

- ☐ Utilisateur actuel
- ☒ Ordinateur local

Pour continuer, cliquez sur Suivant.

Suivant

Annuler

Cliquer sur **Parcourir**.

×

←  Assistant Importation du certificat

Fichier à importer

Spécifiez le fichier à importer.

Nom du fichier :

C:\partage\Informatique\PRT-autorite-certification.crt

Parcourir...

Remarque : plusieurs certificats peuvent être stockés dans un même fichier aux formats suivants :

Échange d'informations personnelles- PKCS #12 (.PFX,.P12)

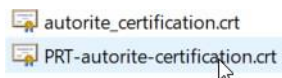
Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.P7B)

Magasin de certificats sérialisés Microsoft (.SST)

Suivant

Annuler

Sélectionner votre certificat de votre autorité de certification.



Cliquer sur **Suivant**



Magasin de certificats

Les magasins de certificats sont des zones système où les certificats sont conservés.

Windows peut sélectionner automatiquement un magasin de certificats, ou vous pouvez spécifier un emplacement pour le certificat.

☐ Sélectionner automatiquement le magasin de certificats en fonction du type de certificat

☒ Placer tous les certificats dans le magasin suivant

Magasin de certificats :

Autorités de certification racines de confiance

Parcourir...

Suivant

Annuler

Cliquer sur **Terminer**.

← Assistant Importation du certificat

Fin de l'Assistant Importation du certificat

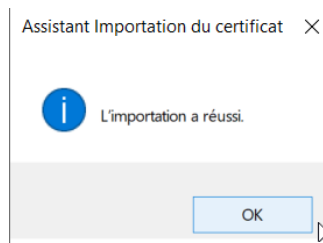
Le certificat sera importé après avoir cliqué sur Terminer.

Vous avez spécifié les paramètres suivants :

Magasin de certificats sélectionné par l'utilisateur	Autorités de certification racines de co
Contenu	Certificat
Nom du fichier	C:\partage\Informatique\PRT-autorite

Terminer	Annuler
----------	---------

L'importation a réussi.



Ouvrir un cmd et faire `gpupdate /force`

Administrateur : Invite de commandes - gpupdate /force

```
Microsoft Windows [version 10.0.17763.2114]
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>gpupdate /force
Mise à jour de la stratégie...
```

FIN.

Installation de certificats racines sur Debian

Prérequis :

- Avoir un routeur pfSense.
- Avoir créée une autorité de certification.

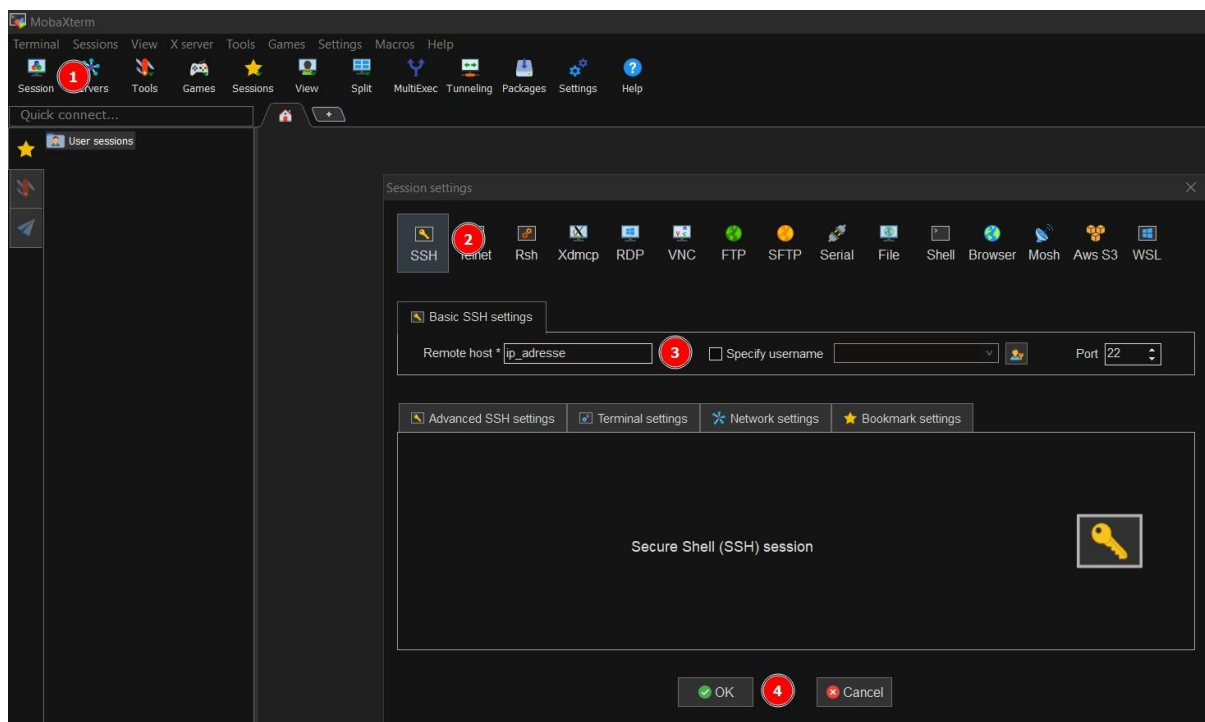
Sur Debian, les certificats racines sont installés dans le répertoire `/etc/ssl/certs`.

L'installation de certificats se fait avec la commande `update-ca-certificates`.

Les certificats (avec l'extension **.crt**) doivent être déposés dans le répertoire `/usr/local/share/ca-certificates`.

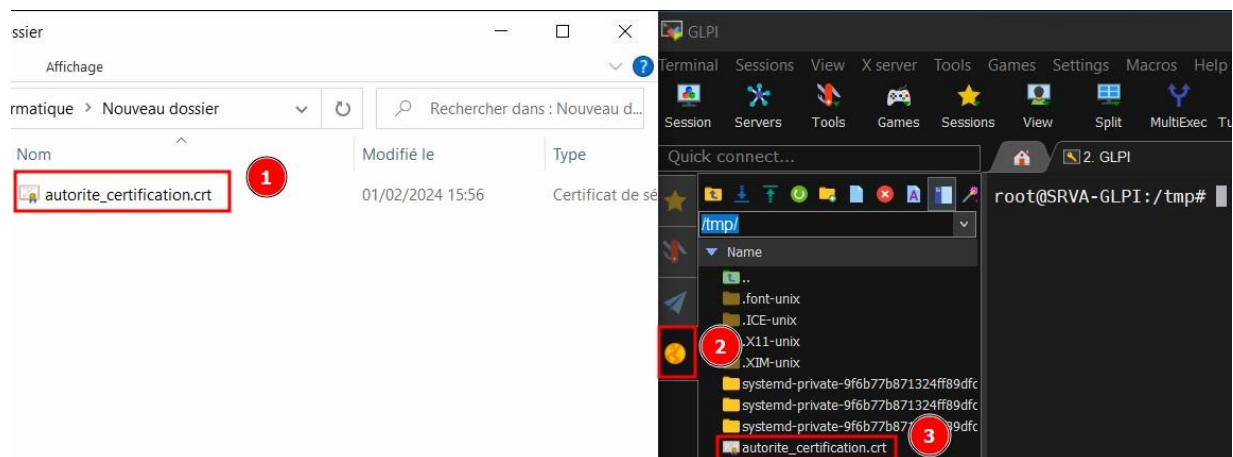
Se connecter en SSH sur la machine Debian via MobaXterm.

Cliquer sur **Session** puis **SSH**. Renseigné **l'adresse IP** de la machine Debian et cliquer sur **OK**.



Transférer le certificat via SFTP dans dossier /tmp.

Pour cela, faire glisser le certificat depuis votre hôte (ici Windows 10) vers votre Debian.



Déplacer le certificats vers /usr/local/share/ca-certificates.

```
mv /tmp/autorite_certification.crt /usr/local/share/ca-certificates/
```

Mettre à jour les certificats.

```
update-ca-certificates
```

FIN.

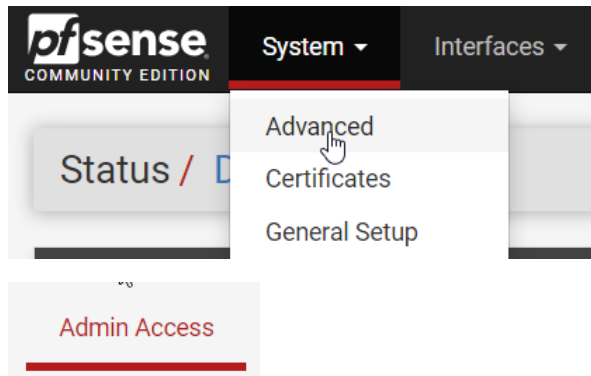
Mettre PfSense en HTTPS

L'objectif est d'accéder à pfSense via https.

Prérequis :

- Avoir un routeur pfSense
- Avoir créer une autorité de certification
- Avoir créer un certificat serveur pour PfSense

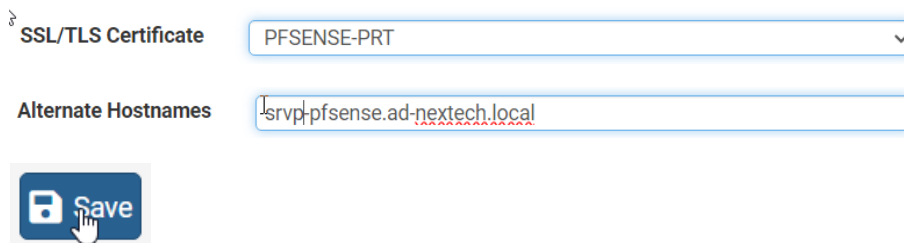
Se rendre dans System>Advanced>Admin access.



Renseigner les champs :

- SSL/TLS Certificate
- Alternate Hostnames

Cliquer sur **Save**.

The image shows the 'Admin Access' configuration page in pfSense. It has two main fields: 'SSL/TLS Certificate' and 'Alternate Hostnames'. The 'SSL/TLS Certificate' field is a dropdown menu with 'PFSense-PRT' selected. The 'Alternate Hostnames' field is a text input containing 'srvp-pfsense.ad-nextech.local'. Below these fields is a blue 'Save' button with a floppy disk icon.

Nous pouvons voir que cela a fonctionné. PfSense va recharger la page web.

The changes have been applied successfully.
One moment...redirecting to https://10.20.0.254/system_advanced_admin.php in 20 seconds.

Pour aller plus loin il va falloir déposer dans le magasin de certificat de notre machine client (ici Windows 10) le certificat de l'autorité de certification.

2 méthodes sont possibles :

- Soit manuellement.
- Soit par GPO si vous disposez d'un domaine.

FIN.