RAPPORT AP-2

CREATION D'UN AUTHORITE DE CERTIFICATION LOCAL ET DEPLOIEMENT DES CERTIFICATS

ETHAN BAMBARA—DASYLVA

BTS SIO 2ÈME ANNÉE 2025-2026

ethan.bambaradasylva@ecole-isitech.fr

Table des matières

CONTEXTE D’INFRASTRUCTURE

Au sein du Domaine BAMBARA.local, les utilisateurs et les administrateurs du domaine doivent accéder à des services web comme GLPI pour signaler des problèmes et créer des tickets, et PFsense afin d’administrer les règles de pare-feu.
Le problème est qu’actuellement, les utilisateurs y accèdent en HTTP et non en HTTPS, ce qui représente une faille de sécurité car les communications vers les différents services ne sont pas chiffrées. Un attaquant peut ainsi effectuer des attaques de type man-in-the-middle et intercepter les communications.
C’est dans ce contexte que nous allons créer une autorité de certification locale au sein de notre domaine, afin de pouvoir créer et signer des certificats SSL/TLS et ainsi accéder aux services en HTTPS.
Avant de passer à l’installation, voici plus de contexte sur notre infrastructure :
Le Domaine BAMBARA.local est hébergé sur l’hyperviseur ESXI-201. Le domaine comprend deux sites différents :

Le site principal, nommé Lyon,
Un site secondaire, nommé Saint-Laurent-du-Maroni (SLT en abrégé).

Chaque site dispose de son propre contrôleur de domaine dédié :

DC-1 pour Lyon,
DC-2 pour Saint-Laurent.

Ces contrôleurs de domaine assurent également les services DNS pour le domaine. Les deux sites ont chacun leur propre réseau, réparti dans différents VLAN, et sont reliés par un VPN IPsec.
Sur les deux sites, on retrouve un pare-feu PFsense sur lequel est configuré le VPN IPsec et les règles des différents réseaux des sites. Les pare-feux ont chacun une IP WAN. Les réseaux sont accessibles directement grâce au commutateur SW11.

TOPOLOGIE RESEAU

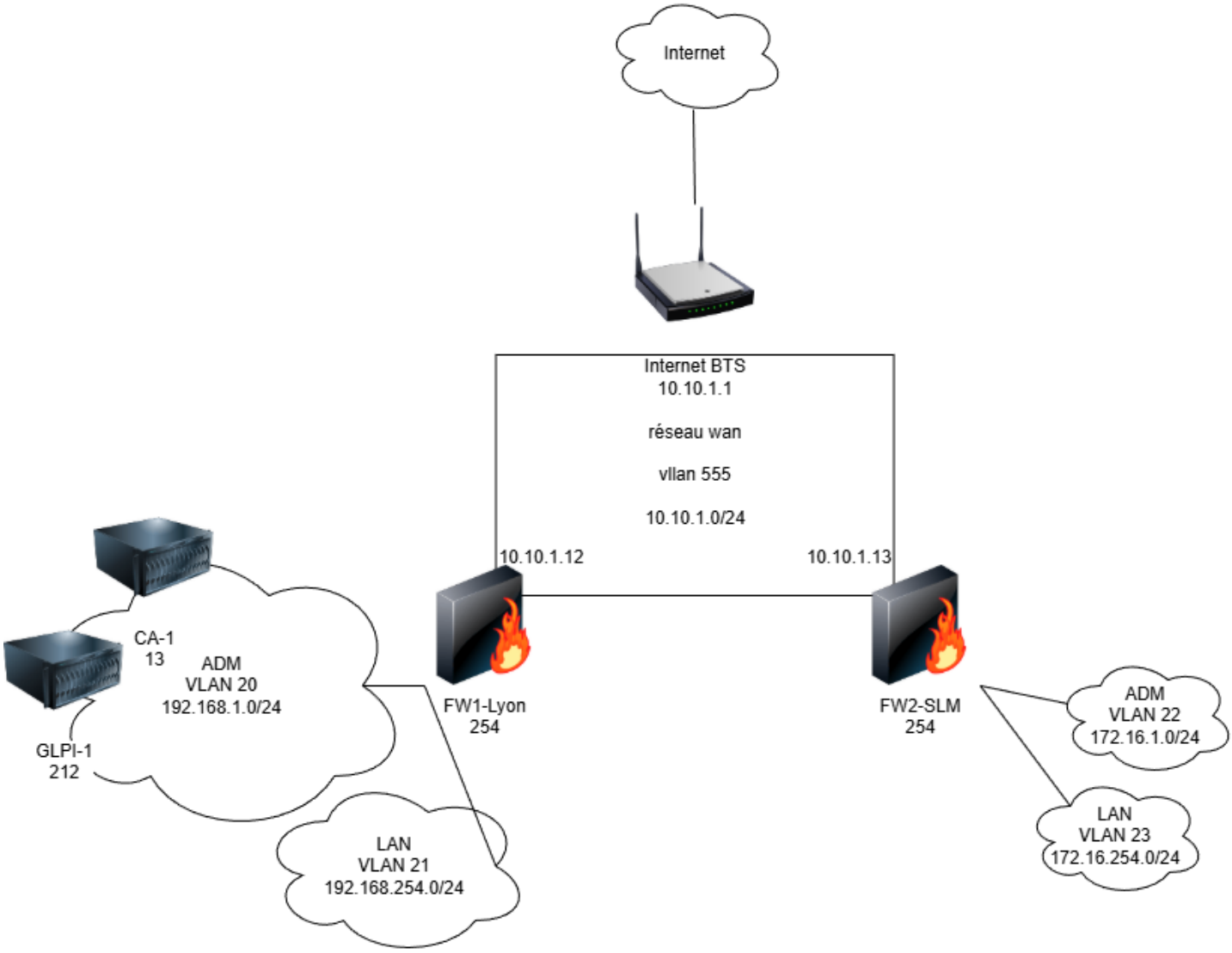


Tableau d'adressage		
N°vlan	Services	Adressage IP
555	Réseau WAN	10.10.1.0/24
20	Réseau ADM LYON	192.168.1.0/24
21	Réseau User LYON	192.168.254.0/24
22	Réseau ADM SLM	172.16.1.0/24
23	Réseau User SLM	172.16.254.0/24
	FW1-Lyon	10.10.1.12/ .254
	FW2-SLM	10.10.1.13/ .254
	CA-1	192.168.1.13
	GLPI-1	192.168.1.212

CAHIER DES CHARGES

Notre projet doit respecter un certain cahier des charges et répondre à certaines problématiques.
L'autorité de certification doit être créée sur une machine fonctionnant sous Debian 10 (Buster).
Dans ce compte rendu, nous n'allons pas détailler l'installation et la création de la machine.
Notre autorité de certification doit répondre aux erreurs liées aux certificats SSL, telles que net::ERR_CERT_COMMON_NAME_INVALID. De plus, nous devrons avoir la capacité de délivrer des certificats pour plusieurs adresses IP et noms de domaine. Nous devrons également créer des certificats SSL pour PFsense et GLPI, afin de pouvoir y accéder en HTTPS.
Nous devrons aussi veiller au déploiement automatique des certificats pour les utilisateurs de notre domaine. Les certificats que nous allons déployer devront être reconnus par tous les navigateurs courants. Enfin, nous devrons veiller à la sécurité des clés privées.

MOYENS TECHNIQUE

Pour répondre à notre besoin de générer et signer des certificats numériques en interne, nous avons choisi d'utiliser Easy-RSA, un outil open source spécialisé dans la gestion d'infrastructures à clé publique (PKI). Easy-RSA, installé sur une machine Linux dédiée, permet de transformer cette machine en une CA locale capable de créer des paires de clés, de signer des certificats pour les serveurs ou les utilisateurs, et de gérer leur cycle de vie. Son principal avantage réside dans sa simplicité d'utilisation et son automatisation des tâches complexes, tout en offrant un contrôle total sur la chaîne de confiance. Après installation et configuration, Easy-RSA nous permet d'initialiser la PKI, de générer le certificat racine de la CA, puis de créer et signer des certificats pour nos différents besoins internes. Cette solution, bien que limitée à un usage privé, garantit une sécurité optimale et une flexibilité adaptée à nos environnements de test et de développement.
Afin d'assurer la reconnaissance et la confiance automatique des certificats émis par notre CA locale sur l'ensemble des postes et serveurs de notre domaine, nous allons procéder à leur déploiement centralisé via notre contrôleur de domaine et les stratégies de groupe. Cette méthode permet d'automatiser l'installation du certificat racine de notre CA dans le magasin de confiance de tous les ordinateurs membres

RAPPORT TECHNIQUE

INSTALLATION & CONFIGURATION D'EASY RSA

Dans un premier Temps nous allons Installez l'outil EASY-RSA sur notre machine Debian.

Pour ce faire exécutez la commande suivante :

Apt install easy-rsa

Ensuite créez un dossier easy-rsa dans votre dossier utilisateur.

Mkdir ~/easy-rsa

Ensuite nous allons faire un lien symbolique vers les package de easy-rsa que nous avons installé tout à l'heure.

Ln -s /usr/share/easy-rsa/* ~/easy-rsa/

Une fois ces étapes réalisées nous pouvons enfin initialiser le dossier pki dans le dossier easy-rsa
Pour ce faire, faites les commandes suivantes :

Cd ~/easy-rsa
. / easyrsa init-pki

Après la second commande ce message s'affichera.

Output
init-pki complete; you may now create a CA or requests.
Your newly created PKI dir is: /home/votreutilisateur /easy-rsa/pki

Une fois le pki initialisé nous devrons créer le certificat racine de l'autorité de certification.
Dans un premier temps nous allons éditer les valeurs dans le fichier vars.

Nano pki/vars

Une fois dans le fichier il y aura plusieurs valeur à changer :

set_var EASYRSA_REQ_COUNTRY Renseigner le code de votre pays
set_var EASYRSA_REQ_PROVINCE Renseignez votre région
set_var EASYRSA_REQ_CITY Renseignez votre ville
set_var EASYRSA_REQ_ORG Renseignez le nom de votre entreprise
set_var EASYRSA_REQ_EMAIL Renseignez votre mail
set_var EASYRSA_REQ_OU Renseignez votre section d'entreprise
set_var EASYRSA_ALGO "ec" laisser les valeur par défaut
set_var EASYRSA_DIGEST "sha512" laisser les valeur par défaut
set_var EASYRSA_KDC_REALM Resnseignez le nom de votre domaine local active directory.
set_var EASYRSA_REQ_CN Renseignez le FQDN de votre serveur

```
set_var EASYRSA_REQ_COUNTRY     "FR"
set_var EASYRSA_REQ_PROVINCE    "Rhone"
set_var EASYRSA_REQ_CITY        "Lyon"
set_var EASYRSA_REQ_ORG "BAMBARA.local"
set_var EASYRSA_REQ_EMAIL       "ethan.bambaradasylva@ecole-isitech.fr"
set_var EASYRSA_REQ_OU          "BAMBARA:local"

# If you want to generate KDC certificates, you need to set the realm here.
set_var EASYRSA_KDC_REALM      "BAMBARA.local"

set_var EASYRSA_REQ_CN          "CA-1.bambara.local"
```

Une fois les valeurs modifier nous allons effectuer la commande suivante pour créer notre CA :

./easyrsa build-ca

L'or de la création plusieurs questions vous serons posez répondez y :

Output
. . .
Enter New CA Key Passphrase: renseignez un mot de passe
Re-Enter New CA Key Passphrase: renseignez un mot de passe
. . .
Common Name (eg: your user, host, or server name) [Easy-RSA CA]: renseignez le FQDN de votre hôte.

Après avoir répondu aux question ce message devrais apparaître.

CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/home/votreutilisateur /easy-rsa/pki/ca.crt

Cela nous confirme la création du certificat racine de notre CA.

DEPLOIEMENT DU CERTIFICAT RACINE VIA GPO

Une fois que nous avons généré le certificat racine de notre autorité de certifications il faut l'importer sur les postes du domaine.

Pour ce faire nous allons le déployer sur les postes par GPO.

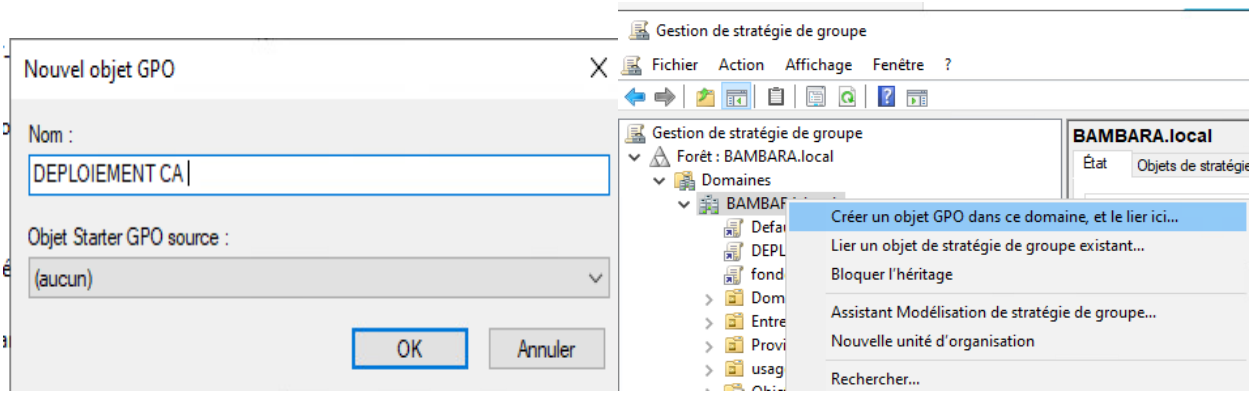
Nous allons d'abord copier le certificat sur notre AD.

Pour ce faire nous exécutons la commande suivante sur notre AD :
Scp userdevotreCA@ipdevotreCA:/chemin/vers/votre/certificat c:\destination\local\désirez

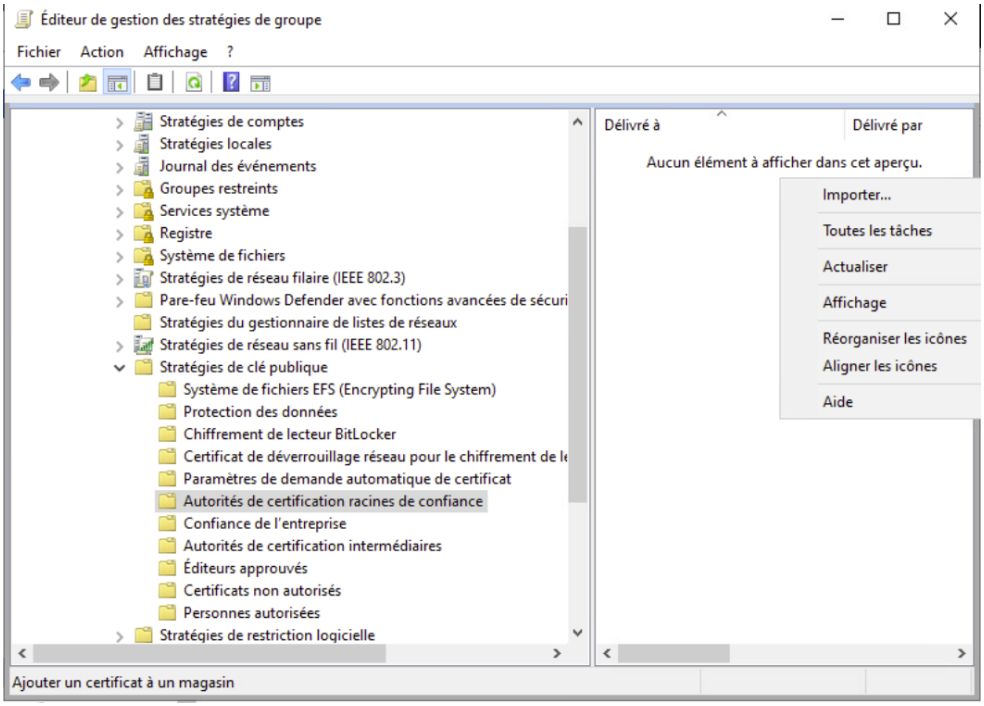
```
PS C:\Users\Administrateur> scp root@192.168.1.13:/ca.crt c:\
root@192.168.1.13's password:
Permission denied, please try again.
root@192.168.1.13's password:
Permission denied, please try again.
root@192.168.1.13's password:
ca.crt                                                    100%  778     0.8KB/s   00:00
```

Vous retrouverez votre certificat dans destination que vous avez indiquez.
Ensuite il faudra mettre le certificat dans le dossier partager que vous allez utiliser dans votre GPO.

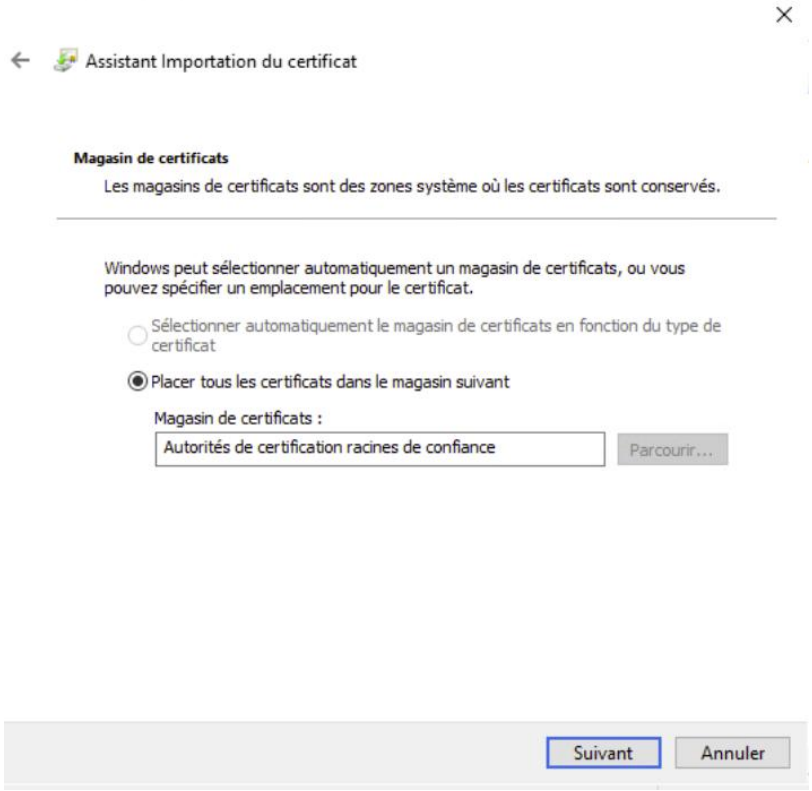
Ensuite ouvrez la console de «Gestion de stratégie de groupe » puis créer une nouvel GPO en lui donnant un nom descriptif. Pour ma part je vais la créer á la racine de mon domaine pour cibler tous les postes de mon domaine.



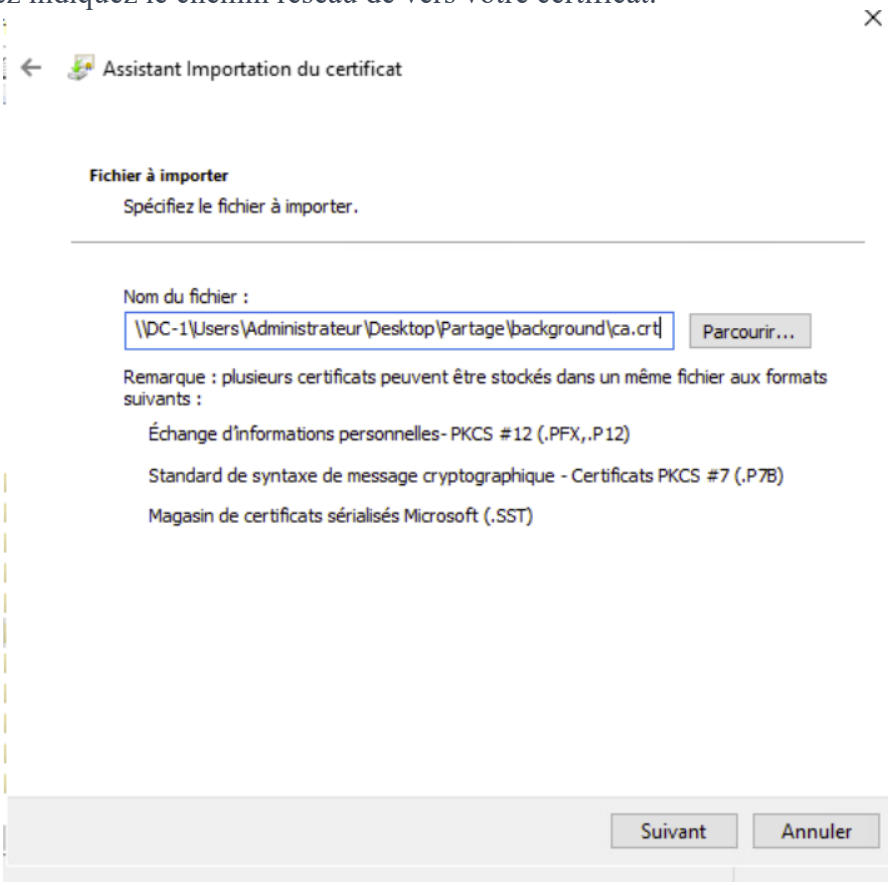
Dans votre GPO allez dans gestion de l'ordinateur > sécurité windows > stratégie de clé publique > autorités de certification racines de confiance puis faites importer.



Vous serrez accueille par un assistant, ici il faudra bien cocher la case « placer tous les certificats dans le magasins suivant » puis indiquez « Autorités de certification racines de confiance ». Puis cliquez sur suivant



Ensuite ici vous devrez indiquez le chemin réseau de vers votre certificat.



Ensuite cliquez sur suivant et cliquez sur terminer.
Une fois la GPO faite nous pouvons faire un GPUdapte /force sur notre DC pour appliquer la GPO.

Une fois que nous avons déployer le certificat de notre autorité de certification il ne nous reste plus qu'à générer les certificats pour les services auxquels nous souhaitons accédez.

Dans notre cas nous souhaitons accédez á l'interface web de PFsense et à un serveur GLPI

Une fois que vous voyez le cadenas, cela veut dire que votre poste reconnait le certificat. Donc notre autorité de certification est fonctionnelle.

Création et signatures de certificat pour des services externes

Maintenant que nous avons créé et déployer notre certificat racine nous pouvons signer nos certificats.

Je vais vous montrer comment les signer depuis un système linux sous Debian utilisant Nginx et sur PFsense.

CREATION & SIGNATURE DU CERTIFICAT POUR NGINX

Sur Debian installez Openssl avec la commande suivante :

apt install openssl

Une fois Openssl installé, nous allons créer une clé privée pour notre futur certificat.
Pour ce faire faites la commande suivante :

Openssl genrsa -out nomsouhaité.key

Ensuite nous allons créer une demande de signature de certificat avec la commande suivante :

Openssl req -new -key votrecléprivé.key -out nom-souhaité.req

Après avoir fait la commande, vous allez devoir répondre à plusieurs questions :

Country Name : renseignez votre pays
State or Province : renseignez votre région
Locality Name : renseignez votre ville
Organization Name : renseignez le nom de votre entreprise
Organizational unit Name : renseignez le nom de votre section
Commom Name : renseignez le FQDN de votre serveur
Email Address : renseignez votre mail

```
root@Support:/etc/nginx/ssl# openssl genrsa -out support-bambara.key
root@Support:/etc/nginx/ssl# openssl req -new -key support-bambara.key -out support-bambara.req
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Rhone
Locality Name (eg, city) []:Lyon
Organization Name (eg, company) [Internet Widgits Pty Ltd]:BAMBARA.local
Organizational Unit Name (eg, section) []:BAMBARA.local
Common Name (e.g. server FQDN or YOUR name) []:support.bambara.local
Email Address []:ethan.bambaradasylva@ecole-isitech.fr

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Après avoir répondus au question votre demande devrais être créer, maintenant nous devons la signé par notre autorité de certification.
Pour ce faire nous allons transférez la demande sur notre Autorité de certification avec la commande suivante.

Scp chemin/vers/votre/demande root@ipdevotreCA /chemins/que/vous/souhaité

```
root@Support:/etc/nginx/ssl# scp support-bambara.req root@192.168.1.13:/
root@192.168.1.13's password:
support-bambara.req                                           100% 1106     2.1MB/s   00:00
```

Une fois que vous avez transférez la demande, sur votre CA depuis le dossier easyrsa, exécuté les commandes suivantes :
./easyrsa import-req /chemin/vers/votre/demande nom-souhaité
./easyrsa sign-req server nom-de-votre-demande

Il vous sera demandé de vérifier la requête, tapez yes et appuyez sur entrée pour confirmer.

Après ça votre certificat devra être créé dans le dossier suivant

~/easy-rsa/pki/issued/

Pour importer le certificat signé sur notre serveur linux nous allons réutiliser la commande scp en changeant la source et la destination de cette dernière :

```
root@Support:/etc/nginx/ssl# scp root@192.168.1.13:/home/administrateur@BAMBARA.local/easy-rsa/pki/iss
ued/support-bambara.crt /etc/nginx/ssl
```

Installer le certificat sur Nginx.
Maintenant pour que notre serveur web puissent utiliser notre certificat sur Nginx il suffit de modifier les champs suivants dans le dossier /etc/nginx/site-enabled/nom-de/votre/site :

Listen 443 ssl ;
Listen [::] : 443 ;

Ssl_certificate /chemin/vers/votre/certificat
Ssl_certificate_key /chemin/vers/votre/clé/privée

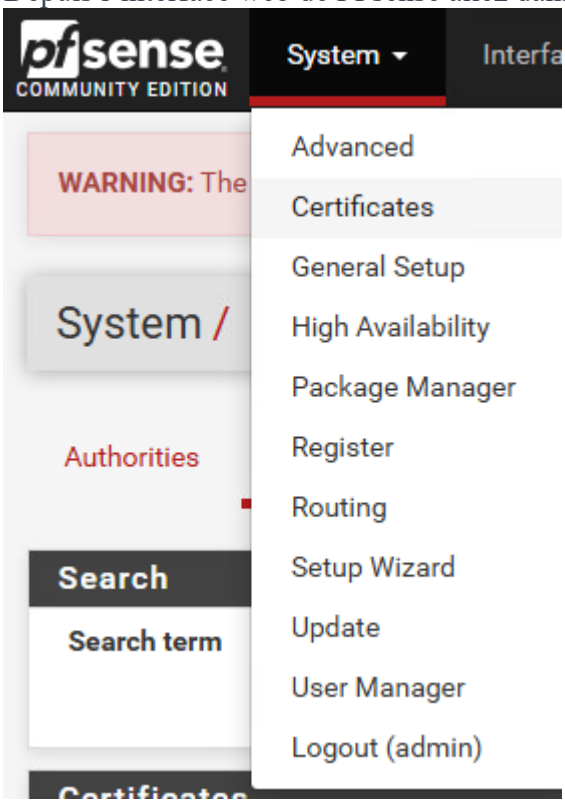
```
server {
    # listen 80;
     #listen [::]:80;

        listen 443 ssl;
        listen [::]:443 ssl;

        ssl_certificate /etc/nginx/ssl/support-bambara.crt;
         ssl_certificate_key /etc/nginx/ssl/support-bambara.key;
```

Sauvegardez le fichier puis redémarré les services de Nginx avec la commande suivante :

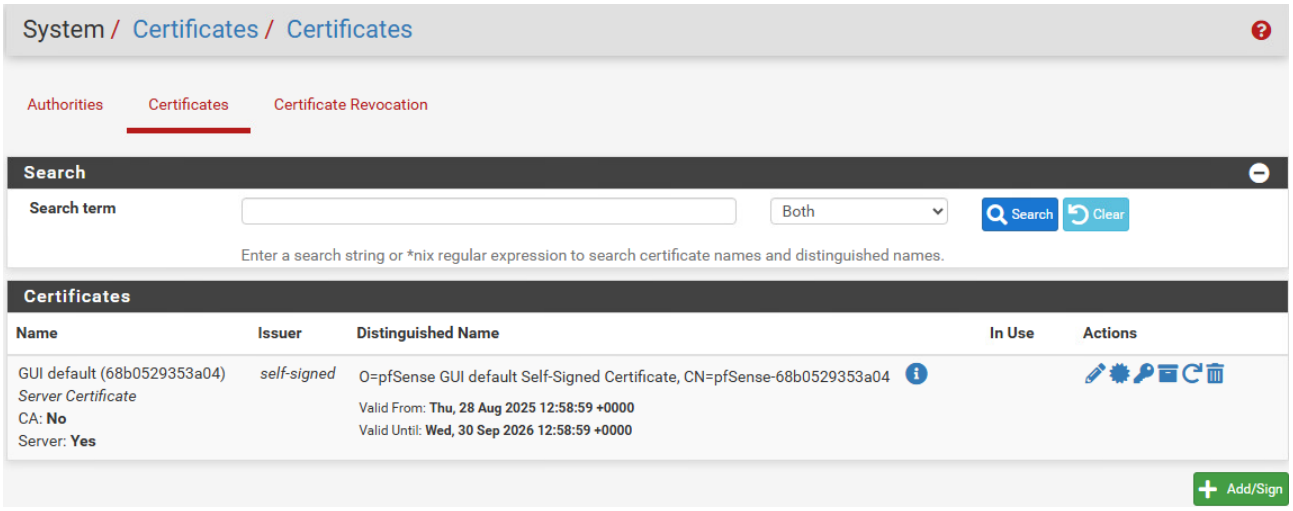
Systemctl restart nginx
Normalement votre site devrait être accessible en https avec votre certificat.

CREATION & SIGNATURE DU CERTIFICAT POUR PFSENSE

Depuis l'interface web de PFsense allez dans l'onglet certificates.



Puis dans la section certificates cliquez sur le bouton Add/



Vous arriverez sur cette page, ici vous devrez remplir plusieur champ :

-Method : selectionnez “Create a certificate Siging Request”

-Descriptive Name : mettez un nom dscriptif

-Key Type : laisser sur RSA et 2048

-Comon Name : mettez le nom complet que vous allez utiliser pour vous connectez au firewall

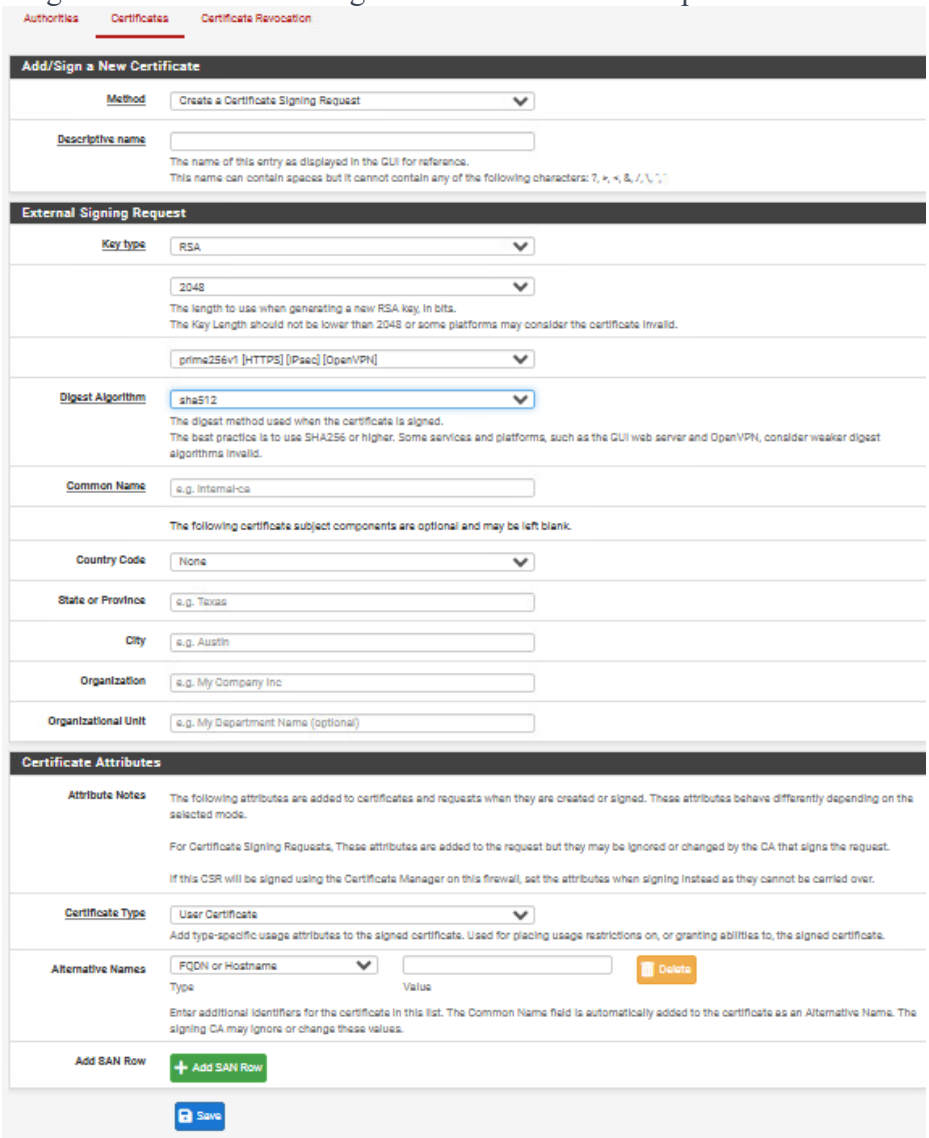
-Country Name : choisisez votre pays

-State or Province : ici renseignez votre région

-City : renseignez votre ville

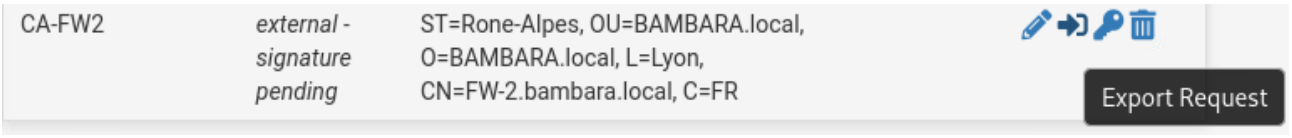
-Organization : renseignez votre entreprise

-Organizatinal Unit : renseignez l’unité de votre entreprise



Une fois les champs remplis, cliquez sur le bouton Save.

Nous venons de créer notre requête de signature, maintenant nous devons la télécharger sur notre autorité de certification pour ce faire cliquez sur le bouton Export Requeté, cela téléchargera la requête dans le dossier téléchargement de votre utilisateur.



Sur votre CA dans votre dossier easy-rsa, nous allons faire la commande suivante pour importer la requête :

. /easyrsa import-req /chemin/vers/votre/requête Nom-de-votre-requête

```
root@CA-1:/home/administrateur@BAMBARA.local/easy-rsa# ./easyrsa import-req /home/administrateur\@BAMB
ARA.local/Téléchargements/CA-FW2.req CA-FW2
* Notice:
Using Easy-RSA configuration from: /home/administrateur@BAMBARA.local/easy-rsa/pki/vars

* Notice:
Using SSL: openssl OpenSSL 3.0.17 1 Jul 2025 (Library: OpenSSL 3.0.17 1 Jul 2025)

* Notice:

The request has been successfully imported with a short name of: CA-FW2
You may now use this name to perform signing operations on this request.
```

Ensuite nous exécutons cette commande pour signer la requête :

./easyrsa sign-req server nom-de-votre-requête.

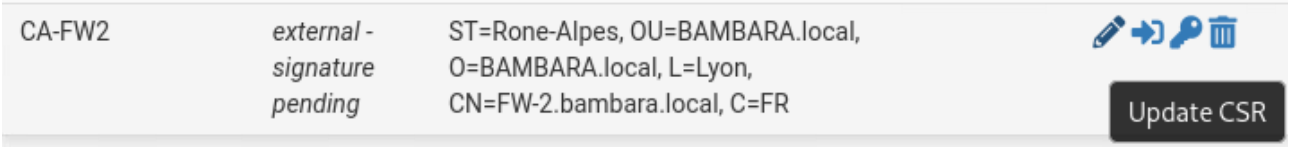
```
root@CA-1:/home/administrateur@BAMBARA.local/easy-rsa# ./easyrsa sign-req server CA-FW2
* Notice:
Using Easy-RSA configuration from: /home/administrateur@BAMBARA.local/easy-rsa/pki/vars

* Notice:
Using SSL: openssl OpenSSL 3.0.17 1 Jul 2025 (Library: OpenSSL 3.0.17 1 Jul 2025)


You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 825 days:

subject=
    commonName                = FW-2.bambara.local
    countryName               = FR
    stateOrProvinceName       = Rone-Alpes
    localityName              = Lyon
    organizationName          = BAMBARA.local
    organizationalUnitName    = BAMBARA.local

X509v3 Subject Alternative Name:
    DNS:FW-2.bambara.local


Type the word 'yes' to continue, or any other input to abort.
  Confirm request details: yes
```

Ici vous devrez écrire « yes » pour continuer.

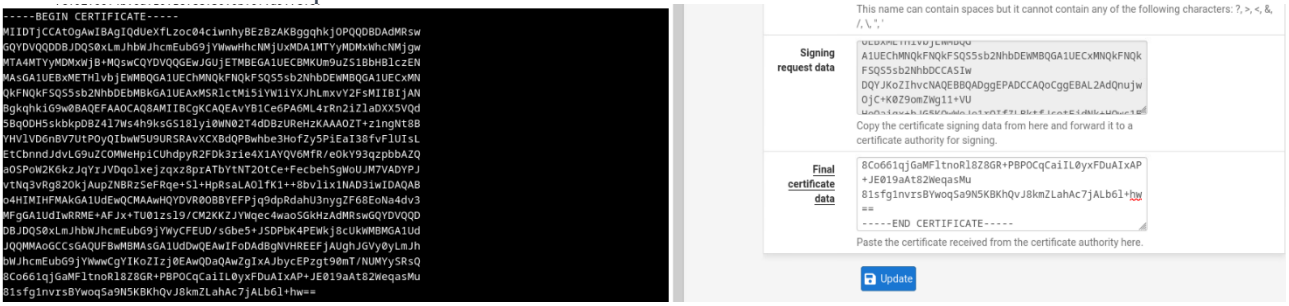
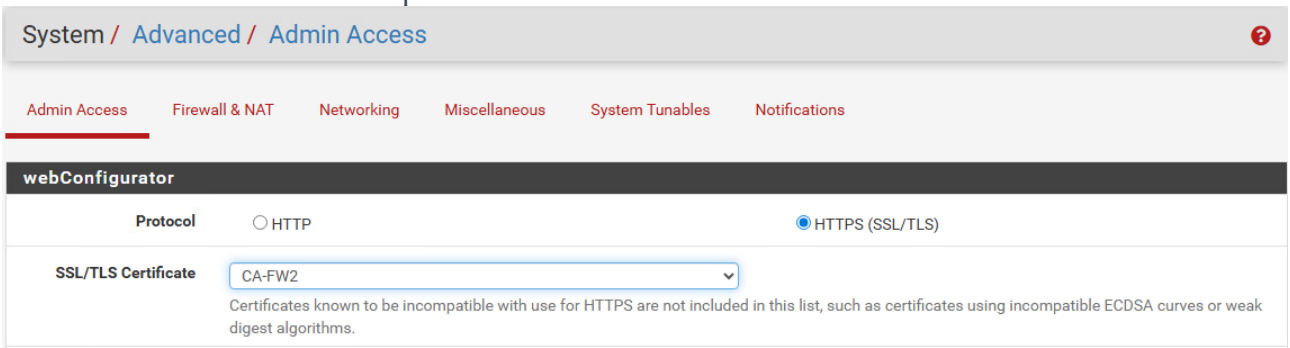
Ensuite ici il faudra renseigner le mot de passe que vous avez définis pour la clé priver de votre CA.
Ensuite votre certificat sera signé.

```
Using configuration from /home/administrateur@BAMBARA.local/easy-rsa/pki/80088cd1/temp.dad9c49f
Enter pass phrase for /home/administrateur@BAMBARA.local/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName            :PRINTABLE:'FW-2.bambara.local'
countryName           :PRINTABLE:'FR'
stateOrProvinceName   :PRINTABLE:'Rone-Alpes'
localityName          :PRINTABLE:'Lyon'
organizationName      :PRINTABLE:'BAMBARA.local'
organizationalUnitName:PRINTABLE:'BAMBARA.local'
Certificate is to be certified until Jan  8 16:20:31 2028 GMT (825 days)

Write out database with 1 new entries
Database updated

* Notice:
Certificate created at: /home/administrateur@BAMBARA.local/easy-rsa/pki/issued/CA-FW2.crt

root@CA-1:/home/administrateur@BAMBARA.local/easy-rsa#
```

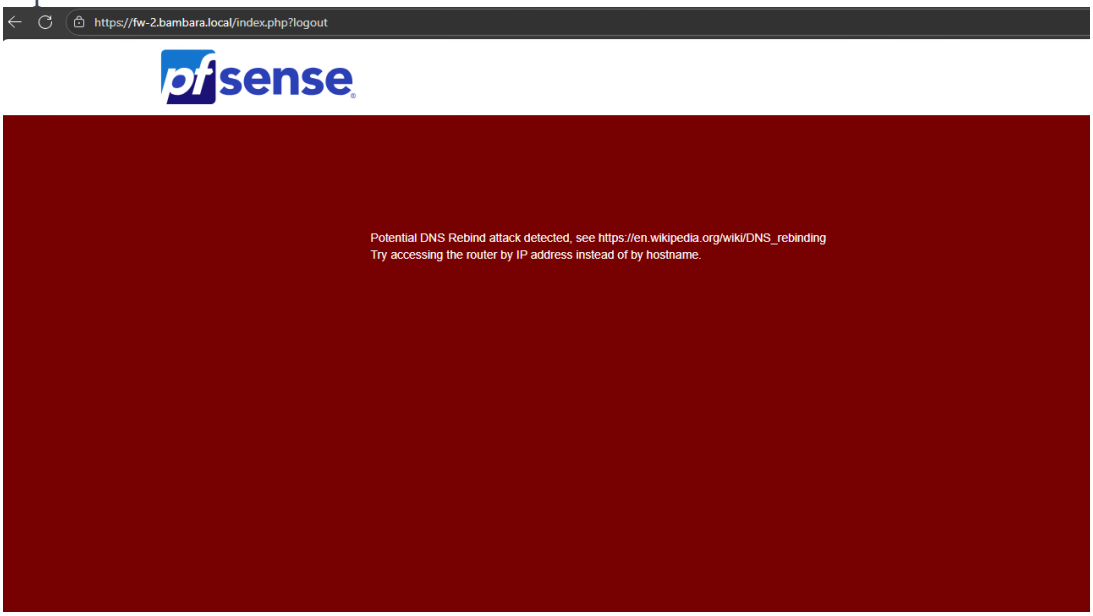
Maintenant retournez sur PFsense puis cliquez sur le bouton « update csr ».



Ici il faudra remplir le champs final certificate data avec les informations du certificat signés.
Copiez les informations de la section « begin certificate » jusqu'à « end certificate » et mettez-les dans champs final certificate. Puis cliquez sur save.


-----BEGIN CERTIFICATE-----
MIIDTjCCAtOgAwIBAgIQdUeXfLzoc04ciwnhyBEzBzAKBggqhkjOPQQDBDAdMRsw
GQYDVQQDDBJDQS0xLmJhbWJhcmEubG9jYWwwHhcNMjUxMDA1MTYyMDMxWhcNMjgw
MTA4MTYyMDMxWjB+MQswCQYDVQQGEwJGUjETMBEGA1UECBMKUm9uZS1BbHBlczEN
MAsGA1UEBxMETHlvbjEWMBQGA1UEChMNQkFNQkFSQS5sb2NhbDEWMBQGA1UECxMN
QkFNQkFSQS5sb2NhbDEbMBkGA1UEAxMSRlctMi5iYW1iYXJhLmxvY2FsMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvYB1Ce6PA6ML4rRn2iZlaDXX5VQd
5BqODH5skbkpDBZ4l7Ws4h9ksGS18lyi0WN02T4dDBzUReHzKAAAOZT+z1ngNt8B
YHVlVDGnBV7UtPOyQIbwW5U9URSRAvXCXBdQPBwhbe3Hof2y5PiEaI38fvFlUIsL
EtCbnndJdvLG9uZCOMWeHpiCUhdpyR2FDk3zie4X1AYQV6MfR/eOkY93qzpbbAZQ
aOSPoW2K6kzJqYrJVDqolxejzqxz8prATbYtNT2OtCe+FecbehSgWoUJM7VADYPJ
vtNq3vRg82OkjAupZNBRzSeFRqe+Sl+HpRsaLAOlfK1++8bvlix1NAD3iwIDAQAB
o4HIMIHFMAkGA1UdEwQCMAAwHQYDVR0OBBYEFPjq9dpRdahU3nygZF68EoNa4dv3
MFgGA1UdIwRRME+AFJx+TU01zsl9/CM2KKZJYWqec4waoSGkHzAdMRswGQYDVQQD
DBJDQS0xLmJhbWJhcmEubG9jYWyCFEUD/sGbe5+JSDPbK4PEWkj8cUkWMBMGA1Ud
JQQMMAoGCCsGAQUFBwMBMAsGA1UdDwQEAwIFoDAdBgNVHREEFjAUghJGVy0yLmJh
bWJhcmEubG9jYWwwCgYIKoZIzj0EAwQDaQAwZgIxAJbycEPzgt90mT/NUMYySRsQ
8Co661qjGaMFltnoRl8Z8GR+PBPOCqCaiIL0yxFDuAIxAP+JE019aAt82WeqasMu
81sfg1nvrsBYwoq5a9N5KBKhQvJ8kmZLahAc7jALb6l+hw==
```

Maintenant pour utiliser le certificat allez dans Advanced > Admin Access, dans le champ ssl/tls certificate choisissez votre certificat et cliquez sur save.




Maintenant essayer d'accéder à PFsense via le nom de domaine que vous avez défini.
```

Si vous vous tomber sur cette page, il faudra activer une options dans PFsense pour autorisé l'accès au firewall depuis cette url.



Dans Advanced > Admin Acess vous pouvez soit cochez la case disable DNS rebind check ou soit renseigner votre url dans Alternative Hostname.