VPN Site-à-site

Configuration du Tunnel OpenVPN

PRESENTATION

Ce document décrit la configuration d'un tunnel OpenVPN Site-à-Site entre les deux pare-feux pfSense du projet, en utilisant le mode SSL/TLS avec une PKI (Infrastructure à Clés Publiques).

Le mode SSL/TLS repose sur une Autorité de Certification (CA) qui signe des certificats pour chaque équipement. Cela apporte le Perfect Forward Secrecy (PFS) : même si une clé de session est compromise, les échanges passés et futurs restent protégés.

PREREQUIS

pfSense A et pfSense B installés et configurés (interfaces WAN/LAN opérationnelles, accès internet vérifié). Se référer à la documentation **DOC-03**.

Rôles des équipements

Équipement	Rôle OpenVPN	Adresse WAN	Adresse LAN
pfSense A	Serveur OpenVPN	172.16.0.10/24	192.168.10.1/24
pfSense B	Client OpenVPN	172.16.0.20/24	192.168.20.1/24

Plan d'adressage du tunnel

Élément	Adresse IP	Rôle
Endpoint tunnel A	10.0.0.1/30	Interface virtuelle VPN — Siège Limoges
Endpoint tunnel B	10.0.0.2/30	Interface virtuelle VPN — Agence Bordeaux
Réseau Site A	192.168.10.0/24	Accessible depuis Site B via le tunnel
Réseau Site B	192.168.20.0/24	Accessible depuis Site A via le tunnel

Vue d'ensemble des étapes

Étape	Action	Réalisée sur
1	Créer l'Autorité de Certification (CA)	pfSense A

2	Créer le certificat Serveur	pfSense A
3	Créer le certificat Client	pfSense A
4	Exporter la CA et le certificat Client	pfSense A
5	Importer la CA et le certificat Client	pfSense B
6	Configurer le serveur OpenVPN	pfSense A
7	Configurer le client OpenVPN	pfSense B
8	Ajouter les règles firewall	pfSense A et B

1. CREATION DE L'AUTORITE DE CERTIFICATION (PFSENSE A)

La CA est la pièce centrale de la PKI. Elle signe les certificats du serveur et du client, garantissant leur authenticité. Elle est créée sur pfSense A et doit ensuite être exportée vers pfSense B pour que celui-ci puisse vérifier les certificats présentés lors de la connexion.

Naviguer vers **System** → **Certificate** → **Authorities** → **Add**.

1.1 PARAMETRES DE LA CA

Champ	Valeur à saisir
Descriptive name	CA VPN SiteASite
Method	Create an internal Certificate Authority
Key type	RSA
Key length	2048 bits
Digest Algorithm	SHA256
Lifetime (days)	365 (1 an)
Common Name	vpn-ca

Country Code	FR
State or Province	Nouvelle-Aquitaine
City	Limoges
Organization	TechConnect

Cliquer sur **Save**. La CA apparaît dans la liste des CAs.

2. CREATION DES CERTIFICATS (PFSENSE A)

Deux certificats sont nécessaires : un certificat Serveur pour pfSense A, et un certificat Client pour pfSense B. Les deux sont créés sur pfSense A et signés par la CA créée à l'étape précédente.

Naviguer vers **System** → **Certificate** → **Certificates** → **Add/Sign**.

2.1 CERTIFICAT SERVEUR (PFSENSE A)

Champ	Valeur à saisir
Method	Create an internal Certificate
Descriptive name	cert-serveur-pfsense-a
Certificate authority	CA_VPN_SiteASite
Key type	RSA
Key length	2048 bits
Digest Algorithm	SHA256
Lifetime (days)	3650
Common Name	pfsense-a-serveur
Certificate Type	Server Certificate

Cliquer sur **Save**.

2.2 CERTIFICAT CLIENT (PFSENSE B)

Cliquer à nouveau sur Add/Sign pour créer le second certificat.

Champ	Valeur à saisir
Method	Create an internal Certificate
Descriptive name	cert-client-pfsense-b
Certificate authority	CA_VPN_SiteASite
Key type	RSA
Key length	2048 bits
Digest Algorithm	SHA256
Lifetime (days)	3650
Common Name	pfsense-b-client
Certificate Type	User Certificate

Cliquer sur **Save**.

✓ Les deux certificats apparaissent maintenant dans la liste **Certificates**, avec la mention **CA_VPN_SiteASite** dans la colonne **Issuer.**

3. EXPORT DES CERTIFICATS DEPUIS PFSENSE A

pfSense B a besoin de deux éléments pour authentifier la connexion : la CA (pour vérifier le certificat présenté par pfSense A) et le certificat Client avec sa clé privée (pour s'identifier auprès de pfSense A).

3.1 EXPORTER LA CA

- Naviguer vers **System** → **Certificate** → **Authorities**.
- Sur la ligne CA_VPN_SiteASite, cliquer sur l'icône **Export CA** (télécharger le certificat).
- Enregistrer le fichier sous le nom : CA_VPN_SiteASite.crt

Exporter uniquement le certificat de la CA (pas la clé privée). La clé privée de la CA reste sur pfSense A et ne doit jamais être partagée.

3.2 EXPORTER LE CERTIFICAT CLIENT

- Naviguer vers **System** → **Certificate** → **Certificates**.
- Sur la ligne **cert-client-pfsense-b**, cliquer sur l'icône **Export Certificate**.
- Enregistrer sous le nom : **cert-client-pfsense-b.crt**
- Cliquer ensuite sur l'icône **Export Key** (clé privée).
- Enregistrer sous le nom : **cert-client-pfsense-b.key**

⚠️ **La clé privée (.key) est confidentielle. Dans un environnement de production, son transfert doit se faire via un canal sécurisé. En laboratoire, un simple copier-coller depuis l'interface web suffit.**

4. IMPORT DES CERTIFICATS SUR PFSENSE B

Les deux fichiers exportés depuis pfSense A doivent être importés sur pfSense B. Cette opération se fait depuis l'interface web de pfSense B (https://192.168.20.1).

4.1 IMPORTER LA CA SUR PFSENSE B

- Naviguer vers **System** → **Certificate** → **Authorities** → **Add**.
- Renseigner les champs suivants :

Champ	Valeur à saisir
Descriptive name	CA_VPN_SiteASite
Method	Import an existing Certificate Authority
Certificate data	Coller le contenu du fichier CA_VPN_SiteASite.crt

Cliquer sur **Save**.

4.2 IMPORTER LE CERTIFICAT CLIENT SUR PFSENSE B

- Naviguer vers **System → Certificate** → **Certificates** → **Add/Sign**.
- Renseigner les champs suivants :

Champ	Valeur à saisir

Method	Import an existing Certificate
Descriptive name	cert-client-pfsense-b
Certificate data	Coller le contenu du fichier cert-client-pfsense-b.crt
Private key data	Coller le contenu du fichier cert-client-pfsense-b.key

Cliquer sur **Save**.

✓ Vérification : dans la liste Certificates de pfSense B, la colonne Issuer doit afficher CA_VPN_SiteASite pour le certificat importé.

5. CONFIGURATION OPENVPN SERVEUR (PFSENSE A)

Depuis l'interface web de pfSense A, naviguer vers **VPN** → **OpenVPN** → **Servers** → **Add**.

5.1 PARAMÈTRES GÉNÉRAUX

Champ	Valeur à saisir
Description	VPN_SiteA_Serveur
Disabled	Décoché (laisser actif)
Server Mode	Peer to Peer (SSL/TLS)
Device mode	tun — Layer 3 Tunnel Mode
Protocol	UDP on IPv4 only
Interface	WAN
Local port	1194

5.2 CONFIGURATION TLS ET CERTIFICATS

Champ	Valeur à saisir

TLS Configuration	Cocher Use a TLS Key → cocher Auto generate
Peer Certificate Authority	CA_VPN_SiteASite
Server certificate	cert-serveur-pfsense-a
DH Parameter Length	2048 bit
ECDH Curve	Use Default
Encryption Algorithm	AES-256-GCM
Auth Digest Algorithm	SHA256
Hardware Crypto	No Hardware Crypto Acceleration

La TLS Key est une couche de sécurité supplémentaire qui protège le handshake TLS lui-même. Elle sera générée automatiquement et devra être copiée sur pfSense B comme la Shared Key dans l'ancienne méthode.

5.3 PARAMÈTRES DU TUNNEL

Champ	Valeur à saisir
IPv4 Tunnel Network	**10.0.0.0/30**
IPv4 Local network(s)	**192.168.10.0/24**
IPv4 Remote network(s)	**192.168.20.0/24**
Concurrent connections	**1**

5.4 PARAMÈTRES AVANCÉS

Champ	Valeur à saisir

Custom options	keepalive 10 60
Verbosity level	3 (recommended)

Cliquer sur **Save**.

5.5 RECUPERATION DE LA TLS KEY

- Retourner dans **VPN** → **OpenVPN** → **Servers** → **icône Edit** (crayon).
- Copier intégralement le bloc de la TLS Key affiché (lignes BEGIN et END comprises).
- Conserver ce texte pour le coller dans pfSense B.

⚠️ La TLS Key doit être strictement identique des deux côtés, tout comme la Shared Key dans l'ancienne méthode.

5.6 RÈGLE FIREWALL WAN

Naviguer vers **Firewall** → **Rules** → **WAN** → **Add** (flèche vers le bas).

Champ	Valeur à saisir
Action	Pass
Interface	WAN
Address Family	IPv4
Protocol	UDP
Source	any
Destination	WAN address
Destination Port	1194
Description	Autoriser tunnel OpenVPN entrant

Cliquer sur **Save** puis **Apply Changes**.

5.7 DESACTIVER LA REGLE RFC 1918 (SPECIFIQUE ENVIRONNEMENT LAB)

Dans un environnement de laboratoire, le réseau WAN utilise une plage d'adresses privées (172.16.0.0/24). Or pfSense bloque par défaut tout trafic provenant d'adresses privées sur l'interface WAN via la règle RFC 1918.

Editer la toute première règle **RFC 1918 networks** et décocher la case tout en bas **Block private networks and loopback addresses .**

⚠️ **Cette règle ne doit être désactivée qu'en environnement de lab. En production avec un vrai WAN public, cette règle doit rester active.**

5.8 RÈGLE FIREWALL INTERFACE OPENVPN

Naviguer vers **Firewall** → **Rules** → **OpenVPN** → **Add**.

Champ	Valeur à saisir
Action	Pass
Interface	OpenVPN
Protocol	any
Source	any
Destination	any
Description	Autoriser trafic inter-sites

Cliquer sur **Save** puis **Apply Changes**.

6. CONFIGURATION OPENVPN CLIENT (PFSENSE B)

Depuis l'interface web de pfSense B (https://192.168.20.1), naviguer vers **VPN** → **OpenVPN** → **Clients** → **Add**.

6.1 PARAMÈTRES GÉNÉRAUX

Champ	Valeur à saisir
Description	VPN_SiteB_Client

Disabled	Décoché (laisser actif)
Server Mode	Peer to Peer (SSL/TLS)
Device mode	tun — Layer 3 Tunnel Mode
Protocol	UDP on IPv4 only
Interface	WAN
Server host or address	172.16.0.10 ← IP WAN de pfSense A
Server port	1194

6.2 CONFIGURATION TLS ET CERTIFICATS

Champ	Valeur à saisir
TLS Configuration	Cocher Use a TLS Key → décocher Auto generate → coller la TLS Key de pfSense A
Peer Certificate Authority	CA_VPN_SiteASite (importée en DOC-VPN-04)
Client certificate	cert-client-pfsense-b (importé en DOC-VPN-04)
Encryption Algorithm	AES-256-GCM
Auth Digest Algorithm	SHA256
Hardware Crypto	No Hardware Crypto Acceleration

⚠️ **L'algorithme de chiffrement et de hachage doit être identique à celui configuré sur pfSense A. Toute différence empêche l'établissement du tunnel.**

6.3 PARAMÈTRES DU TUNNEL

Champ	Valeur à saisir
IPv4 Tunnel Network	10.0.0.0/30
IPv4 Remote network(s)	192.168.10.0/24

Cliquer sur **Save**.

6.4 RÈGLE FIREWALL WAN

Cette fois-ci, il sera juste nécessaire de désactiver la règle **RFC 1918.**

Editer la toute première règle **RFC 1918 networks** et décocher la case tout en bas **Block private networks and loopback addresses .**

6.5 REGLE FIREWALL INTERFACE OPENVPN

Même procédure que sur pfSense A. Naviguer vers **Firewall** → **Rules** → **OpenVPN** → **Add**.

Champ	Valeur à saisir
Action	Pass
Interface	OpenVPN
Protocol	any
Source	any
Destination	any
Description	Autoriser trafic inter-sites

Cliquer sur **Save** puis **Apply Changes**.