



Création d'un serveur VPN (OpenVPN) sur Opnsense

Documentation



Alexandre FAUBLADIER-ANETTE

Institution des Chartreux

12/05/2025

Table des matières

Introduction	3
Création du serveur OpenVPN sur Opnsense	3
Introduction	3
Création des certificats et autorité	3
Création du serveur OpenVPN	5
Conclusion	6

Auteur	Version	Date
Killex8569	V0.1	08/05/2025
Killex8569	V1	08/05/2025

Introduction

Dans un objectifs d'accéder au réseau depuis un accès distant, notre objectifs est de mettre en place un serveur OpenVPN qui nous permet en tant qu'utilisateurs (mobile et pc) de pouvoris accéder au réseau interne.

Le serveur VPN nous permet ici de pouvoirs se connecter directement au Firewall et donc d'avoir la possibilité de géré les routes, les moyens de communication etc... directement via des règles de parefeu classique. Cette option est bien plus pratique et utilisée que de créer un serveur OpenVPN sur une machine.

A la fin de ce tuto, vous serez en mesure de mettre les éléments suivants en place sur votre infrastructure :

- Mise en place d'un accès VPN pour votre réseau
- Mise en place de règle de gestion en fonction de votre
- Compréhension du fonctionnement des certificats
- Mise en place de route permettant au VPN d'accéder au autres VLAN

Création du serveur OpenVPN sur Opnsense

Introduction

Pour commencer, vous allez avoir besoin de mettre à jour votre Parefeu Opnsense. Pour cela vous pouvez vous rendre dans **“Système → Firmware → Statut”** puis cliquez sur **“rechercher les mises à jours”**. Une fois que votre parefeu est à jour et à redémarrer, nous allons pouvoirs commencer l'installation et la mise en place du serveur OpenVPN (j'utilise ici uniquement un serveur OpenVPN car je considère que c'est la solution la plus répendu mais aussi la plus facile à mettre en place sur plusieurs appareils différent.)

Création des certificats et autorité

Pour pouvoirs utiliser votre VPN, vous allez devoirs créer des utilisateurs. Chaque utilisateurs devront posséder un mot de passe et un certificat lui permettant de se déclarer comme un client pour le serveur VPN. Cependant en plus de tous cela, il nous est nécessaire de devoirs créer une autorité de certification serveur qui sera utiliser par Opnsense pour valider la connexion. Rendez-vous dans **Système → Trust → Autorité**. Une fois rendu dans cette onglet, vous allez pouvoirs créer votre premier certificat.

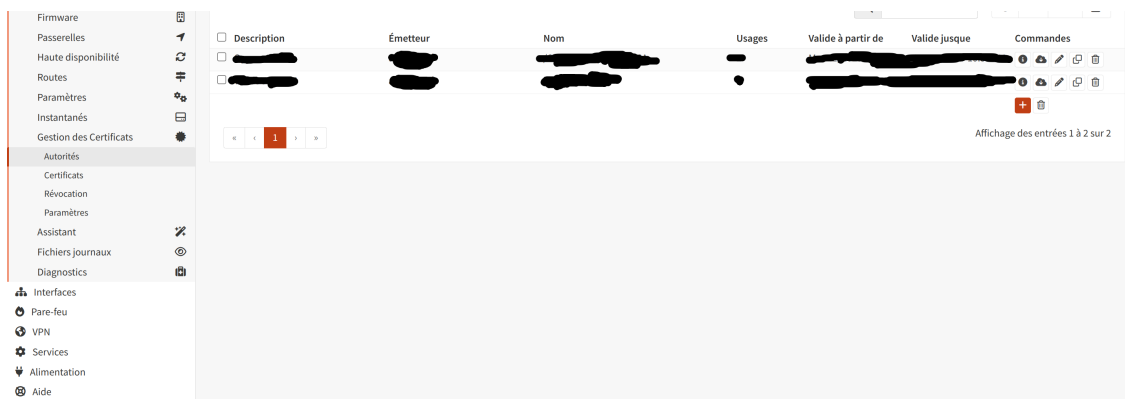


Figure 13 - Ajout d'un certificat coté serveur'

Une fois sur cette page, nous allons pouvoirs créer notre autorité de certification, cliquez sur **“+”**. Puis renseigner les informations suivantes :

- **Nom** : CA_Opnsense (par exemple)
- **Méthode** : “Create an internal Certificate Authority”
- **Type de clé** : Vous pouvez le laisser par défaut (par défaut : RSA-2048)
- **Algorithme de Hachage** : Vous pouvez le laisser par défaut (par défaut : SHA256)
- **Durée de vie** : 825

×

Éditer le certificat

aide complète

?

Méthode

Créer une Autorité de certification interne

?

Description

CA_TUUTO

▼

Clé

?

Type de Clé

RSA-2048

?

Algorithme de Hachage

SHA256

?

Émetteur

auto-signé

?

Durée de vie (jours)

825

▼

Général

?

Pays (C)

France

?

État ou province (ST)

?

Lieu (L)

?

Organisation (O)

?

Unité Organisationnelle

?

Adresse courriel

?

Nom Commun

CA_TUTO

?

OCSP uri

▼

Sortie (format PEM)

Annuler

Sauvegarder

Figure 13 - Ajout d'un certificat coté serveur'

Une fois le certificat ajouter, nous allons pouvoir ajouter un certificat serveur. Pour cela rendez vous dans la section **“Système → Trust → Certificat”**. Puis cliquez sur **“+”** et renseigner les informations suivantes :

Éditer le certificat

×

1 Méthode

Créer un certificat interne

1 Description

OPNsense-VPN-CA

▼ Clé

1 Type

Certificat Serveur

1 Emplacement de la clé privée

Sauvegarder sur ce pare-feu

1 Type de Clé

RSA-2048

1 Algorithme de Hachage

SHA256

1 Émetteur

CA_TUUTO

1 Durée de vie (jours)

397

▼ Général

1 Pays (C)

France

1 État ou province (ST)

1 Lieu (L)

1 Organisation (O)

1 Unité Organisationnelle

1 Adresse courriel

1 Nom Commun

1 OCSP uri

Annuler

Sauvegarder

Figure 13 - Ajout d'un certificat coté serveur'

Attention : Pensez bien à renseigner l'émetteur comme votre autorité de certificat créer juste avant, ne laisser pas par défaut "auto-signer". Normalement les informations du certificat devrait se remplir automatiquement une fois votre emetteur choisi ! (comme par exemple le pays ou la régions.)

Création du serveur OpenVPN

Très bien une fois que tout les pré-requis on été réunni, nous allons pouvoirs commencer. En premier, nous allons nous rendre dans la section **"VPN → OpenVPN → serveur"**. En passant par le wizard, il y aura la possibilité de créer automatiquement les 2 règles nécessaires pour autoriser le flux provenant des clients VPN.Sinon, il faudra les ajouter à la main, ça fonctionne très bien aussi.

- Type de serveur d'authentification : Local User Access
- Autorité de certification : Votre_autorité_de_certification
- Certificat : votre_certificat
- Dans la partie General OpenVPN Server Information, renseigner les paramètres suivants

VPN: OpenVPN: Serveurs [legacy]

Information générale

1
Désactivé
☐

1
Description
OPENVPN_TUTO

1
Mode Serveur
Pair à Pair (SSL/TLS)

1
Protocole
UDP

1
Interface en mode
tun

1
Interface
WAN

1
Port local
443

Paramètres de Chiffrement

1
Authentification TLS
Activé - Authentification seulement

1
Clé partagée TLS
☒ Générer automatiquement une clé partagée d'authentification TLS.

1
Autorité de Certification du correspondant
CA_TUUTO

1
Liste de Révocation de Certificats du correspondant
Aucune Liste de Révocation de Certificats (CRL) définie.
Créer un sous **Système: Certificats**.

1
Certificat Serveur
Web GUI TLS certificate *In Use

1
Algorithme de cryptage (obsolète)
Aucun

1
Empreinte de l'Algorithme d'Authentification
SHA1 (160-bit)

1
Profondeur du Certificat
Un (Client+Serveur)

Paramètres du Tunnel

1
Tunnel Réseau IPv4
10.0.70.0/24

1
Tunnel Réseau IPv6

1
Rediriger la Passerelle
☐

1
Réseau Local IPv4
172.16.10.0/24

1
Réseau Local IPv6

OPNsense (c) 2014-2025 Deciso B.V.

Figure 13 - Ajout d'un certificat coté serveur'

Conclusion

Pour créer cette documentation, je me suis aider de ce tuto en ligne retrouvable [ICI](#)