

VPN OpenVPN site à site sur pfSense

Auteur : M. Grégory Bernard - info@osnet.eu

mercredi 28 octobre 2009 – v.1.0

Licence : [Creative Commons](http://creativecommons.org/licenses/by-nc/3.0/) CC-by-nc

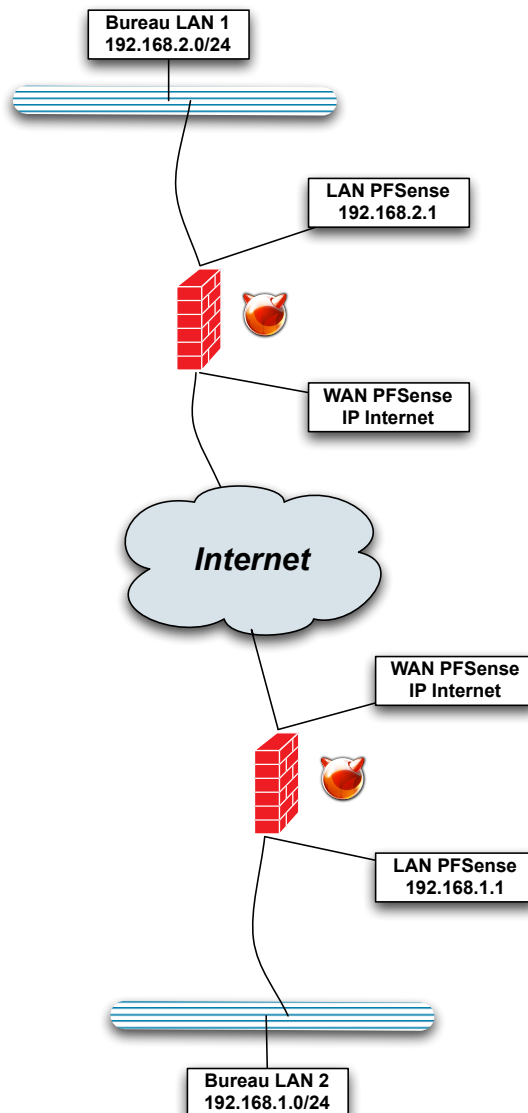


Pour installer pfSense veuillez graver une image ISO sur un CD et installer l'image sur un PC ou faire l'acquisition de l'une de nos appliances <http://www.osnet.eu> avec un système pré configuré.

Différents exemples de configuration figurent sur notre site Internet <http://www.osnet.eu/fr/content/liste-configuration-pfsense>

Objectif initial

Comme en matière de réseau un bon schéma vaut mieux que de long discours, je vous propose de regarder le schéma ci-dessous:



Côté serveur

Etablissement du pool d'adresse des Tunels

Objectif : établir les pools d'adresses destinées aux VPN distants.

Nous avons ici utilisé le pool 192.168.3.0/24 et

Si vous prévoyez d'avoir de très nombreux réseaux, je vous conseille d'établir un plan d'adressage qui ne soit pas basé sur un /24, mais sur un /27 ou /28

Cliquez sur le bouton  situé sur la page VPN --> OpenVPN --> (Onglet) Server

Vous arrivez alors sur une page telle que celle-ci :

Dans «protocol» sélectionnez «TCP»

Pour «Local port» sélectionnez le port 1194 ou un autre port inoccupé de votre réseau : **attention : Il doit y avoir un port par tunnel que vous établirez.**

Tunnel 1 : 1194 -- Tunnel 2 : 1195 -- Tunnel 3 : 1196 -- ...

«Adress pool» représente le bloc d'adresses qui sera assigné au tunnel côté serveur.

Vous n'êtes pas obligé de remplir le champs «Local network».

«Remote network» doit correspondre à l'adresse IP du LAN distant (ou LAN client).

Dans «Cryptography» choisissez une méthode d'encryption cohérente et similaire des deux côtés du VPN.

La méthode d'authentification pour un Tunnel point à point est «Shared Key»

Génération de la clé depuis un boîtier Alix

Les boîtiers Alix configurés avec NanoBSD ont la particularité de monter leur OS en RO (Read Only). Cela vous interdit donc de faire des manipulation sur l'OS... Vous devez donc monter l'OS en mode RW (Read Write) avant de pouvoir générer la clé partagée.

1. Connectez-vous sur votre boîtier pfSense en SSH

2. Montez le système RW

```
pfsense:~# /etc/rc.conf_mount_rw
```

3. Générez votre clé de secret partagé

```
pfsense:~# openvpn --genkey --secret shared.key
```

```
pfsense:~# more shared.key
```

```
#
```

```
# 2048 bit OpenVPN static key
```

```
#
```

```
-----BEGIN OpenVPN Static key V1-----
```

```
f3e19d185593cfb903df8e196f34f49c
```

```
2f4d6457dec543df196dc7c9c33516df
```

```
01dc426879e026da53999d268056f92f
```

```
970e759444449eb8c6e3272635361ad6
```

```
22b5ffef49a7cf7b1ff269e6635f5b17
```

```
016a65a135425794900439a16e9bf916
```

```
524ea70dd85fabe8cc720a350ff37348
```

```
1705315d0a35085f9bd0a2355d09b193
```

```
786d7c9f5024897aea975e6b4a138b5c
```

```
91758bf147e1d2d8aba0fed16a8aba29
```

```
7be017d249867c592814958d00c7c906
```

```
5c994ca67085246b9eebedcea4192ccd
```

```
0ec6fd988df906b53927dca6498c07cc
```

```
14f250351162338e2e86118b2f608edf
```

```
3fe3847bb8fb2438b6baf74321998830
```

```
3f8b955aa9f350f545bfb52ffda93e02
```

```
-----END OpenVPN Static key V1-----
```

4. Copier - coller la clé dans la configuration dans la section «Shared Key»

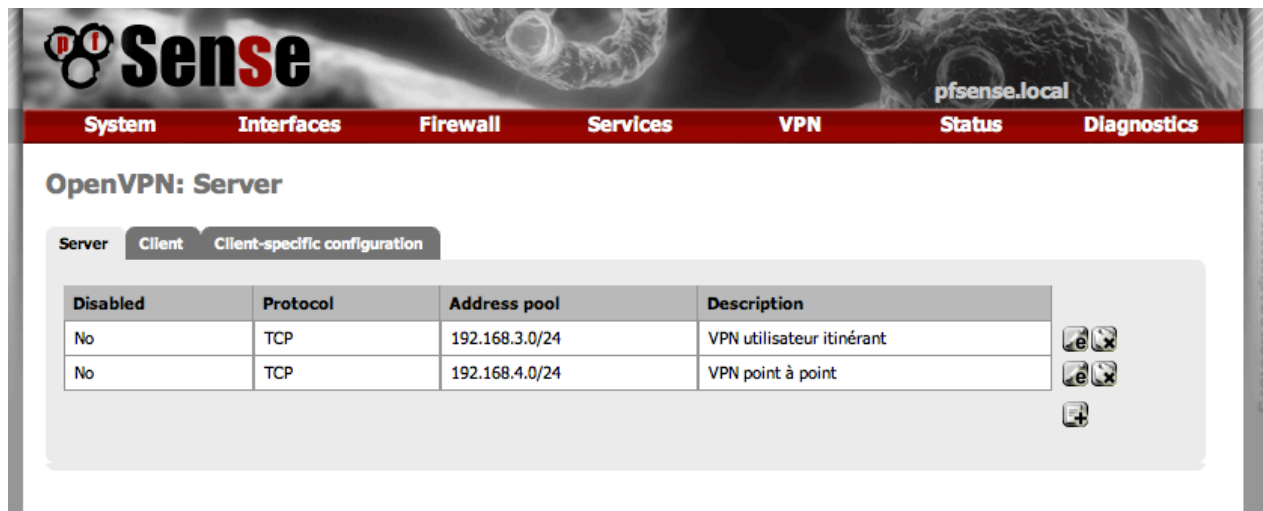
5. Enfin remontez votre firewall en mode RO

```
pfSense:~# /etc/rc.conf_mount_ro
```

Si vous ne parvenez pas à vous connecter sur votre firewall vous pouvez copier-coller la clé exposée ci-dessus (ne le dite à personne !!). Elle doit être copié avec les signes -----BEGIN OpenVPN Static key V1----- idem pour la fin.

Fixez les options complémentaires de la configuration si besoin est.

Enregistrez votre configuration... vous devriez vous retrouver à la page suivante :



Côté client

Connectez-vous sur le firewall côté client.

Allez à la section VPN --> OpenVPN --> (Onglet) Client

Cliquez sur le bouton



Vous vous retrouverez sur la page de configuration du VPN côté client.

Dans «Protocol» sélectionnez «TCP»

Dans «Server Address» saisissez l'adresse WAN de votre Serveur VPN.

Dans «Server Port» indiquez le même Port TCP que celui que vous avez indiqué sur votre serveur.

Dans «Interface IP» indiquez l'adresse du réseau Local côté Client.

Dans «Remote Network» indiquez l'adresse du réseau Local côté Serveur.


Pour «Cryptography» et «Authentication Method» indiquez des paramètres identique sur les deux firewalls.

Enregistrez votre configuration.

Firewall


Il vous reste une dernière étape pour pouvoir avoir un VPN qui fonctionne : la configuration de votre firewall. Côté Serveur vous devez accepter les connexion entrante sur le port TCP qui va relayer la connexion VPN.

Allez dans Firewall --> Rules --> (Onglet) WAN

Cliquez sur le 

Ajoutez une règle à peu près similaire à celle figurant ci-dessous.

Bien évidemment le port TCP doit être celui que vous avez configuré dans la section «Server Port». Vous devriez avoir une configuration similaire à celle-ci :

<input type="checkbox"/>	<input checked="" type="checkbox"/>	TCP/UDP	*	*	*	1195	*		OpenVPN remote in Ok	
--------------------------	-------------------------------------	---------	---	---	---	------	---	--	----------------------	---

Une règle pour chaque VPN configuré doit être ajoutée avec à chaque fois un port TCP différent.

Pour une meilleure sécurité, vous pouvez limiter les connexion à l'adresse IP public du tunel côté Client.

Pour débuser votre configuration vous pouvez temporairement activer le log...

Votre règle devrait ressembler à cela :

Firewall: Rules: Edit

Action	<input type="button" value="Pass"/> <small>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 to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.</small>
Disabled	<input type="checkbox"/> Disable this rule <small>Set this option to disable this rule without removing it from the list.</small>
Interface	<input type="button" value="WAN"/> <small>Choose on which interface packets must come in to match this rule.</small>
Protocol	<input type="button" value="TCP/UDP"/> <small>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</small>
Source	<input type="checkbox"/> not <small>Use this option to invert the sense of the match.</small> Type: <input type="button" value="any"/> Address: <input type="text" value=""/> / <input type="button" value="31"/> <input type="button" value="Advanced"/> - Show source port range
Source OS	OS Type: <input type="button" value="any"/> <small>Note: this only works for TCP rules</small>
Destination	<input type="checkbox"/> not <small>Use this option to invert the sense of the match.</small> Type: <input type="button" value="any"/> Address: <input type="text" value=""/> / <input type="button" value="31"/>
Destination port range	from: <input type="button" value="(other)"/> <input type="text" value="1195"/> to: <input type="button" value="(other)"/> <input type="text" value="1195"/> <small>Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port</small>

Sauvegardez votre configuration.

Et voilà !!

A bientôt et n'oubliez pas d'acheter votre firewall pfSense chez www.osnet.eu - merci.