

DOCUMENTATION

Fonctionnelle
&
Technique

Installation de pfsense et configuration.

SOMMAIRE

Table des matières

1.	Qu'est-ce que pfsense ?	3
2.	comment installer pfsense	3
2.1	Installation de pfsense	4
2.2	Premier démarrage de pfSense	7
2.3	Première connexion à l'interface d'administration de pfSense	9
2.3.1	Se connecter à l'interface web de PfSense.....	9
2.3.2	L'assistant de configuration Web	9
3.	Mise en place de la redondance.....	12
4.	Activation du serveur DHCP	14
5.	Liaison de l'active directory	15
6.	VPN Client to site	16
6.1	Création des certificats	16
6.1.1	Certificat autorités	16
6.1.2	Certificat de serveur.....	17
6.2	Paramétrer le serveur VPN	18
6.3	Récupérer les fichiers de configuration client OpenVPN.....	20
6.3.1	Installer openvpn-client-export.....	20
6.3.2	Récupérer les fichiers.....	21
7.	VPN Site to site	21
7.1	Configuration du serveur	21
7.2	Connexion du client	22
8.	DMZ 23	
9.	lien 25	

1. QU'EST-CE QUE PFSENSE ?

pfSense est un système d'exploitation open source basé sur FreeBSD et spécialement conçu pour être utilisé comme pare-feu, routeur et point d'accès VPN. Voici un aperçu de ses principales caractéristiques et fonctionnalités :

1. Firewall avancé : pfSense offre une gamme complète de fonctionnalités de pare-feu, y compris la gestion des règles de filtrage, la détection d'intrusion, la prévention des intrusions (IDS/IPS), la prévention des fuites DNS, etc.
2. Routing robuste : En tant que routeur, pfSense gère le routage entre réseaux, le NAT (Network Address Translation), la liaison de plusieurs connexions Internet (load balancing), et le failover pour assurer la redondance.
3. VPN : Il prend en charge différents types de VPN, notamment IPsec, OpenVPN, et L2TP, permettant ainsi de créer des connexions sécurisées entre différents réseaux ou pour permettre un accès distant sécurisé.
4. Proxy et filtrage web : pfSense peut être configuré pour agir comme un proxy transparent ou explicite avec des fonctionnalités de filtrage web pour contrôler l'accès aux sites et aux contenus.
5. Serveur DHCP et DNS : Il fournit des services DHCP (Dynamic Host Configuration Protocol) pour attribuer automatiquement des adresses IP aux appareils du réseau et peut servir de serveur DNS pour résoudre les noms d'hôtes.
6. Équilibrage de charge et haute disponibilité : pfSense prend en charge l'équilibrage de charge sur plusieurs connexions Internet pour optimiser l'utilisation de la bande passante et garantir la disponibilité du réseau.
7. Surveillance du trafic : Il offre des outils de surveillance du trafic en temps réel, y compris des graphiques et des tableaux de bord détaillés sur l'utilisation de la bande passante et d'autres statistiques réseau.
8. Interface utilisateur conviviale : pfSense dispose d'une interface web conviviale qui permet une configuration facile à travers différents modules et options.
9. Extensions et plugins : Il est extensible grâce à un large éventail de plugins et d'extensions qui ajoutent des fonctionnalités supplémentaires telles que la prise en charge de services de filtrage antivirus, de serveurs de messagerie, etc.

pfSense est largement utilisé dans les environnements professionnels et domestiques en raison de sa fiabilité, de ses performances et de sa flexibilité. C'est une solution polyvalente pour sécuriser et gérer les réseaux informatiques.

2. COMMENT INSTALLER PFSENSE

Voici les propriétés de la machine virtuelle que nous utilisons, il y aura deux VM une principale et une secondaire :

- ➔ pfSense 2.7.2
- ➔ 1v CPU
- ➔ 512 Mo de RAM.
- ➔ 32 Go de disque dur.

➔ 3 cartes réseau, une pour le WAN avec une ip donner par le DHCP de la box, une pour le LAN qui serra configurer en statique et une dernière pour la haute disponibilité.

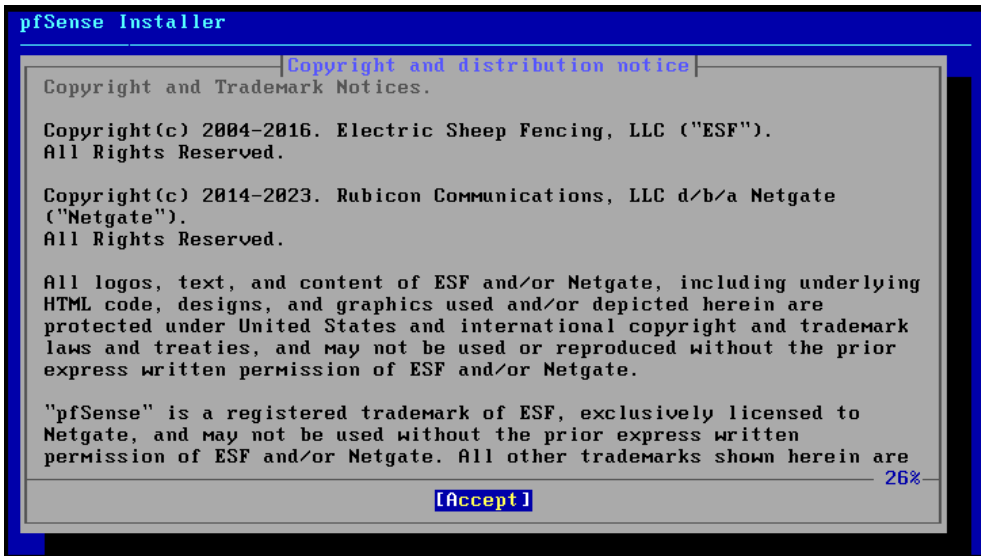
2.1 Installation de pfsense

Maintenant que notre VM est configurée selon notre besoin, nous allons pouvoir la démarrer. La VM va automatiquement démarrer sur le fichier d'installation ISO de pfSense.

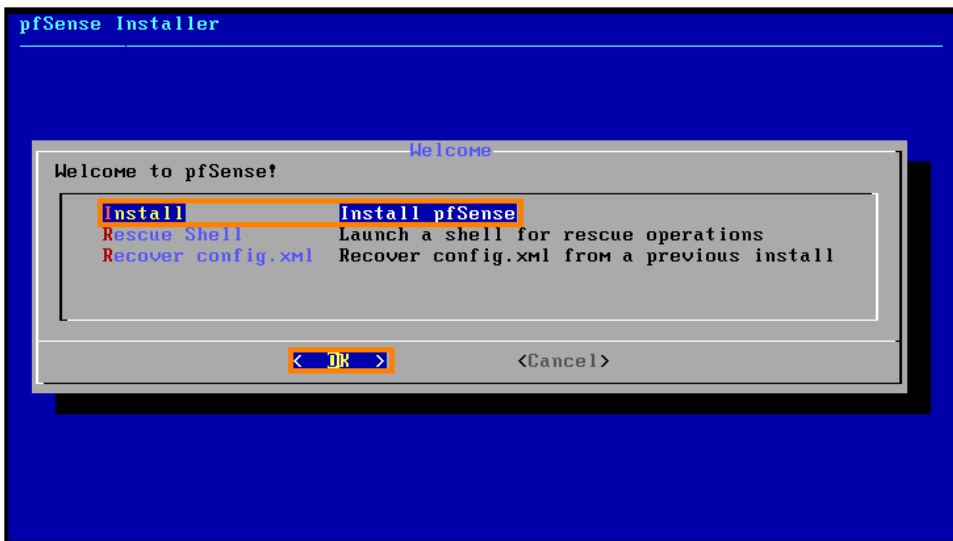
L'installateur de pfSense va d'abord analyser la configuration matérielle de la VM et charger l'assistant d'installation.

```
pci028: <ACPI PCI-PCI bridge> at device 24.1 on pci0
pci029: <ACPI PCI-PCI bridge> at device 24.2 on pci0
pci030: <ACPI PCI-PCI bridge> at device 24.3 on pci0
pci031: <ACPI PCI-PCI bridge> at device 24.4 on pci0
pci032: <ACPI PCI-PCI bridge> at device 24.5 on pci0
pci033: <ACPI PCI-PCI bridge> at device 24.6 on pci0
pci034: <ACPI PCI-PCI bridge> at device 24.7 on pci0
acpi_acad0: <AC Adapter> on acpi0
atkbdc0: <Keyboard controller (i8042)> port 0x60,0x64 irq 1 on acpi0
atkbd0: <AT Keyboard> irq 1 on atkbdc0
kbd0 at atkbd0
atkbd0: [GIANT-LOCKED]
psm0: <PS/2 Mouse> irq 12 on atkbd0
psm0: [GIANT-LOCKED]
WARNING: Device "psm" is Giant locked and may be deleted before FreeBSD 14.0.
psm0: Model IntelliMouse, device ID 3
acpi_syscontainer0: <System Container> on acpi0
orm0: <ISA Option ROMs> at iomem 0xc0000-0xc7fff,0xc8000-0xc9fff,0xca000-0xcacfff,0xcb000-0xcffff,0xcc000-0xccfff,0xcd000-0xdffff,0xe0000-0xe7fff pnpid ORM0000 o
n isa0
vga0: <Generic ISA VGA> at port 0x3c0-0x3df iomem 0xa0000-0xbffff pnpid PNP0900
on isa0
Timecounter "TSC-low" frequency 1896440000 Hz quality 1000
Timecounters tick every 10.000 msec
█
```

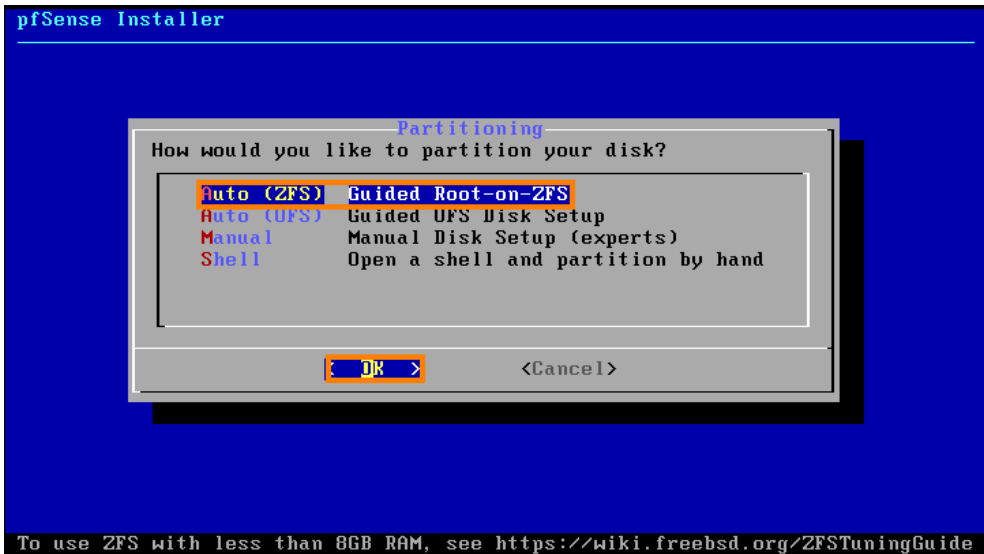
Une fois le chargement terminé, veuillez accepter le contrat d'utilisation de pfSense (Tapez sur Entrée).



Pour poursuivre l'installation, sélectionnez "Install pfSense" et appuyez sur Entrée.

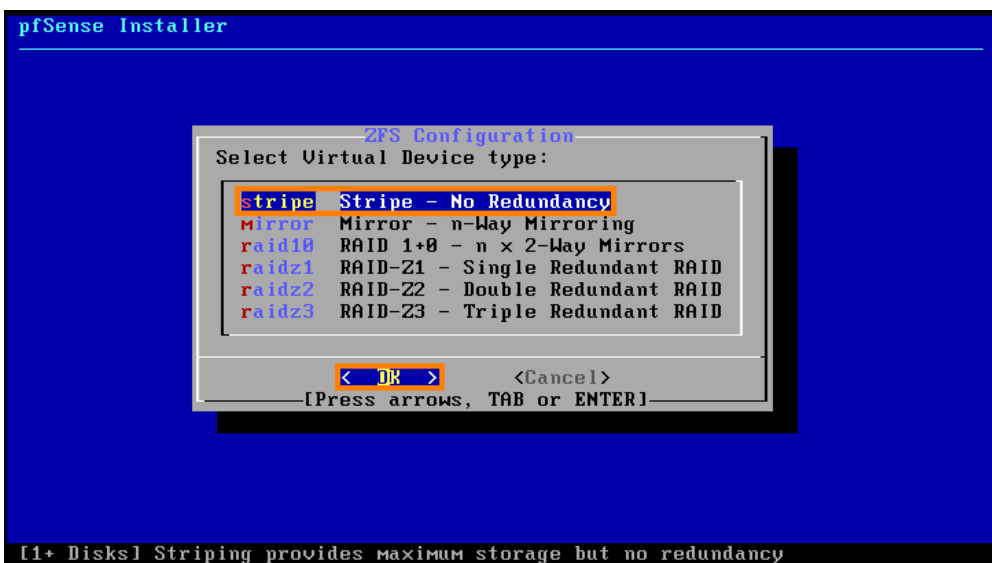


A l'étape de partitionnement du disque, nous allons utiliser le mode "**Auto (ZFS)**" présélectionné et appuyer sur **Entrée**.

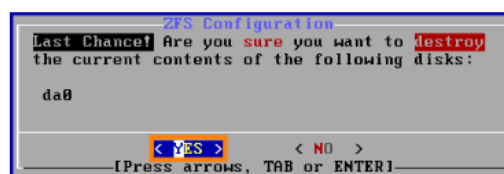
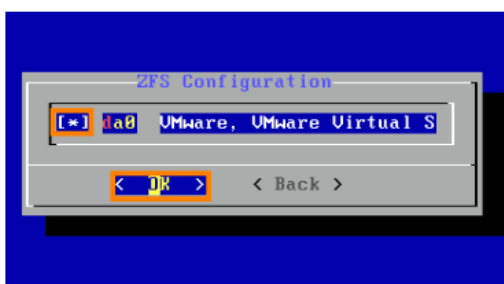


Au travers du système de fichier ZFS, pfSense peut-être installé sur de multiples disques pour assurer une disponibilité accrue du pare-feu.

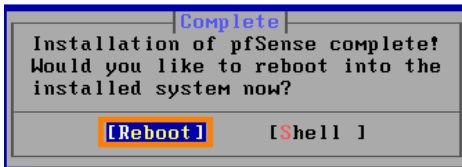
Dans notre cas, nous allons faire une installation sans redondance (mode stripe). Appuyez sur Entrée.



Pour sélectionner le disque dur virtuel, appuyez sur Espace puis sur Entrée et sélectionner "Yes" (flèche gauche et Entrée).



L'installation est relativement rapide. Une fois achevée, validez le redémarrage de la VM.



2.2 Premier démarrage de pfSense

Au premier démarrage, pfSense détecte automatiquement les interfaces réseau. La plupart du temps, vous verrez l'interface WAN rattachée à l'interface em0 correspondant à la première interface ajoutée. L'interface LAN quant à elle sera rattachée à l'interface em1, correspondant à la deuxième interface ajoutée à la VM.

```
FreeBSD/amd64 (pfSense.home.arp) (ttyv0)
VMware Virtual Machine - Netgate Device ID: d4f7d4fa69d64052c10b
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.193/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: █
```

Comme on peut le voir, la configuration IP de l'interface WAN a été attribuée par le serveur DHCP de mon réseau. Nous allons configurer l'interface LAN avec sa configuration IP adéquate.

Pour modifier la configuration IP de notre interface LAN, nous allons procéder comme suit :

Choisissez l'option 2.

```
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.193/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 2
```

Ensuite, nous allons sélectionner l'interface LAN en entrant l'option 2 et indiquer que nous n'allons pas configurer l'interface via DHCP

```
Available interfaces:
1 - LAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
```

Enfin, nous allons définir la configuration IP de notre interface manuellement :

- Adresse IP de l'interface LAN : 192.168.10.254
- Masque de sous-réseau (en notation CIDR) : 24 = 255.255.255.0
- Pas de passerelle
- Pas de configuration IPv6
- Pas de serveur DHCP IPv4 - il pourra être configuré par la suite depuis l'interface Web

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.100.1
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none
>
Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on LAN? (y/n) n
```

Une fois terminé, l'URL pour accéder à l'interface Web d'administration de pfSense s'affiche et faire "Entrée" pour terminer.

2.3 Première connexion à l'interface d'administration de pfSense

2.3.1 Se connecter à l'interface web de PfSense

Depuis le poste client (c'est-à-dire depuis notre réseau LAN virtuel), nous allons nous connecter à l'interface Web d'administration de pfSense à l'adresse IP "https://192.168.10.254/".

Au préalable, il est nécessaire de configurer l'interface réseau de la machine virtuelle cliente comme suit :

- Adresse IPv4 : 192.168.10.2
- Masque : 255.255.255.0 ou /24
- Passerelle : 192.168.100.1
- Serveur DNS : 1.1.1.1 ou celui de votre choix

Le certificat de sécurité SSL utilisé pour la connexion HTTPS est auto-signé, il est donc normal d'avoir un avertissement de sécurité. Il est possible, selon vos besoins de définir un certificat provenant d'une autorité de certification d'entreprise ou publique.

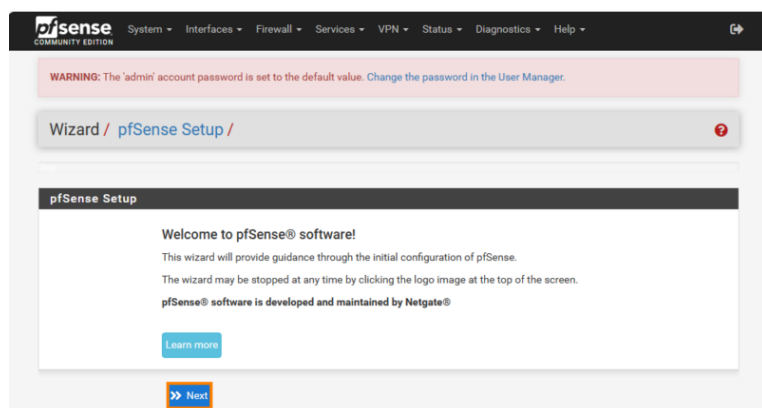
Pour vous connecter à l'interface Web d'administration, il est nécessaire de saisir l'identifiant et le mot de passe prédéfini à l'installation. Voici les identifiants par défaut :

Identifiant : admin

Mot de passe : pfsense (à modifier par la suite)

2.3.2 L'assistant de configuration Web

Une fois connecté, l'assistant de configuration Web s'ouvrira. Cliquez sur "Next".



Cliquez à nouveau sur "Next" pour valider les modalités de support fourni par l'éditeur.

Wizard / pfSense Setup / Netgate® Global Support is available 24/7

Step 1 of 9

Netgate® Global Support is available 24/7

Our 24/7 worldwide team of support engineers are the most qualified to diagnose your issue and resolve it quickly, from branch office to enterprise – on premises to cloud.

We offer several support subscription plans tailored to fit different environment sizes and requirements. Many companies around the world choose Netgate support because:

- Support is available 24 hours a day, seven days a week, including holidays.
- Support engineers are located around the world, ensuring that no support call is missed.
- Our support engineers hold many prestigious network engineer certificates and have years of hands-on experience with networking.

Learn more

Next

Ici, nous allons préciser les serveurs DNS de notre firewall pfSense, à savoir "1.1.1.1" et "8.8.8.8", et cliquer sur "Next". Adaptez ces valeurs si vous le souhaitez.

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname

pfSense

Name of the firewall host, without domain part.

Examples: pfsense, firewall, edgefw

Domain

home.arpa

Domain name for the firewall.

Examples: home.arpa, example.com

Do not end the domain name with 'local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

1.1.1.1

Secondary DNS Server

8.8.8.8

Override DNS

☒

Allow DNS servers to be overridden by DHCP/PPP on WAN

Next

A cette étape, nous allons configurer le serveur de temps qui est important pour bénéficier de logs à jour. Sélectionnez le fuseau horaire correspondant à votre emplacement puis cliquez sur "Next".

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname

2.pfsense.pool.ntp.org

Enter the hostname (FQDN) of the time server.

Timezone

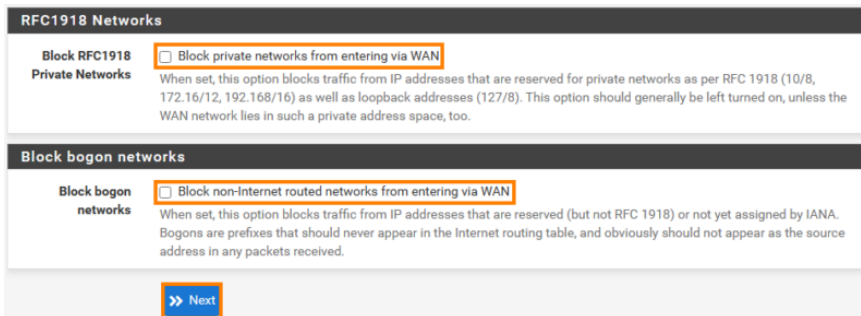
Europe/Paris

Next

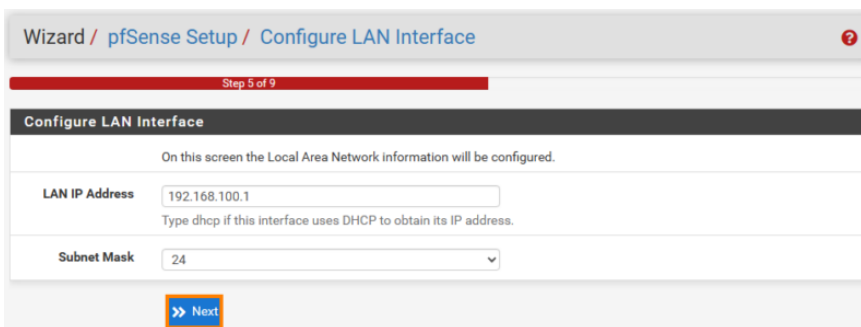
DOCUMENTATION – GLPI

Page : 10 sur 25

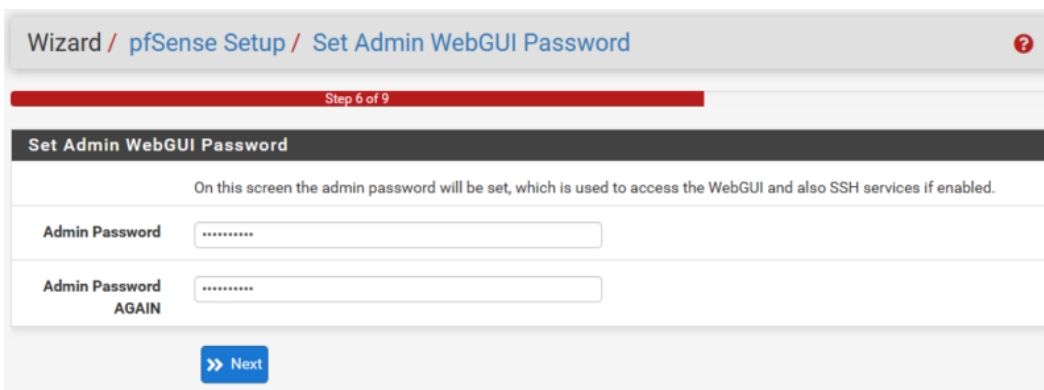
A l'étape 4, conservez les paramètres prédéfinis par pfSense pour la configuration de l'interface WAN en veillant à décocher les 2 options suivantes : "Block private networks from entering via WAN" et "Block non-Internet routed networks from entering via WAN". Ces deux paramètres, lorsque pfSense est installé dans un réseau local existant (lab virtuel), permet de ne pas bloquer le trafic reposant sur des adresses IP privée. Ici, entre notre box internet et pfSense.



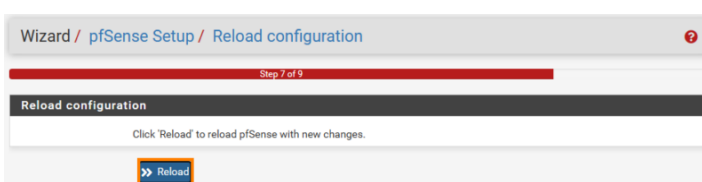
A l'étape 5 de l'assistant, conservez la configuration de l'interface LAN que nous avons fait en amont.



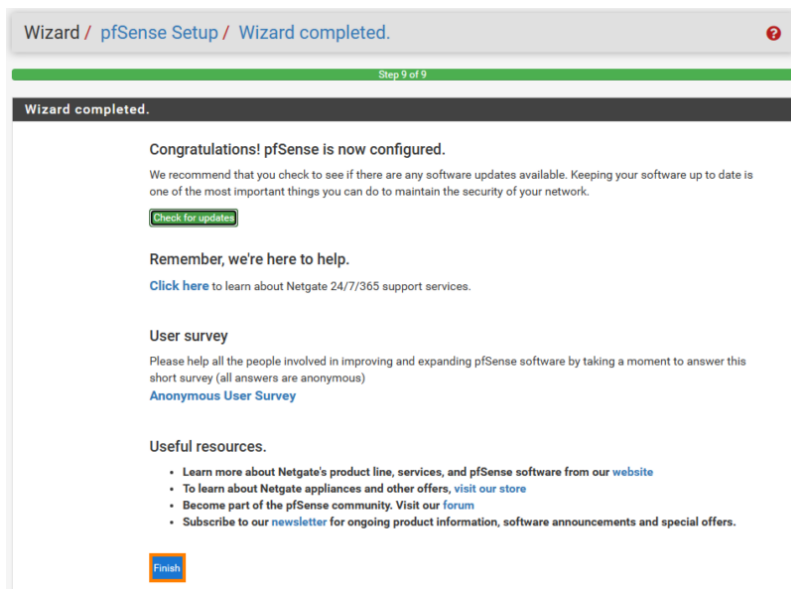
A l'étape 6 de l'assistant, définissez un nouveau mot de passe et cliquer sur "Next".



A l'étape 7, cliquez sur "Reload" afin de recharger la configuration de pfSense avec les informations que nous venons de définir.



Après quelques secondes, nous arrivons à la fin de l'assistant de configuration. Nous pouvons cliquer sur "Finish" pour accéder au tableau de bord.



3. MISE EN PLACE DE LA REDONDANCE

La mise en place d'une redondance nous permettra en cas de crache d'un des routeurs de toujours avoir accès aux réseaux et aux différents services. Des adresses IP virtuelles seront utilisées.

Nous allons connecter les routeurs entre eux grâce à une troisième interface réseau.

Le serveur principal aura l'IP 172.16.0.1/30 et le secondaire 172.16.0.2/30.

On commence par créer l'adresse virtuelle 192.168.10.1/24 sur le serveur principal, cette adresse sera la Gateway de notre réseau.

Se rendre dans Firewall > Virtual IPs créer une adresse.

- Type : CARP
- Interface : LAN
- Adresse : 192.168.10.1 /24
- Virtual IP Password : Azerty68
- VHID Group : 1

Firewall / Virtual IPs / Edit

Edit Virtual IP

Type: ☐ IP Alias ☒ CARP ☐ Proxy ARP ☐ Other

Interface: LAN

Address type: Single address

Address(es): 192.168.10.1 / 24
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password:
Enter the VHID group password. Confirm

VHID Group: 1
Enter the VHID group that the machines will share.

Advertising frequency: 1 0
Base Skew
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description: CARP LAN
A description may be entered here for administrative reference (not parsed).

[Save](#)

Sur le serveur principal se rendre dans System>High Availability

System / High Availability

State Synchronization Settings (pfsync)

Synchronize states: ☒ pfsync transfers state insertion, update, and deletion messages between firewalls.
Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.
This setting should be enabled on all members of a failover group.
Clicking "Save" will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

Synchronize Interface: PFSYNC
If Synchronize States is enabled this interface will be used for communication.
It is recommended to set this to an interface other than LAN! A dedicated interface works the best.
An IP must be defined on each machine participating in this failover group.
An IP must be assigned to the interface on any participating sync nodes.

Filter Host ID: e7e85589
Custom pf host identifier carried in state data to uniquely identify which host created a firewall state.
Must be a non-zero hexadecimal string 8 characters or less (e.g. 1, 2, ff01, abcdef01).
Each node participating in state synchronization must have a different ID.

pfsync Synchronize Peer IP: 172.16.0.2
Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

Configuration Synchronization Settings (XMLRPC Sync)

Synchronize Config to IP: 172.16.0.2
Enter the IP address of the firewall to which the selected configuration sections should be synchronized.

XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!
Do not use the Synchronize Config to IP and password option on backup cluster members!

Remote System Username: admin
Enter the webConfigurator username of the system entered above for synchronizing the configuration.
Do not use the Synchronize Config to IP and username option on backup cluster members!

Remote System:

Remote System Password	<input type="password"/> Enter the webConfigurator password of the system entered above for synchronizing the configuration. Do not use the Synchronize Config to IP and password option on backup cluster members!	<input type="password"/> Confirm
Synchronize admin	<input type="checkbox"/> synchronize admin accounts and autoupdate sync password. By default, the admin account does not synchronize, and each node may have a different admin password. This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.	
Select options to sync	<input checked="" type="checkbox"/> User manager users and groups <input checked="" type="checkbox"/> Authentication servers (e.g. LDAP, RADIUS) <input checked="" type="checkbox"/> Certificate Authorities, Certificates, and Certificate Revocation Lists <input checked="" type="checkbox"/> Firewall rules <input checked="" type="checkbox"/> Firewall schedules <input checked="" type="checkbox"/> Firewall aliases <input checked="" type="checkbox"/> NAT configuration <input checked="" type="checkbox"/> IPsec configuration <input checked="" type="checkbox"/> OpenVPN configuration (Implies CA/Cert/CRL Sync) <input checked="" type="checkbox"/> DHCP Server settings <input checked="" type="checkbox"/> DHCP Relay settings <input checked="" type="checkbox"/> DHCPv6 Relay settings <input checked="" type="checkbox"/> WoL Server settings <input checked="" type="checkbox"/> Static Route configuration <input checked="" type="checkbox"/> Virtual IPs <input checked="" type="checkbox"/> Traffic Shaper configuration <input checked="" type="checkbox"/> Traffic Shaper Limiters configuration <input checked="" type="checkbox"/> DNS Forwarder and DNS Resolver configurations <input checked="" type="checkbox"/> Captive Portal <input checked="" type="checkbox"/> Toggle All	

4. ACTIVATION DU SERVEUR DHCP

Nous allons utiliser le serveur DHCP de pfSense pour donner automatiquement une ip a machine dans le réseau LAN.

Se rendre dans Service>DHCP Server et sélectionner l'interface LAN.

Configurer le pool d'adresses, la gateway et le(s) serveur(s) DNS.

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / DHCP Server / LAN

WAN LAN CARP

General DHCP Options

DHCP Backend: Kea DHCP

Enable: ☒ Enable DHCP server on LAN interface

Deny Unknown Clients: ▾
 When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed in a static mapping on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.

Ignore Client Identifiers: ☐ Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
 This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Primary Address Pool

Subnet: 192.168.10.0/24

Subnet Range: 192.168.10.1 - 192.168.10.254

Address Pool Range: From To

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Server Options

WINS Servers: WINS Server 1, WINS Server 2

DNS Servers (highlighted with a yellow box): 192.168.10.3, 192.168.10.4, 8.8.8.8, 1.1.1.1

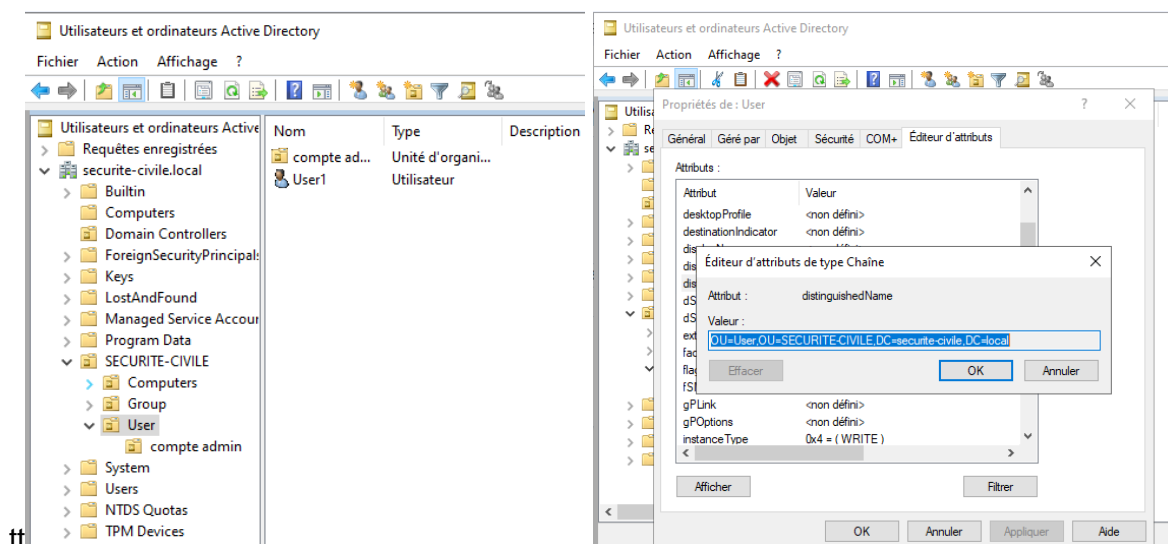
Other DHCP Options

Gateway: 192.168.10.1 (highlighted with a yellow box)

The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter none for no gateway assignment.

5. LIAISON DE L'ACTIVE DIRECTORY

Nous allons connecter notre serveur LDAP Active directory Windows pour pouvoir s'identifier plus tard au VPN.



Nous aurons besoin de la « BASE DN » et « Authentication containers » pour connecter le serveur.

Se rendre dans System>User Manager>Authentication Servers. On ajoute un nouveau serveur.

Nous aurons besoin de configurer ses valeurs :

- Descriptive name : SECURITE-CIVILE
- Hostname or IP address : 192.168.10.3
- Search scope : entire level
- Base DN : DC=securite-civile,DC=local
- Authentication containers : OU=User,OU=SECURITE-CIVILE,DC=securite-civile,DC=local
- Bind anonymous : Décochez
- Bind credentials
 - User : Authentication containers
 - Password : Azerty68
- User naming attribute : samAccountName

- Allow unauthenticated bind : Décochez

Note : On peut utiliser le bouton « Select a container » pour sélectionner le bon, il faut quand même mettre une valeur pour pouvoir utiliser cette fonction.

On peut vérifier le bon fonctionnement dans Diagnostics>Authentication

6. VPN CLIENT TO SITE

Nous allons créer un VPN client to site qui a pour but de connecter les clients au réseau 10.0.8.0/24 et avoir accès au réseau 192.168.10.0/24. Nous utiliserons le port 443 pour que le VPN soit RoadWarrior et donc non bloquer par les pare-feux. Les clients se connecteront avec leurs identifiants Windows Active Directory.

6.1 Création des certificats

6.1.1 Certificat authorities

Aller dans System>Certificates>Authorities

Ajouter un nouveau certificat.

Entrer les paramètres suivants :

Descriptive Name

S2SCA

Method

Create an internal Certificate Authority

Randomize Serial

Checked

Key Type

RSA, 2048 (or higher)

Digest Algorithm

sha256 (or higher)

Lifetime (days)

3650

Common Name

S2SCA

6.1.2 Certificat de serveur

Aller dans System>Certificates>Certificates

Ajouter un nouveau certificat.

Entrer les paramètres suivants :

Method

Create an internal Certificate

Descriptive Name

serverA

Certificate Authority

S2SCA

Key Type

RSA, 2048 (or higher)

Digest Algorithm

sha256 (or higher)

Lifetime (days)

398

Common Name

serverA

Subject Component Fields

Les champs contiennent des données copiées de l'autorité de certification et sont facultatifs, mais ils peuvent être définis pour refléter l'emplacement du serveur.

Certificate Type

Server Certificate

6.2 Paramétrer le serveur VPN

Se rendre dans VPN>OpenVPN et cliquez sur Wizard pour créer le vpn avec l'assistant.

Type de serveur : pour notre utilisation nous utiliserons LDAP.

Wizard / OpenVPN Remote Access Server Setup /

OpenVPN Remote Access Server Setup

This wizard will provide guidance through an OpenVPN Remote Access Server Setup .

The wizard may be stopped at any time by clicking the logo image at the top of the screen.

Select an Authentication Backend Type

Type of Server

NOTE: If unsure, leave this set to "Local User Access."

[Next](#)

On sélectionne ou ajoute notre serveur LDAP.

Wizard / OpenVPN Remote Access Server Setup / LDAP Server Selection

Step 1 of 11

LDAP Server Selection

OpenVPN Remote Access Server Setup Wizard

LDAP Authentication Server List

LDAP servers

[Add new LDAP server](#) [Next](#)

On sélectionne les certificats créer précédemment ou on en créer des nouveaux.

Wizard / OpenVPN Remote Access Server Setup / Certificate Authority Selection

Step 5 of 11

Certificate Authority Selection

OpenVPN Remote Access Server Setup Wizard

Choose a Certificate Authority (CA)

Certificate Authority

[Add new CA](#) [Next](#)

On peut modifier le nom, l'interface, le port dans notre cas on va utiliser le 443 pour le RoadWarrior.

Server Setup	
OpenVPN Remote Access Server Setup Wizard	
General OpenVPN Server Information	
Description	<input type="text" value="OPENVPN RoadWarrior"/> <p>A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.</p>
Endpoint Configuration	
Protocol	<input type="text" value="UDP on IPv4 only"/> <p>Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.</p>
Interface	<input type="text" value="WAN"/> <p>The interface where OpenVPN will listen for incoming connections (typically WAN.)</p>
Local Port	<input type="text" value="1194"/> <p>Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.</p>

IPv4 Tunnel Network pour le réseau du VPN et IPv4 Local Network pour le réseau local a atteindre.

Tunnel Settings	
IPv4 Tunnel Network	<input type="text" value="10.0.8.0/24"/> <p>This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.</p>
Redirect IPv4 Gateway	<input type="checkbox"/> Force all client generated traffic through the tunnel.
IPv4 Local Network	<input type="text" value="192.168.10.0/24"/> <p>This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.</p>
Concurrent Connections	<input type="text" value="100"/> <p>Specify the maximum number of clients allowed to concurrently connect to this server.</p>

On spécifie les serveurs DNS à utiliser.

DNS Server 1	<input type="text" value="192.168.10.3"/> <p>DNS server IP to provide to connecting clients.</p>
DNS Server 2	<input type="text" value="192.168.10.4"/> <p>DNS server IP to provide to connecting clients.</p>
DNS Server 3	<input type="text" value="8.8.8.8"/> <p>DNS server IP to provide to connecting clients.</p>
DNS Server 4	<input type="text" value="1.1.1.1"/> <p>DNS server IP to provide to connecting clients.</p>

On fini par lui faire créer les règles de pare-feu automatiquement.

Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration ?

Step 10 of 11

Firewall Rule Configuration

OpenVPN Remote Access Server Firewall Rules

Rules control passing or blocking network traffic as it flows through the firewall.

Rules must be added which allow traffic to reach the OpenVPN server IP address and port, as well as to allow traffic from connected clients inside the OpenVPN tunnel.

The options on this step can add automatic rules to pass this traffic, or rules can be configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule ☒ Add a rule to permit connections to this OpenVPN server instance from clients anywhere on the Internet.

Traffic from clients through VPN

OpenVPN rule ☒ Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

[» Next](#)

6.3 Récupérer les fichiers de configuration client OpenVPN

6.3.1 Installer openvpn-client-export

Grace au package « openvpn-client-export » nous pourrons récupérer les fichiers de configuration du VPN.

Se rendre dans System>Package Manager> Available Packages et rechercher puis installer « openvpn-client-export ».

System / Package Manager / Available Packages ?

Installed Packages Available Packages

Search

Search term Both

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
openvpn-client-export	1.9.2	Exports pre-configured OpenVPN Client configurations directly from pfSense software.

Package Dependencies:

[openvpn-client-export-2.6.7](#) [openvpn-2.6.8_1](#) [zip-3.0_1](#) [7-zip-23.01](#)

[+ Install](#)

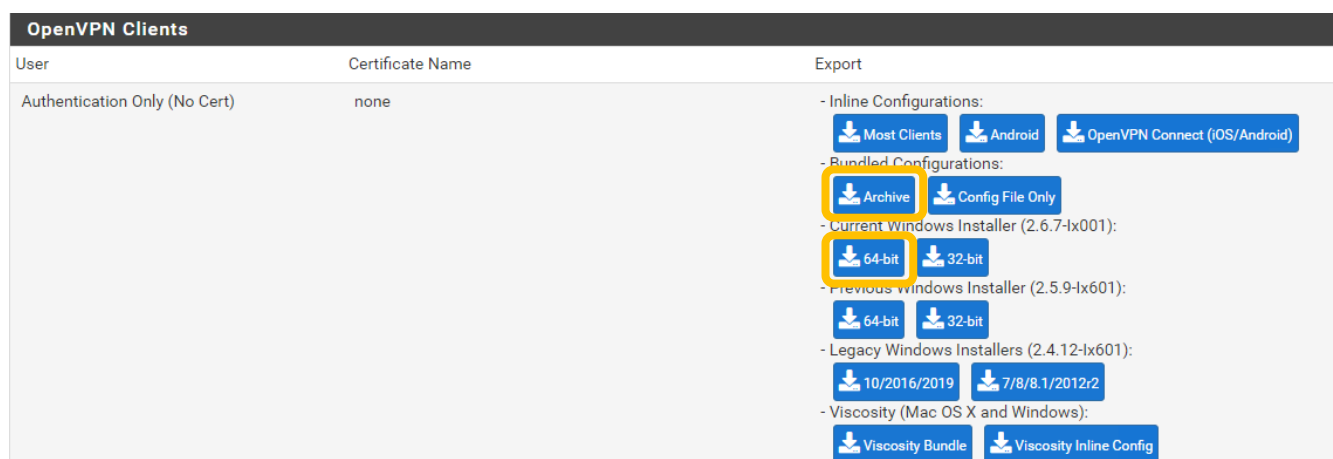
6.3.2 Récupérer les fichiers

Se rendre dans VPN>OpenVPN>Client Export

Se rendre en bas de la page et télécharger les fichiers.

Bundle Configuration : Fichiers de configuration si l'application openVPN est déjà installer

Current Windows installer : Installeur du logiciel avec configuration du vpn pour Windows.



Il ne reste plus qu'à se connecter au VPN avec ses identifiants Windows.

7. VPN SITE TO SITE

Nous allons créer un VPN site to site qui a pour but de connecter les sites de Strasbourg (192.168.200.0/24) au site de Mulhouse (192.168.100.0/24)

7.1 Configuration du serveur

Se rendre dans VPN>OpenVPN>Servers et Créer un nouveau serveur.

- Description : Choisir un nom
- Server mode : Peer to Peer (Shared key)
- IPv4 Tunnel Network : 10.0.11.0/30
- IPv4 Remote network(s) : 192.168.200.0/24

General Information	
Description	<input type="text" value="OVPN-SRV-MUL-1"/> <p>A description of this VPN for administrative reference.</p>
Disabled	<input type="checkbox"/> Disable this server Set this option to disable this server without removing it from the list.
Unique VPN ID	Server 1 (ovpns1)
Mode Configuration	
Server mode	<input type="text" value="Peer to Peer (Shared Key)"/>
WARNING: OpenVPN has deprecated shared key mode as it does not meet current security standards. Shared key mode will be removed from future versions. Convert any existing shared key VPNs to TLS and do not configure any new shared key OpenVPN instances.	
Device mode	<input type="text" value="tun - Layer 3 Tunnel Mode"/> <p>"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2.)</p>
Endpoint Configuration	
Protocol	<input type="text" value="UDP on IPv4 only"/>
Interface	<input type="text" value="WAN"/> <p>The interface or Virtual IP address where OpenVPN will receive client connections.</p>
Local port	<input type="text" value="1194"/> <p>The port used by OpenVPN to receive client connections.</p>
Tunnel Settings	
IPv4 Tunnel Network	<input type="text" value="10.0.11.0/30"/> <p>This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.</p> <p>A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.</p>
IPv6 Tunnel Network	<input type="text"/> <p>This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.</p>
IPv4 Remote network(s)	<input type="text" value="192.168.200.0/24"/> <p>IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.</p>

7.2 Connexion du client

Se rendre dans VPN>OpenVPN>Clients et Ajouter un nouveau serveur.

- Description : Choisir un nom
- Server mode : Peer to Peer (Shared key)
- Server host or address : 192.168.1.67
- IPv4 Tunnel Network : 10.0.11.0/30
- IPv4 Remote network(s) : 192.168.100.0/24

General Information	
Description	OVPN-CLIENT-MUL-1 A description of this VPN for administrative reference.
Disabled	<input type="checkbox"/> Disable this client Set this option to disable this client without removing it from the list.
Unique VPN ID	Client 1 (ovpnc1)
Mode Configuration	
Server mode	Peer to Peer (Shared Key)
WARNING: OpenVPN has deprecated shared key mode as it does not meet current security standards. Shared key mode will be removed from future versions. Convert any existing shared key VPNs to TLS and do not configure any new shared key OpenVPN instances.	
Device mode	tun - Layer 3 Tunnel Mode "tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2.)
Endpoint Configuration	
Protocol	UDP on IPv4 only
Interface	WAN The interface used by the firewall to originate this OpenVPN client connection
Local port	<input type="text"/> Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.
Server host or address	192.168.1.67 The IP address or hostname of the OpenVPN server.
Server port	1194 The port used by the server to receive client connections.
Tunnel Settings	
IPv4 Tunnel Network	10.0.11.0/30 This is the IPv4 virtual network or network type alias with a single entry used for private communications between this client and the server expressed using CIDR notation (e.g. 10.0.8.0/24). This should be left blank in most cases as servers typically provide addresses to clients dynamically. The second usable address in this network will be assigned to the client virtual interface. Ensure the Topology setting matches the server when using SSL/TLS and TUN modes or the interface address may not be configured properly. A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot receive settings from the server dynamically. This mode is not compatible with several options, including Exit Notify, and Inactive.
IPv6 Tunnel Network	<input type="text"/> This is the IPv6 virtual network or network alias with a single entry used for private communications between this client and the server expressed using CIDR notation (e.g. fe80::/64). When set static using this field, the ::2 address in the network will be assigned to the client virtual interface. Leave blank if the server is capable of providing addresses to clients.
IPv4 Remote network(s)	192.168.100.0/24 IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.

On peut aller dans Status>OpenVPN pour voir s'ils sont bien connectés. On peut ensuite tester avec des pings si on arrive bien à accéder aux deux réseaux.

Il peut nécessiter de mettre en place des règles des pare-feu.

8. DMZ

Pour la DMZ nous avons le réseau 192.168.20.0/24. Dans ce réseau se trouve le serveur eBrigade et les deux routeurs y sont connectés. Il y a une adresse virtuelle en 192.168.20.1 qui correspond à la passerelle du réseau et permet une haute disponibilité dans ce réseau.

Le but de la DMZ est que l'on puisse accéder depuis le WAN à la page web du serveur eBrigade.

Aller dans Firewall>NAT>Port Forward et créer une nouvelle redirection et modifier :

- Destination : WAN Address
- Destination port range : Other : 780
- Redirect target IP : 192.168.20.3
- Redirect target port : http

Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

Disabled ☐ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP/UDP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source [Display Advanced](#)

Destination ☐ Invert match. WAN address Type Address/mask

Destination port range Other 780 Other 780
From port Custom To port Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP Address or Alias 192.168.20.3
Type Address
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Redirect target port HTTP Port Custom

Pour sécurise là on créer une règle de pare-feu qui interdit l'accès de la DMZ au LAN.

Firewall / Rules / Edit

Edit Firewall Rule

Action Block
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.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface LAN
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol Any
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match DMZ subnets Source Address

Destination

Destination ☐ Invert match LAN subnets Destination Address

9. LIEN

https://www.it-connect.fr/tuto-vmware-workstation-lab-virtuel-pfsense/#IV_Premiere_connexion_a_linterface_dadministration_de_pfSense

<https://www.adrienfuret.fr/2017/02/28/pfsense-redondance-carp/>

<https://docs.netgate.com/pfsense/en/latest/recipes/openvpn-s2s-tls.html#create-certificate-structure>

<https://docs.netgate.com/pfsense/en/latest/recipes/openvpn-ra.html>