À envoyer à
M. Kevin Roth
Kevin.ROTH@infobureau.fr

Installation e configuration de pfSense®

Qu'est-ce que pfsense®?

pfSense® est un ***pare-feu*** et un *routeur* gratuit open source qui propose également une gestion unifiée des menaces, load balancing, multi WAN, etc.

pfSense peut être installé sur la plupart des matériels courants, y compris les vieux ordinateurs et les systèmes embarqués. pfSense est généralement configuré et exploité via une interface Web conviviale (GUI), ce qui facilite l'administration même pour les utilisateurs ayant une connaissance limitée des réseaux. Généralement, on n'a jamais besoin d'utiliser le terminal ou de modifier les fichiers de configuration pour configurer le firewall/routeur. Même les mises à jour logicielles peuvent être exécutées à partir de l'interface utilisateur Web.

Qu'est-ce qu'un pare-feu en général ? - Pourquoi avons-nous besoin de tout cela ?

Le pare-feu est un périphérique physique (mais il peut aussi être «virtuel») qui protège votre réseau d'entreprise contre les menaces externes. En termes simples, c'est un MUR contre les dangers extérieurs à votre réseau d'entreprise.

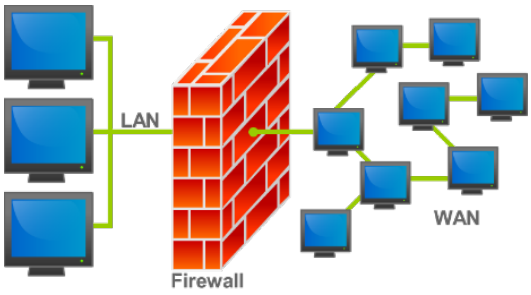


photo tirée de: www.alyfa.net

La fonction principale du pare-feu est de "stopper" les menaces externes en les empêchant de se propager aux PC de votre réseau d'entreprise, endommageant les données et les appareils,en analysant le trafic Web entrant sur votre réseau d'entreprise et en le bloquant quand et s'il est malveillant.

En règle générale, le service de pare-feu géré comprend:

Contrôle des applications - Bloquer ou limiter les applications ou fonctionnalités spécifiques pour maximiser la productivité des employés sur n'importe quel appareil.

Filtrage du contenu Web - Bloquer l'accès aux sites Web malveillants ou répréhensibles en exploitant une base de données de menaces qui classe les sites Web en fonction de leur contenu.

Grâce à un pare-feu, vous pouvez également filtrer le trafic sortant vers Internet, en créant de véritables «règles» de navigation et en bloquant l'accès aux contenus indésirables et / ou dangereux.

Retour au Sommaire

Il existe également des appareils encore plus complexes et personnalisables, donc qui offrent potentiellement plus de services, sont appelés «**Firewall géré**» , en anglais: « **Managed Firewall** »

Un pare-feu géré est un service tiers qui empêche tout accès non autorisé au réseau tout en permettant aux utilisateurs du service d'accéder à des données externes vérifiées. Le fournisseur de pare-feu géré fournit des services de détection / prévention des menaces en ligne qui minimisent le risque d'accès extérieur aux données du réseau, aux VPN, aux serveurs, aux e-mails, aux postes de travail (par exemple, les ordinateurs portables) et aux données stockées dans les portails clients du commerce électronique.

C'est un mur qui devient une PORTE
Vous êtes absent du bureau et avez besoin de récupérer un fichier enregistré sur le serveur de l'entreprise? Ou devez-vous utiliser ce programme que vous avez installé uniquement sur le PC de bureau?

C'est un mur, mais aussi un PONT
Grâce à un pare-feu, vous pouvez également connecter les réseaux de bureaux différents et distants ensemble, permettant aux utilisateurs de travailler comme s'ils se trouvaient dans un seul réseau local

Le pare-feu vous permet de travailler même lorsque vous n'êtes pas au bureau, rendant ainsi les serveurs et les PC de votre réseau d'entreprise accessibles même de l'extérieur.

Évidemment, vous pouvez agir au niveau de la sécurité pour décider quels périphériques autoriser la connexion et lesquels bloquer, mais en fait, ce sera comme si vous aviez toujours le PC de votre entreprise à portée de main.

Un pare-feu est un élément essentiel du système de sécurité de l'entreprise.
Sans cela, le réseau est exposé aux menaces. Un pare-feu empêche les forces destructrices et perturbatrices d'entrer et contrôle le trafic réseau entrant et sortant en fonction de paramètres de sécurité que peuvent être contrôlé et perfectionné.

À ce stade, il est naturel de dire que le pare-feu matériel est un dispositif très important pour la sécurité, et ce serait une bonne idée pour chaque entreprise ou professionnel d'en avoir un.

Au fil du temps, les pare-feu ont évolué et, en plus de réguler le trafic entrant et sortant, ils peuvent également:

- ✓ Réglementer les entrées VPN, c'est-à-dire gérer les connexions au bureau en toute sécurité même lorsque je suis absent;
- ✓ Effectuer une analyse antivirus du trafic de navigation, des fichiers et des e-mails avant le téléchargement;
- ✓ Effectuer des filtres Web et de contenu, c'est-à-dire bloquer le trafic vers des catégories de sites ou par exemple bloquer des applications peer to peer;
- ✓ Gérer de nombreuses autres fonctions à appliquer en fonction du cas d'utilisation.

Retour au Sommaire

Il existe de nombreux fabricants de pare-feu en plus de pfsense. Par exemple, nous pouvons évaluer les achats d'équipements: **Cisco**, **Paloalto**, **Fortinet**, **Kerio**, **Sophos**…

Chaque fabricant propose des solutions adaptées aux petites / moyennes / grandes entreprises.

Il est important de savoir qu'il existe également des pare-feu fonctionnant sur le réseau cloud.

Par exemple, les pare-feu virtuels protègent les données et applications, améliorant la microsegmentation en ajoutant une détection et une protection avancées des menaces dans les environnements VMware ESXi, Microsoft Hyper-V et KVM avec des politiques de sécurité cohérentes, une visibilité approfondie et un contrôle centralisé.

Ils peuvent protéger également uncentre de données au cloud public tout en protégeant les données et applications dans les environnements Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) et Oracle Cloud Infrastructure (OCI) avec, comme indiqué précédemment, des politiques de sécurité automatisées et cohérentes, une visibilité approfondie, et contrôle centralisé.

Voici quelques exemples de **Managed Firewall** :

Retour au Sommaire

SOMMAIRE

Chapitre porte

Dans les pages suivantes, la procédure étape par étape pour configurer les fonctions décrites ci-dessus sera expliquée avec une explication d'accompagnement :

Dans ce tutoriel, nous utiliserons trois machines virtuelles:
• Une machine agira en tant que «client PC» (Win 10 vers.20H2)
• Une autre machine agira en tant que «Serveur [ad ds,dns]» (Win Server 2019 vers 1809)
• Une autre machine agira en tant que «Firewall» (PfSense 2.4.5 p1)

Il sera possible de récupérer toutes **les images** en haute résolution en cliquant ici ou s'il s'agit d'une version imprimée, au lien suivant: https://drive.google.com/drive/u/5/folders/19jDoq29RcYz5FWwdADRSE42P4Jn6dyu6

Il sera possible de récupérer une **vidéo** expliquant l'installation sur pfsense à ce lien. Ou s'il s'agit d'une version imprimée, au lien suivant : https://www.youtube.com/watch?v=MgZM7b_7Wyg&feature=youtu.be

pfSense Documentation : https://docs.netgate.com/pfsense/en/latest/

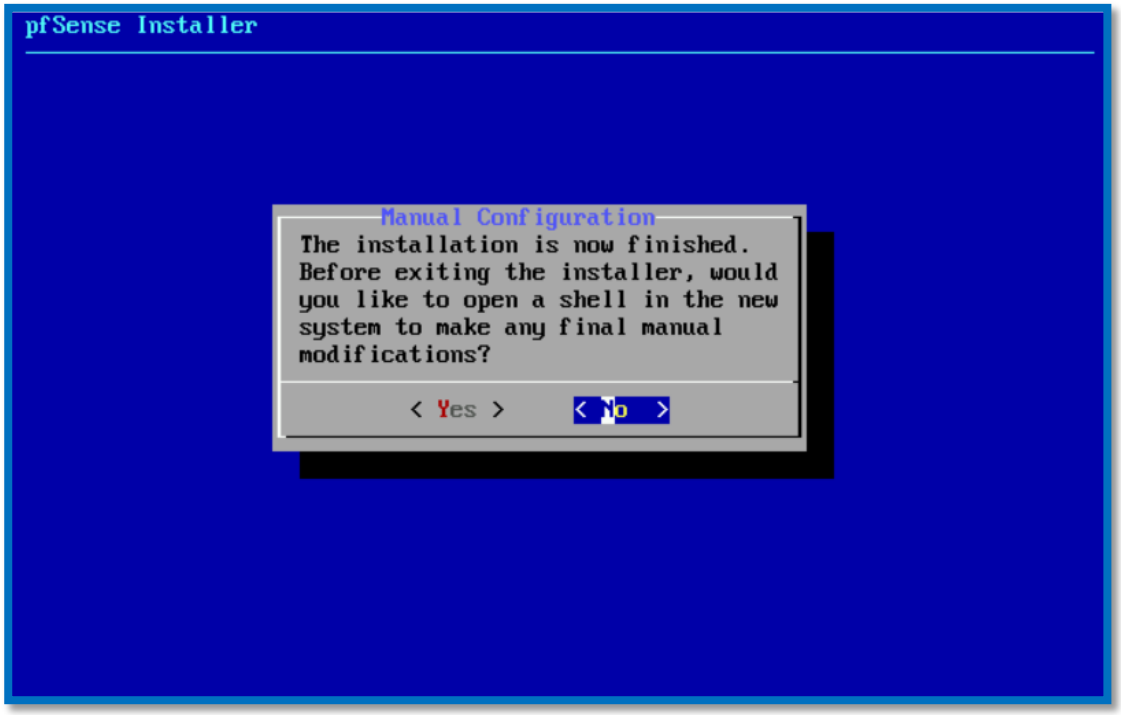
Raccourci	Explication
Firewall	Para-feu
WAN	Wide area network - Réseau étendu
LAN	Local area network - Réseau local
GUI	Graphics user interface – Interface graphique
Troubleshooting	Aide au dépannage
Subnet mask	Passerelle par défaut
CMD	Command prompt - invite de commandes
Adresse MAC	Media Access Control - adresse physique d’un périphérique réseau

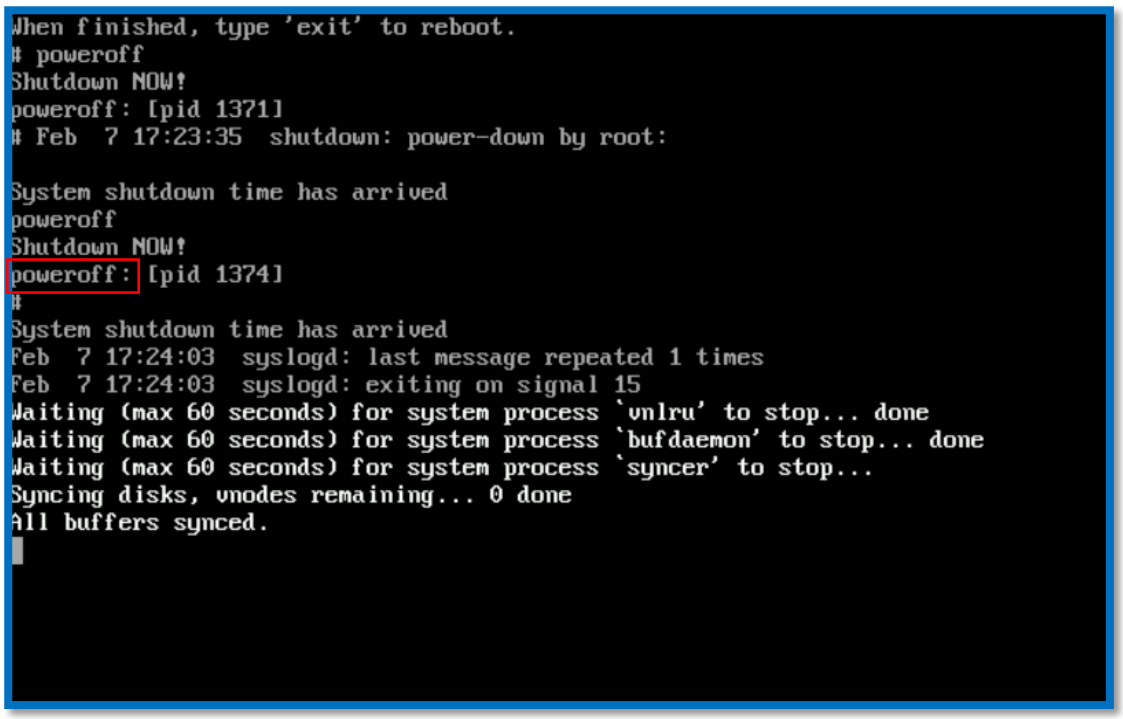
Retour au Sommaire

Conseils d'installation PfSense

À l'heure actuelle où ce guide a été écrit, pfSense n'adore pas le système de démarrage UEFI (firmware basé sur UEFI), il sera donc nécessaire de mettre en place un système de démarrage classique (comme MBR, Master Boot Record)

Lorsque l'installation de pfSense est terminée, entrez dans le shell et exécutez la commande "***poweroff***" pour que le système s'éteigne. Ce faisant, nous aurons la possibilité de supprimer/ejecter notre support d'installation et de redémarrer la machine, puis de poursuivre la configuration avec un redémarrage.





Retour au Sommaire

Configuration initiale sur la ligne de commande de PfSense

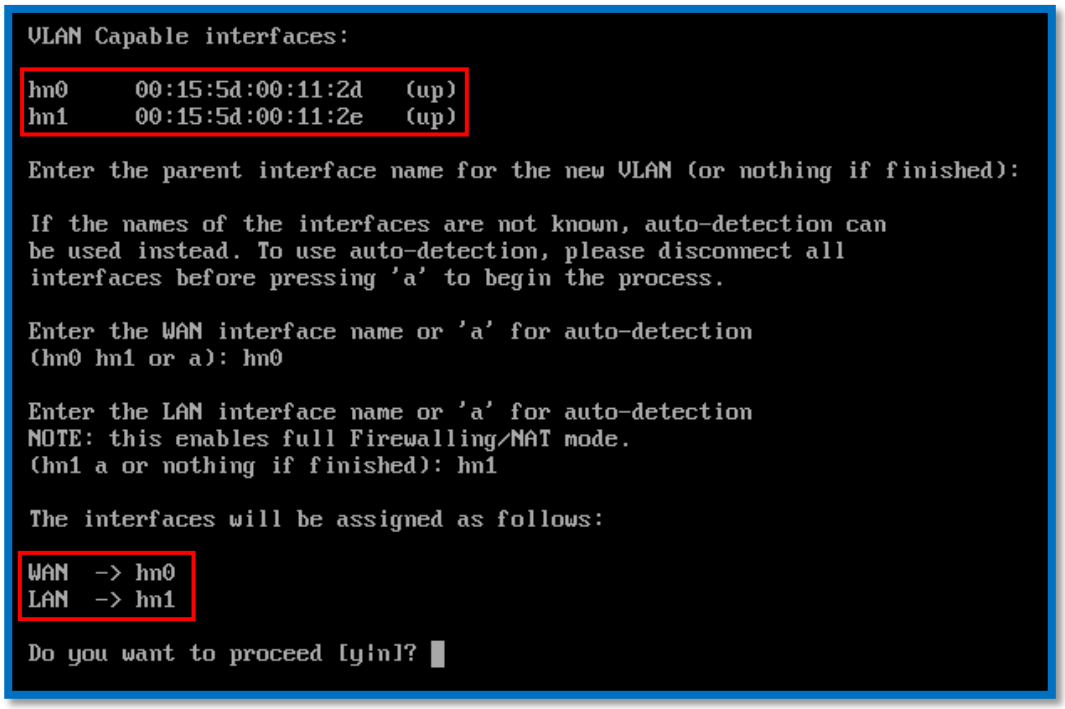
A la fin de l'installation, le wizard nous invitera à insérer (dans notre cas avec seulement deux cartes réseau disponibles) quelle carte réseau définir comme ***WAN*** et comme ***LAN***.

Rappelles toi: WAN c'est le réseau étendu (internet), LAN c'est le réseau local.

Bien sûr, nous pouvons avoir différents *WAN* et différents *LAN*, nous allons donc les configurer en conséquence.

Ensuite, nous allons entrer via les commandes "hn0, hn1" (et / ou autres dans le cas d'autres cartes réseau de notre machine) pour définir le (ou les) WAN et LAN.

Dans ce cas, notre WAN (dans ce cas hn0) sera le réseau public, donc le réseau auquel nous nous connecterons pour nous connecter à Internet, tandis que le LAN (dans ce cas hn1) sera notre réseau local



Après avoir configuré hn0, hn1 et / ou d'autres cartes réseau, nous pouvons confirmer les paramètres qui viennent d'être définis pour nous retrouver dans ce menu.

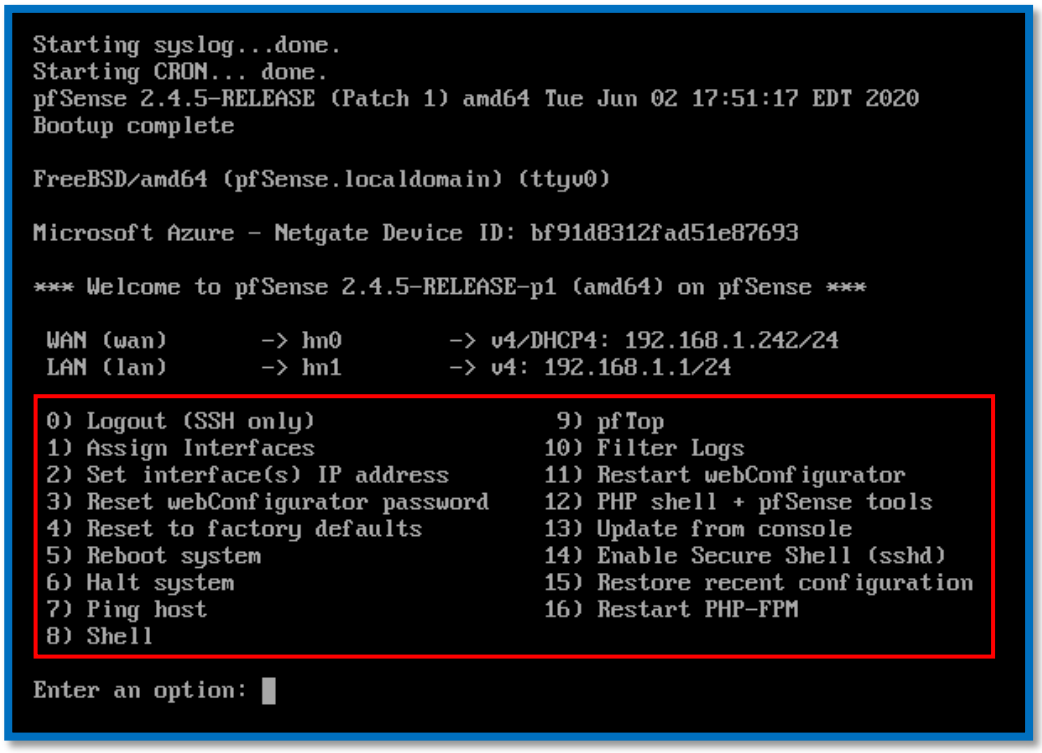
Petit astuce:
Pour comprendre de quelles cartes réseau il s'agit, il suffira de vérifier l'adresse MAC, puis d'identifier les cartes réseau afin de faire la bonne configuration.

Retour au Sommaire

C'est possible de voir sur cette capture d'écran, toute la liste des adresses IP associées à chaque carte réseau (il est possible de ne voir aucune adresse IP en cas d'erreurs ou en cas de modifications à la volée (on the fly)

Depuis cet écran, comme vous pouvez le voir, vous pouvez effectuer diverses opérations :

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



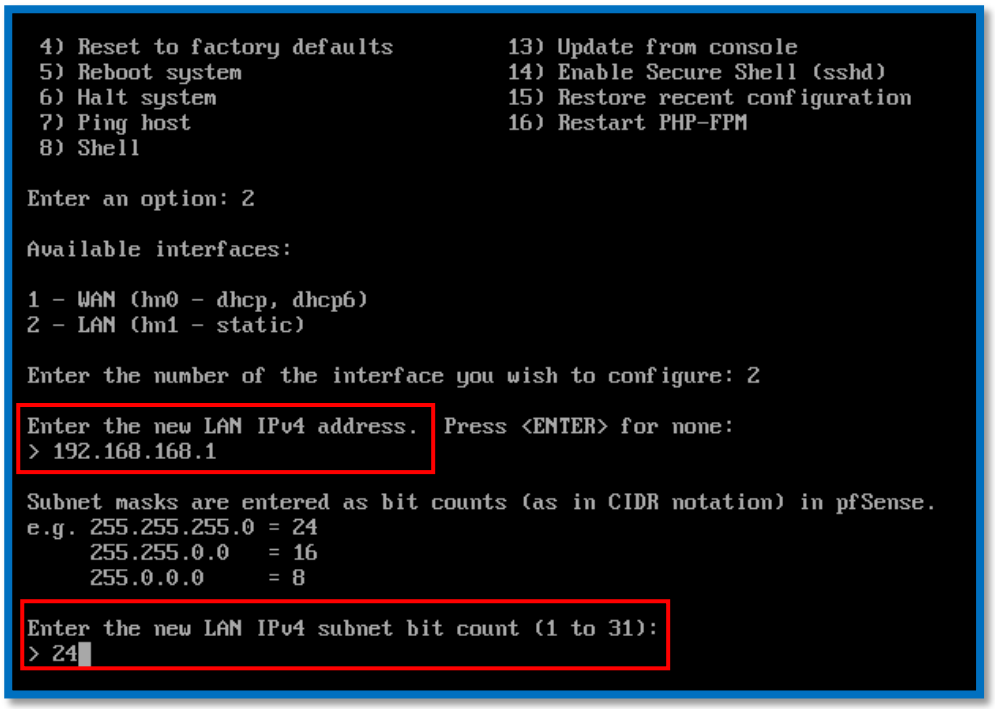
Dans ce cas précis, le dhcp (*hn0*) a été configuré dans le WAN, et une adresse IP statique (*hn1*)dans le LAN

Retour au Sommaire

Il sera donc nécessaire de définir une adresse IP fixe pour le LAN de manière à toujours disposer d'une adresse physique pour accéder au pare-feu.

Il est généralement recommandé de saisir l'adresse IP du pare-feu avec le dernier octet ".***254***".
puis, par exemple, avec le formulaire suivant : "*192.168.10.**254*** ".
(cit. M. Kevin Roth).

Dans ce cas, écrir "2" (ainsi option 2) (Set Interfaces IP address)
La prochaine commande à écrire sera l'adresse IP fixe que nous voulons avoir pour entrer dans l'interface graphique (GUI) de pfsense. Puis en insérant la subnet mask immédiatement après (in CIDR notation), donc 24 pour la subnet mask « 255.255.255.0 »



Si l'adresse WAN a été bien configurée, nous devrions pouvoir accéder à l'interface graphique sans problème, simplement en écrivant l'adresse IP du serveur dans la barre d'adresse du navigateur.

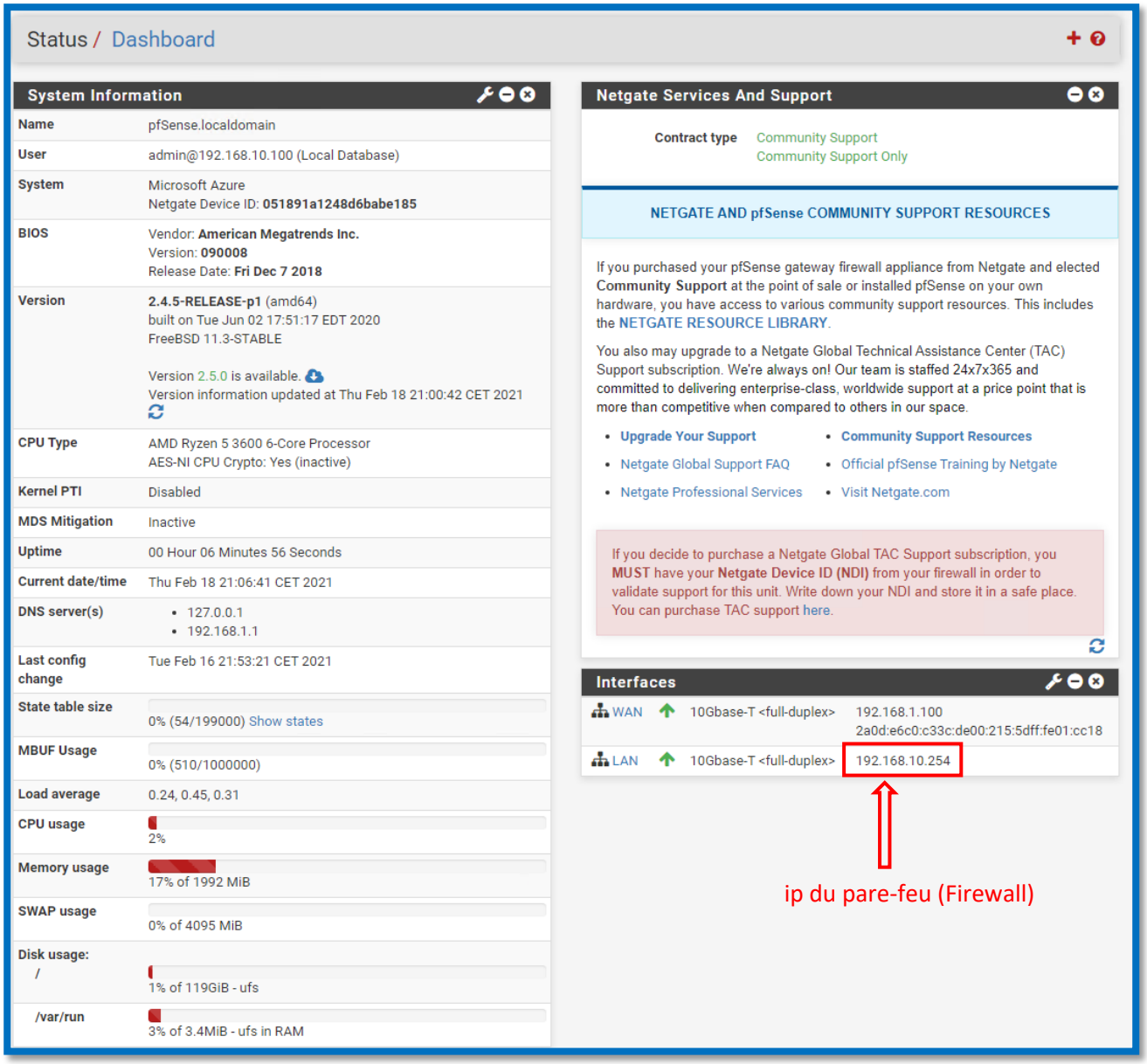
Si tout a été bien configuré depuis le début, en supposant qu'il existe une connexion Internet fonctionnelle du côté WAN, puis en définissant également l'adresse de la passerelle sur la machine cible, la connexion Internet devrait fonctionner parfaitement. (sur la version PfSense 2.4.5 p1)

Retour au Sommaire

Configuration pfsense

***Username (ID par défaut)* : admin**
***Password (Mot de passe par défaut)* : pfsense**

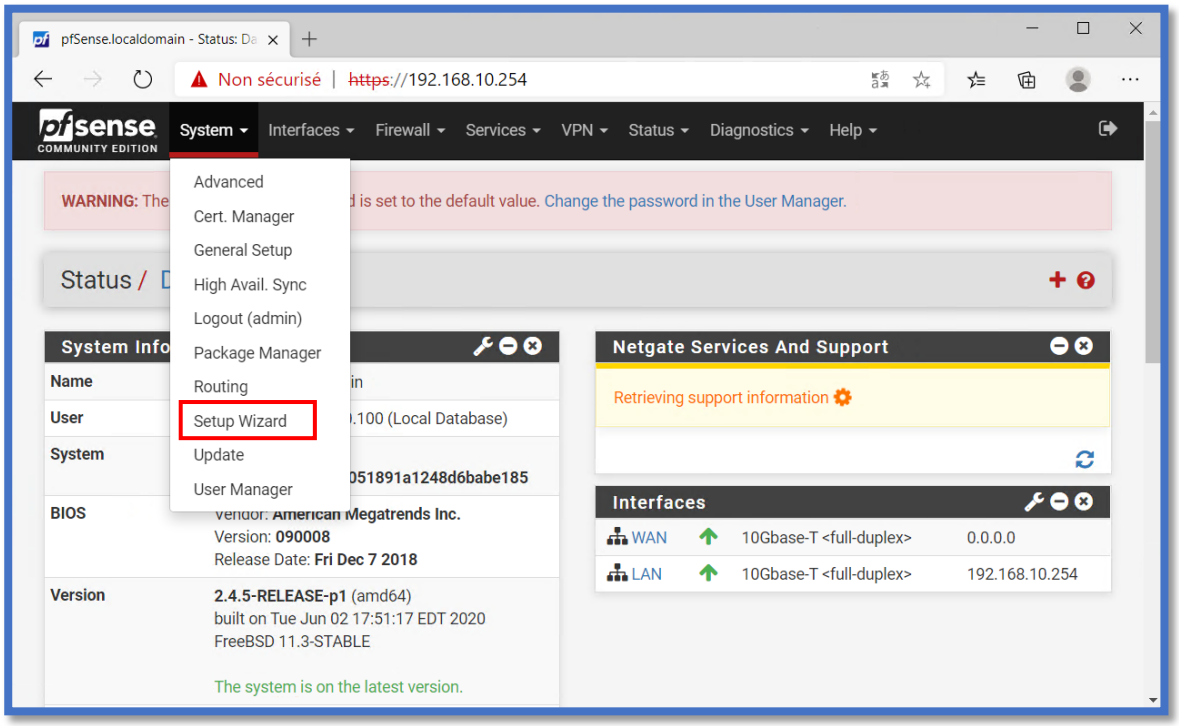
A partir de cet écran, vous pouvez voir la page d'accueil de l'interface graphique pfsense (GUI)



Si tout a été bien configuré, au moins sur la version actuelle de pfsense (PfSense 2.4.5 p1), en entrant ainsi l'adresse pfsense comme **passerelle par defaut (gateway),** la connexion Internet devrait fonctionner correctement.

Retour au Sommaire

Au début immédiatement après la connexion, (log in) vous pouvez faire une courte configuration. Si vous l'avez sauté par erreur, vous pouvez refaire la configuration en cliquant sur "***Setup Wizard***"



Avertissement!: *Il est fortement recommandé, pour des raisons évidentes de sécurité, de changer le mot de passe le plus rapidement possible.*

Ensuite, vous pouvez aller configurer (via la procédure ci-dessus) des paramètres de base, voici les plus utilisés:

General Information: Hostname, Domain, Primary/Secondaty DNS Server
Time Server Information: Time server hostname, Timezone
Wan Interface Type, Mac address of the WAN, MTU, MSS
Static IP configuration, DHCP Client configuration, PPOE/PPTP Configuration
Configuration LAN Interface: LAN IP address, subnet mask
WebGUI Password

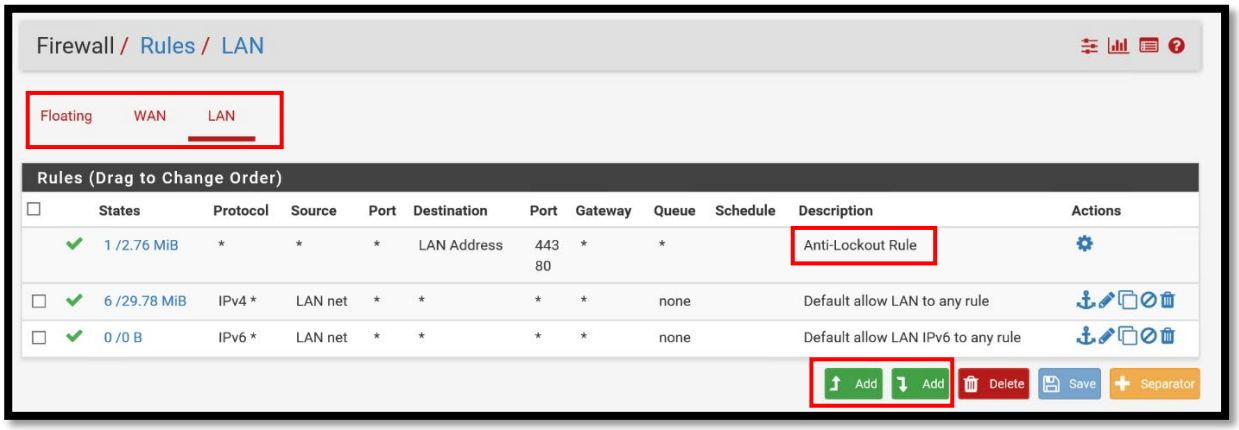
La page principale peut être personnalisable mais il est bon / utile d'avoir des informations dans un seul écran qui peuvent être intéressantes à première vue. Par exemple:

- La version pfsense actuellement utilisée et la version mise à jour téléchargeable via un lien direct.
- Uptime : *utile pour savoir s'il y a eu un redémarrage, puis un problème.*
- DNS Server
- Dernière configuration modifiée
- Load average : utile pour connaître immédiatement les ressources utilisées
- CPU usage : utile pour connaître immédiatement les ressources utilisées
- Memory usage : utile pour connaître immédiatement les ressources utilisées
- Disk usage : utile pour connaître immédiatement les ressources utilisées
- Interfaces : WAN et LAN : utile pour savoir immédiatement s'il y a des problèmes à ce niveau

Retour au Sommaire

Ajouter des regles de blocage et ouverure - LAN > WAN

Pour bloquer certains, ports dans ipv4 / ipv6, il est nécessaire de aller sur la section Firewall, plus précisément dans la section : "***Firewall / Rules*** ". Dans ce cas, nous allons configurer les règles dans la section LAN, puis dans la section " ***Firewall / Rules / LAN*** ".



Ainsi, une fois que vous avez accédé à la fenêtre susmentionnée, vous pouvez ajouter de nouvelles règles.

Comme vous pouvez le voir sur la capture d'écran ci-dessus, il est déjà possible d'avoir un aperçu des règles de base déjà présentes dans le pare-feu.

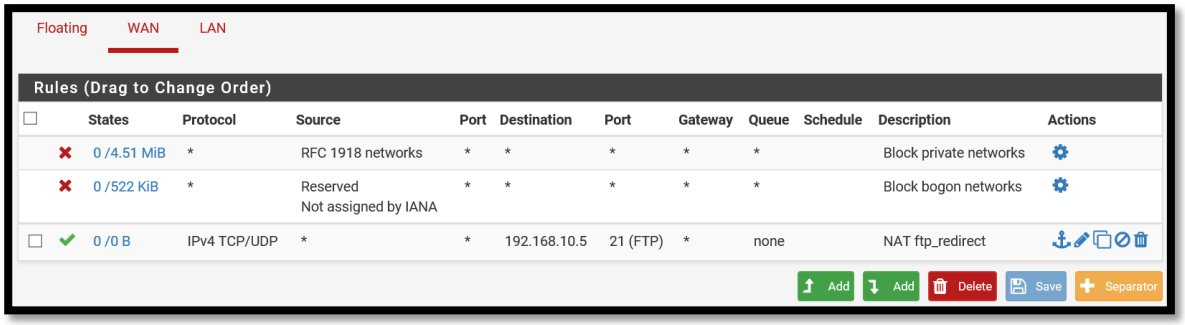
Évidemment, il est également possible de supprimer les règles existantes à l'exception de la principale "***Anti-Lockout Rule***" qui empêche l'utilisateur de déranger / refuser l'accès à l'interface graphique (GUI) du pare-feu en question par erreur. Fondamentalement c'est une activation de la port 80 et 443 côté LAN. Ceci est configurable sur la page ‘’*System* > *Advanced*‘’ page sous : ‘’*Anti-lockout*‘’.

Par défaut, tout le trafic du LAN peut se dérouler sans problème. (*Default allow to any rule*) à la fois en ipv4 et en ipv6 (donc avec deux règles distinctes et séparées).

Pour ajouter des règles il faut donc cliquer sur le bouton "***Add***".
Il est donc possible de remarquer qu'il existe deux boutons « *Add* » distincts et séparés.

Le bouton avec la flèche pointant vers le haut injecte la règle en position haute, tandis que le bouton avec la flèche vers le bas insère la règle dans la position ci-dessous, pour une question de "*priorité*".

Partie WAN

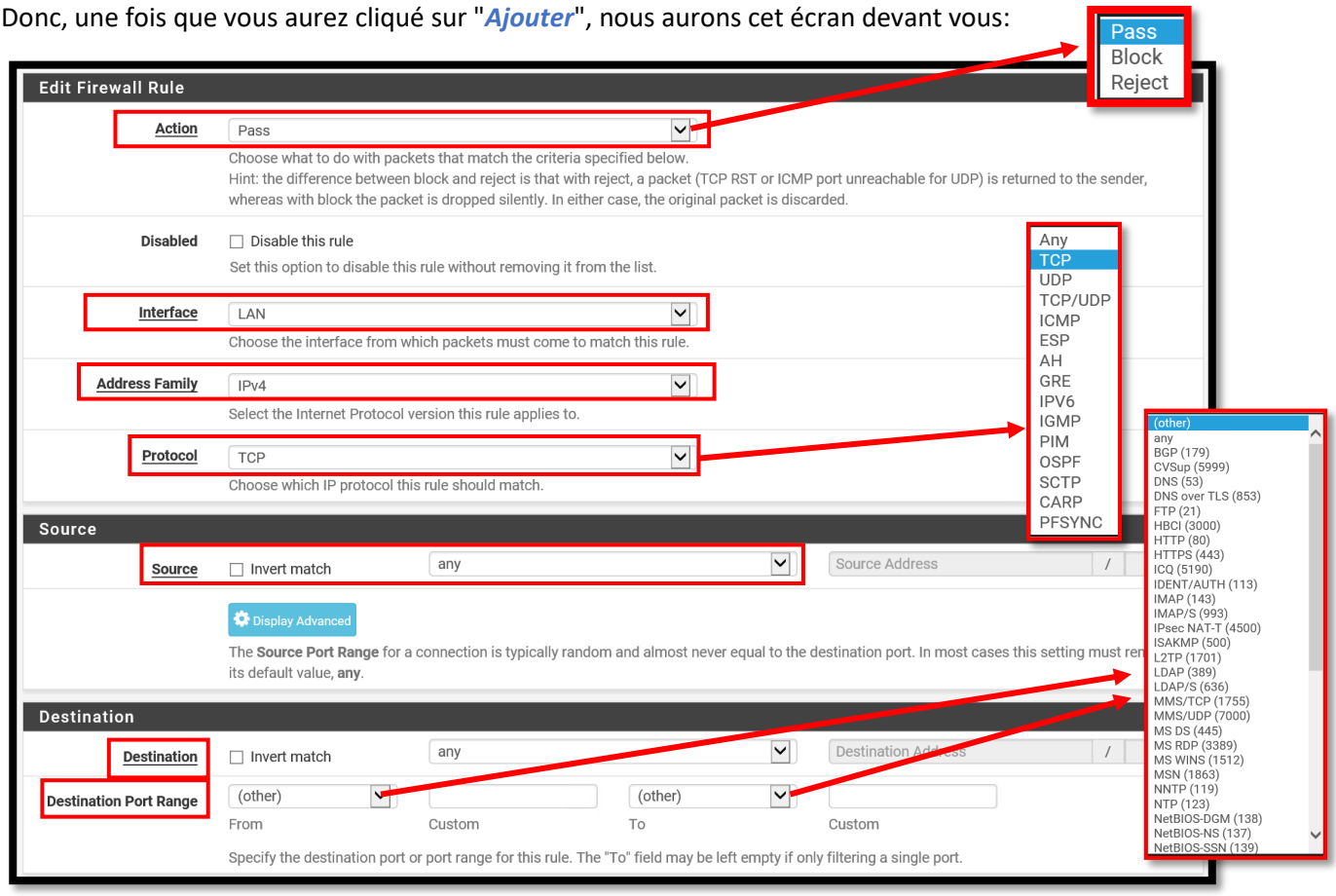


Du côté WAN, cependant, il y a, encore une fois par défaut, deux blocs.
Le premier (ayant comme source, RFC1918 Network) évite l'accès au routeur côté WAN
Le deuxième il y a pour bloquer le trafic malveillant ou un sous-réseau inutilisé qui a été détourné pour une utilisation malveillante. Par conséquent, les listes Bogon sont destinées à filtrer le trafic « invalide » sur Internet.

Esthétiquement parlant, il est également possible d'ajouter des «Separator» afin d'avoir une section «Rules» plus claire et plus compréhensible.

Retour au Sommaire

Donc, une fois que vous aurez cliqué sur "***Ajouter***", nous aurons cet écran devant vous:



Nous avons donc trois options dans le champ "***Action***",: « ***Pass, Block et Reject.*** ». A partir de ce menu, il est donc possible d'insérer des règles de verrouillage ou d'ouverture. Après cela, nous avons d'autres options alors:

Rappelles toi

Pass : La règle autorise les paramètres sélectionnés
Block : La règle bloque les paramètres définis, mais le paquet est abandonné et rien n'est renvoyé au programme/système d'envoi. Ainsi, un attaquant ne peut pas savoir s'il a déjà atteint sa destination ou un pare-feu.
Reject : La règle reject les paramètres définis, ainsi une réponse est renvoyée au programme/système émetteur lui indiquant que le "paquet a été abandonné". Dans la plupart des cas, Reject est plus utilisé lors du dépannage, pour voir ce qui se passe réellement, vous pouvez utiliser Reject pour dépanner votre règle et pour voir ce qui se passe, puis vous pouvez le remplacer par un bloc pour minimiser le trafic sur le réseau.

- **Interface**: L'interface sur laquelle appliquer la règle. (LAN ou WAN)
- **Address Family** : Sélectionnez le protocole Internet auquel la règle sera appliquée (ipv4, ipv6, ipv4+ipv6)
- **Protocol:** Le type de protocole: TCP, UDP, TCP/UPD, ICMP, ESP,AH,GRE,IPV6,IGMP,PIM et plus..
- **Source**: D'où vient le trafic et où va le trafic. (Des fonctions avancées sont également disponibles)
- **Destination** : Si vous le souhaitez, pfsesne a déjà une liste de certains ports prêts.
  Dans les options supplémentaires, il est possible d'enregistrer le paquet de cette règle ou non.
- **Destination Port Range** : il est possible d'indiquer la destination du port d'entrée et de sortie. Il est donc possible via le menu de spécifier un port prédéfini (DNS, DNS sur TLS, HTTP, HTTPS, LDAP, IMAP, POP3, RADIUS, SSH et plus ..).
  À partir de ce menu, il est possible de sélectionner une plage de ports précédemment définie dans le menu « Pare-feu / Alias / IP ».
  Ce qui facilite en fait l'insertion d'une plage de portes, beaucoup plus ordonnées, qui autrement impliquerait la création de plus de règles, donc de plus de lignes.
- **Log** : Indiquez si vous souhaitez que le pare-feu gère les paquets de journaux
- **Description** : Vous pouvez saisir une brève description de la règle (maximum 52 caractères).
- **Advanced Options** : Des options avancées sont également disponibles, avec des paramètres spécifiques tels que: « source OS », « Diffserv Code Point », « Tag », « Tagged », « VLAN Prio/Set » et plus..

Retour au Sommaire

Il est donc évident de préciser qu'une règle qui doit agir du LAN vers le WAN (*LAN>WAN*) doit avoir comme "*Source*" "*LAN Net*" et comme "*Destination*" "*Wan Net*" avec le port specifiée en entrée et en sortie (ou une plage/range des ports spécifiée auparavant).

Dans ce cas, l'interface en question doit être du côté "*LAN*", "l'Adress Family" et le "*Protocol*" doit être spécifiée en fonction du protocole que nous voulons bloquer ou ouvrir.

Rappelez-vous: le positionnement des règles est important et suit une règle de priorité précise. Le pare-feu voit et traite en effet les règles en fonction de leur position dans la liste. Si en amont nous avons une règle qui ouvre tout, le pare-feu lui donnera la priorité et non les autres règles immédiatement après.

Dans l'exemple ci-dessous, par exemple, nous pouvons voir que (en plus de la règle par défaut que nous avons vue précédemment) une règle de blocage sur des ports spécifiques a été insérée immédiatement après (dans ce cas la liste "***custom_port***" a été définie). Ainsi, le pare-feu verra tout d'abord la deuxième règle qui spécifie que sur la plage de ports personnalisée de Wan à Lan, il y a une règle «***Pass***» (icône verte gauche) sur Address_family ipv4 + ipv6 sur le protocole TCP / UDP.

La troisième règle est à la place une règle "Block" (fonctionnant toujours du Wan au LAN) fonctionnant en Ipv4 + ipv6 sur n'importe quel port.

Ainsi, le système traitera d'abord la première règle, ouvrant ainsi les ports indiqués, après quoi, si aucun de ces ports n'est pris en compte, il passera à la règle suivante qui refuse effectivement tout accès.

Règle d'ouverture

Règle de blocage

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓	2 /2.62 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙
✓	0 /0 B	IPv4+6 TCP/UDP	LAN net	*	WAN net	custom_port	*	none			⚓ ✎ ⧉ ⊘ 🗑
✗	0 /0 B	IPv4+6 *	LAN net	*	WAN net	*	*	none			⚓ ✎ ⧉ ⊘ 🗑
✓	2 /2.26 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	⚓ ✎ ⧉ ⊘ 🗑
✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	⚓ ✎ ⧉ ⊘ 🗑

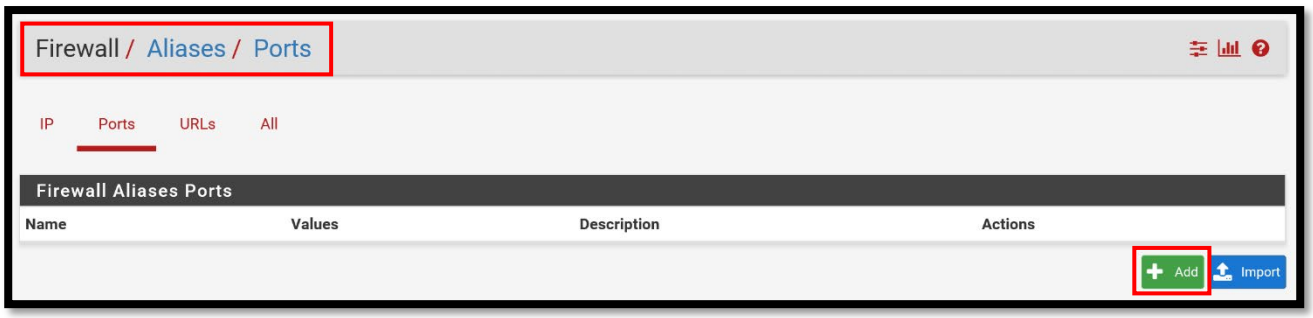
Add | Add | Delete | Save | Separator

Retour au Sommaire

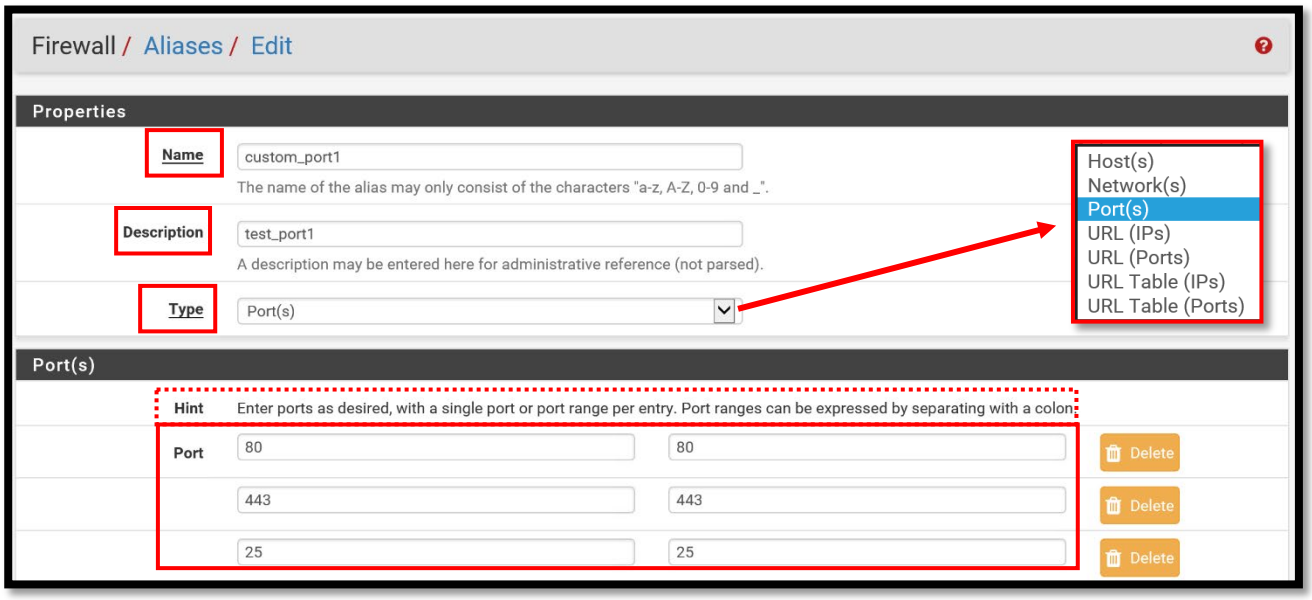
Comment créer des listes de portes (paragraphe bonus)

Comme spécifié précédemment, il est possible de créer des listes de ports à placer ultérieurement dans les règles de notre pare-feu afin d'avoir une liste propre et efficace.

Il faut donc se rendre dans la section "Pare-feu / Alias / Ports" où apparaîtra l'interface graphique (GUI) suivante :



Ensuite, vous devez cliquer sur le bouton "**Ajouter**" pour accéder à la section souhaitée.
Nous nous retrouverons donc dans la section suivante:



Nous pouvons voir sur l'image ci-dessus qu'il est possible de donner un nom personnalisé à notre range de ports, une brève description et évidemment le type (dans notre cas on va insérer des ports mais il est aussi possible d'ajouter une plage d'adresses IP, d'URL , etc.).

Il est donc possible d'ajouter les ports paramétrés sous forme de ports uniques spécifiques comme dans la capture d'écran ci-dessus (80-80) ou sous forme de « range » (par exemple du port 2000 au port 2100 il faut simplement mettre 2000 sur la section à gauche et 2100 à la section à droite)

N'oubliez pas: n'oubliez pas de sauvegarder vos modifications! Afin d'éviter que le travail effectué précédemment ne part en fumée.

Retour au Sommaire

Créer une règle de redirection de port, WAN>LAN (Port Forwarding)

Lorsque l'on parle de redirection de port, le terme anglais correspondant est: '' ***port forwarding*** ''.

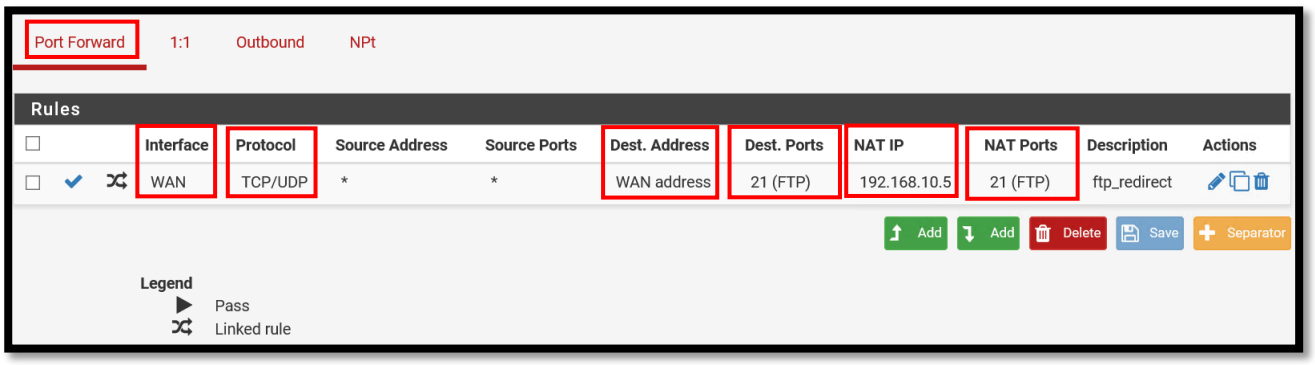
Les règles NAT vous permettent de traduire une adresse IP publique en une adresse IP privée un port de l'extérieur vers l'intérieur, par exemple pour la publication d'un serveur Web.

Donc dans ce cas ci-dessous, nous allons configurer une règle de redirection de port pour accéder à notre serveur AD via FTP, Ainsi, notre serveur sera accessible via notre pare-feu.

On va donc dresser le flux sur les ports FTP (21) vers l'adresse (locale) de notre serveur AD, toujours sur le port 21, Par conséquent, côté WAN on utilisera toujours le même port (21, par défaut).

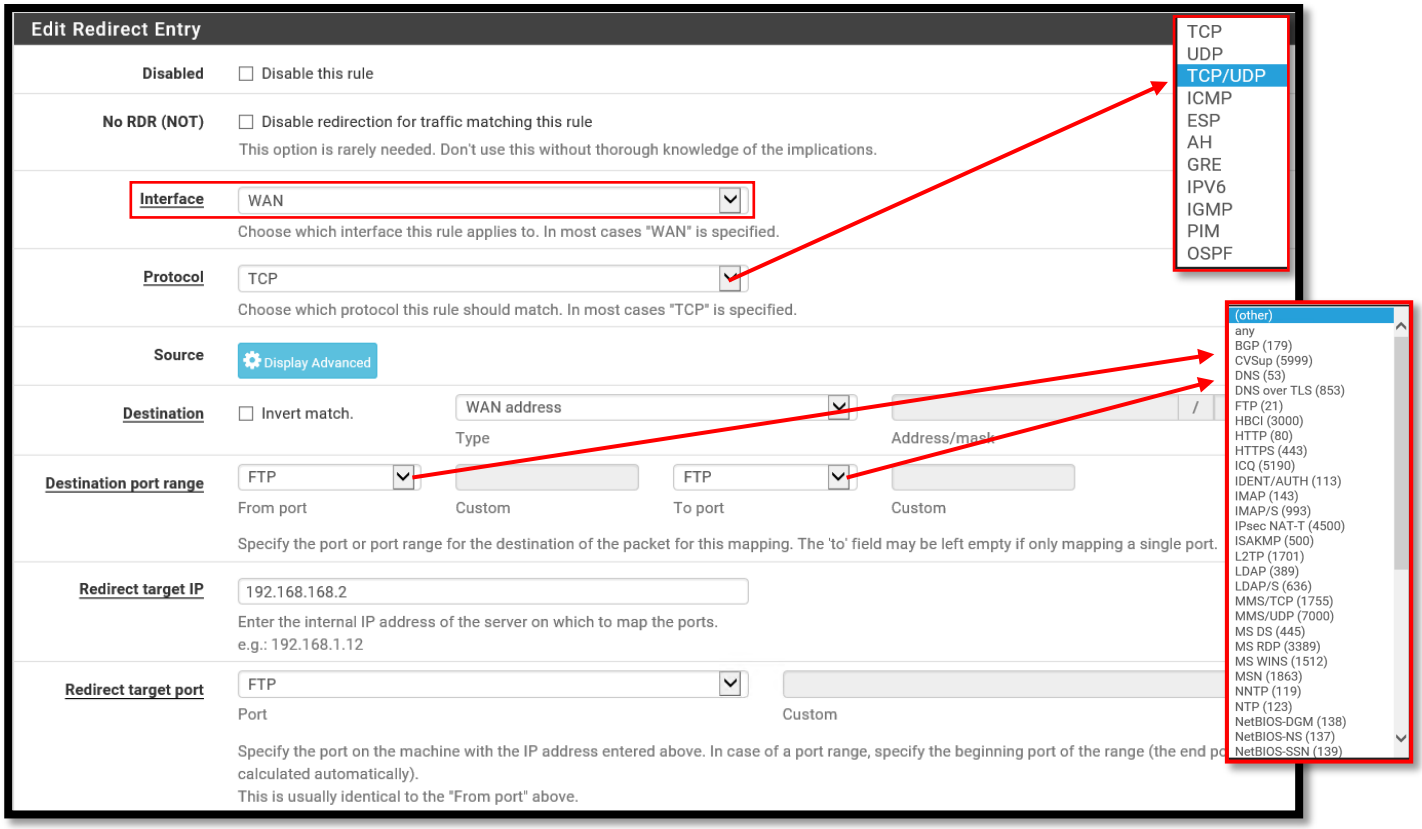
Autrement dit, une requête envoyée sur l'adresse IP WAN du pfSense, sur le port 21 soir automatiquement redirigée vers l'adresse IP **192.168.168.2** sur le port **21**.

Il faut donc aller dans l'interface graphique suivante: ''***Firewall / NAT***./ Port Forward''



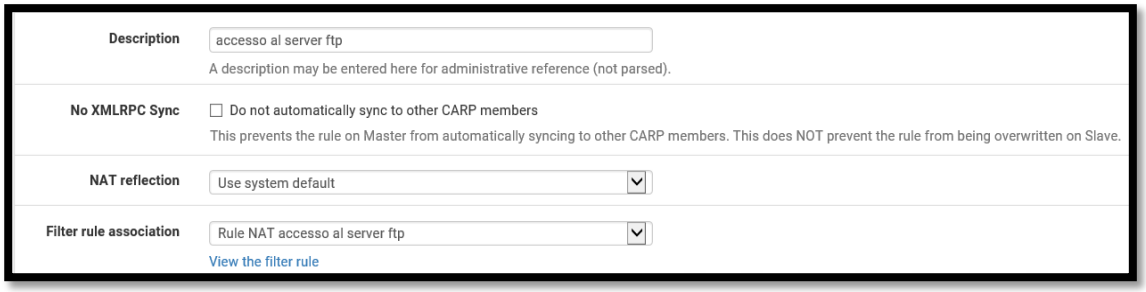
Puis cliquez sur le bouton "***Add***", (si c'est la première règle, il n'y a pas d'importance entre les deux boutons "Add"), en effet lorsque il y a plusieurs règles, l'ordre pourra avoir son importance.
Donc nous aurions cet écran devant nous :

Retour au Sommaire



Voici donc la GUI de configuration:

- **Interface**: vous pouvez choisir entre ‘’WAN‘’ et ‘’LAN‘’. Dans notre cas, ce sera ‘’***WAN”***. Car la requête du poste client va à l'interface ‘’WAN‘’ du pare-feu en question (pfSense).
- **Destination**: dans notre cas ce sera: "***WAN Address***", car le client va envoyer sa requête sur adresse IP (public) ‘’WAN‘’ de pfSense.
- **Destination port range**: ‘’21‘’ (FTP), donc ce soir du port ‘’21‘’ au port ‘’21‘’. Dans ce cas, nous n'avons donc pas besoin d'une plage/range de ports.
- **Protocol**: le protocole ‘’FTP‘’ utilise des connexions ‘’TCP‘’ séparées pour transférer les données et contrôler les transferts.
- **Redirect target:** IP: ‘’192.168.168.2’’, car c'est l'adresse IP du serveur cible (notre serveur AD)
- **Redirect target port**: ‘’FTP‘’, car il s'agit d'un flux ‘’FTP‘’ sur le port par défaut.
- **Description**: indiquez une description pour décrire l'usage de cette règle. Cela peut être très important au cas où plusieurs sys admin auraient accès au pare-feu, pour des raisons évidentes.
- **Nat reflection:** fait référence à la possibilité d'accéder à des services externes à partir du réseau interne en utilisant l'adresse IP externe (généralement ip publique).



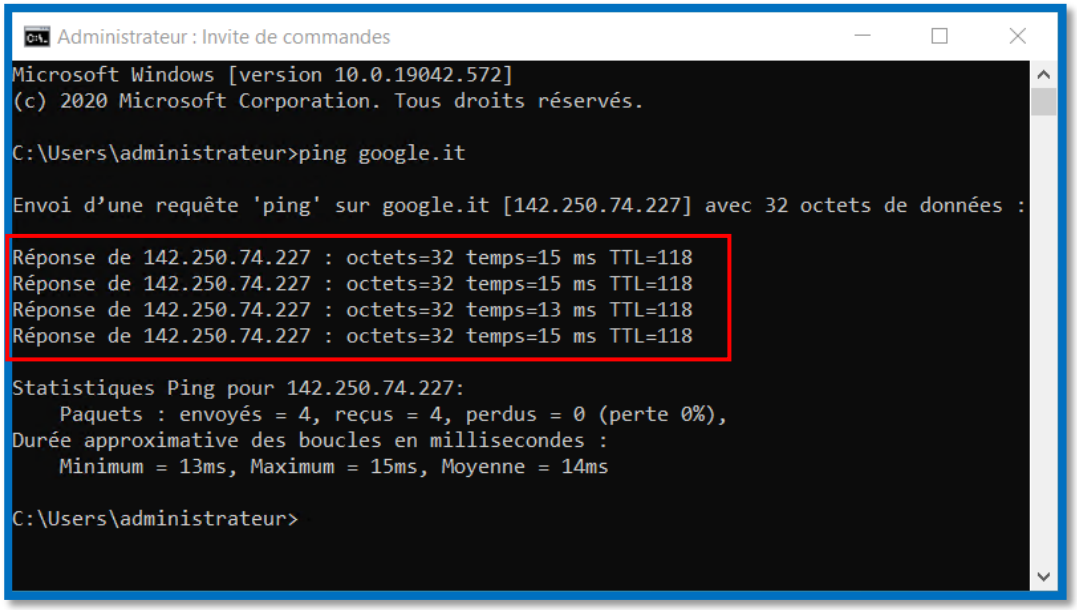
Retour au Sommaire

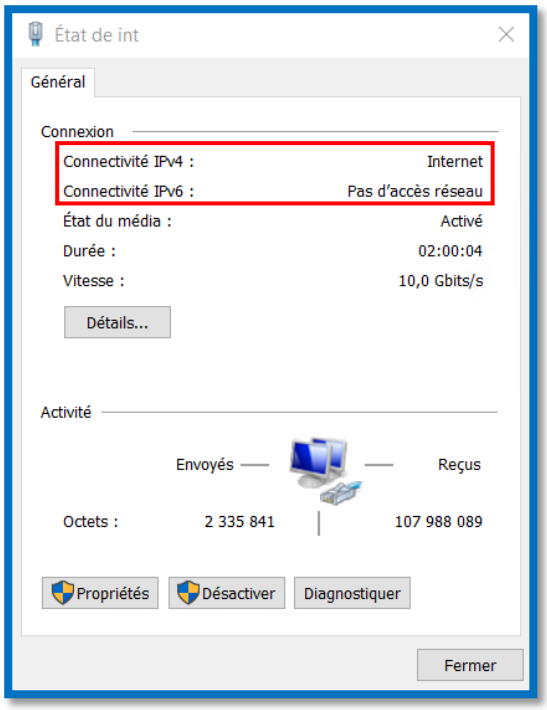
Vérifier la connexion à internet

Vous pouvez voir que la connexion Internet fonctionne en l'envoyant à partir de un « ping » via Vou en cliquant sur la carte réseau cible sur:
Panneau de configuration \ Tous les Panneaux de configuration \ Centre Réseau et partage

Il est possible aussi d'avoir une confirmation visuelle instantanée (à l'oeil nu) grâce à la petite icône en bas à droite > 🖵

Trivialement, vous pouvez vérifier la connexion simplement en ouvrant le navigateur et en essayant d'ouvrir une page Web aléatoire.





Retour au Sommaire

Troubleshooting (Dépannage de la connectivité réseau)

La liste suivante couvre presque toutes les causes d'échec de la connectivité sortante dans les scénarios d'utilisation courants. Chaque test suppose que les éléments ci-dessus ont été vérifiés.

Interface WAN

- Vérifiez que l'adresse IP WAN est correcte (Interfaces> WAN).
  L'utilisation d'une adresse incorrecte pourrait entraîner l'échec du FAI à fournir le trafic vers depuis le pare-feu, entre autres problèmes.
- Vérifiez que l'adresse IP WAN a le masque de sous-réseau correct (Interfaces> WAN)
  Un masque de sous-réseau incorrect tel que / 1 pourrait causer des problèmes de connectivité à de grandes parties d'Internet, l'utilisation de / 32 pour un masque peut empêcher la découverte / l'utilisation de la passerelle.
- Vérifiez que le WAN a une passerelle et que l'adresse IP de la passerelle est correcte (Interfaces> WAN.
  Cela interférera avec le NAT sortant automatique et la gestion de la route vers / de la répons.
- Vérifiez que la passerelle WAN est définie par défaut (Système> Routage
  Sans passerelle par défaut, le trafic n'a pas de chemin de sorti.
- Vérifiez que la passerelle WAN affiche en ligne (état> passerelles).
  Si ce n'est pas le cas, vérifiez les paramètres WAN et les paramètres de passerelle ou utilisez une autre adresse IP de moniteur.
- Vérifiez que la passerelle WAN définie est réellement la passerelle par défaut (Diagnostics> Routes)
  Une autre source telle qu'un VPN peut avoir changé la passerelle par défaut.

Interface LAN

- Vérifiez que l'adresse IP du LAN est correcte (Interfaces> LAN)
  L'utilisation d'une adresse IP non valide (par exemple .0 ou .255 dans un / 24) entraînera des problèmes pour atteindre les adresses localement et ne fonctionnera pas correctement.
- Vérifiez que le masque de sous-réseau LAN est correct (Interfaces> LAN)
  L'utilisation d'un masque de sous-réseau incorrect, tel que / 32, empêchera les autres hôtes du LAN de trouver le LAN à utiliser comme passerelle et vice versa.
- Vérifiez que le LAN n'a PAS de passerelle définie (Interfaces> LAN)
  Cela interférera avec le NAT sortant automatique.
- Vérifiez que le LAN n'a PAS défini "Bloquer les réseaux privés" (Interfaces> LAN
- Vérifiez que le LAN n'a PAS défini «Bloquer les réseaux Bogon» (Interfaces> LAN)
  Voir au dessus.

Retour au Sommaire

Pare-feu / règles

- Vérifiez le journal du pare-feu pour les connexions bloquées à partir du réseau local (État> Journaux système, onglet Pare-feu)
  Si des blocages sont observés, vérifiez la règle qui a bloqué et ajustez les règles en conséquence (Pare-feu> Règles, onglet LAN)
- Vérifiez que la règle LAN autorise tous les protocoles, ou au moins les ports TCP et UDP, à atteindre DNS et HTTP / HTTPS, et autorise ICMP à effectuer des tests. (Pare-feu> Règles, onglet LAN)
  Ne pas autoriser UDP ferait échouer le DNS, entre autres. De même, sur une règle DNS, l'utilisation d'UDP uniquement et non de TCP / UDP entraînera l'échec des requêtes plus volumineuses.
  Ne pas autoriser ICMP entraînerait l'échec du ping, mais d'autres protocoles peuvent fonctionner
  Ne pas autoriser TCP entraînerait l'échec de HTTP, HTTPS et d'autres protocoles.
- Vérifiez que la règle LAN autorise une destination de tout (Pare-feu> Règles, onglet LAN)
  Le trafic destiné à Internet nécessitera une destination «toute». L'utilisation d'une mauvaise destination ne permettrait pas au trafic d'atteindre Internet (par exemple, "réseau WAN" qui n'est que le sous-réseau de l'interface WAN, PAS Internet.)
- Vérifiez que la règle LAN n'a pas de passerelle incorrecte (Pare-feu> Règles, onglet LAN)
  S'il est configuré pour quitter par une autre passerelle non WAN (éventuellement cassée), les connexions échoueront.

NAT sortant

- Vérifiez le NAT sortant, assurez-vous qu'il est défini pour NAT sortant automatique sauf si Manuel est requis (Pare-feu> NAT, onglet Sortant).
  Des paramètres NAT incorrects empêcheront le trafic d'atteindre le WAN.
- Vérifiez les règles NAT sortantes manuelles, si elles sont utilisées, pour vous assurer que la source du trafic local correspond.
  Des paramètres NAT incorrects empêcheront le trafic d'atteindre le WAN

Tests diagnostiques

- Vérifiez la connectivité depuis le pare-feu lui-même: essayez d'envoyer un ping à 8.8.8.8 (Diagnostics> Ping)
  Si cela ne fonctionne pas, assurez-vous que les paramètres WAN, la passerelle, etc.
- Vérifier DNS: essayez de rechercher pfsense.org (Diagnostics> Recherche DNS)
  Si cela ne fonctionne pas, corrigez / modifiez les serveurs DNS sur Système> Général
- Test NAT: essayez d'envoyer une requête ping à 8.8.8.8 (Diagnostics> Ping) en utilisant le LAN comme adresse source
  Si cela échoue mais que les autres tests fonctionnent, le problème est probablement NAT sortant (voir les vérifications de la passerelle WAN / LAN ci-dessus)

Retour au Sommaire

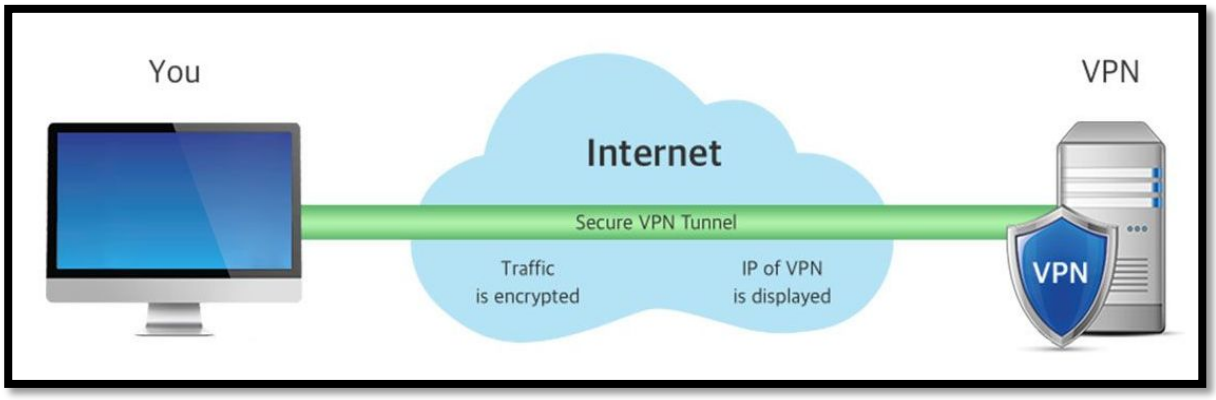
VPN signifie : ***Virtual Private Network***

Configurer un VPN ‘’client-to-site’’

Qu'est-ce qu'un réseau VPN?

Un réseau VPN est trivialement un réseau privé virtuel, une connexion/tunnel privé/chiffré, qui passe par internet (donc dans le wan).

Sur la photo ci-dessous, nous pouvons voir sous forme graphique comment un VPN "*fonctionne*"



Les VPN sont des outils très populaires, grâce auxquels vous pouvez à la fois protéger votre connexion et masquer l'adresse IP, contournant ainsi les blocages régionaux imposés par certains sites Internet. En termes encore plus simples, un VPN est un système qui joue le rôle d'intermédiaire entre l'ordinateur de l'utilisateur et les sites (ou services) utilisés, cachant son identité (la connexion, via un VPN, peut apparaître comme si elle provenait d'un autre pays) et protection du trafic entrant et sortant.

Avec le VPN, nous pouvons permettre aux utilisateurs d'un réseau LAN (une entreprise par exemple) de se connecter au réseau de l'entreprise (ou à une infrastructure cloud) en toute sécurité via un canal VPN «hôte à site» dans ce cas. Ensuite, nous verrons comment permettre à des utilisateurs uniques de se connecter au serveur VPN puis à partir de ce dernier d'accéder à l'infrastructure gérée sur le LAN pfsense.

Il est bon de noter que sur la configuration VPN il est possible de choisir le type de chiffrage, qui sera crucial dans nos choix de paramètres en fonction de la connexion et en fonction de la puissance du matériel sur lequel notre pare-feu est installé et du client machine en question puisque les deux doivent faire le travail pour compresser / décompresser tous les fichiers qui passent par le tunnel.

Donc, en bref, un cryptage plus fort signifie également plus d'utilisation des données et plus de puissance requise par le matériel pour compresser et décompresser les fichiers.

Retour au Sommaire

Ainsi, un VPN bien structuré peut offrir de grands avantages à une entreprise:

- ✓ Etend la connectivité géographique ;
- ✓ Améliore la sécurité là où les lignes de données n'ont pas été cryptées;
- ✓ Réduit les coûts d'exploitation;
- ✓ Réduit le temps de transit et les coûts de transport pour les clients éloignés;
- ✓ Simplifie la topologie du réseau, au moins dans certains scénarios;
- ✓ Offre la possibilité de réseaux mondiaux;
- ✓ Fournit un support réseau;
- ✓ Assure la compatibilité avec les réseaux à large bande;
- ✓ Offre un temps de retour sur investissement plus rapide que le transport traditionnel des lignes WAN
- ✓ Montre une bonne économie d'échelle.

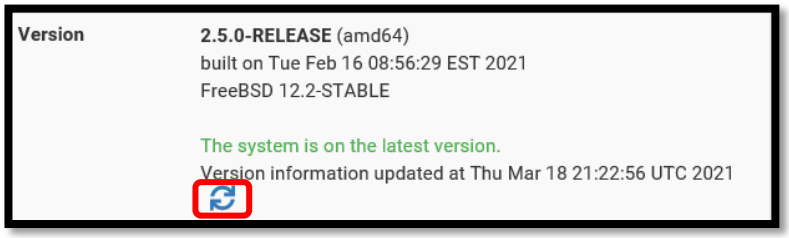
Dans ce pages, nous allons installer un VPN SSL (***OpenVPN***)

Conseils au préalables

Il est bien de vérifier, comme dans tous les cas, que notre vpn est à jour, avant d'effectuer toute opération pour des raisons évidentes liées à la sécurité.

Dans certaines versions de pfsense, il peut arriver que vous ne puissiez pas installer le module ‘’*openvpn-client-export* ‘’ en raison d'un bogue sur la version 2.4.5 . Alors vérifiez que la version pfsense est mise à jour pour éviter tout problème.
À la date de rédaction, la version la plus récente de pfsense est la version 2.5.0

Vous pouvez facilement mettre à jour la version pfsense simplement en allant sur la page principale et en cliquant sur les deux flèches en forme de cercle dans l'onglet "***Version***" comme vous pouvez le voir sur la capture d'écran ci-dessous.



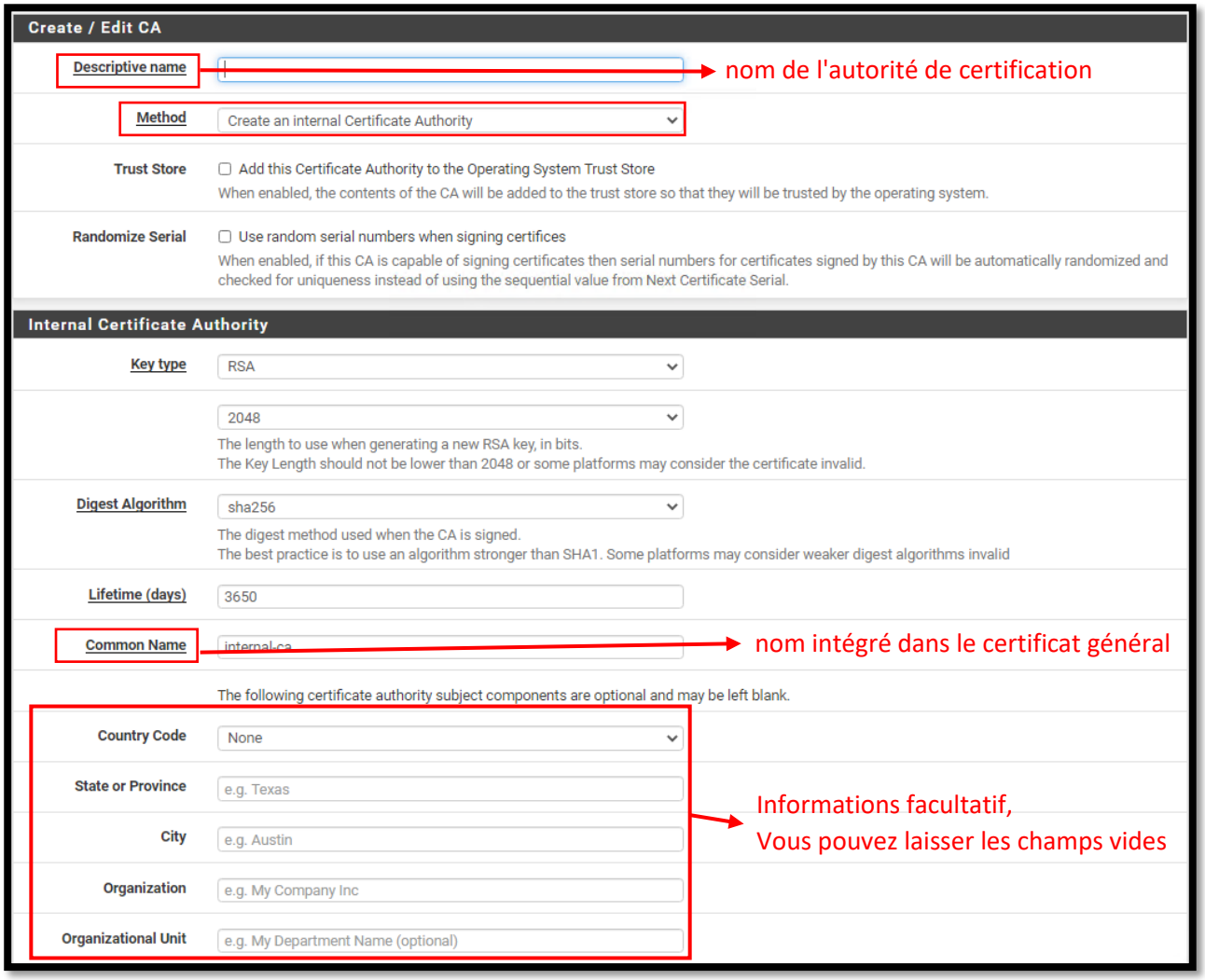
Retour au Sommaire

Les différentes étapes de configuration d'un serveur VPN :

1.Création d'une autorité de certification

La première étape consiste à créer une autorité de certification ; un VPN SSL a besoin d'un certificat.

Vous devrez aller dans le menu "*System / Cert.Manager*" dans l'onglet "*CAs*" Cliquez sur "*Add/Ajouter*" + Add puis remplissez le formulaire qui s'ouvre.

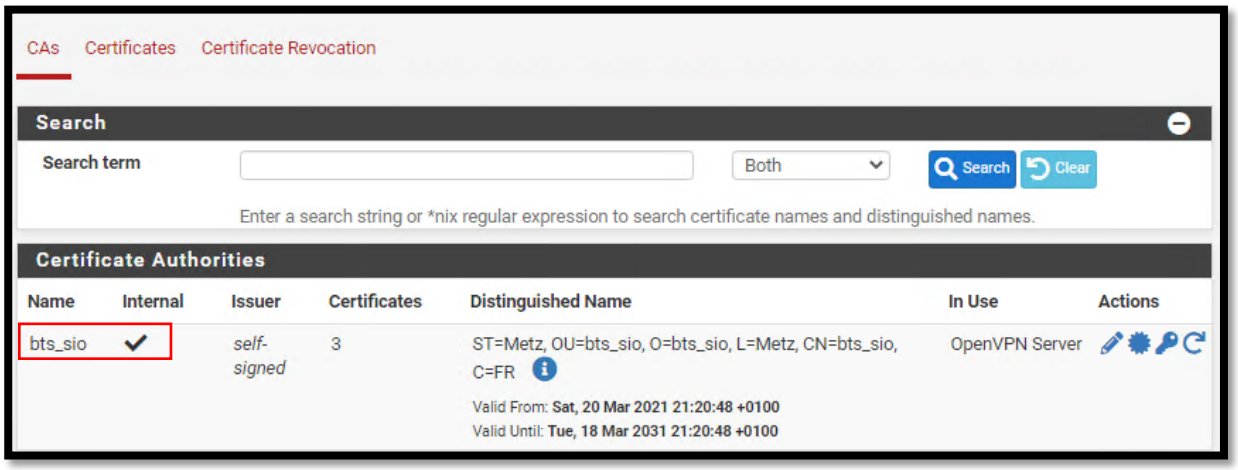


Retour au Sommaire

Certains de ces paramètres clés, que nous trouvons, dans le formulaire de configuration d'une autorité de certification :

- ✓ Description name: nom de l'autorité de certification
- ✓ Method : Dans notre cas, nous créons une autorité de certification interne
- ✓ Lifetime (days) : la validité du certificat est de 10 ans par défaut
- ✓ Common Name: le nom intégré dans le certificat général
- ✓ Contry code, State or Province, City: information complémentaire
- ✓ Organization, Organizational Unit: information complémentaire

Enfin, nous pouvons cliquer sur Enregistrer, puis vérifier la création réelle du certificat (comme vous pouvez le voir sur la capture d'écran ci-dessous), puis …



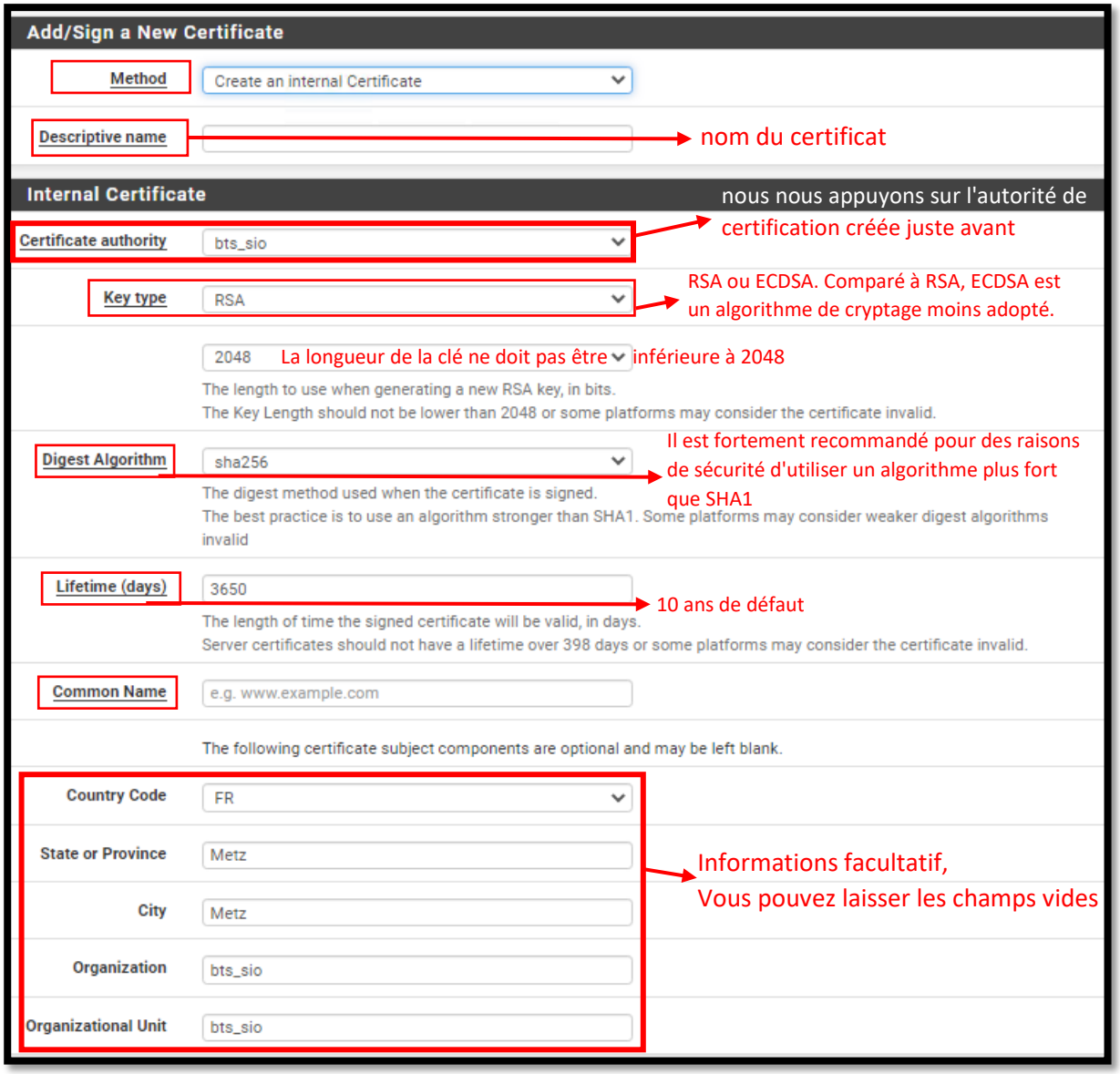
… continuer la configuration.

Retour au Sommaire

2.Création d'un certificat ‘’serveur‘’

Nous allons maintenant configurer un certificat de serveur.
Vous devrez aller dans le menu "*System / Cert.Manager*" dans l'onglet "*Certificates*" Cliquez sur "*Add*" 

puis remplissez le formulaire qui s'ouvre.

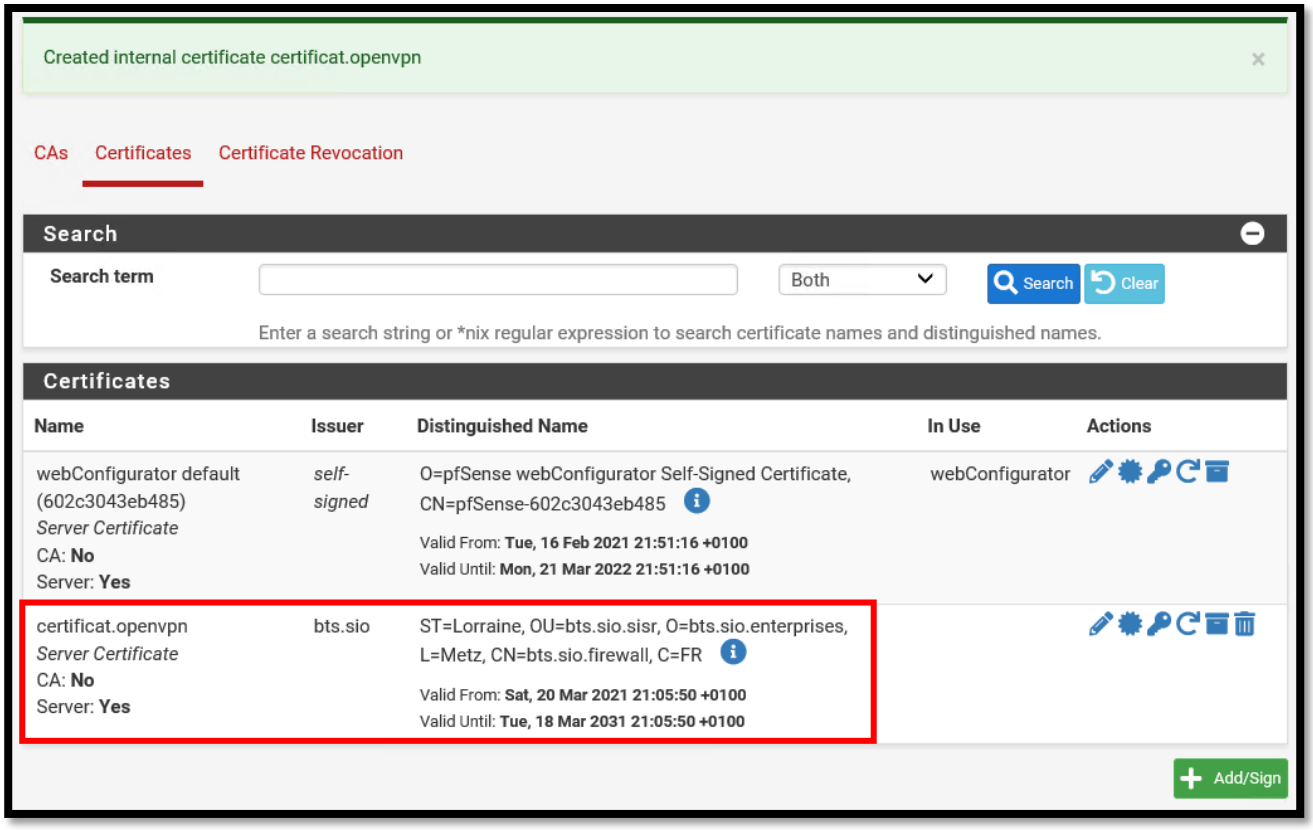


Certains de ces paramètres clés, que nous trouvons, dans le formulaire de configuration d'un certificat ‘’serveur :

- ✓ Method : Dans notre cas, nous créons une autorité de certification interne
- ✓ Description name: nom de l'autorité de certification
- ✓ Certificate authority : nous nous appuyons sur l'autorité de certification créée juste avant
- ✓ Lifetime (days) : la validité du certificat est de 10 ans par défaut (3650 days)
- ✓ Common Name: le nom intégré dans le certificat général
- ✓ Contry code, State or Province, City, Organization, Organizational Unit: information complémentaire
- ✓ **Certificate Type :** ce sera un certificat de type : server

Retour au Sommaire

Sur la capture d'écran suivante, nous pouvons voir que notre certificat (interne) a été créé :

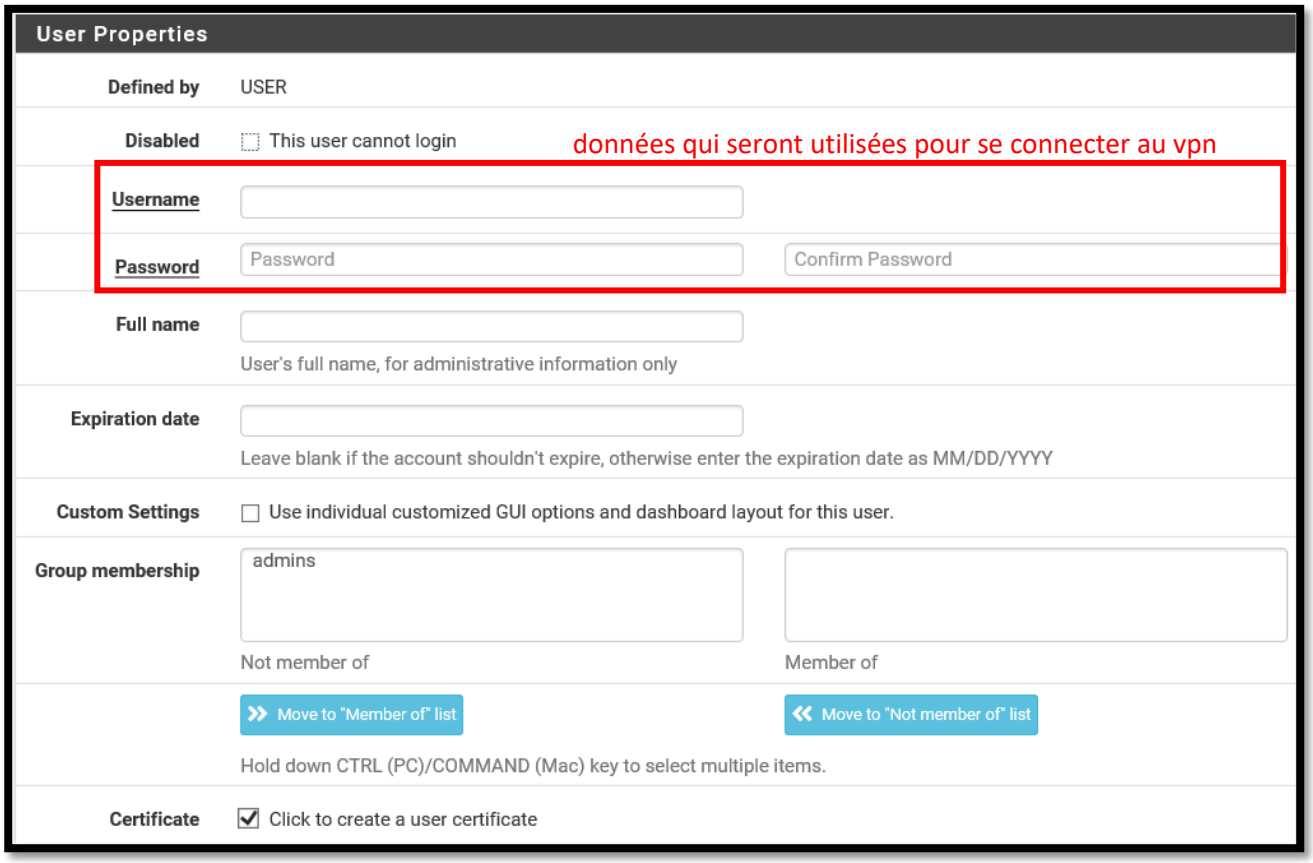


Retour au Sommaire

3. Création d'un utilisateur local (avec certificat joint)

Nous allons maintenant configurer un certificat de serveur.
Vous devrez aller dans le menu "*System / User Manager*" dans l'onglet "*Users*" Cliquez sur "*Add/Ajouter*" 

puis remplissez le formulaire qui s'ouvre.

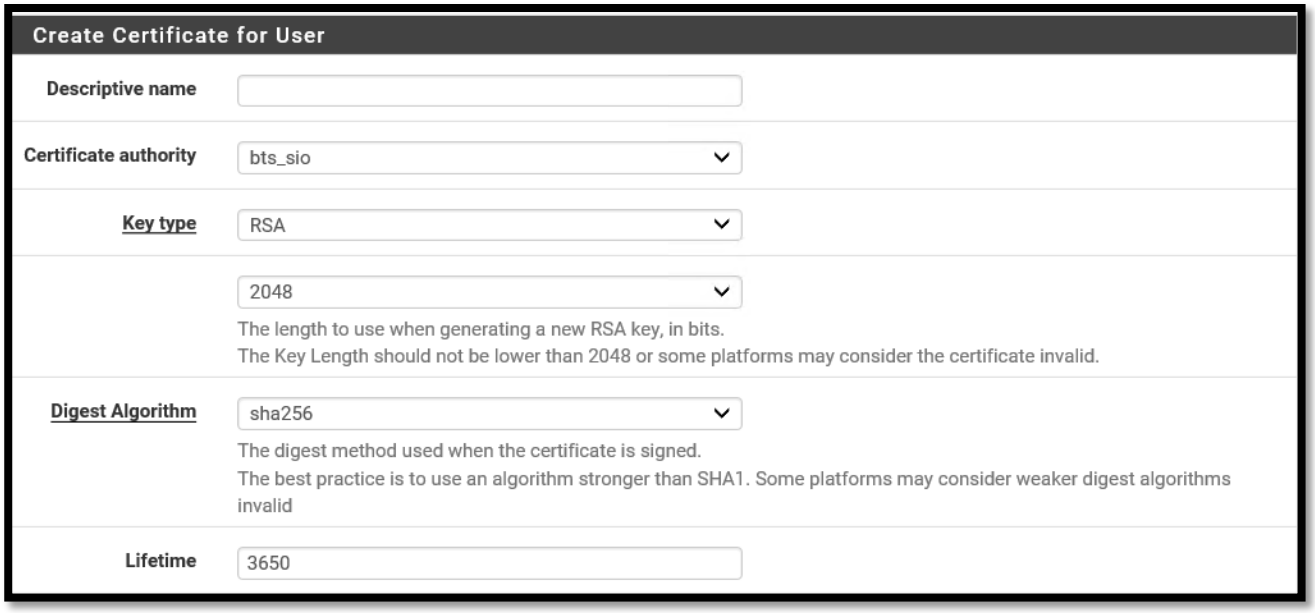


Certains de ces paramètres clés, que nous trouvons, dans le formulaire de configuration d'un utilisateur :

- ✓ Username : Nom d'utilisateur que nous utiliserons pour nous connecter à la VPN
- ✓ Password: Mot de passe que nous utiliserons pour nous connecter à la VPN
- ✓ Full name : Facultatif, à titre informatif uniquement
- ✓ Certificate : Cliquez sur cette case pour afficher le formulaire de création de certificat utilisateur affiché ci-dessous:

Nous pouvons utiliser la base de données AD ou un autre annuaire LDAP pour l'authentification VPN. Dans ce cas il est possible de paramétrer les configurations utiles dans l'onlet «***Authentification Servers***» puis de déclarer notre annuaire. Dans tous les cas, un nouvel utilisateur doit être créé pour avoir au moins un utilisateur intégré dans la configuration.

Retour au Sommaire



Dans cette fenêtre ci-dessus, nous trouverons les paramètres suivants à configurer:

- ✓ Descriptive name : nom du certificat utilisateur
- ✓ Certificate authority:
- ✓ Key type :
- ✓ Digest alhorithm :
- ✓ Lifetime : par défaut c'est toujours 10 ans.

Dans ce champ, il est possible de spécifier une clé SSH mais dans ce turorial, nous laisserons ce champ vide.

Enfin, cliquez simplement sur le bouton "***Save***" 

Retour au Sommaire

4.Créer une configuration de serveur OpenVPN

Nous allons maintenant créer la configuration OpenVPN.
Vous devrez aller dans le menu "*VPN / OpenVPN*" dans l'onglet "*Servers*" Cliquez sur "*Add/Ajouter*" 

puis remplissez la configuration :

Certains de ces paramètres clés, que nous trouvons, dans la configuration du server OpenVPN:

GENERAL INFORMATION

- ✓ Server mode : Remote Access (SSL/TLS + User Auth)
- ✓ Backend fot authentification : Local Database. Parce que est un compte local que nous utiliserons pour nous connecter au VPN, mais si nous avions configuré un annuaire LDAP comme «AD», nous le trouverons ici dans la liste.
- ✓ Protocol : Le protocole que nous utiliserons sera en UDP.
- ✓ Interface : l'interface sera le WAN, car la connexion entrante sera prise en compte par l'interface WAN pfsense.
- ✓ Local port : Par défaut, le port 1194 est utilisé mais il est fortement recommandé d'insérer un autre port pour des raisons de sécurité.

CRYPTOGRAPHIS SETTINGS

- ✓ Peer Certificate Authority : ici nous trouvons notre autorité de certification
- ✓ Server certificate : Ici, nous allons insérer le certificat créé avant
- ✓ Encrypted Algorithm : Par défaut, un algorithme "AES -256-CBC" est actuellement inclus et doit être paramétré en fonction des besoins spécifiques et en fonction de l'environnement qui varie évidemment d'un cas à l'autre.

TUNNEL SETTINGS

- ✓ IPv4 Tunnel Network : est le réseau que nous voulons utiliser pour le VPN, Pfsense dans ce cas nous recommande, comme vous pouvez le voir sur l'interface graphique, de saisir l'adresse suivante: *''10 .0.8.0 / 24* "
- ✓ IPv6 Tunnel Network : même paramètre précédent, uniquement en Ipv6
- ✓ Redirect Ipv4/Ipv6 Gateway : Il force simplement tout le trafic à travers le tunnel VPN (s'il n'est pas coché, le trafic pourra sortir à la fois via le VPN et via notre réseau Internet)
- ✓ Ipv4/Ipv6 Local Network : Ici, nous allons sélectionner tous les réseaux accessibles par le VPN, vous pouvez entrer plusieurs réseaux et / ou sous-réseaux avec une virgule
- ✓ Concurrent connections : Le nombre de connexions simultanées max. que nous voulons autoriser

CLIENT SETTINGS

- ✓ Dynamic IP : Ce paramètre, s'il est activé, permet aux utilisateurs de se connecter même si l'adresse IP change. Il est utile pour les utilisateurs connectés en déplacement, par exemple.
- ✓ Topology : Subnet ou net30. Vous pouvez sélectionner les deux. L'option net30 offre un réseau isolé, de sorte que chaque client qui se connecte avec cette option est connecté à un sous-réseau isolé (/30) afin de ne pas avoir de liens avec des connexions simultanées actives dans le VPN. L'inconvénient est que nous utiliserons 4 adresses IP pour chaque utilisateur (adresse ip pc, adresse de passerelle pfsense (gateway) , adresse de sous-réseau / 30 et une adresse de broadcast)

Retour au Sommaire

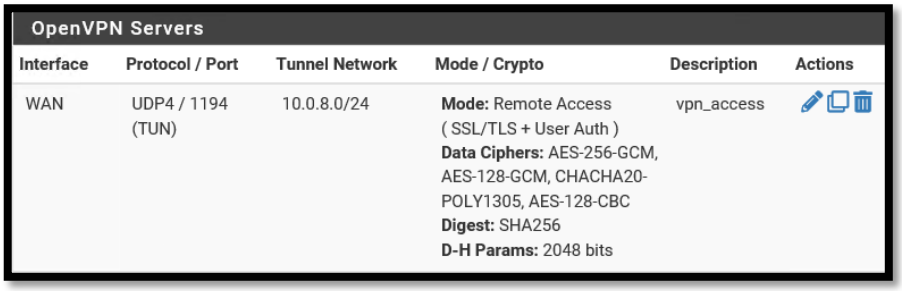
ADVANCED CLIENT SETTINGS

- ✓ DNS Default Domain : Offre la possibilité de définir un DNS par défaut, dans ce cas il est recommandé de saisir l'adresse DNS du serveur AD DS **example: AD_DS_Server.local*
- ✓ DNS Server enable : Il offre la possibilité de sélectionner jusqu'à 4 serveurs DNS, par exemple on peut saisir l'adresse du serveur DNS de l'organisation cible pour pouvoir résoudre les adresses internes, puis accéder aux applications qui ont un addresse local/privé.
- ✓ Block Outside DNS: Il vous permet de forcer les PC sous Windows 10 à utiliser le DNS de l'organisation cible. Il est recommandé d'activer cette option.

ADVANCED CONFIGURATION

- ✓ Custom options: vous pouvez saisir des options personnalisées / supplémentaires, dans ce champ il est recommandé de saisir le code '' **auth-nocache** '' pour des raisons évidentes liées à la sécurité (contre le vol des données d'authentification)

À ce stade, nous pouvons enregistrer la configuration et vérifier qu'elle a été ajoutée correctement.

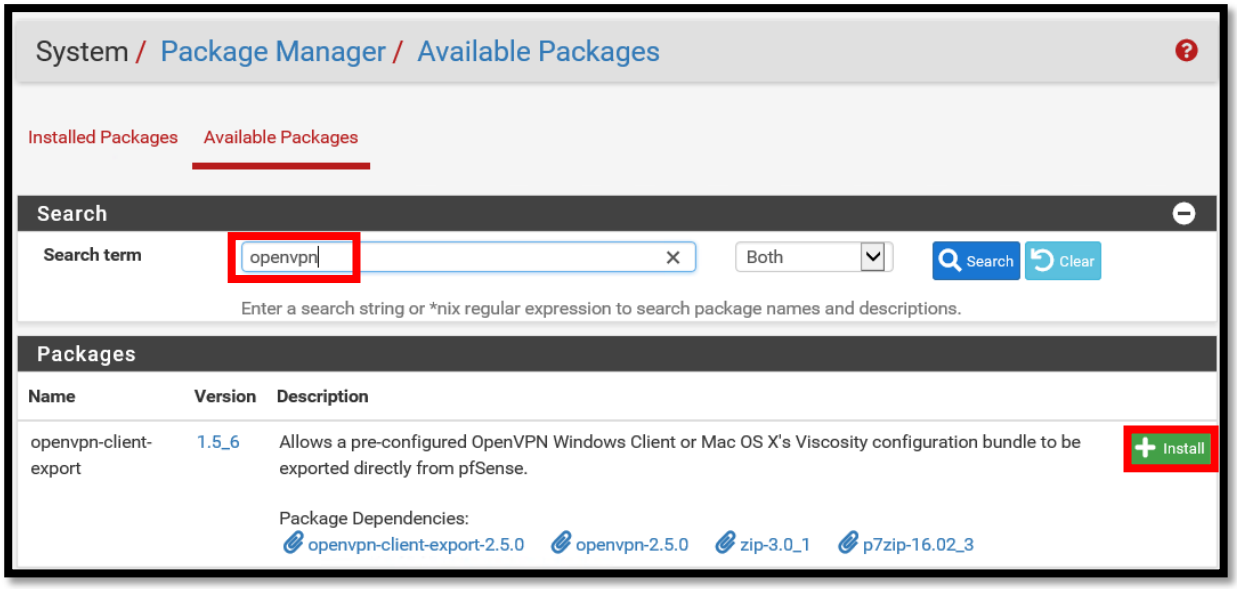


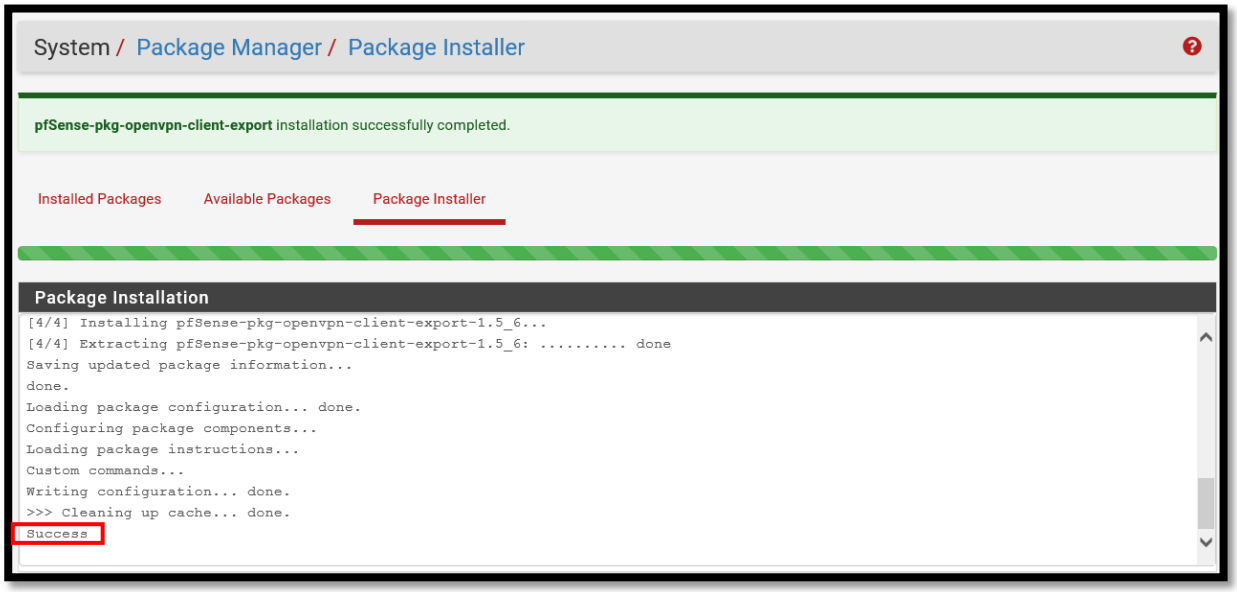
Retour au Sommaire

5.Export de la configuration OpenVPN

À ce stade, nous devrions installer un package supplémentaire sur le pare-feu via le menù "*System / Packet Manager* " dans l'onglet "*Avaiable Packages*" puis cliquez sur "*Search term*".
Recherchez ensuite le package «*openvpn client export*», puis installez et confirmez l'installation du package en question. Comme dans les images ci-dessous:

Tout cela car pfsense, de base n'offre pas la possibilité d'exporter la configuration au format OpenVPN.





Il est possible de vérifier la bonne installation via la ligne à la fin de l'installation "***Success***"

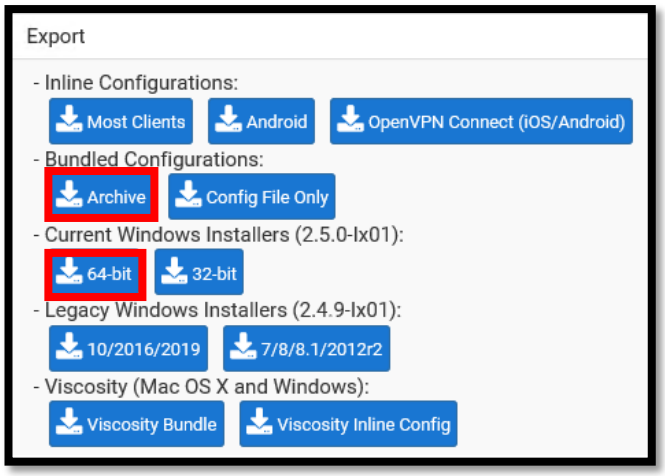
Retour au Sommaire

Une fois l'installation du package précédent réussie, vous pouvez le trouver dans la section : "*VPN / OpenVPN*" dans l'onglet "*Client Export*". De là, nous pouvons exporter la configuration OpenVPN.

Analysons le paramètre principal du menu de configuration:

- ✓ Host Name Resolution : Si nous nous connectons au VPN via l'adresse de connexion publique, nous pouvons laisser l'option "Interface IP Address" sélectionnée. Mais vous pouvez également mettre en place une installation de type "hostname" pour intégrer le nom de domaine dans la configuration VPN. Cela peut être intéressant si un portail VPN SSL a été utilisé. Dans la plupart des cas, une adresse IP publique est donc utilisée.

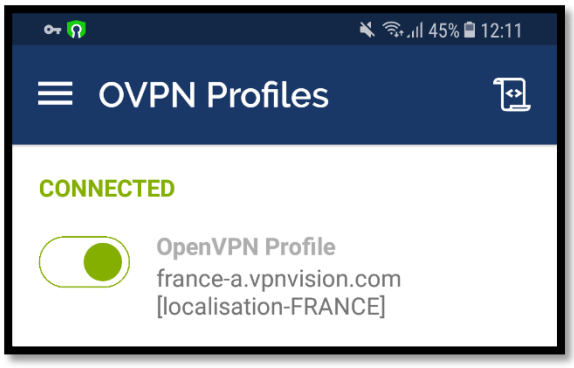
Si nous avons besoin, pour une raison quelconque, de nous connecter depuis un client avec une version d'OpenVPN inférieure à la version ''*2.4*'', nous pouvons activer le paramètre «*Legacy client*» qui rend la configuration VPN rétrocompatible avec les clients qui viennent d'être mentionnés.



À ce stade, pour vous connecter au VPN, vous pouvez télécharger le fichier de configuration. Le suffit de télécharger le zip "Archive" présenté sur "Configurations groupées"

Pour une installation sous Windows, puis avec une client OpenVPN, il suffit de télécharger le setup "64/32bit" présent sur la ligne : "Current Windows Installer"

De la même manière, il est possible d'exporter la configuration vers des clients MAC, IOS ou Android.



Retour au Sommaire

6.Création des règles de pare-feu et openvpn

Dans certaines versions de pfsense, une règle est créée automatiquement lors de la création du serveur VPN

Utilisation du menu "*Pare-feu / Règles*" dans le onlet "*WAN*" Cliquez sur "*Add*" pour ajouter une nouvelle règle

Dans notre cas les options seront les suivantes, mais il est évidemment possible de les personnaliser selon les besoins :

- Action: l'action sélectionnée sera “Pass”
- Interface: WAN, car la demande viendra du reseau WAN
- Address Family: Ipv4
- Protocol : Le protocole sera UDP, comme nous l'avons vu précédemment.
- Source : Toujours Any, car nous ne connaissons pas les adresses IP des clients. En dehors des cas particuliers.
- Destination : la destination sera l'adresse WAN de notre pare-feu / Firewall (Wan address)
- Destination Port Range: Ici, c’est possible définir la port personnalisé (par défaut est 1194)
  Log: il y a la possibilité d'avoir un fichier journal concernant les connexions OpenVPN
- Description: c’est possible saisir une description pour ‘’ *référence administrative* ‘’ .

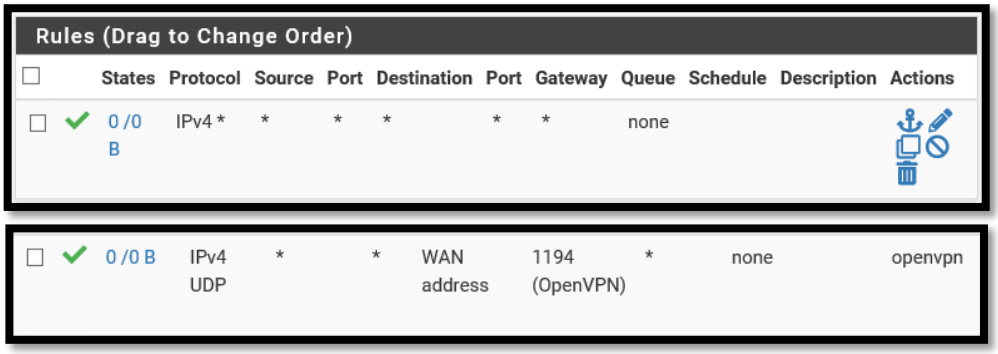
A la fin de la configuration, il est nécessaire de sauvegarder et d'appliquer les modifications

Maintenant c’est possible de trouver l’onglet "*OpenVPN*" sur le menù "*Firewall / Rules* "
Nous allons donc insérer une règle ici (ou plus de règle selon le cas)

- Action: l'action sélectionnée sera “Pass”
- Interface: OpenVPN
- Address Family: IPV4 (selon la configuration précédente)
- Protocol : selon le cas spécifique.
- Source : toujours any
- Destination : la destination sera l'hôte cible
- Destination Port Range: Ici, vous pouvez définir le port de destination
- Log: il y a la possibilité d'avoir un fichier journal concernant les connexions OpenVPN.

Il faut donc saisir toutes les règles nécessaires pour autoriser les flux

Pour de courtes sessions de test, il est possible de tout ouvrir pendant une **courte période**, puis de tout relier pour des raisons évidentes de sécurité.



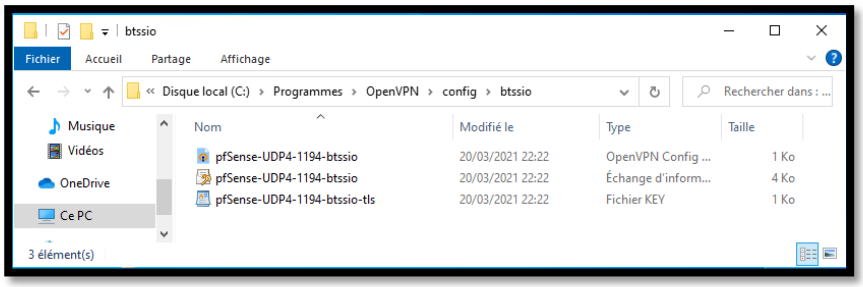
lien sur le forum netgate pour plus d'informations

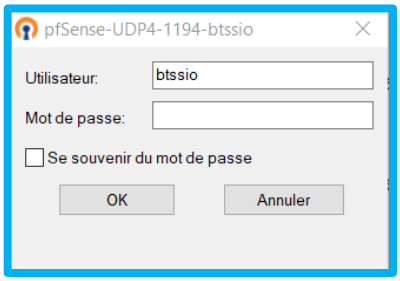
Retour au Sommaire

7.Test de connexion VPN

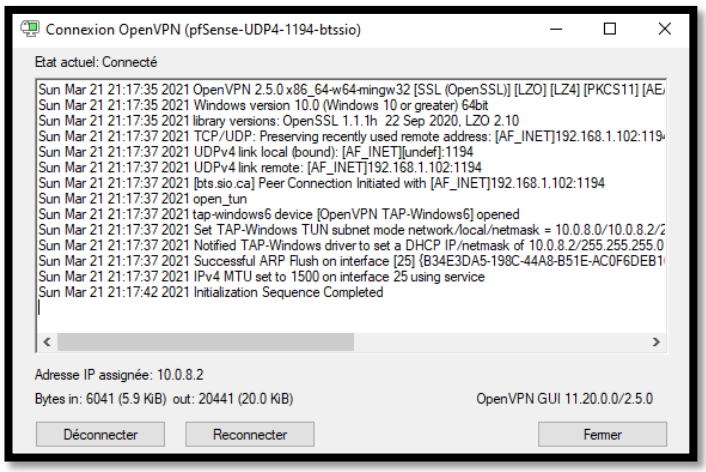
C'est le moment de vérité!

En supposant que, comme indiqué ci-dessus, nous avons téléchargé notre configuration pfsense et que nous avons déjà installé le client OpenVPN dans notre système d'exploitation, il nous suffit maintenant de déplacer les fichiers de configuration vers le dossier OpenVPN. Le dossier en question varie en fonction du chemin d'installation choisi lors de l'installation mais il est généralement possible de le trouver par défaut sur: " ***C:\Program Files\OpenVPN\config*** "





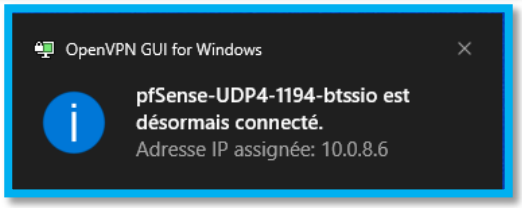
Vous pouvez renommer le dossier en question avec le fichier avec l'extension "*.ovpn*" pour avoir un nom personnalisé pour l'utilisateur.



Une fois que tout est configuré, il suffit de démarrer le logiciel OpenVPN et à partir de la petite icône en bas à droite de la barre Windows, sélectionnez «Connecter».

Si vous avez plusieurs configurations enregistrées, il sera possible de choisir la configuration souhaitée.

Après cela, il nous sera demandé d'entrer le nom d'utilisateur et le mot de passe.
Si tout se passe bien, une petite notification de Windows 10 nous avertira que la connexion a réussi.



Retour au Sommaire

Retour au Sommaire

Retour au Sommaire

Conclusion

Ca repond aux besoin de qui?

Il est bien de se souvenir que :
Sans ces systèmes et les fonctionnalités qu'ils offrent, la sécurité informatique serait sérieusement compromise. Aujourd'hui, il est quasiment impossible pour une entreprise de se passer de ces systèmes fondamentaux.

Par conséquent, un pare-feu peut certainement être utile à à toutes les entreprises qui ont un réseau plus ou moins complexe, ainsi à toute entreprise disposant d'un réseau local et ayant donc besoin de protection et de sécurité, mais aussi de fonctionnalités supplémentaires grâce à des pare-feu gérables.

En effet avoir un PC (serveur ou réseau) sans pare-feu, c'est comme laisser sa porte d'entrée ouverte à tout le monde avec les clés !

Exemple d'utilisation d'un pare-feu pour un réseau d'entreprise:

Il est possible de créer des règles pour limiter le trafic sur youtube, de manière à éviter que le trafic sur ce site particulier ne cause des problèmes de saturation à l'ensemble du réseau de l'entreprise. de la même manière, il est possible de refuser complètement l'accès à des sites spécifiques de manière à ne pas créer de distractions pour les employés.

Il est possible de créer un VPN de manière à ce que les employés puissent travailler à distance en toute sécurité, en ayant la possibilité d'accéder aux fichiers sur le serveur local, augmentant efficacement la productivité et l'efficacité par rapport aux méthodes plus rudimentaires.

Contraintes

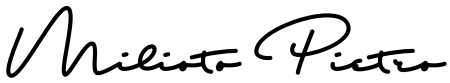
Un pare-feu n'est pas gratuit. C'est indéniable. il faut donc acheter des appareils spécifiques et des équipements de réseau qui ont un certain coût. Le faut avoir des compétences d'administration. Le technicien qui vient réparer ou mettre en œuvre de nouvelles fonctionnalités a également un coût, et il doit avoir des compétences spécifiques

L'une des premières questions que se posent de nombreux entrepreneurs lors de l'embauche d'un fournisseur de services de pare-feu est la suivante: "*Combien cela me coûtera-t-il?*" C'est une question parfaitement naturelle à poser. Mais voici la meilleure question: "*Dans quelle mesure l'utilisation d'un pare-feu géré peut-elle me sauver / m'aider?*"

Dans toute analyse coûts / avantages, il est toujours important d'évaluer le risque d'utiliser ou d'ignorer un outil ou une ressource en particulier. Si vous n'utilisez pas de solutions de pare-feu, le risque peut être assez élevé.

Ne sous-estimez jamais cet aspect, car un bon pare-feu peut vous éviter de nombreux problèmes et ralentissements, ce qui ne ferait que perdre votre temps et votre argent.

Retour au Sommaire



Retour au Sommaire