

Hepia

Haute École du Paysage, d'Ingénierie et d'Architecture

Ingénierie et Systèmes de Communication

Année académique 2021/2022

Université d'été

Pare-feu pfSense

Genève, 23 Septembre 2021

Étudiants :

Antoine Baud

Sergio Guarino

Professeure :

Noria Foukia

Table des matières

Introduction	2
1. Installation de pfSense.....	3
2. Configuration des environnements virtuels	3
Configuration VMWare.....	3
Configuration VM Linux	4
Configuration réseau pfSense	5
3. Connexion au pare-feu.....	6
4. Ajout de règles de sécurité	10
5. Protection contre des attaques DoS	13
6. Configuration d'un serveur VPN	14
7. Configuration d'un serveur PPPoE	21
Machine hôte (Debian 10)	21

Introduction

Le but de ce projet est d'étudier pfSense, un pare-feu logiciel open source basé sur FreeBSD. Il inclut également des logiciels tiers qui peuvent être installés à la demande et qui agrandissent les fonctionnalités de pfSense.

Le pare-feu a été installé et testé dans des environnement virtuel (VMWare). Les fonctionnalités qui ont été testées sont les suivantes :

- Mise en place de règles de gestion du trafic
- Protection contre des attaques DoS
- Configuration d'un VPN
- Service d'authentification PPPoE

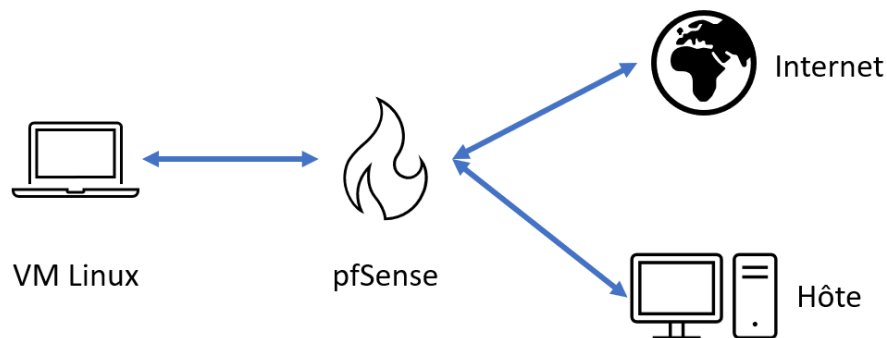
La version de pfSense utilisée est la 2.5.2.

1. Installation de pfSense

Les fichiers sources du pare-feu sont téléchargeables depuis le site web de pfSense www.pfsense.org. Pour l'installation, nous avons suivi le guide du site pfSense (docs.netgate.com) et installé le pare-feu avec les options par défaut. Il n'y a pas eu de problématiques ou de remarques particulières sur cette première étape.

2. Configuration des environnements virtuels

Après avoir complété l'installation, il a fallu configurer les cartes réseau des machines virtuelles pour obtenir l'architecture correcte au bon fonctionnement du système.



Configuration VMWare

La machine virtuelle Linux (OS choisi : Lubuntu) a une seule interface réseau et est connectée au réseau appelé **VMnet1**.

Network connection

☐ Bridged: Connected directly to the physical network
☐ Replicate physical network connection state

☐ NAT: Used to share the host's IP address

☐ Host-only: A private network shared with the host

☒ Custom: Specific virtual network

VMnet1 (Host-only) ▼

☐ LAN segment:
▼

LAN Segments... Advanced...

Le pare-feu a deux interfaces réseaux, une connectée à **VMnet1** et l'autre a été connectée en **NAT** avec la machine hôte, mais une connexion **Bridged** aurait également été un choix correct.

The image shows two side-by-side screenshots of the 'Network connection' dialog box in VMware. Both screenshots have the same options: 'Bridged: Connected directly to the physical network' (unselected), 'Replicate physical network connection state' (unchecked), 'NAT: Used to share the host's IP address' (selected in the left, unselected in the right), 'Host-only: A private network shared with the host' (unselected), 'Custom: Specific virtual network' (unselected in the left, selected in the right), and 'LAN segment:' (empty dropdown). In the left screenshot, the 'Custom' dropdown shows 'VMnet0'. In the right screenshot, it shows 'VMnet1 (Host-only)'. At the bottom of each dialog are 'LAN Segments...' and 'Advanced...' buttons.

Le tableau suivant resume le résultat souhaité.

machine	IPv4	masque de sous-réseau	configuration réseau (VMware)
passerelle par défaut	192.168.1.1	255.255.255.0	-
hote	192.168.1.X	255.255.255.0	-
pfSense (WAN)	192.168.1.100	255.255.255.0	NAT/bridged
pfSense (LAN)	192.168.2.1	255.255.255.0	host-only
workstation01	192.168.2.2	255.255.255.0	host-only

Configuration VM Linux

Utilisateur	mot de passe
Alice	labo
Root	labo

La configuration des interfaces réseaux sous Ubuntu passe par les fichiers se trouvant sous `/etc/netplan/`. Nous éditons le fichier `01-netcfg.yaml`, comme suit:

```
alice@workstation01:~$ cat /etc/netplan/01-netcfg.yaml
network:
  version: 2
  ethernets:
    ens33:
      addresses: [192.168.2.2/24,]
      gateway4: 192.168.2.1
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1,]
```

Après avoir édité le fichier, nous appliquons la nouvelle configuration

```
alice@workstation01:~$ sudo netplan apply
```

Nous redémarrons le service networking

```
alice@workstation01:~$ sudo /etc/init.d/networking restart
```

Puis nous contrôlons les paramètres de l'interface

```
alice@workstation01:~/Téléchargements$ netstat -rn
Table de routage IP du noyau
Destination      Passerelle      Genmask          Indic   MSS  Fenêtre  irtt  Iface
0.0.0.0          192.168.2.1     0.0.0.0          UG      0 0      0 ens33
192.168.2.0      0.0.0.0         255.255.255.0    U       0 0      0 ens33
alice@workstation01:~/Téléchargements$ ping -c 3 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=0.539 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=0.683 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=64 time=0.702 ms

--- 192.168.2.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2043ms
rtt min/avg/max/mdev = 0.539/0.641/0.702/0.075 ms
alice@workstation01:~/Téléchargements$ ping -c 3 google.ch
PING google.ch (172.217.168.3) 56(84) bytes of data.
64 bytes from zrhlls03-in-f3.1e100.net (172.217.168.3): icmp_seq=1 ttl=109 time=23.1 ms
64 bytes from zrhlls03-in-f3.1e100.net (172.217.168.3): icmp_seq=2 ttl=109 time=19.6 ms
64 bytes from zrhlls03-in-f3.1e100.net (172.217.168.3): icmp_seq=3 ttl=109 time=20.1 ms

--- google.ch ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 19.657/20.977/23.160/1.563 ms
alice@workstation01:~/Téléchargements$
```

Configuration réseau pfSense

Les interfaces réseau du pare-feu doivent être configurées manuellement. Pour ce faire :

1. Sélectionner l'option 1) Assign interfaces

```
Should VLAN be setup now [y|n]? n
Enter the WAN interface name or `a` for auto-detection (em0 em1 or a): em0
Enter the LAN interface name or `a` for auto-detection (em0 em1 or a): em1
The interfaces will be assigned as follows:
WAN -> em0
LAN -> em1
Do you want to proceed [y|n]? y
Writing configuration...done.
One moment while the settings are reloading... done!
```

2. Sélectionner l'option 2) Set interface(s) IP address

```

Enter the number of the interface you wish to configure: 1
Configure IPv4 address WAN interface via DHCP? (y/n) n
Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.1.100
Enter the new WAN IPv4 subnet bit count (1 to 31): 24
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> 192.168.1.1
Configure IPv6 address WAN interface via DHCP6? (y/n) n
Enter the new WAN IPv6 address. Press <ENTER> for none:
> <ENTER>
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
Appuyer sur <ENTER> pour valider la configuration

```

3. Retourner sur l'option 2) pour configurer l'interface em1

```

Enter the new WAN IPv4 address. Press <ENTER> for none:
> 192.168.2.1
Enter the new WAN IPv4 subnet bit count (1 to 31): 24
For a WAN, enter the new WAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> <ENTER>
Enter the new WAN IPv6 address. Press <ENTER> for none:
> <ENTER>
Do you want to enable the DHCP server on LAN (y/n) n
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

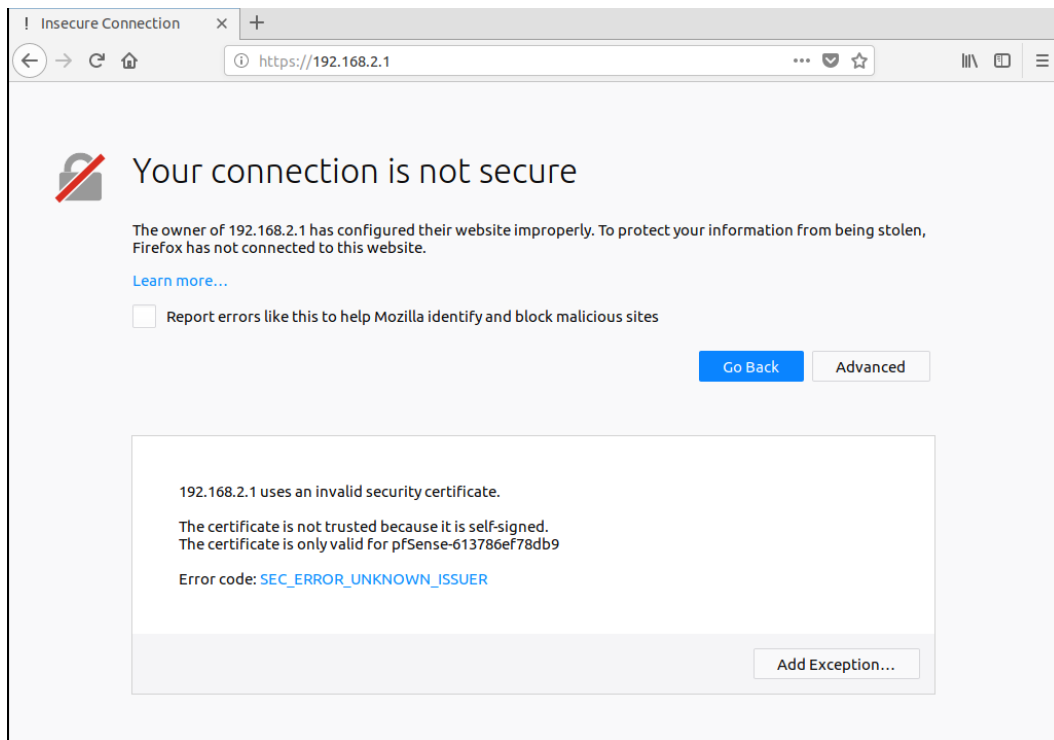
```

4. Contrôler avec l'option 7) Ping host que la communication est établie

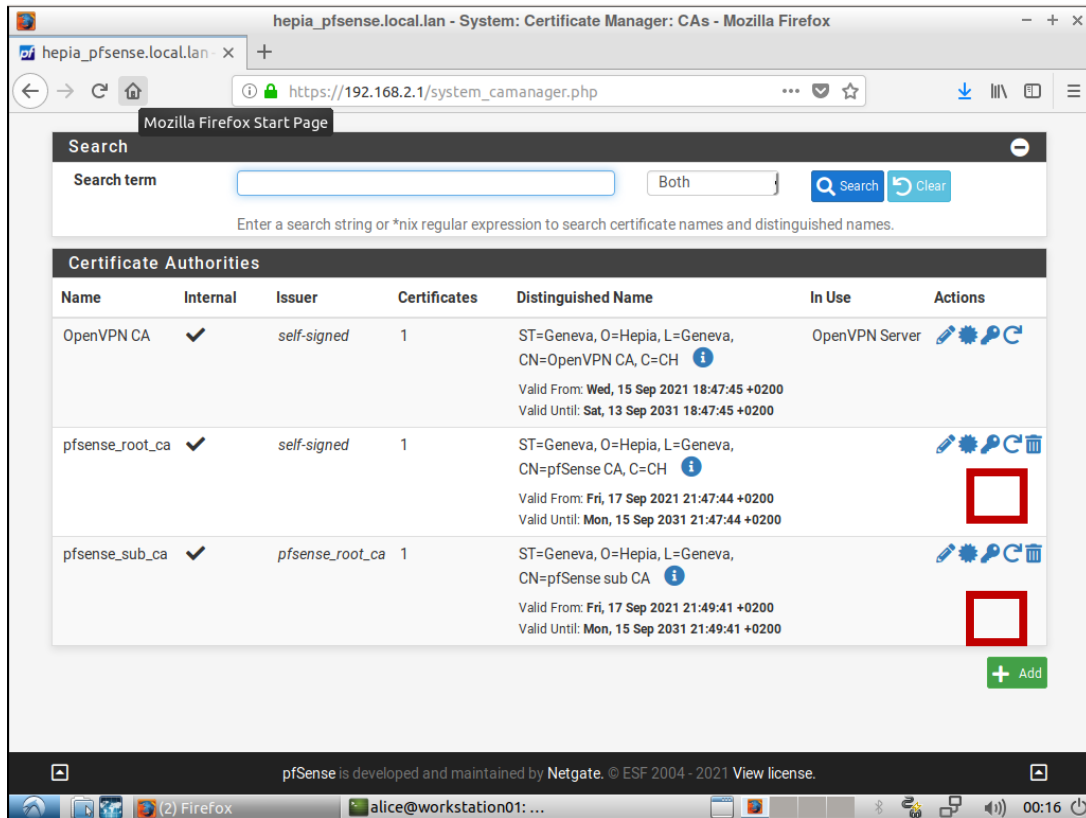
3. Connexion au pare-feu

Utilisateur	mot de passe
Admin	labo

Après avoir configuré la machine : Workstation01 et la machine : pfSense, nous accédons à la console d'administration. Selon nos paramètres, la console est accessible à la page <https://192.168.2.1> depuis la machine : Workstation01. Avant d'y accéder, on nous informe que la connexion n'est pas sécurisée.



Dans un premier temps, nous ajoutons une exception. Puis, nous sécuriserons les communications avec la console d'administration. Nous créons un root CA et un sub CA depuis le menu : System > Certificate Manager > CAs > +Add.



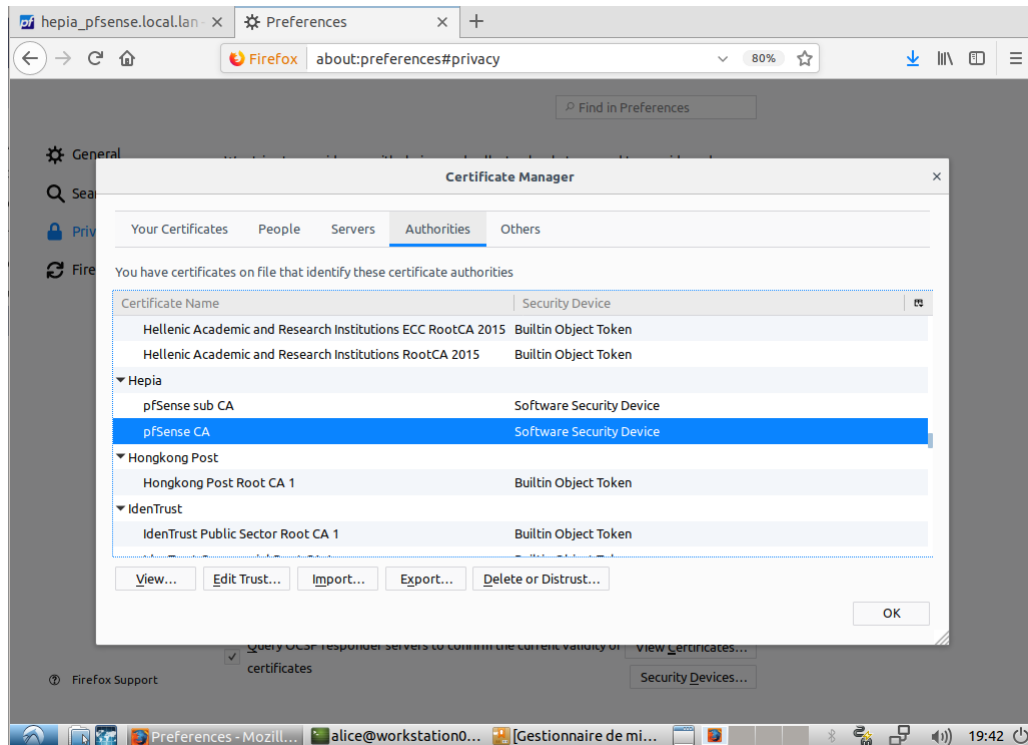
Nous exportons les certificats (en cliquant sur l'icône mise en évidence dans la figure ci-dessus) et les copions dans le répertoire `/etc/ca-certificates/update.d/`.

```
alice@workstation01:~$ sudo cp ~/Téléchargements/*.crt /etc/ca-certificates/update.d/
```

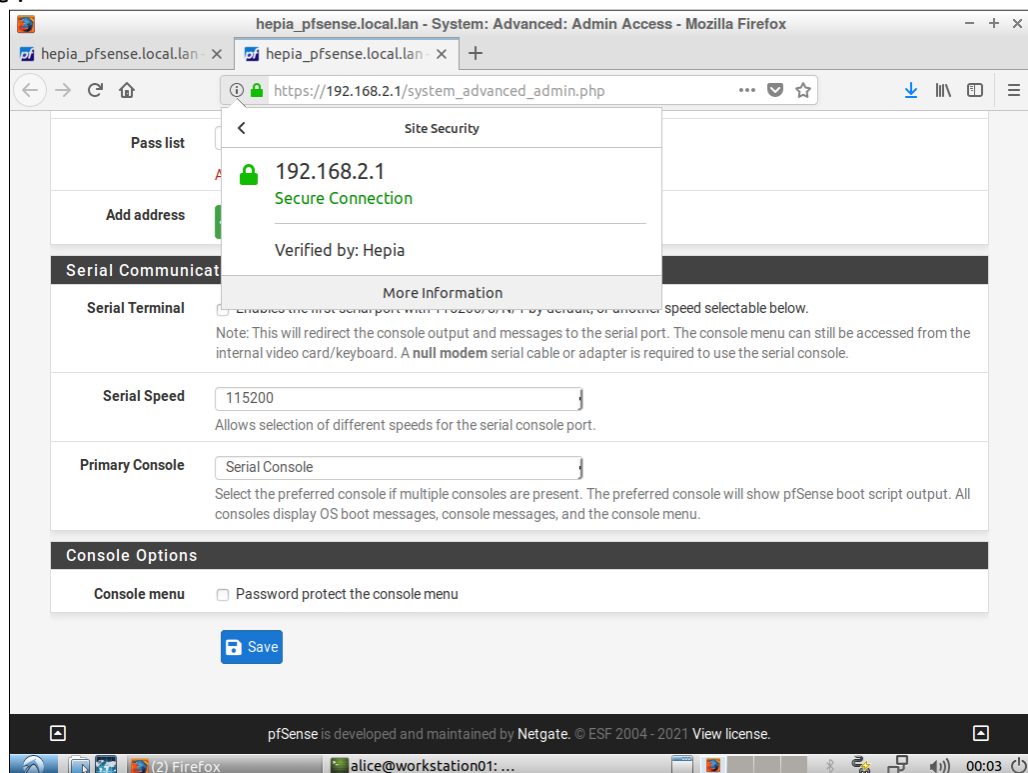
Puis nous mettons à jour le système afin qu'il puisse le reconnaître

```
alice@workstation01:~$ sudo update-ca-certificates
```

Nous devons encore importer le root CA dans notre navigateur. Pour importer le root certificat (`pfsense_root_ca.crt`) dans le navigateur (Firefox), nous l'ouvrons avec l'URL suivante : `about:preferences#privacy`. Dans la section Certificates, nous cliquons sur le bouton View Certificates.... Dans l'onglet Autorities, nous téléversons le certificat en activant les options :



Finalement, nous pouvons constater que la communication avec la console d'administration est sécurisée :

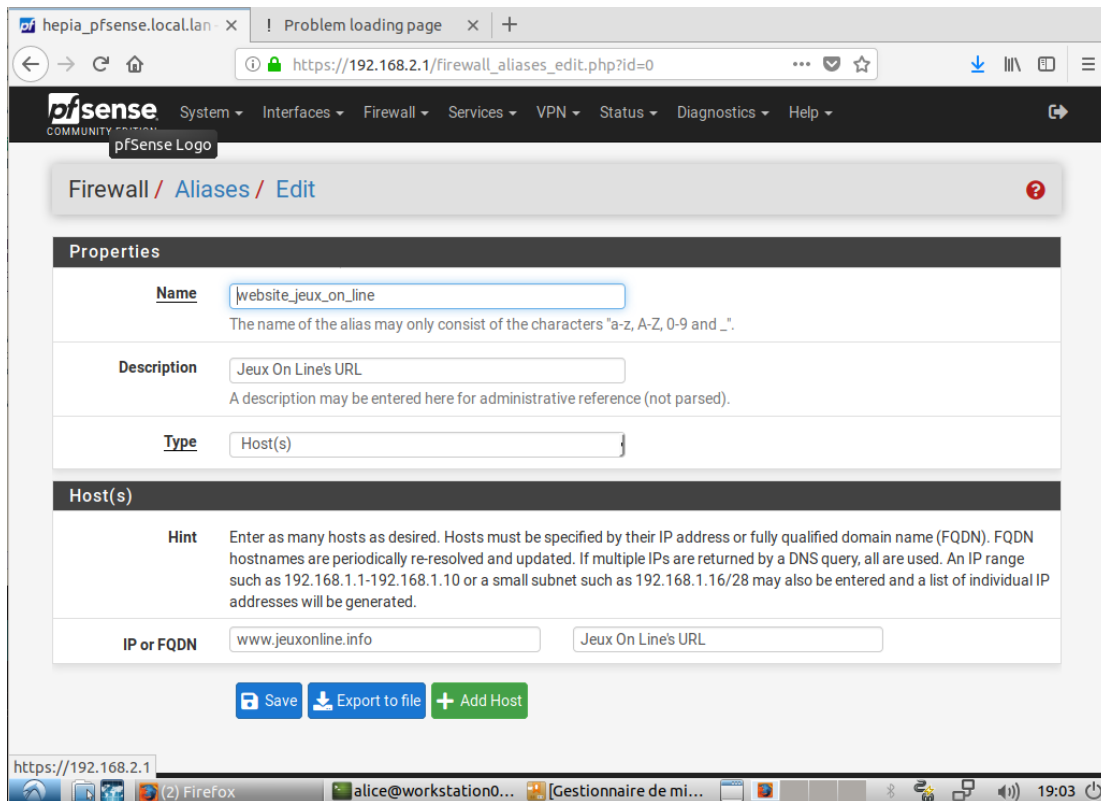


4. Ajout de règles de sécurité

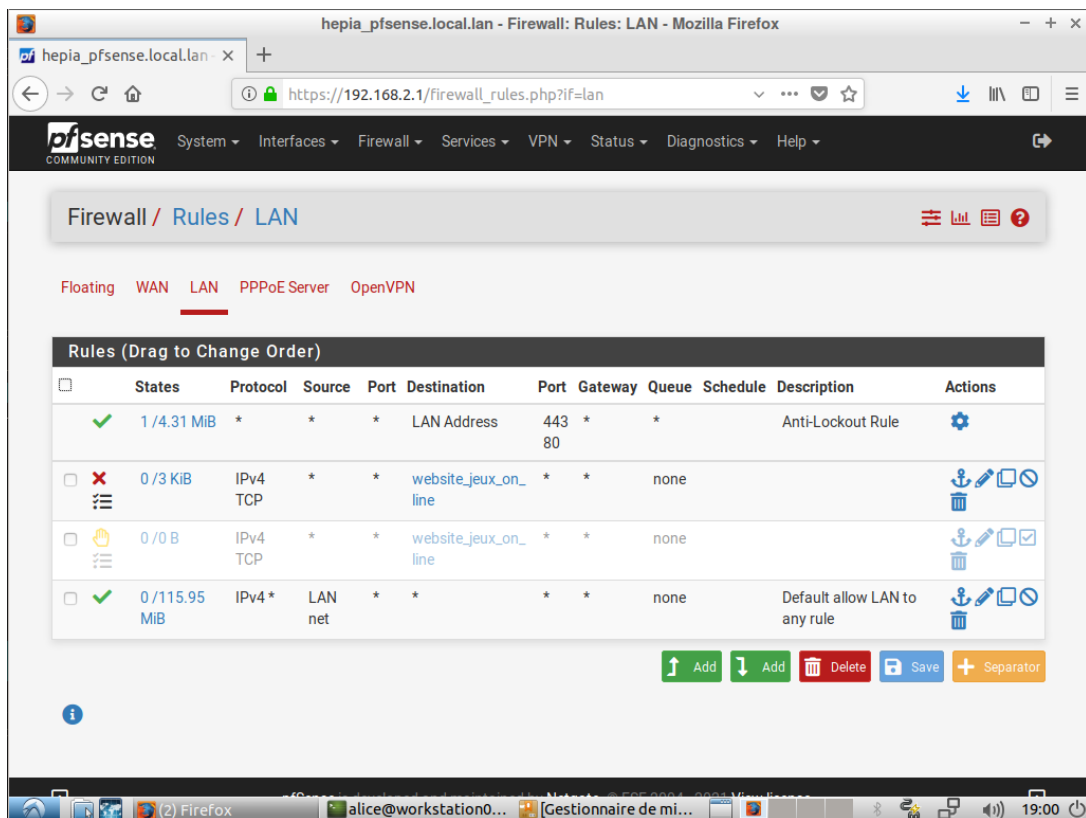
Types de règles :

pass	Autorise la communication
block	Détruit le paquet sans informations supplémentaires
reject	Renvoie le paquet à la source

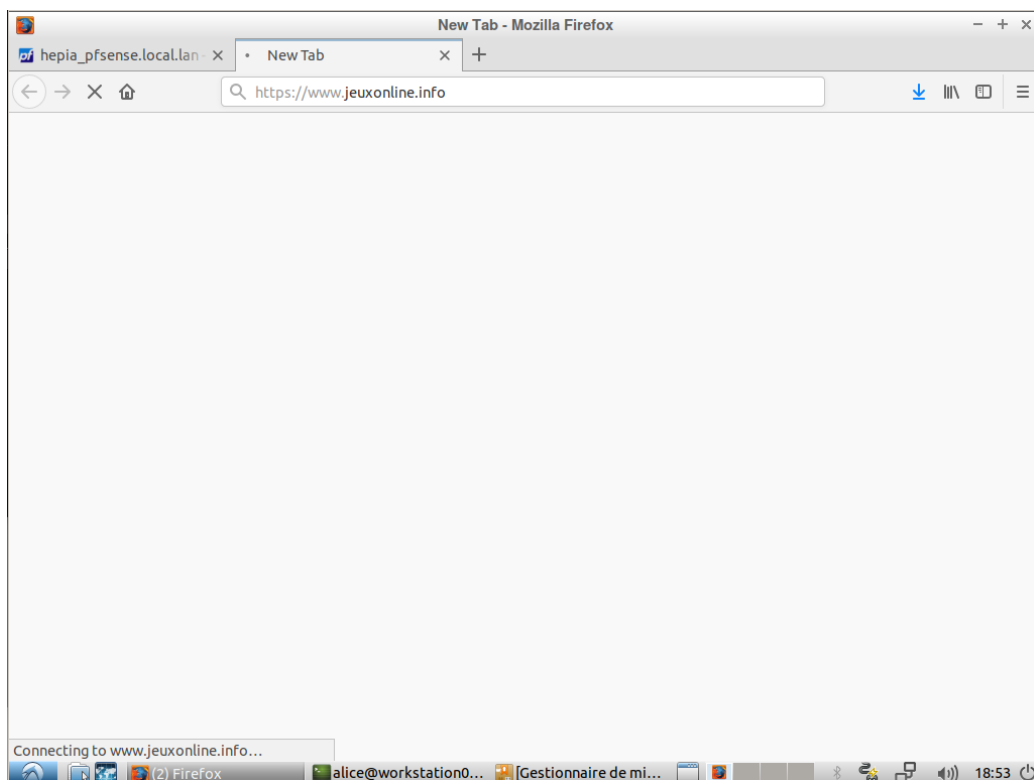
Avant de définir les règles d'autorisation d'accès sur certains sites, nous définissons un alias. Nous naviguons à travers les menus : Firewall > Aliases > URLs > +Add pour créer un nouvel Alias.



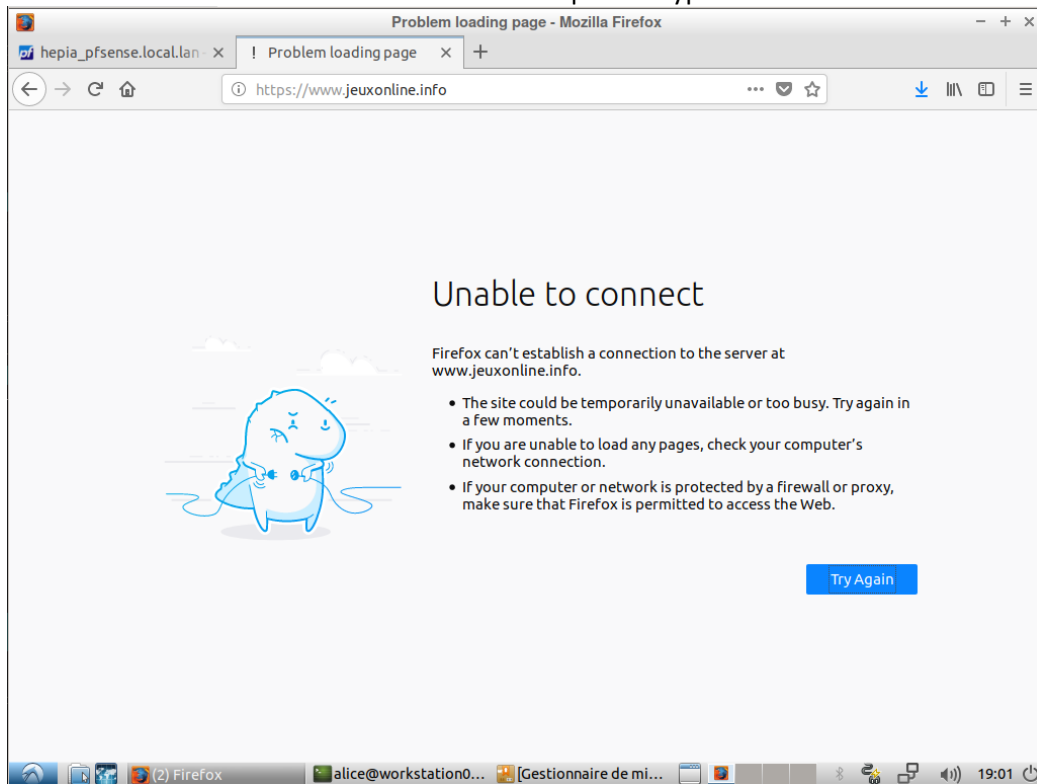
Pour souligner la différence de comportement entre une règle de type block et une règle de type reject, nous définissons chacun de ces types sur la même URL.



Voici les résultats obtenus pour le type reject:



Voici les résultats obtenus pour le type block :



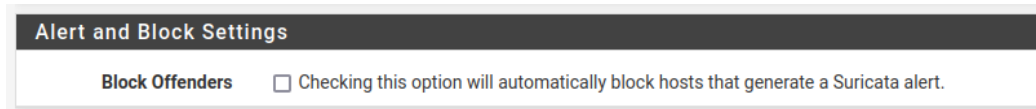
Lors de la définition de règle, il faut également prendre garde à bloquer l'adresse IPv4/IPv6 du site concerné. Si ça n'est pas le cas, le site <https://www.jeuxonline.info> pourrait être atteignable avec l'IP 188.165.237.164. À noter également que les journaux (Status > System Logs > Firewall) ne fournissent pas d'informations sur les rejets :

	Time	Interface	Source IP	Destination IP	Protocol
×	Sep 21 19:01:05	WAN	192.168.1.1:5353	224.0.0.251:5353	UDP
×	Sep 21 19:01:05	WAN	192.168.1.1:5353	224.0.0.251:5353	UDP
×	Sep 21 19:01:18	LAN	192.168.2.2:35100	188.165.237.164:443	TCP:S
×	Sep 21 19:01:18	LAN	192.168.2.2:35102	188.165.237.164:443	TCP:S
×	Sep 21 19:01:19	LAN	192.168.2.2:35104	188.165.237.164:443	TCP:S
×	Sep 21 19:01:19	LAN	192.168.2.2:35106	188.165.237.164:443	TCP:S
×	Sep 21 19:01:19	LAN	192.168.2.2:35108	188.165.237.164:443	TCP:S
×	Sep 21 19:01:19	LAN	192.168.2.2:35110	188.165.237.164:443	TCP:S
×	Sep 21 19:02:06	WAN	192.168.1.1:5353	224.0.0.251:5353	UDP
×	Sep 21 19:02:06	WAN	192.168.1.149:5353	224.0.0.251:5353	UDP
×	Sep 21 19:02:06	WAN	192.168.1.1:5353	224.0.0.251:5353	UDP
×	Sep 21 19:02:06	WAN	192.168.1.1:5353	224.0.0.251:5353	UDP
×	Sep 21 19:02:06	WAN	192.168.1.1:5353	224.0.0.251:5353	UDP
×	Sep 21 19:03:06	WAN	192.168.1.1:5353	224.0.0.251:5353	UDP
×	Sep 21 19:03:06	WAN	192.168.1.149:5353	224.0.0.251:5353	UDP
×	Sep 21 19:03:06	WAN	192.168.1.1:5353	224.0.0.251:5353	UDP
×	Sep 21 19:03:06	WAN	192.168.1.1:5353	224.0.0.251:5353	UDP
×	Sep 21 19:03:06	WAN	192.168.1.1:5353	224.0.0.251:5353	UDP
×	Sep 21 19:04:06	WAN	192.168.1.1:5353	224.0.0.251:5353	UDP

5. Protection contre des attaques DoS

Entre les paramètres par défaut de pfSense, on ne trouve pas une protection spécifique contre des attaques DoS. On a donc cherché entre les différentes extensions à disposition pour trouver la solution adéquate et finalement nous avons opté pour une appelée Suricata.

Lors de la création des règles de gestion de Suricata, il y a la possibilité d'automatiser le processus de blocage des attaquants, au travers l'option suivante :



Suricata peut également générer des alertes en cas de comportements suspects (et qui peuvent être définis par nous).

Pour tester le bon fonctionnement de cette protection, on essaie d'abord un attaque DoS sans protection. En premier lieu, on démarre un serveur web sur la machine qui sera la victime de l'attaque. Pour ce faire on utilise la commande python suivante :

```
sudo python3 -m http.server 7777
```

Ensuite, on lance l'attaque (en utilisant le même code que le TP DDoS vu l'année passée). On remarque que le site web n'est plus joignable déjà après quelques secondes (et quelques milliers de requêtes par seconde).

Si on effectue à nouveau l'attaque après avoir activé Suricata, après quelques secondes, l'adresse IP source de l'attaque est bloqué, permettant ainsi au site web de continuer de fonctionner.

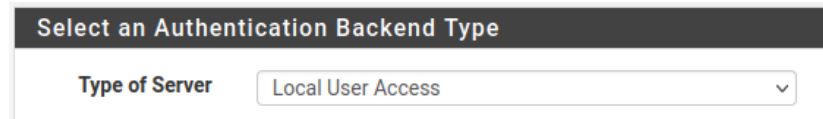
Last 500 Hosts Blocked by Suricata			
Note: Only blocked IP addresses from Legacy Mode interfaces are shown! For inline IPS mode interfaces, dropped IP addresses are highlighted on the ALERTS tab.			
#	Blocked IP	Alert Description	Remove
1	192.168.150.1 	SURICATA STREAM Packet with invalid ack - 09/23/2021-20:49:58	
1 host IP address is currently being blocked.			

Ceci est donc très utile dans le cas où l'attaque provient d'une machine avec un seul IP source. La règle n'est malheureusement pas efficace dans le cas où il s'agirait d'une attaque distribuée, puisqu'il n'y aurait pas moyen de distinguer entre des vraies et des fausses requêtes.

6. Configuration d'un serveur VPN

Pour la configuration d'un VPN, pfSense offre 3 possibilités qui sont pre-intégrées : L2TP, IPsec et OpenVPN. Pour ce projet nous avons choisi OpenVPN.

pfSense offre un outil d'assistance à la configuration du VPN. Ci-dessous sont détaillées les étapes avec le détail des paramètres choisis.

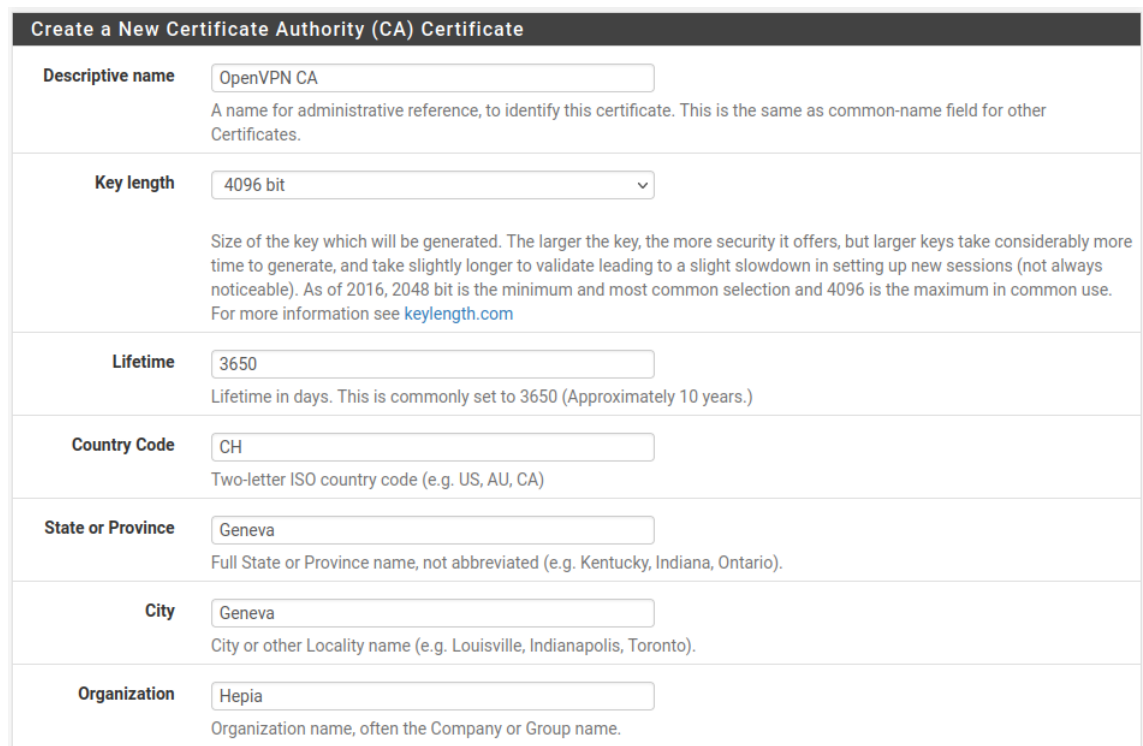


Select an Authentication Backend Type

Type of Server: Local User Access

Local User Access signifie que l'authentification est gérée par le pare-feu. Un utilisateur va devoir être créé à la fin de la configuration.

Ci-dessous la création des certificats :



Create a New Certificate Authority (CA) Certificate

Descriptive name: OpenVPN CA
A name for administrative reference, to identify this certificate. This is the same as common-name field for other Certificates.

Key length: 4096 bit
Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com

Lifetime: 3650
Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)

Country Code: CH
Two-letter ISO country code (e.g. US, AU, CA)

State or Province: Geneva
Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).

City: Geneva
City or other Locality name (e.g. Louisville, Indianapolis, Toronto).

Organization: Hepia
Organization name, often the Company or Group name.

Create a New Server Certificate	
Descriptive name	<input type="text" value="OpenVPN SC"/> A name for administrative reference, to identify this certificate. This is also known as the certificate's "Common Name."
Key length	<input type="text" value="4096 bit"/> Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com
Lifetime	<input type="text" value="365"/> Lifetime in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.
Country Code	<input type="text" value="CH"/> Two-letter ISO country code (e.g. US, AU, CA)
State or Province	<input type="text" value="Geneva"/> Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).
City	<input type="text" value="Geneva"/> City or other Locality name (e.g. Louisville, Indianapolis, Toronto).
Organization	<input type="text" value="Hepia"/> Organization name, often the Company or Group name.

Ensuite on configure le port et le protocole de communication

General OpenVPN Server Information	
Interface	<input type="text" value="WAN"/> The interface where OpenVPN will listen for incoming connections (typically WAN.)
Protocol	<input type="text" value="UDP on IPv4 only"/> Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.
Local Port	<input type="text" value="1194"/> 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.
Description	<input type="text" value="VPN Eval w/ pfSense"/> 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.

On active également la communication TLS :

Cryptographic Settings	
TLS Authentication	<input checked="" type="checkbox"/> Enable authentication of TLS packets.
Generate TLS Key	<input checked="" type="checkbox"/> Automatically generate a shared TLS authentication key.
TLS Shared Key	<input type="text"/> Paste in a shared TLS key if one has already been generated.
DH Parameters Length	4096 bit Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.
Data Encryption Negotiation	<input checked="" type="checkbox"/> Enable negotiation of Data Encryption Algorithms between client and server. The best practice is keep this setting enabled.
Data Encryption Algorithms	<div> <div>AES-256-GCM</div> <div>AES-128-GCM</div> <div>CHACHA20-POLY1305</div> </div> <p>List of algorithms clients can negotiate to encrypt traffic between endpoints. The best practice is to use the exact algorithms listed above, in that order. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips. Edit the server after finishing the wizard for additional choices.</p>
Fallback Data Encryption Algorithm	AES-256-CBC (256 bit key, 128 bit block) The algorithm used to encrypt traffic between endpoints when data encryption negotiation is disabled or fails.
Auth Digest Algorithm	SHA256 (256-bit) The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.
Hardware Crypto	No Hardware Crypto Acceleration The hardware cryptographic accelerator to use for this VPN connection, if any.

Dans la configuration réseau, on a décidé de cocher l'option Inter-Client Communication, qui permet, à une machine connectée au VPN, de communiquer avec les autres clients présents dans le réseau derrière le pare-feu.

Tunnel Settings	
Tunnel Network	192.168.42.0/24 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.
Redirect Gateway	<input type="checkbox"/> Force all client generated traffic through the tunnel.
Local Network	192.168.253.0/24 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.
Concurrent Connections	3 Specify the maximum number of clients allowed to concurrently connect to this server.
Allow Compression	Refuse any non-stub compression (Most secure) Allow compression to be used with this VPN instance, which is potentially insecure.
Compression	Disable Compression [Omit Preference] Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may expose data. This setting has no effect if compression is not allowed. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.
Type-of-Service	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
Inter-Client Communication	<input checked="" type="checkbox"/> Allow communication between clients connected to this server.
Duplicate Connections	<input type="checkbox"/> Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.

Client Settings	
Dynamic IP	<input checked="" type="checkbox"/> <p>Allow connected clients to retain their connections if their IP address changes.</p>
Topology	<div>Subnet – One IP address per client in a common subne ▼</div> <p>Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".</p>
DNS Default Domain	<div>Local DNS</div> <p>Provide a default domain name to clients.</p>
DNS Server 1	<div>192.168.253.25</div> <p>DNS server IP to provide to connecting clients.</p>
DNS Server 2	<div>1.1.1.1</div> <p>DNS server IP to provide to connecting clients.</p>
DNS Server 3	<div>1.0.0.1</div> <p>DNS server IP to provide to connecting clients.</p>
DNS Server 4	<div>8.8.8.8</div> <p>DNS server IP to provide to connecting clients.</p>
NTP Server	<div>time.cloudflare.com</div> <p>Network Time Protocol server to provide to connecting clients.</p>
NTP Server 2	<div>2.us.pool.ntp.org</div> <p>Network Time Protocol server to provide to connecting clients.</p>
NetBIOS Options	<input type="checkbox"/> <p>Enable NetBIOS over TCP/IP. If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.</p>
NetBIOS Node Type	<div>none ▼</div> <p>Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).</p>
NetBIOS Scope ID	<div></div> <p>A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID.</p>
WINS Server 1	<div></div> <p>A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.</p>
WINS Server 2	<div></div> <p>A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.</p>

Enfin, la dernière étape nous permet de créer automatiquement les règles que le pare-feu doit mettre en place pour le bon fonctionnement du VPN.

Firewall Rule Configuration	
Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.	
Traffic from clients to server	
Firewall Rule	<input checked="" type="checkbox"/>
Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.	
Traffic from clients through VPN	
OpenVPN rule	<input checked="" type="checkbox"/>
Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.	
Configuration Complete!	
The configuration is now complete.	
To be able to export client configurations, browse to System->Packages and install the OpenVPN Client Export package.	

À la fin de la procédure, on nous demande d'installer le paquet OpenVPN Client Export pour pouvoir exporter la configuration pour se connecter au VPN.

Outre que la configuration, dans le menu OpenVPN -> Client Export Utility on a la possibilité de télécharger le client OpenVPN pour différent OS. Dans notre cas, on a dû cocher aussi l'option Legacy Client, car le client mis à disposition par pfSense était en version 2.4.9.

OpenVPN Server	
Remote Access Server	VPN Eval w/ pfSense UDP4:1194
Client Connection Behavior	
Host Name Resolution	Interface IP Address
Verify Server CN	Automatic - Use verify-x509-name where possible Optionally verify the server certificate Common Name (CN) when the client connects.
Block Outside DNS	<input type="checkbox"/> Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.
Legacy Client	<input checked="" type="checkbox"/> Do not include OpenVPN 2.5 settings in the client configuration. When using an older client (OpenVPN 2.4.x), check this option to prevent the exporter from placing known-incompatible settings into the client configuration.
Silent Installer	<input type="checkbox"/> Create Windows installer for unattended deploy. Create a silent Windows Installer for unattended deploy. Since this installer is not signed, you may need special software to deploy it correctly.
Use Random Local Port	<input type="checkbox"/> Use a random local source port (lport) for traffic from the client. Without this set, two clients may not run concurrently.
Certificate Export Options	
PKCS#11 Certificate Storage	<input type="checkbox"/> Use PKCS#11 storage device (cryptographic token, HSM, smart card) instead of local files.
Microsoft Certificate Storage	<input type="checkbox"/> Use Microsoft Certificate Storage instead of local files.
Password Protect Certificate	<input type="checkbox"/> Use a password to protect the pkcs12 file contents or key in Viscosity bundle.
Proxy Options	
Use A Proxy	<input type="checkbox"/> Use proxy to communicate with the OpenVPN server.

Avant de pouvoir se connecter à la VPN il faut créer un utilisateur dans la database du pare-feu. Ceci peut-être fait depuis le menu System -> User Manager. Lors de la création de l'utilisateur, on a également la possibilité de lui assigner des certificats.

The screenshot displays the pfSense User Manager 'Edit' page for a user named 'vpn'. The breadcrumb trail at the top is 'System / User Manager / Users / Edit'. Below the breadcrumb, there are tabs for 'Users', 'Groups', 'Settings', and 'Authentication Servers', with 'Users' being the active tab. The 'User Properties' section contains the following fields:

- Defined by:** USER
- Disabled:** ☐ This user cannot login
- Username:** vpn
- Password:** Two masked password fields (****).
- Full name:** VPN user (with a note: 'User's full name, for administrative information only').
- Expiration date:** 12/31/2021 (with a note: 'Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY').
- Custom Settings:** ☐ Use individual customized GUI options and dashboard layout for this user.
- Group membership:** A list containing 'admins'.
- Buttons:** '>> Move to "Member of" list' and '<< Move to "Not member of" list'.
- Footer note:** 'Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.'

The 'Certificate' section is checked with the option 'Click to create a user certificate'. Below this is the 'Create Certificate for User' section with the following fields:

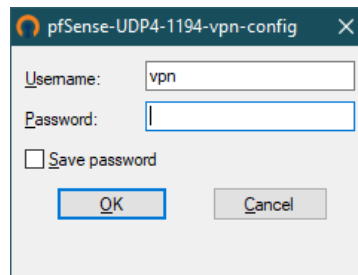
- Descriptive name:** VPN user CA
- Certificate authority:** OpenVPN CA (dropdown)
- Key type:** RSA (dropdown)
- Key length:** 4096 (dropdown, with a note: 'The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.').
- Digest Algorithm:** sha256 (dropdown, with a note: 'The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid.').
- Lifetime:** 3650 (dropdown).

The 'Keys' section at the bottom contains two fields:

- Authorized SSH Keys:** A text area with a note: 'Enter authorized SSH keys for this user'.
- IPsec Pre-Shared Key:** A text field.

Après la création de l'utilisateur, on peut tester la connexion VPN. Ceci a été fait depuis une machine Windows (qui est la machine hôte de la VM).

Lors de la connexion, une fenêtre d'authentification s'affiche :



C'est où on rentre l'identifiant que l'on vient de créer. Après quelques instants, on est bien connectés et le pare-feu nous a assigné une nouvelle adresse IP, interne à son réseau.

On peut tester le bon fonctionnement de la VPN en faisant un ping sur le poste client qui est derrière le pare-feu. Si on fait un ping avant de se connecter au VPN, on obtient le résultat suivant :

```
C:\Users\sergi>ping 192.168.253.25 -n 2

Pinging 192.168.253.25 with 32 bytes of data:
Request timed out.
Request timed out.

Ping statistics for 192.168.253.25:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
```

Si on fait un ping après s'être connectés :

```
C:\Users\sergi>ping 192.168.253.25 -n 2

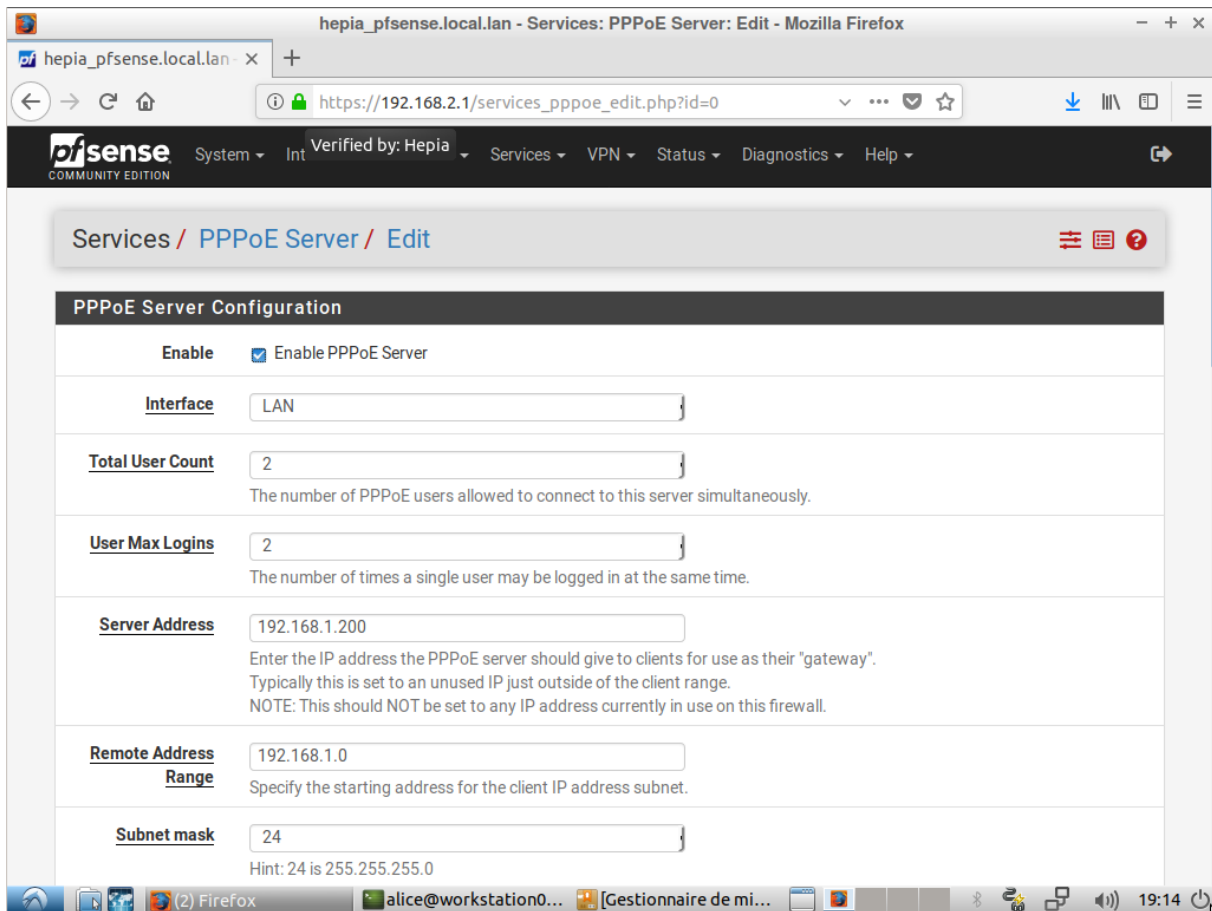
Pinging 192.168.253.25 with 32 bytes of data:
Reply from 192.168.253.25: bytes=32 time=1ms TTL=64
Reply from 192.168.253.25: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.253.25:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

On peut donc constater que la connexion VPN a bien fonctionné.

7. Configuration d'un serveur PPPoE

Depuis la console d'administration pfSense, nous créons un serveur PPPoE, comme suit :

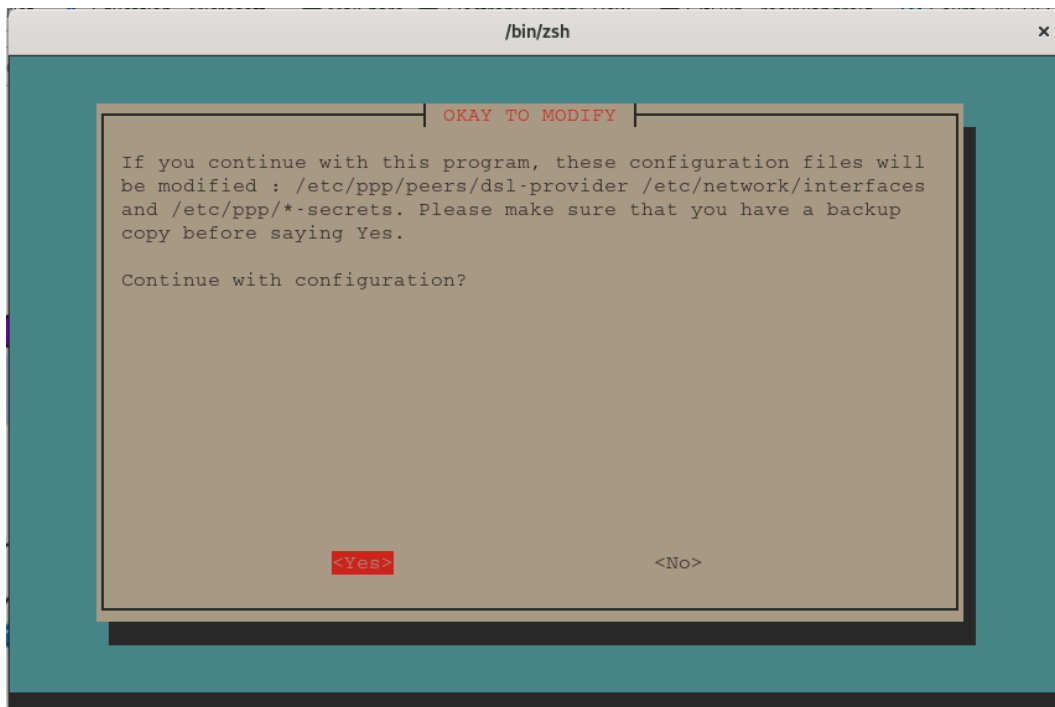


Tous les autres paramètres n'ont subi aucune modification hormis l'User Table. Nous avons défini arbitrairement qu'Alice pourrait se connecter avec le mot de passe labo sur le poste qui possède l'IP 192.168.2.2.

Machine hôte (Debian 10)

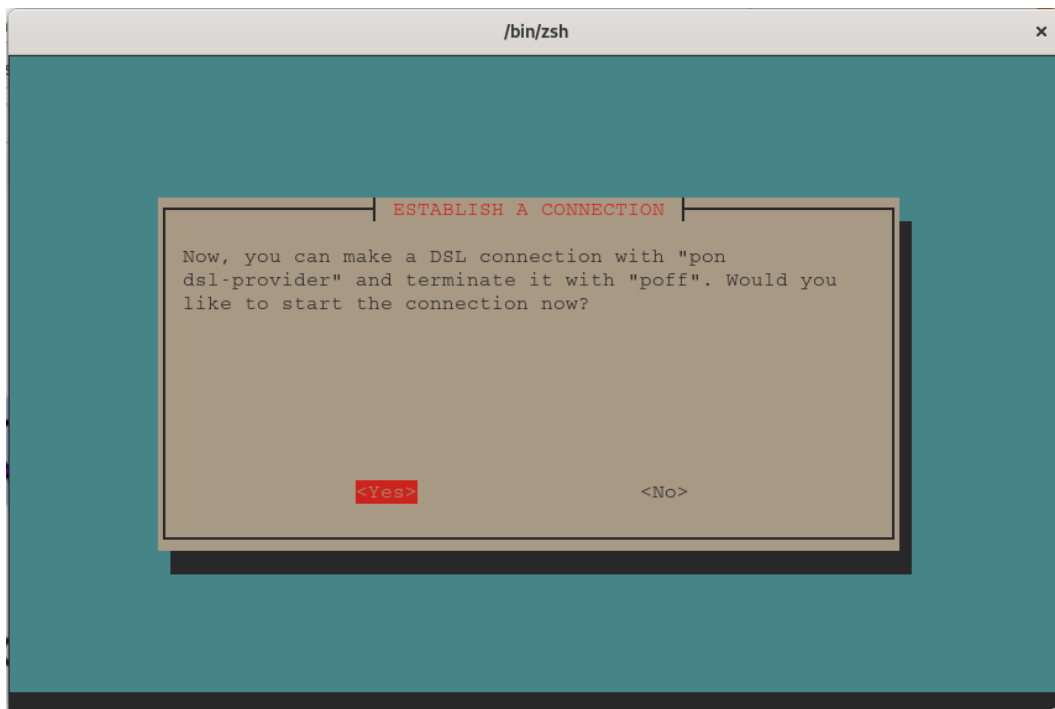
Une fois que le serveur est en place, nous configurons un poste de travail qui se trouve hors du réseau local. La commande ci-dessous modifie les fichiers `/etc/ppp/peers/dsl-provider` et `/etc/network/interfaces`

```
sudo pppoeconf
```



Avant de continuer, nous nous copions les fichiers mentionnés :

```
baud@debian ~ % sudo cp /etc/network/interfaces{,.bak}
baud@debian ~ % ls -sla $_
4 -rw-r--r-- 1 root root 470 Sep 19 15:42 /etc/network/interfaces.bak
baud@debian ~ % sudo cp /etc/ppp/peers/dsl-provider{,.bak}
baud@debian ~ % ls -sla $_
4 -rw-r----- 1 root dip 221 Sep 19 15:44 /etc/ppp/peers/dsl-provider.bak
```



Nous pouvons initier une nouvelle connexion de la façon suivante :

```
baud@debian ~ % pon dsl-provider
Plugin rp-pppoe.so loaded.
baud@debian ~ % plog
tail: cannot open '/var/log/syslog' for reading: Permission denied
baud@debian ~ % sudo plog
[sudo] password for baud:
Sep 21 19:16:36 debian pppd[9966]: remote IP address 192.168.1.200
Sep 21 19:16:36 debian pppd[9966]: primary   DNS address 192.168.2.1
baud@debian ~ %
```

Nous pouvons contrôler les périodes de connexion comme l'illustre la capture d'écran suivante :

