



NICOLAS LECA

ROUTEUR / SWITCH

**EN COLLABORATION AVEC JAKUB
WERLINSKI (BINÔME INFORMATIQUE)**

1. Introduction

1.1. Explication du concept

Au cœur de notre infrastructure réseau, nous avons déployé un ensemble d'équipements essentiels : un routeur, un commutateur et un point d'accès. Ces trois éléments jouent un rôle central dans la gestion des communications au sein de notre réseau. Ils assurent la connectivité et le routage des données entre les divers appareils et sous-réseaux de manière efficace et sécurisée.

Dans cette configuration, nous garantissons une connectivité fiable et optimale tant pour les périphériques câblés que sans fil. Le commutateur et le routeur gèrent le trafic de manière efficace, tandis que le point d'accès offre une connectivité sans fil sécurisée. Voici les détails des adresses et des mots de passe associés à chaque équipement :

Elément	Type	Adresse	Mot de passe
Routeur	PfSense	10.0.0.1/29	Azerty13!
Commutateur	Netgear GS108Ev3.	10.0.0.2/29	Azerty13!
Point d'accès	D-Link DAP-1360	192.10.10.250/24	Azerty13!

1.2. Les dispositifs

1.2.1. Routeur (PfSense)



Notre routeur est une solution **PfSense**, un pare-feu réseau polyvalent qui offre une gamme de fonctionnalités avancées. Il assure une protection contre les menaces, facilite les connexions VPN sécurisées et simplifie la gestion du réseau pour les petites et moyennes entreprises.

1.2.2. Commutateur (Netgear GS108Ev3)



Notre commutateur, un **Netgear GS108Ev3**, se distingue par son interface graphique conviviale facilitant la configuration et la gestion du réseau. Il prend en charge les VLAN pour une segmentation efficace du réseau, et ses huit ports Gigabit garantissent des connexions rapides et fiables pour nos appareils.

1.2.3. Point d'accès (D-Link DAP-1360)



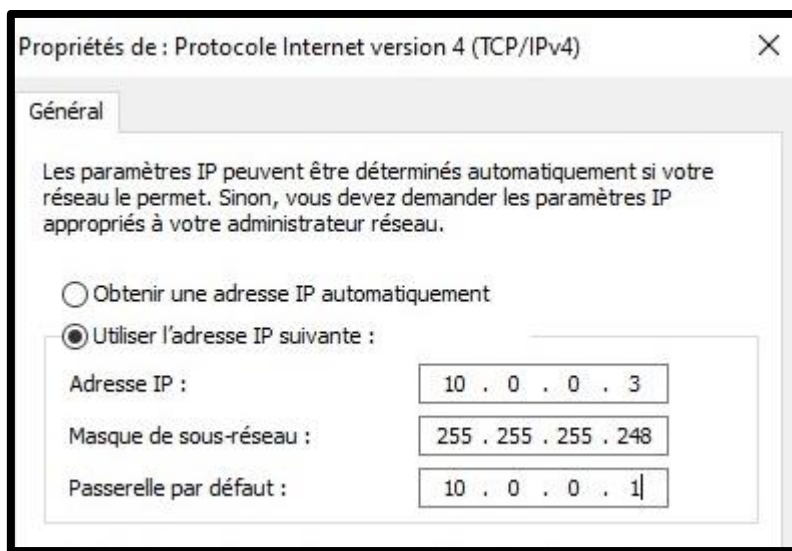
Enfin, notre point d'accès sans fil **D-Link DAP-1360** offre une connectivité rapide et sécurisée. Avec ses fonctionnalités avancées et sa facilité d'installation, il étend la portée de notre réseau sans fil et améliore la connectivité pour les utilisateurs.

2. Mise en place

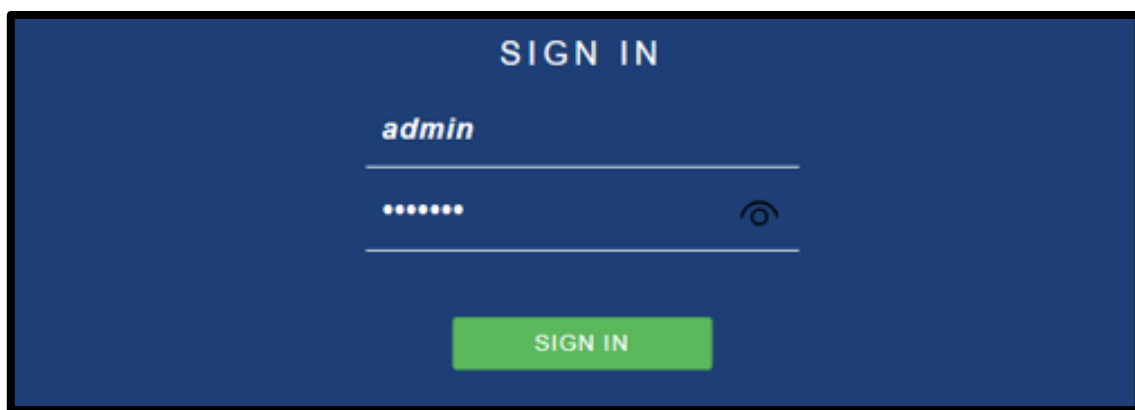
2.1. PfSense

2.1.1. Configuration Basique

1. Après avoir installé pfSense, nous accédons à son interface web via l'adresse LAN (10.0.0.1) et les paramètres par défaut (admin/pfSense).



2. Après l'installation de pfSense, nous y accédons via l'interface web en utilisant l'adresse LAN (10.0.0.1) et les paramètres par défaut (admin/pfSense).



3. Dans l'interface, nous passons par le wizard de la configuration basique pour introduire les détails tels que le nom d'hôte, le domaine et le fuseau horaire.

General Information

On this screen the general pfSense parameters will be set.

Hostname
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw

Domain

Time Server Information

Please enter the time, date and time zone.

Time server hostname
Enter the hostname (FQDN) of the time server.

Timezone

Configure WAN Interface

On this screen the Wide Area Network information will be configured.

SelectedType

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask

4. Nous personnalisons également le mot de passe (Azerty13!). La configuration basique de pfSense est alors complète.

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI.

Admin Password

.....

Admin Password AGAIN

.....

👁

2.1.2. Configuration des cartes réseau

1. Configuration de la carte réseau WAN

Interfaces / WAN (em0)

General Configuration

Enable

☒ Enable interface

Description

WAN

Enter a description (name) for the interface here.

IPv4 Configuration Type

DHCP

▼

IPv6 Configuration Type

None

▼

Reserved Networks

Block private networks and loopback addresses

☐

Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks

☐

Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

2. Configuration de la carte réseau LAN

Interfaces / LAN (re0)

General Configuration

Enable

☒ Enable interface

Description

LAN

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

Static IPv4 Configuration

IPv4 Address

10.0.0.1

/ 29

IPv4 Upstream gateway

None

+ Add a new gateway

3. Configuration de la carte réseau DMZ

Interfaces / DMZ (re1)

General Configuration

Enable

☒ Enable interface

Description

DMZ

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

Static IPv4 Configuration

IPv4 Address

176.7.1.5

/ 29

IPv4 Upstream gateway

None

+ Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the [Add gateway](#) button.

On local area network interfaces the upstream gateway should be "none".

Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).

Gateways can be managed by [clicking here](#).

2.1.3. Configuration des VLANs sur pfSense

1. Nous configurons les interfaces réseaux virtuels dans **Interfaces -> Assignements -> VLANs**. Nous créons les **VLANs 10, 20 et 30**.

Interfaces / VLANs

Interface Assignments Interface Groups Wireless **VLANs** QinQs PPPs GREs GIFs Bridges LAGGs

Interface	VLAN tag	Priority	Description	Actions
re0 (lan)	10		VLAN Entreprise	
re0 (lan)	20		VLAN WIFI	
re0 (lan)	30		Réseau d'urgence	

+ Add

Configuration du VLAN 10 :

VLAN Configuration

Parent Interface re2 (b4:b0:24:ca:5d:6f) - lan
Only VLAN capable interfaces will be shown.

VLAN Tag 10
802.1Q VLAN tag (between 1 and 4094).

VLAN Priority 0
802.1Q VLAN Priority (between 0 and 7).

Description VLAN 10 Entreprise
A group description may be entered here for administrative reference (not parsed).

Configuration du VLAN 20

VLAN Configuration

Parent Interface re2 (b4:b0:24:ca:5d:6f) - lan
Only VLAN capable interfaces will be shown.

VLAN Tag 20
802.1Q VLAN tag (between 1 and 4094).

VLAN Priority 0
802.1Q VLAN Priority (between 0 and 7).

Description VLAN WIFI
A group description may be entered here for administrative reference (not parsed).

Configuration du VLAN 30

VLAN Configuration

Parent Interface	re2 (b4:b0:24:ca:5d:6f) - lan
Only VLAN capable interfaces will be shown.	
VLAN Tag	30
802.1Q VLAN tag (between 1 and 4094).	
VLAN Priority	0
802.1Q VLAN Priority (between 0 and 7).	
Description	Réseau d'urgence
A group description may be entered here for administrative reference (not parsed).	

2. Activation des VLANs dans **Interface Assignements**.

Interface Assignements Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

Interface	Network port	
WAN	em0 (c8:7f:54:ce:1a:7e)	
LAN	re0 (10:27:f5:26:e7:48)	Delete
DMZ	re1 (10:27:f5:26:e6:43)	Delete
VLAN10	VLAN 10 on re0 - lan (VLAN Entreprise)	Delete
VLAN20	VLAN 20 on re0 - lan (VLAN WIFI)	Delete
Available network ports:	VLAN 30 on re0 - lan (Réseau d'urgence)	+ Add

3. Finalement, nous allons configurer chacun des VLANs en leur cliquant dessus comme cela est indiqué ici :

Configuration VLAN10

Interfaces / OPT2 (re0.10)

General Configuration

Enable

☒ Enable interface

Description

VLAN10

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

Static IPv4 Configuration

IPv4 Address

192.1.1.254

/

24

IPv4 Upstream gateway

None

+ Add a new gateway

Configuration VLAN20

General Configuration

Enable

☒ Enable interface

Description

VLAN20

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

Static IPv4 Configuration

IPv4 Address

192.10.10.254

/

24

IPv4 Upstream gateway

None

Configuration VLAN30

Interfaces / **OPT4 (re0.30)**

General Configuration

Enable ☒ Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4 Configuration

IPv4 Address
 /

IPv4 Upstream gateway

4. Après avoir activé les **VLANs** dans **Interface Assignements**, nous configurons chacun d'entre eux en définissant les règles nécessaires dans **Firewall -> Rules**.

The screenshot shows the Mikrotik WinBox Firewall configuration interface. A red box labeled '1' highlights the 'Firewall' menu in the top navigation bar. A dropdown menu is open, and a red box labeled '2' highlights the 'Rules' option. In the background, the 'VLAN Assignments' tab is visible, with a red box labeled '4' highlighting 'VLAN30' in the list. Below the list, a table with columns 'Source', 'Port', 'Destination', 'Port', and 'Gateway' is partially visible. A yellow warning banner states: 'Interface will be blocked until pass rules are added. Click the button to add a rule.' At the bottom right, a green 'Add' button with an upward arrow icon is highlighted with a red box labeled '5'.

Ainsi nous configurons chacun de nos VLANs comme cela est indiqué ici :

Configuration VLAN10

Edit Firewall Rule	
<u>Action</u>	Pass Choose what to do with packets that match the criteria specified below.
<u>Interface</u>	VLAN10 Choose the interface from which packets must come to match this rule.
<u>Address Family</u>	IPv4+IPv6 Select the Internet Protocol version this rule applies to.
<u>Protocol</u>	Any Choose which IP protocol this rule should match.
Source	
<u>Source</u>	☐ Invert match any
Destination	
<u>Destination</u>	☐ Invert match any

Configuration VLAN20

Edit Firewall Rule	
<u>Action</u>	Pass Choose what to do with packets that match the criteria specified below.
<u>Interface</u>	VLAN20 Choose the interface from which packets must come to match this rule.
<u>Address Family</u>	IPv4+IPv6 Select the Internet Protocol version this rule applies to.
<u>Protocol</u>	Any Choose which IP protocol this rule should match.

Source		
<u>Source</u>	☐ Invert match	any

Destination		
<u>Destination</u>	☐ Invert match	any

Configuration VLAN30

Edit Firewall Rule	
<u>Action</u>	Pass

Choose what to do with packets that match the criteria specified below.

<u>Interface</u>	VLAN30
------------------	--------

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

<u>Address Family</u>	IPv4+IPv6
-----------------------	-----------

Select the Internet Protocol version this rule applies to.

<u>Protocol</u>	Any
-----------------	-----

Choose which IP protocol this rule should match.

Source		
<u>Source</u>	☐ Invert match	any

Destination		
<u>Destination</u>	☐ Invert match	any

5. Nous ajoutons un DHCP Relay pour canaliser les plages d'adresses IP configurées sur notre serveur AD1 (**Services -> DHCP Relay**).

DHCP Relay Configuration

Enable ☒ Enable DHCP Relay on interface

Interface(s)
 LAN
 VLAN10
 VLAN20
 VLAN30
Interfaces without an IP address will not be shown.

CARP Status VIP
 none
Used to determine the HA MASTER/BACKUP status. DHCP Relay will be stopped with status.

☐ Append circuit ID and agent ID to requests
If this is checked, the DHCP Relay will append the circuit ID (pfSense interface number) to requests.

Destination server
 192.7.1.1
This is the IPv4 address of the server to which DHCP requests are relayed.

Save **+ Add server**

6. Nous interdisons la communication sortante depuis les **VLANs 20 et 10** vers le **VLAN 30** pour des raisons de sécurité.

Floating	WAN	LAN	DMZ	VLAN10	VLAN20	VLAN30
----------	-----	-----	-----	--------	--------	--------

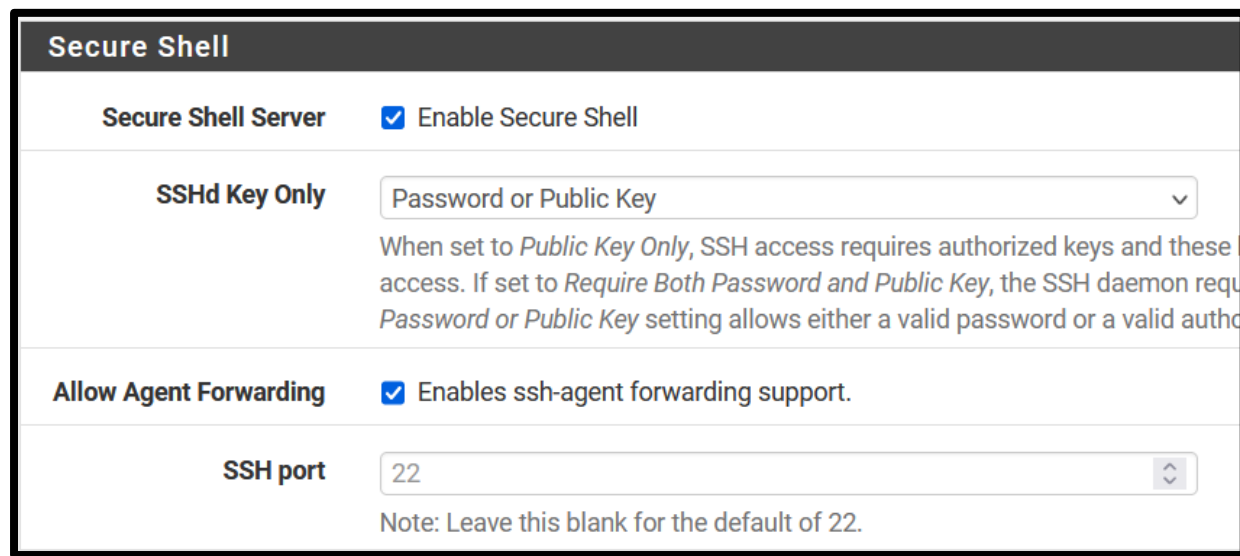
Rules (Drag to Change Order)

☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
☐	 0/1 KiB	IPv4 *	VLAN10 net	*	VLAN30 net	*	*	none		
☐	 0/3.79 GiB	IPv4+6 *	*	*	*	*	*	none		

Floating	WAN	LAN	DMZ	VLAN10	VLAN20	VLAN30				
Rules (Drag to Change Order)										
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
☐	 0/0 B	IPv4 *	VLAN20 net	*	VLAN30 net	*	*	none		
☐	 0/13.33 MiB	IPv4+6 *	*	*	*	*	*	none		

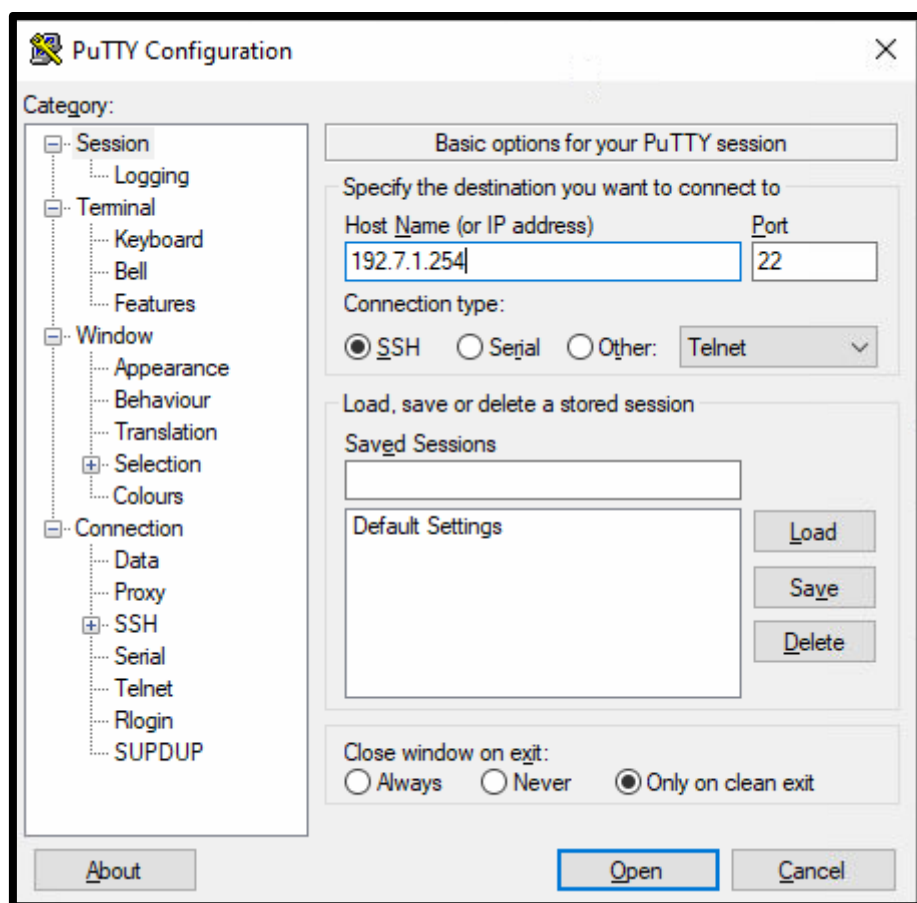
2.1.4. Configuration de la connexion en SSH

1. Pour accéder à pfSense via SSH, nous configurons cette fonctionnalité dans **System** -> **Advanced** -> **Admin Access**.



The screenshot shows the 'Secure Shell' configuration page in pfSense. The 'Secure Shell Server' section has a checkbox 'Enable Secure Shell' which is checked. Below it, the 'SSHd Key Only' dropdown is set to 'Password or Public Key'. A note explains that 'Public Key Only' requires authorized keys, while 'Require Both Password and Public Key' requires both. The 'Allow Agent Forwarding' checkbox is also checked, with a note that it enables ssh-agent forwarding support. The 'SSH port' is set to 22, with a note to leave it blank for the default of 22.

2. Après avoir configuré l'accès SSH côté pfSense, nous y accédons via un outil tel que PuTTY.



The screenshot shows the PuTTY Configuration dialog box. The 'Category' list on the left has 'SSH' selected. The 'Basic options for your PuTTY session' section shows 'Host Name (or IP address)' set to 192.7.1.254 and 'Port' set to 22. The 'Connection type' is set to 'SSH'. The 'Load, save or delete a stored session' section shows a list of 'Saved Sessions' with 'Default Settings' selected. The 'Close window on exit' section has 'Only on clean exit' selected. The 'Open' button is highlighted.

```
192.7.1.254 - PuTTY
| Password for admin@pfSense.pfsense.s7pl:
| End of keyboard-interactive prompts from server
pfSense - Serial: 230216180901976 - Netgate Device ID: 63b5b0bfal26e59c586e

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

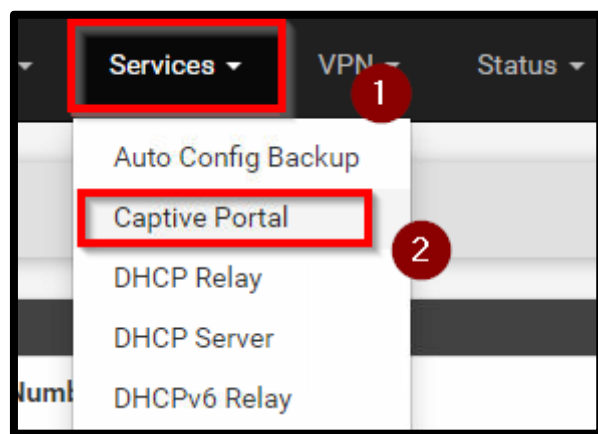
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.154/24
LAN (lan)      -> re0      -> v4: 10.0.0.1/29
DMZ (opt1)     -> rel      -> v4: 176.7.1.5/29
VLAN10 (opt2)  -> re0.10   -> v4: 192.7.1.254/24
VLAN20 (opt3)  -> re0.20   -> v4: 192.70.10.254/24
VLAN30 (opt4)  -> re0.30   -> v4: 192.7.10.254/24

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

Enter an option: █
```

2.1.5. Configuration de Portail Captif

1. Pour configurer le portail captif, nous nous rendrons dans **Services -> Captive Portal -> Add**



2. Nous configurons l'interface réseau sur laquelle le portail captif sera utilisé (dans notre cas, VLAN20).



3. Nous activons une fenêtre contextuelle ainsi que le site par défaut, dans notre cas Google.

Logout popup window	☒ Enable logout popup window If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.
Pre-authentication redirect URL	http://google.fr Set a default redirection URL. Visitors will be redirected to this URL after authentication only if the captive portal doesn't know where to redirect them. This field will be accessible through \$PORTAL_REDIRECTURL\$ variable in captiveportal's HTML pages.
After authentication Redirection URL	http://google.fr Set a forced redirection URL. Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated.

4. Ensuite, nous configurons le serveur d'authentification.

Authentication	
Authentication Method	Use an Authentication backend Select an Authentication Method to use for this zone. One method must be selected. - "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers. - "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button. - "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.
Authentication Server	Local Database You can add a remote authentication server in the User Manager . Vouchers could also be used, please go to the Vouchers Page to enable them.
Secondary authentication Server	Local Database You can optionally select a second set of servers to authenticate users. Users will then be able to login using separated HTML inputs. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.
Reauthenticate Users	☐ Reauthenticate connected users every minute If reauthentication is enabled, request are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in; The cached credentials are necessary for the portal to perform automatic reauthentication requests.
Local Authentication Privileges	☒ Allow only users/groups with "Captive portal login" privilege set

5. Nous ajoutons le groupe d'utilisateurs ayant accès au portail captif (**System -> User Manager -> Groups -> Add**) et nous lui attribuons les privilèges nécessaires.

Groups			
Group name	Description	Member Count	Actions
Portail	Utilisateurs du portail	0	  
admins	System Administrators	1	 
all	All Users	1	 

Nous la modifions pour qu'elle aurait les privilèges de « **User – Services: Captive Portal login** »

6. Enfin, nous créons un profil utilisateur qui aura les droits d'accès au portail captif (**System -> User Manager -> User**).

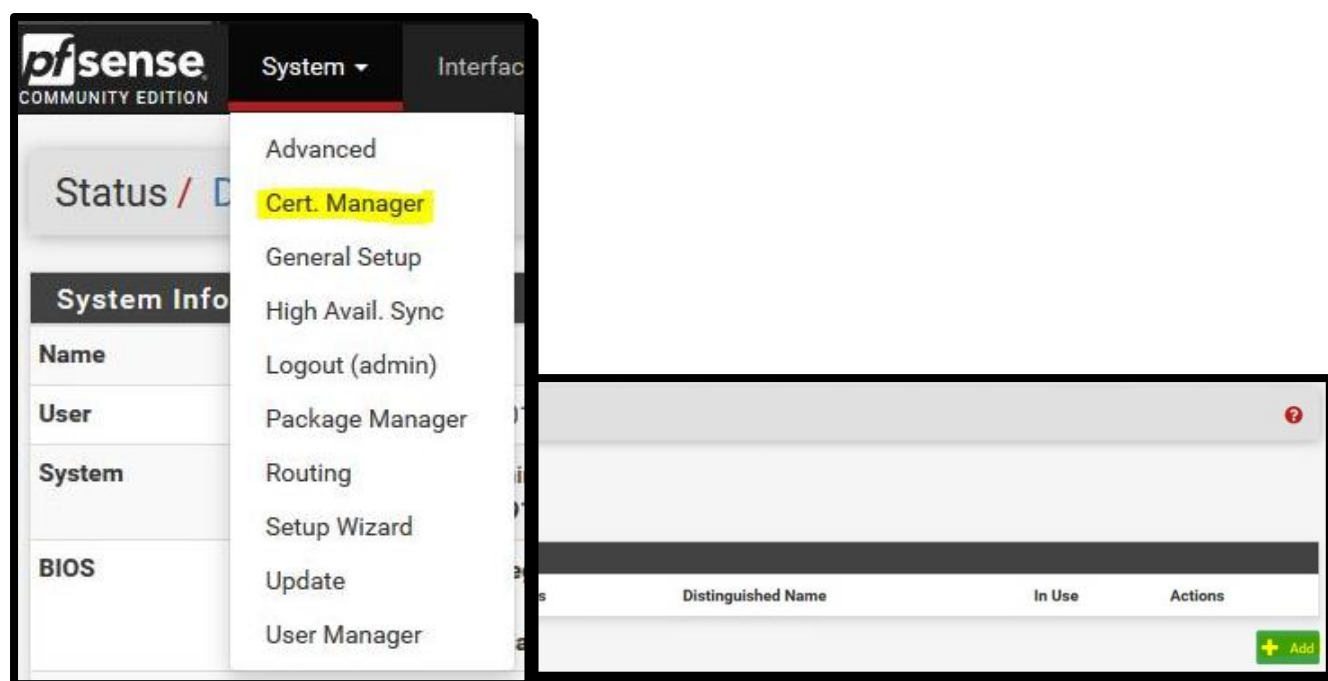
User Properties	
Defined by	USER
Disabled	☐ This user cannot login
Username	technicien
Password	***** *****
Full name	 User's full name, for administrative information only
Expiration date	 Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY
Custom Settings	☐ Use individual customized GUI options and dashboard layout for this user.
Group membership	admins Not member of Portail Member of

2.1.6. Configuration du VPN

Pour accéder à distance à notre réseau, nous allons configurer l'accès via un VPN (Réseau Virtuel Privé), qui nous offre un accès sécurisé.

2.1.6.1 Création d'autorité de certificat

1. Accédez à **Système -> Cert. Manager**, puis cliquez sur "**Add**" pour créer un certificat nécessaire pour le VPN.



2. Choisissez un nom pour votre autorité de certification, par exemple "**VPNS1P1**", et conservez les autres paramètres par défaut. Enregistrez ensuite.

Create / Edit CA

Descriptive name

VPNS1P1

The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '.

Method

Create an internal Certificate Authority

Trust Store

☐ Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial

☐ Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Voici le certificat que nous venons de créer :

Certificate Authorities				
Name	Internal	Issuer	Certificates	Distinguished Name
VPNS1P1	✓	self-signed	2	CN=VPNS1P1 ⓘ Valid From: Tue, 26 Mar 2024 09:44:51 +0100 Valid Until: Fri, 24 Mar 2034 09:44:51 +0100

2.1.6.2 Création de certificat

1. Sous l'autorité de certification créée précédemment, cliquez sur "**Add/Sign**" pour créer un certificat.

Name	In Use	Actions
Configurator Self-Signed Certificate, 585b1f61a12 		     
2 Mar 2021 09:53:51 +0100		
Apr 2022 10:53:51 +0200		

 Add/Sign

2. Sélectionnez "**Certificat interne**" comme méthode et nommez-le, par exemple, "**Certificat VPN**".

Add/Sign a New Certificate

Method

Create an internal Certificate

Descriptive name

Certificat VPN

The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, " , ' , ,

3. Choisissez l'autorité de certification que vous avez créée précédemment.

Internal Certificate

Certificate authority

VPNS1P1

Key type

RSA

4. Configurez le type de certificat comme étant "**Certificat de serveur**" et enregistrez-le.

Certificate Attributes

Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

For Internal Certificates, these attributes are added directly to the certificate as shown.

Certificate Type Server Certificate ▼
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names FQDN or Hostname
Type Value

Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

Add + Add

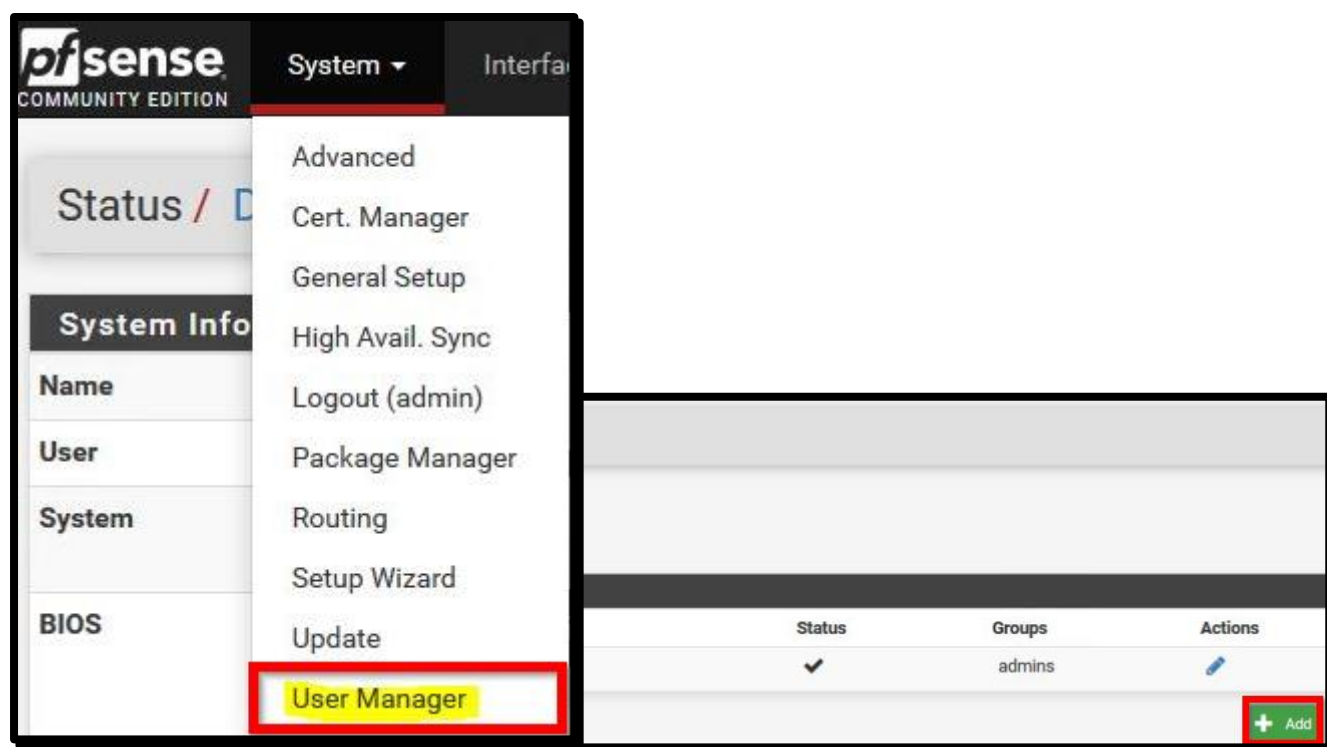
Save

Voici notre certificat que nous venons de créer :

Certificates		
Name	Issuer	Distinguished Name
GUI default (659d0996681a8) Server Certificate	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-659d0996681a8 i
CA: No		Valid From: Tue, 09 Jan 2024 09:53:42 +0100
Server: Yes		Valid Until: Mon, 10 Feb 2025 09:53:42 +0100
Certificat VPN Server Certificate	VPNS1P1	subjectAltName=, CN=Certificat VPN i
CA: No		Valid From: Tue, 26 Mar 2024 09:44:51 +0100
Server: Yes		Valid Until: Mon, 28 Apr 2025 10:44:51 +0200

2.1.6.3 Création des Utilisateurs du VPN

1. Accédez à **Système** -> **User Manager** et cliquez sur **"ADD"** pour ajouter des utilisateurs VPN.



2. Saisissez l'identifiant de l'utilisateur et le mot de passe, puis cochez **"Créer un certificat utilisateur"**.

The image shows the 'User Properties' form in pfSense. The 'Username' field contains the text 'invite' and the 'Password' field contains masked characters. Both fields are highlighted with red boxes. Below the form, there are two buttons: 'Move to "Member of" list' and 'Move to "Not member of" list'. Below these buttons, there is a text prompt: 'Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.' At the bottom, there is a checkbox labeled 'Certificate' which is checked, and a button labeled 'Click to create a user certificate' next to it. This entire section is highlighted with a red box.

3. Saisissez le nom du certificat et sélectionnez l'autorité de certification précédemment créée. Enregistrez les paramètres.

Create Certificate for User

Descriptive name

Certificat user

Certificate authority

VPNS1P1

Puis nous cliquons sur le bouton **Save**.

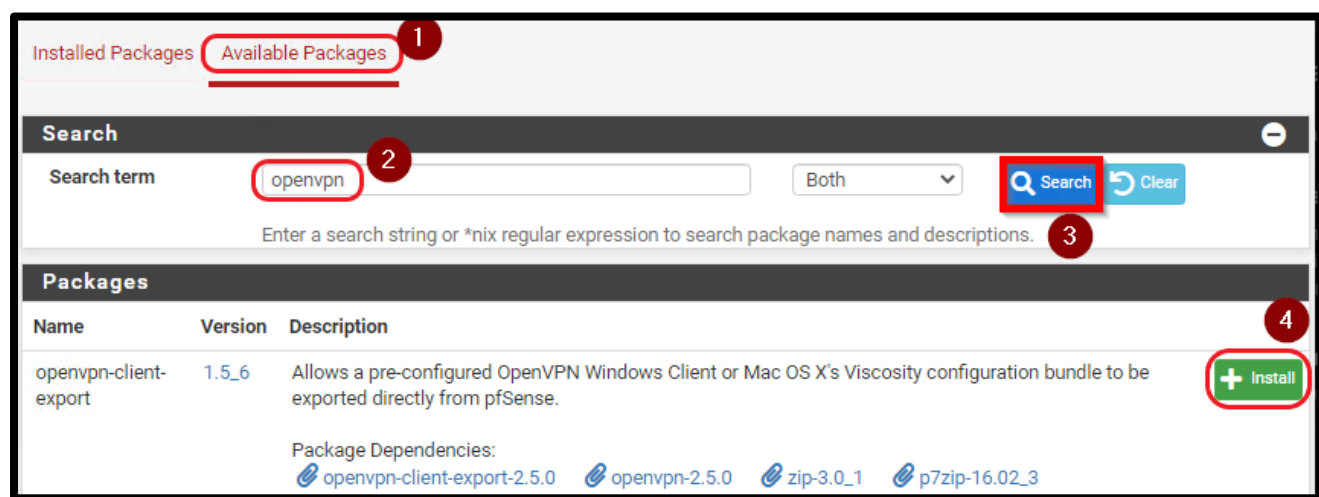
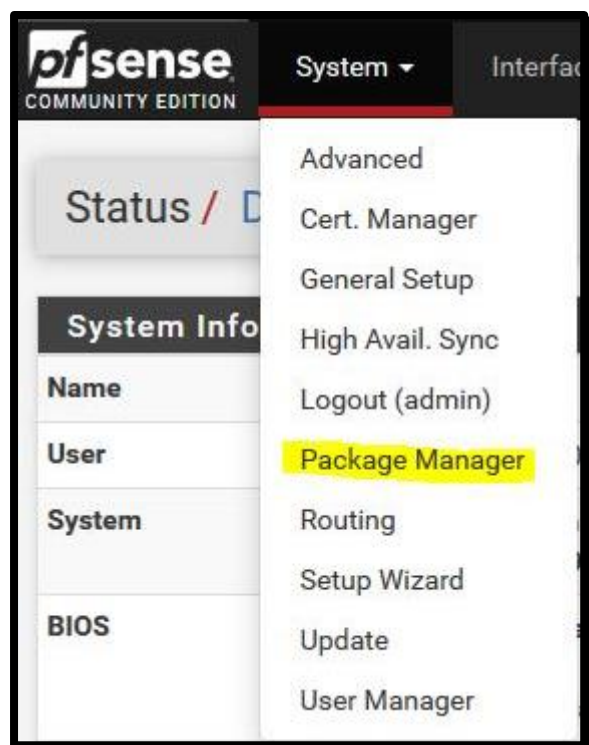
Voici l'utilisateur du VPN que nous venons de créer :

Users				
	Username	Full name	Status	Groups
☐	 admin	System Administrator	✓	admins
☐	 invite		✓	

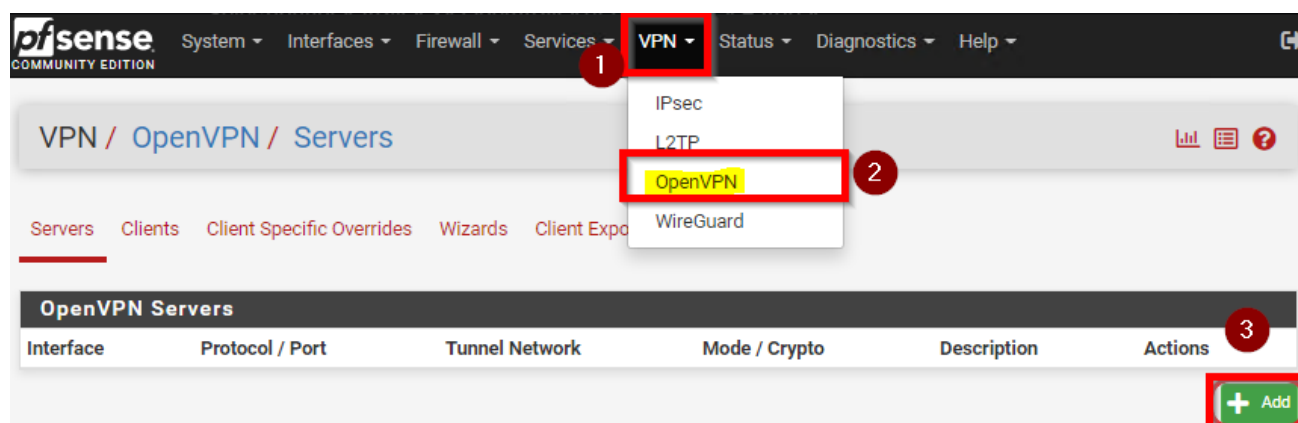
2.1.6.4 Installation et configuration du serveur OpenVPN

Il s'agit d'un utilitaire pour exporter la configuration client au format .ovpn.

1. Allez dans **Système** -> **Gestionnaire de paquets** -> **Paquets disponibles**, recherchez "openvpn" et installez-le.



2. Configurez le serveur en allant dans **VPN -> OpenVPN -> Ajouter**.



3. Configurez le nom du serveur, le mode en "**Accès distant (SSL/TLS)**", et spécifiez le port local.

General Information

Description
A description of this VPN for administrative reference.

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

Mode Configuration

Server mode
Remote Access (SSL/TLS)

Device mode
"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and complete mode.
"tap" mode is capable of carrying 802.3 (OSI Layer 2.)

Endpoint Configuration

Protocol
UDP on IPv4 only

Interface
The interface or Virtual IP address where OpenVPN will receive client connections.

Local port
The port used by OpenVPN to receive client connections.

4. Dans la section '**Paramètres cryptographiques**', nous allons choisir **VPNS1P1** comme notre « **Autorité de certification homologue** » et le certificat du serveur comme « **Certificat VPN** » :

Peer Certificate Authority VPNS1P1

Server certificate Certificat VPN (Server: Yes, CA: VPNS1P1, In Use)

Certificates known to be incompatible with use for OpenVPN are not included in this digest algorithms.

5. Dans la section '**Paramètres du tunnel**', nous allons configurer l'**IPv4 Tunnel Network** sur 10.210.10.0/24 (adresse du réseau VPN). Nous allons cocher la case '**Rediriger la passerelle IPv4**'. Ensuite, nous allons paramétrer le nombre de '**Connexions simultanées**' sur 20, correspondant au nombre de connexions pouvant être établies simultanément.

Tunnel Settings

IPv4 Tunnel Network 10.210.10.0/24

This is the IPv4 virtual network used for private communications between peers. It is in CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server and the remaining usable addresses will be assigned to connecting clients.

Redirect IPv4 Gateway ☒ Force all client-generated IPv4 traffic through the tunnel.

Concurrent connections 20

Specify the maximum number of clients allowed to concurrently connect to this server.

6. Dans la section **Client Settings**, nous allons cocher la case **Dynamic IP** :

Client Settings

Dynamic IP ☒ Allow connected clients to retain their connections if their IP address changes.

7. Dans la section **Advanced Configuration** nous mettons la valeur **auth-nocache**, ce qui signifie que les identifiants ne seront pas mis en cache :

Advanced Configuration

Custom options

auth-nocache

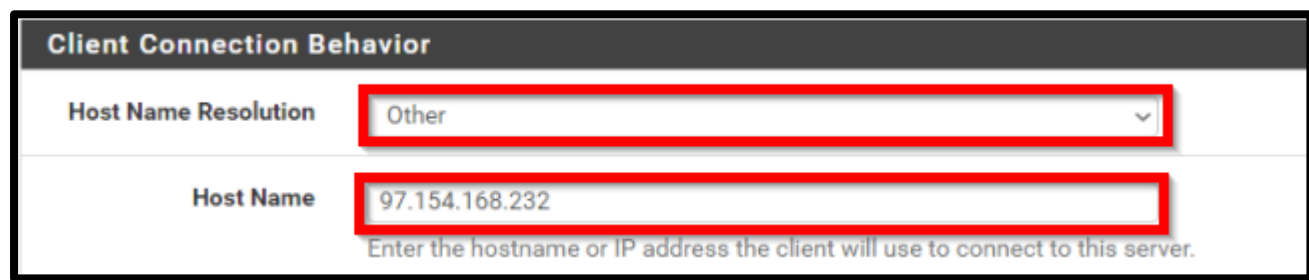
Enter any additional options to add to the OpenVPN server configuration file.
EXAMPLE: push "route 10.0.0.0 255.255.255.0"

Après avoir apporté toutes ces modifications, nous pouvons enfin sauvegarder nos changements. Notre serveur VPN est maintenant créé :

OpenVPN Servers			
Interface	Protocol / Port	Tunnel Network	Mode / Crypto
WAN	UDP4 / 20155 (TUN)	10.210.10.0/24	Mode: Remote Access (SSL/TLS) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits

2.1.6.5 Exportation de la configuration VPN pour le Client

1. Pour exporter la configuration de notre client OpenVPN, nous allons dans **VPN -> OpenVPN -> Export client**, où nous allons configurer le champ de **résolution de nom d'hôte** en "Autre" et le champ de **nom d'hôte** en l'adresse IP publique de notre WAN, dans notre cas 97.154.168.232.



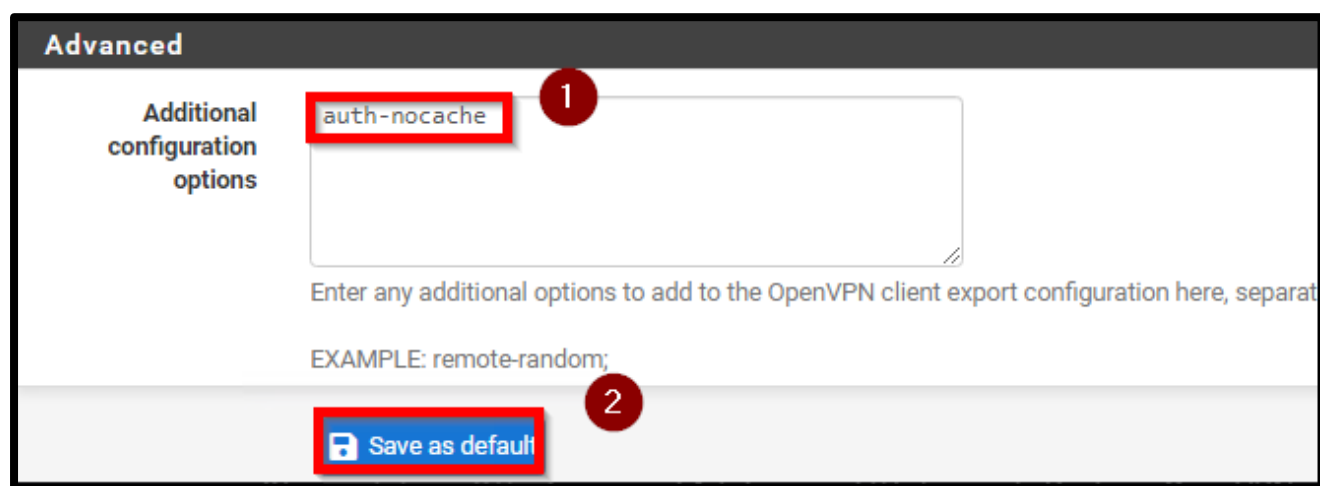
Client Connection Behavior

Host Name Resolution: Other

Host Name: 97.154.168.232

Enter the hostname or IP address the client will use to connect to this server.

2. Dans la section '**Avancé**', nous allons saisir les mêmes paramètres que ceux utilisés dans la configuration du serveur VPN et nous cliquons sur 'Save as default' :



Advanced

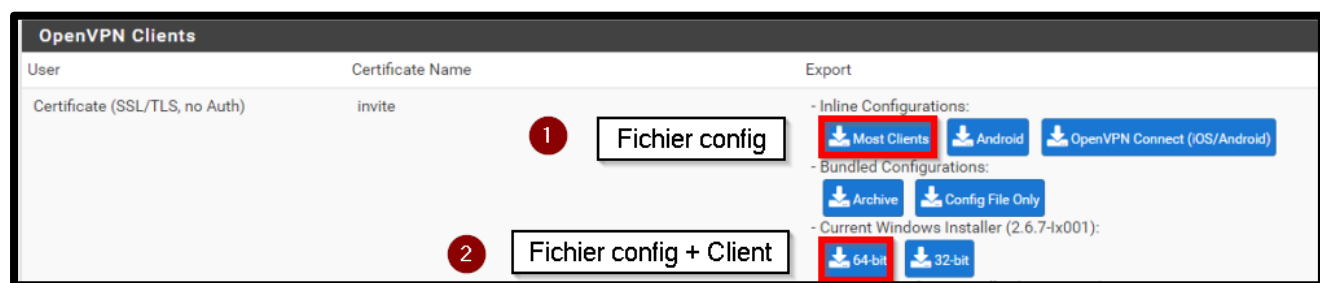
Additional configuration options: auth-nocache

Enter any additional options to add to the OpenVPN client export configuration here, separated by semicolons.

EXAMPLE: remote-random;

Save as default

3. Enfin, toujours sur la même page, nous allons télécharger la configuration de notre OpenVPN. Soit uniquement le fichier de configuration si nous disposons déjà d'un client, soit avec le logiciel client si nous n'en avons pas encore :

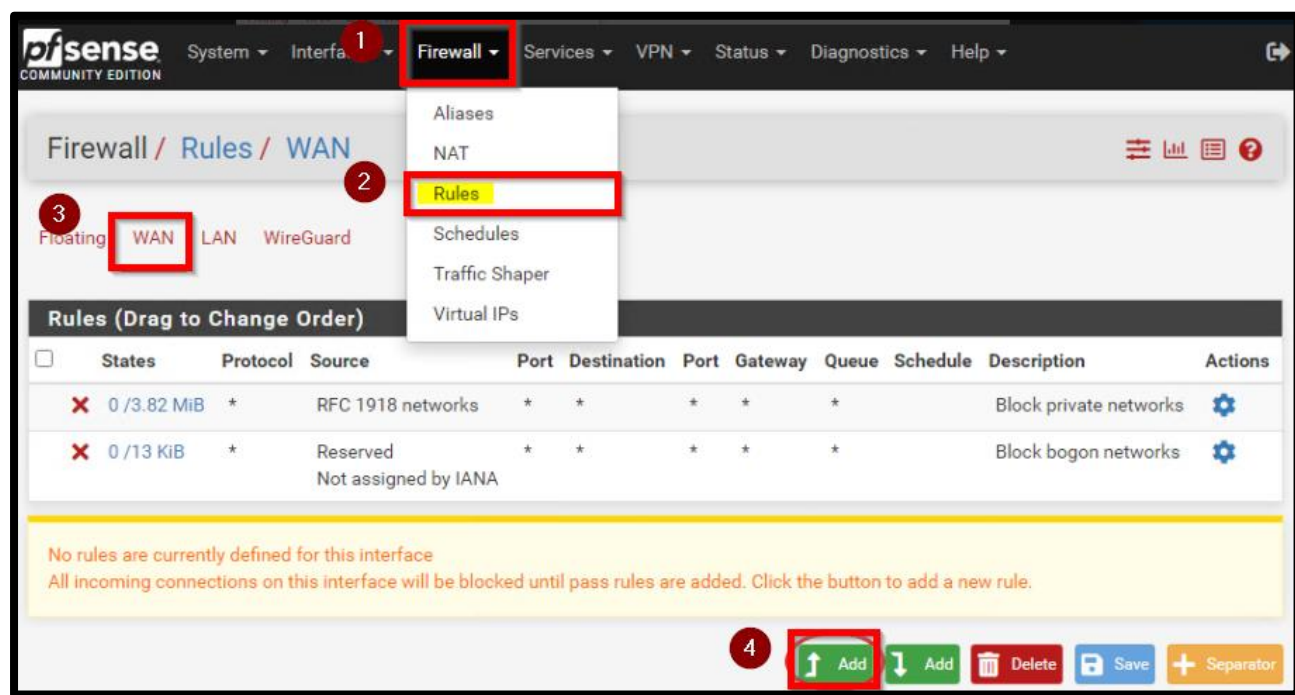


OpenVPN Clients

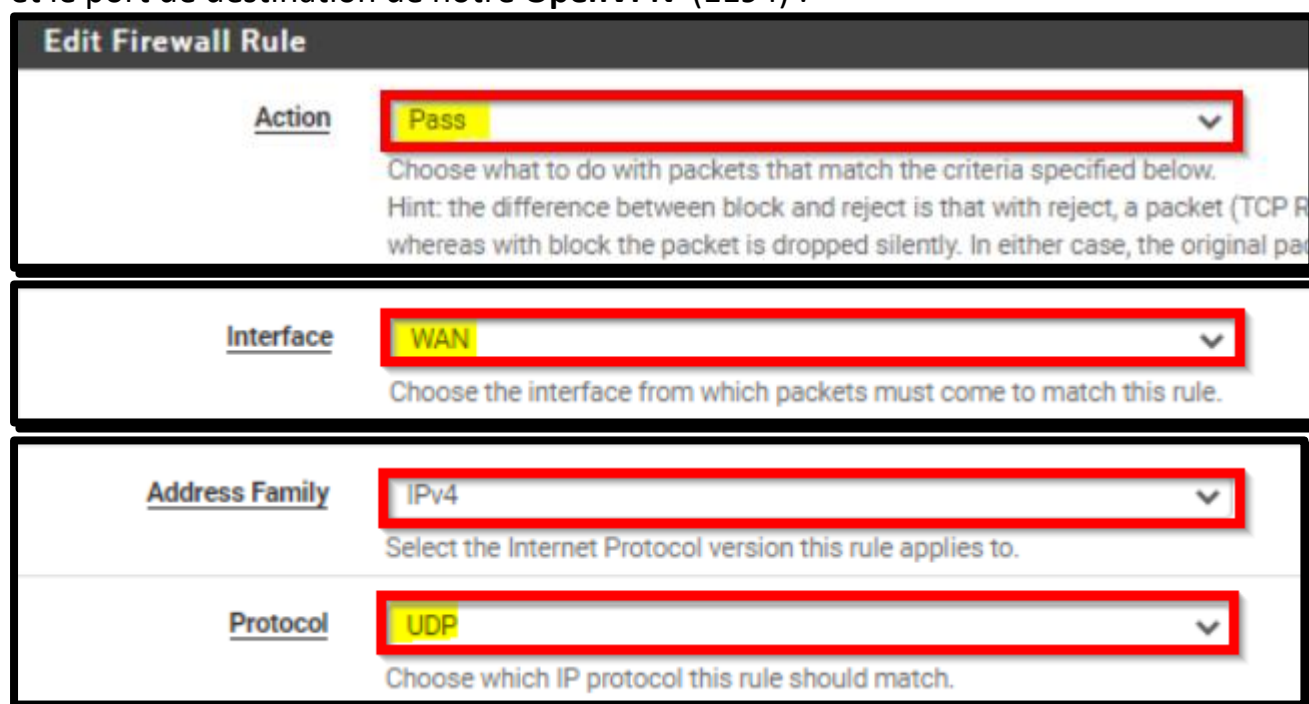
User	Certificate Name	Export
Certificate (SSL/TLS, no Auth)	invite	1 Fichier config 2 Fichier config + Client - Inline Configurations: Most Clients, Android, OpenVPN Connect (iOS/Android) - Bundled Configurations: Archive, Config File Only - Current Windows Installer (2.6.7-1x001): 64-bit, 32-bit

2.1.6.6 Configuration du Pare-Feu (NAT)

1. Pour permettre le passage par le WAN, nous devons configurer les règles de pare-feu. Pour ce faire, nous nous rendrons dans les **règles de pare-feu** -> **WAN**, où nous cliquerons sur **Ajouter**.



2. Là-dedans, nous allons autoriser le passage du protocole **UDP** à travers notre **WAN** et le port de destination de notre **OpenVPN** (1194) :



Source

Source
☐ Invert match

any

Destination

Destination
☐ Invert match

WAN address

Destination Port Range

OpenVPN (1194)

From
Custom
To

OpenVPN (1194)

On sauvegarde les changements.

3. Ensuite, nous allons configurer les règles de pare-feu de l'interface OpenVPN en accédant à **'Firewall' -> 'Rules' -> 'OpenVPN'**, où nous cliquons sur **Ajouter** :

Floating
WAN
LAN
OpenVPN
WireGuard

Rules (Drag to Change Order)

☐
States
Protocol
Source
Port
Destination
Port
Gateway
Queue

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button

Add

4. Là-dedans, nous allons mettre les paramètres suivants :

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below
Hint: the difference between block and reject is that with reject, a packet is returned to the sender, whereas with block the packet is dropped silently

Interface

OpenVPN

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

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

Protocol Any
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match any

Destination

Destination ☐ Invert match any

5. Ensuite, nous nous rendons dans **Interfaces** -> **Assignations**, où nous ajoutons notre interface **OpenVPN**.

6. Puis, dans **Firewall** -> **NAT** -> **Port Forward**, nous cliquons sur **Add** :

pfSense COMMUNITY EDITION

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

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NAT

Rules

☐	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports
4 ↑ Add						

7. Sur la page qui s'affiche, nous allons configurer les paramètres suivants :

Interface	WAN			
	Choose which interface this rule applies to. In most cases "WAN" is specified.			
Address Family	IPv4			
	Select the Internet Protocol version this rule applies to.			
Protocol	TCP			
	Choose which protocol this rule should match. In most cases "TCP" is specified.			

Source	☐ Invert match.	Any		
		Type	Address/mask	
Source port range		Any	Any	
		From port	To port	
		Custom	Custom	
	Specify the source port or port range for this rule. This is usually random and almost never equal to the destination port range (e.g. 'any'). The 'to' field may be left empty if only filtering a single port.			
Destination	☐ Invert match.	WAN address		
		Type	Address/mask	
Destination port range		Other	20155	Other 20155
		From port	To port	
		Custom	Custom	
	Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.			

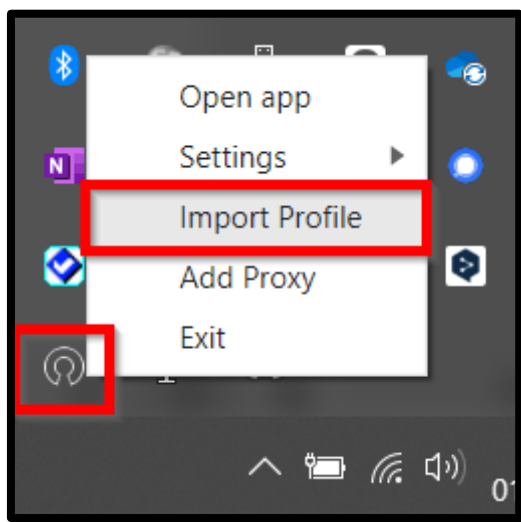
Redirect target IP	OPENVPN address	
	Type	
	Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4. In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1).	
Redirect target port	OpenVPN	
	Port	Custom
	Specify the port on the machine with the IP address entered above. In case of a port range, start and end ports are calculated automatically. This is usually identical to the "From port" above.	
Description	Accès VPN	
	A description may be entered here for administrative reference (not parsed).	

Filter rule association	Pass
--------------------------------	------

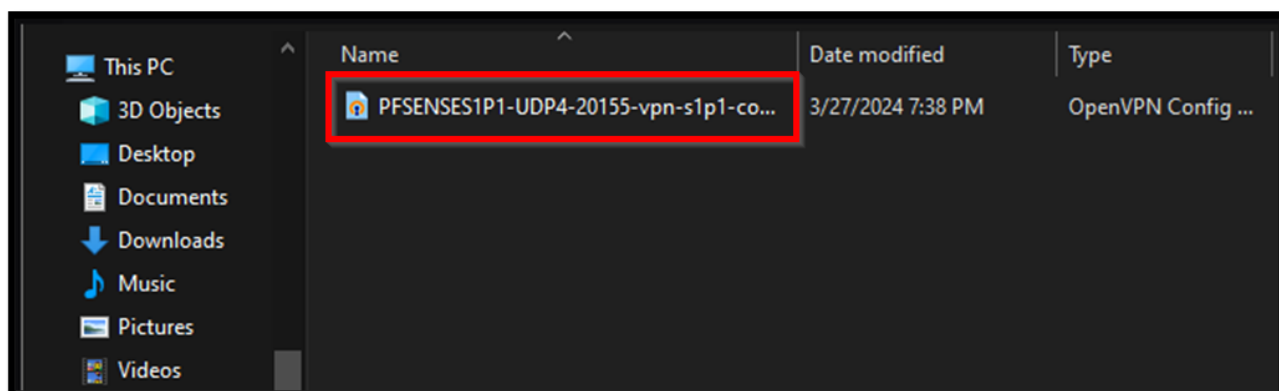
Finalement nous sauvegardons les changements.

2.1.6.7 Les tests

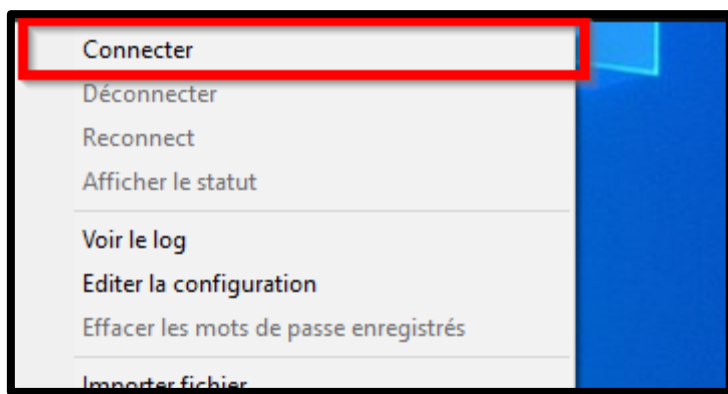
1. Pour tester la fonctionnalité, nous avons téléchargé le fichier de configuration de notre client. Pour l'appliquer, nous allons faire un clic droit sur notre barre des tâches, puis sélectionner '**Importer le fichier...**' :



Ensuite, nous choisissons le fichier à importer :



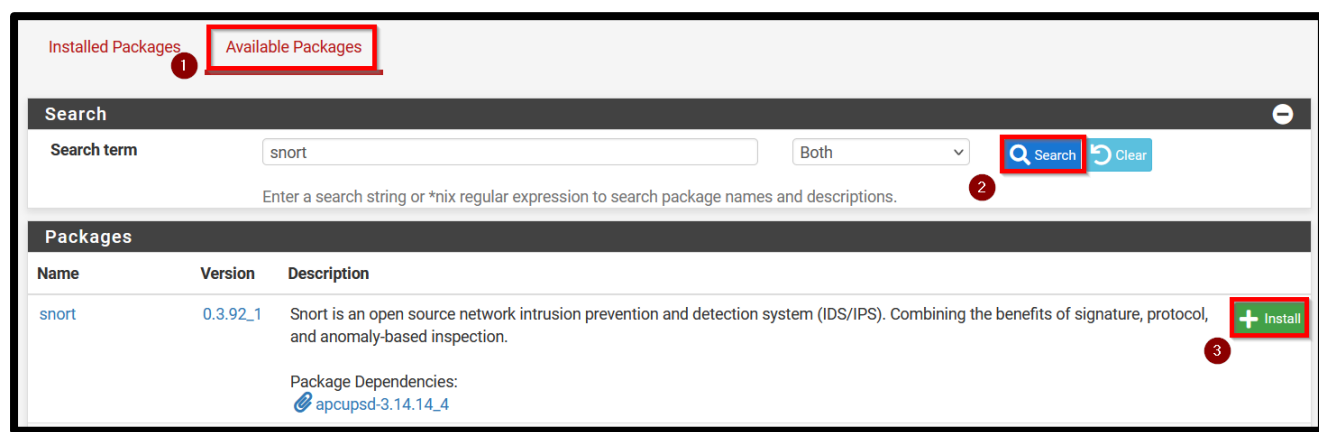
2. Après la mise en place de notre configuration, nous allons tout simplement cliquer encore une fois sur notre barre des tâches afin de choisir le bouton **Connecter** :



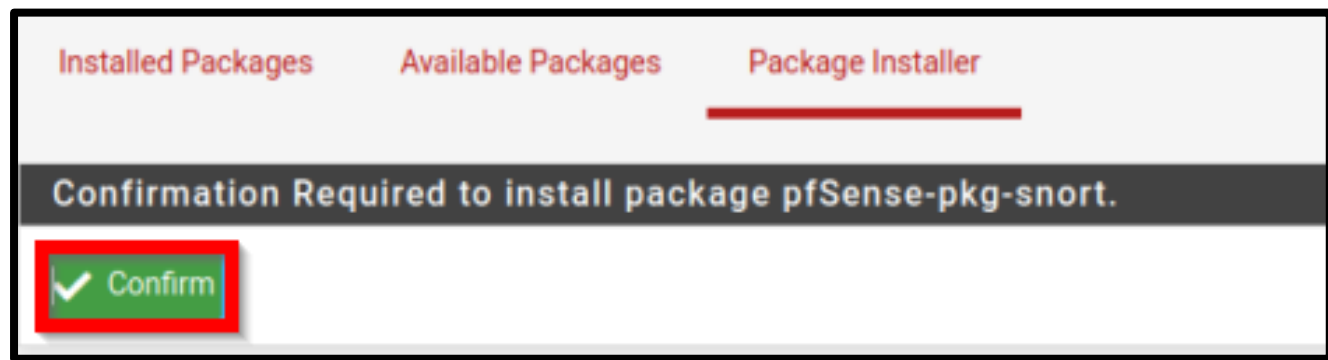
2.1.7. Installation de SNORT

SNORT est un logiciel qui nous permet la détection et la protection contre les menaces. Tout comme OpenVPN, c'est une extension installable via le gestionnaire des paquets.

1. Pour commencer notre installation, nous allons dans **Système** -> **Gestionnaire de paquets** -> **Paquets disponibles**, où nous allons rechercher notre extension en tapant le mot-clé « snort » dans la barre de recherche et cliquer sur le bouton **Installer** :

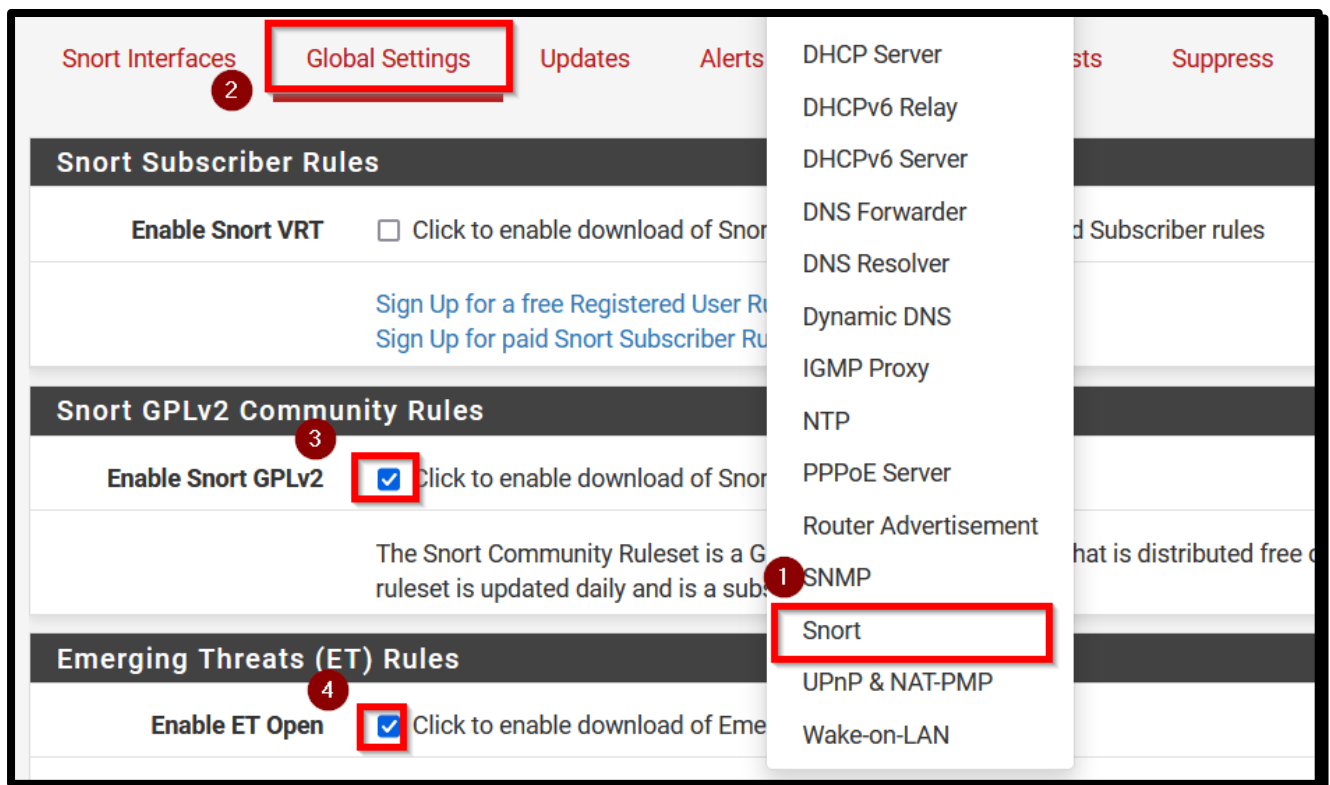


Puis nous le confirmons :

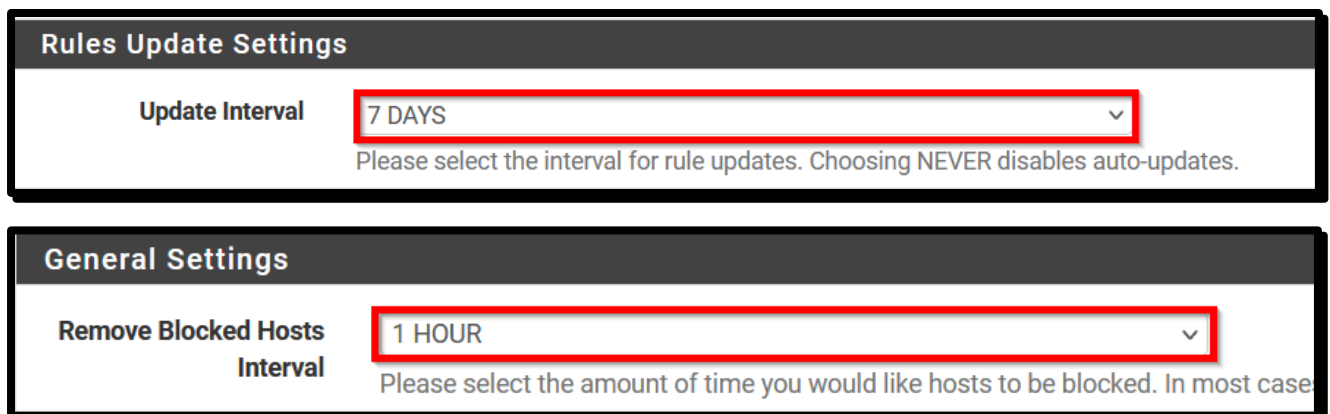


2. Une fois l'installation achevée, nous nous rendons dans **Services** -> **Snort** -> **Paramètres globaux**, où nous choisissons les listes de règles définissant les méthodes de détection des menaces :

Dans notre cas nous allons prendre le paquet communautaire **GPLv2** et **ET Open** :



3. Ensuite, un peu plus bas sur la même page, nous sélectionnons l'intervalle des mises à jour ainsi que l'option de blocage d'accès à notre réseau en cas d'activité suspecte :



Après cela, nous sauvegardons nos changements.

4. Ensuite, nous allons dans **Services -> Snort -> Updates**, afin de mettre à jour notre nouveau service installé :

Snort Interfaces Global Settings **Updates** Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt

1

Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	fb7b793adffe719bbaa49a85456f637b	Monday, 01-Apr-24
Emerging Threats Open Rules	Not Enabled	Not Enabled
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort AppID Open Text Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set

Last Update: Apr-01 2024 23:38 Result: **Success**

Update Rules **Update Rules** Force Update

2

5. Une fois la mise à jour terminée, nous nous rendons dans **Services -> Snort -> Snort Interfaces**, afin d'ajouter une interface d'écoute :

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Syn

1

Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
☐ LAN (re2)	✓ ↻	AC-BNFA	DISABLED	Réseau local	✎ 📄 🗑

2 **+ Add**

Nous sélectionnons l'interface sur laquelle Snort écoutera ainsi que sa description :

WAN Settings

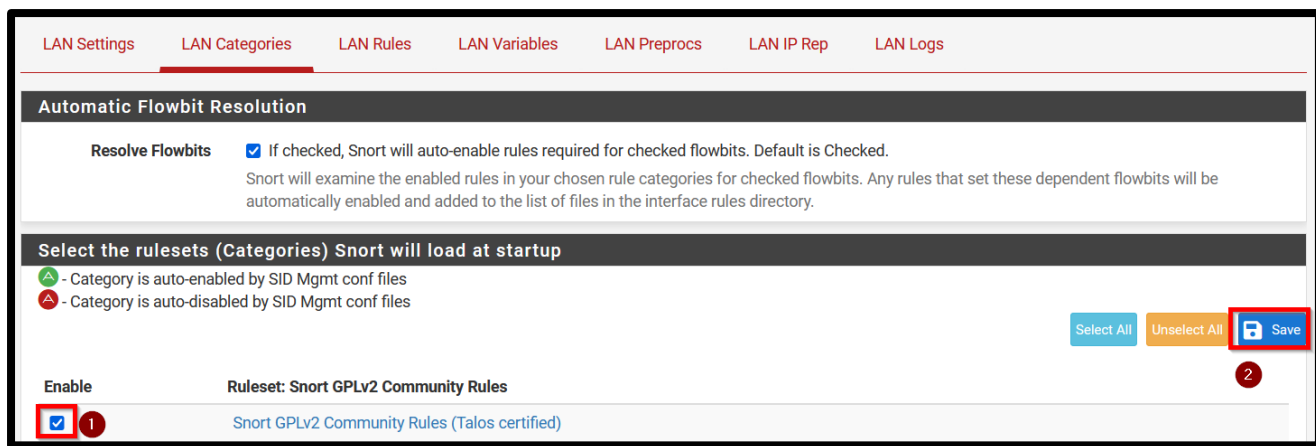
General Settings

Enable ☒ Enable interface

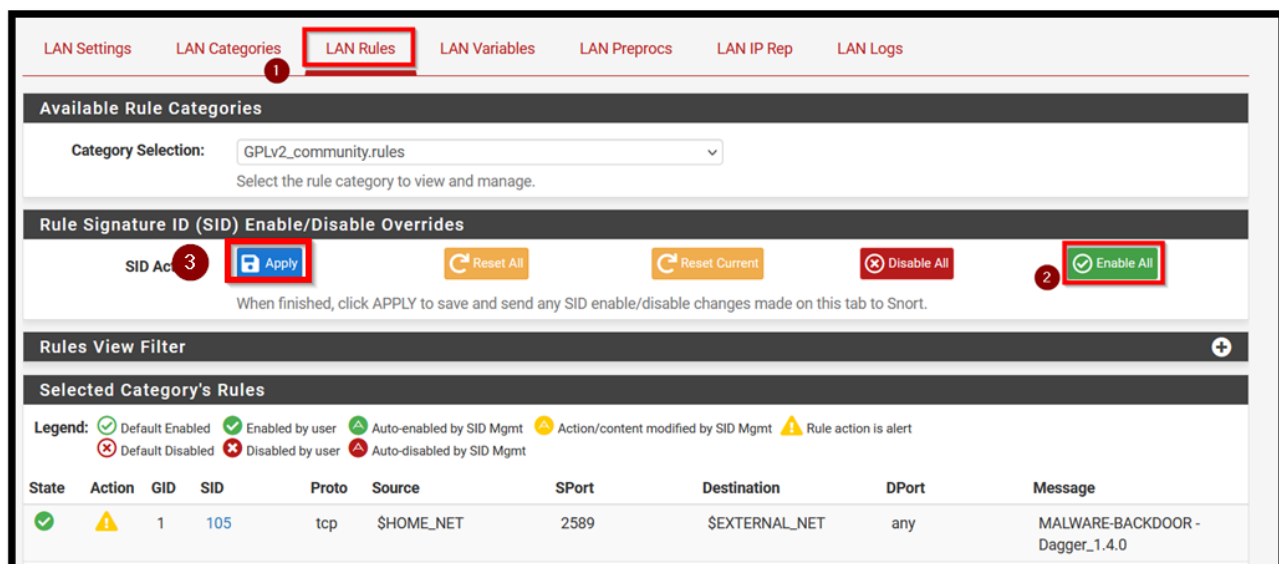
Interface **LAN (re2)**
Choose the interface where this Snort instance will inspect traffic.

Description **Réseau locale**
Enter a meaningful description here for your reference.

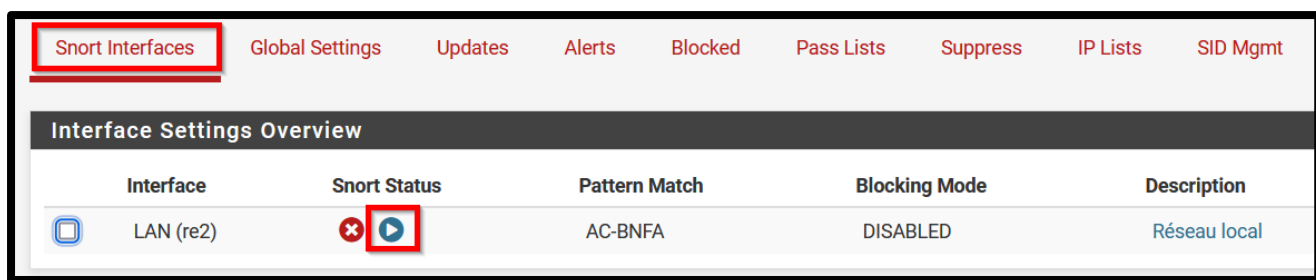
6. Une fois paramètres sauvegardés, nous allons dans **Services -> Snort -> Interface Settings -> LAN – Catégories** de règle qu'on vient de créer, afin de les activer :



7. Après les avoir activées, nous avons la possibilité d'activer les règles une par une sur la page **Règles LAN**. Dans notre cas, nous avons choisi d'activer toutes les règles :



8. Lorsque nos règles sont correctement paramétrées, nous devons nous rendre sur la page **Snort Interfaces** afin d'activer le mode d'écoute :



Notre service de détection d'intrusion est désormais prêt à être utilisé!

2.2.Netgear

2.2.1 Configuration Basique

1. L'adresse d'usine de notre switch est **192.168.0.239**. Nous changeons également le mot de passe en **Azerty13!** (mot de passe par défaut : « **password** »). Nous réglons notre commutateur sur **10.0.0.2/29**.

Switch Information

Product Name	GS308E
Switch Name	
Serial Number	5W272A5F05D58
MAC Address	94:18:65:7B:D5:DD
Bootloader Version	V1.00.03
Firmware Version	V1.00.11EN
DHCP Mode	Disable ☐ Refresh
IP Address	10.0.0.2
Subnet Mask	255.255.255.248
Gateway Address	10.0.0.1

2. Configuration des VLANS dans « **VLAN -> 802.1Q -> VLAN Configuration** ».

VLAN Identifier Setting

☐	VLAN ID	Port Members
☐	1	1 5
☐	10	1 2 3 4 5
☐	20	1 5 6 7
☐	30	1 5 8

VLAN Membership

Options VLAN ID Group Operation

Ports

1

2

3

4

5

6

7

8

VLAN Membership

Options VLAN ID 10 Group Operation

Ports 1 2 3 4 5 6 7 8

T U U U U U U

VLAN Membership

Options VLAN ID 20 Group Operation

Ports 1 2 3 4 5 6 7 8

T U U U U U U

VLAN Membership

Options VLAN ID 30 Group Operation

Ports 1 2 3 4 5 6 7 8

T U U U U U U

PVID Configuration

☐	Port	PVID
☐	1	1
☐	2	10
☐	3	10
☐	4	10
☐	5	1
☐	6	20
☐	7	20
☐	8	30

2.3. D-Link

2.3.1 Configuration Basique

1. Pour accéder à notre DAP-1360, nous utilisons l'adresse <http://192.168.0.50/>.

WIRELESS CONNECTION SETUP WIZARD

If you would like to utilize our easy to use web-based wizard to assist you in connecting your DAP-1360 to the wireless network, click on the button below.

[Launch Wireless Setup Wizard](#)

Note: Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the D-Link Access Point.

2. Configuration du point d'accès selon les indications.

WELCOME TO THE D-LINK WI-FI SETUP WIZARD

Give your Wi-Fi network a name.

Wireless Network Name

(using up to 32 characters)

Give your Wi-Fi network a password.

Wi-Fi Password

(Between 8 and 63 characters)

[Prev](#)

[Next](#)

[Cancel](#)

3. Après le redémarrage nous allons nous connecter avec le compte admin sans le mot de passe.

LOGIN

Log in to the Access Point

UserName:

Password:

[Log In](#)

Please login in one minute

4.

DEVICE NAME

Device Name allows you to configure this device more easily. You can enter "**http://**device name" into your web browser instead of IP address for configuration. (Default: http://dlinkap)

Device Name :

LAN IPV4 CONNECTION TYPE

Choose the IPv4 mode to be used by the Access Point

MY LAN Connection is : ▼

STATIC IP ADDRESS LAN CONNECTION TYPE:

Enter the IPv4 Address information.

IP Address :

Subnet Mask :

Gateway Address :

Primary DNS Server :

Secondary DNS Server :

3. Configuration d'accès sans fil :

WIRELESS NETWORK SETTINGS :

Enable Wireless : Always Add New

Wireless Mode : Access Point Site Survey

Wireless Network Name : WIFI S7P1 **(Also called the SSID)**

802.11 Mode : Mixed 802.11n, 802.11g and 802.11b

Wireless Channel : 1

Enable Auto Channel Scan : ☒

Channel Width : Auto 20/40MHz

Visibility Status : ☒ **Visible** ☐ **Invisible**

WIRELESS SECURITY MODE :

Security Mode : WPA-Personal

3. Les Tests

1. Tentative d'accès du VLAN10 vers le VLAN10 :

```

C:\Users\stagiaire>ping 192.7.1.254

Envoi d'une requête 'Ping' 192.7.1.254 avec 32 octets de données :
Réponse de 192.7.1.254 : octets=32 temps<1ms TTL=64
Réponse de 192.7.1.254 : octets=32 temps<1ms TTL=64
Réponse de 192.7.1.254 : octets=32 temps<1ms TTL=64
Réponse de 192.7.1.254 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.7.1.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\stagiaire>
```

2. Tentative d'accès du VLAN10 vers le VLAN20 :

```
C:\Users\stagiaire>ping 192.70.10.254

Envoi d'une requête 'Ping' 192.70.10.254 avec 32 octets de données :
Réponse de 192.70.10.254 : octets=32 temps<1ms TTL=64
Réponse de 192.70.10.254 : octets=32 temps<1ms TTL=64
Réponse de 192.70.10.254 : octets=32 temps<1ms TTL=64
Réponse de 192.70.10.254 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.70.10.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\stagiaire>
```

3. Tentative d'accès du VLAN10 vers le VLAN30 :

```
C:\Users\stagiaire>ping 192.7.10.254

Envoi d'une requête 'Ping' 192.7.10.254 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.7.10.254:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),

C:\Users\stagiaire>
```

4. L'adresse DHCP attribuée correspond bien à l'étendue du VLAN10.

