Présentation Projet SecureTech

Introduction

SecureTech Industries est une petite entreprise spécialisée dans la production et la commercialisation de solutions technologiques de haute sécurité. La société possède un siège social et une succursale. En raison de la nature sensible de ses produits, elle a des exigences élevées en matière de sécurité pour ses infrastructures informatiques.

Objectifs :

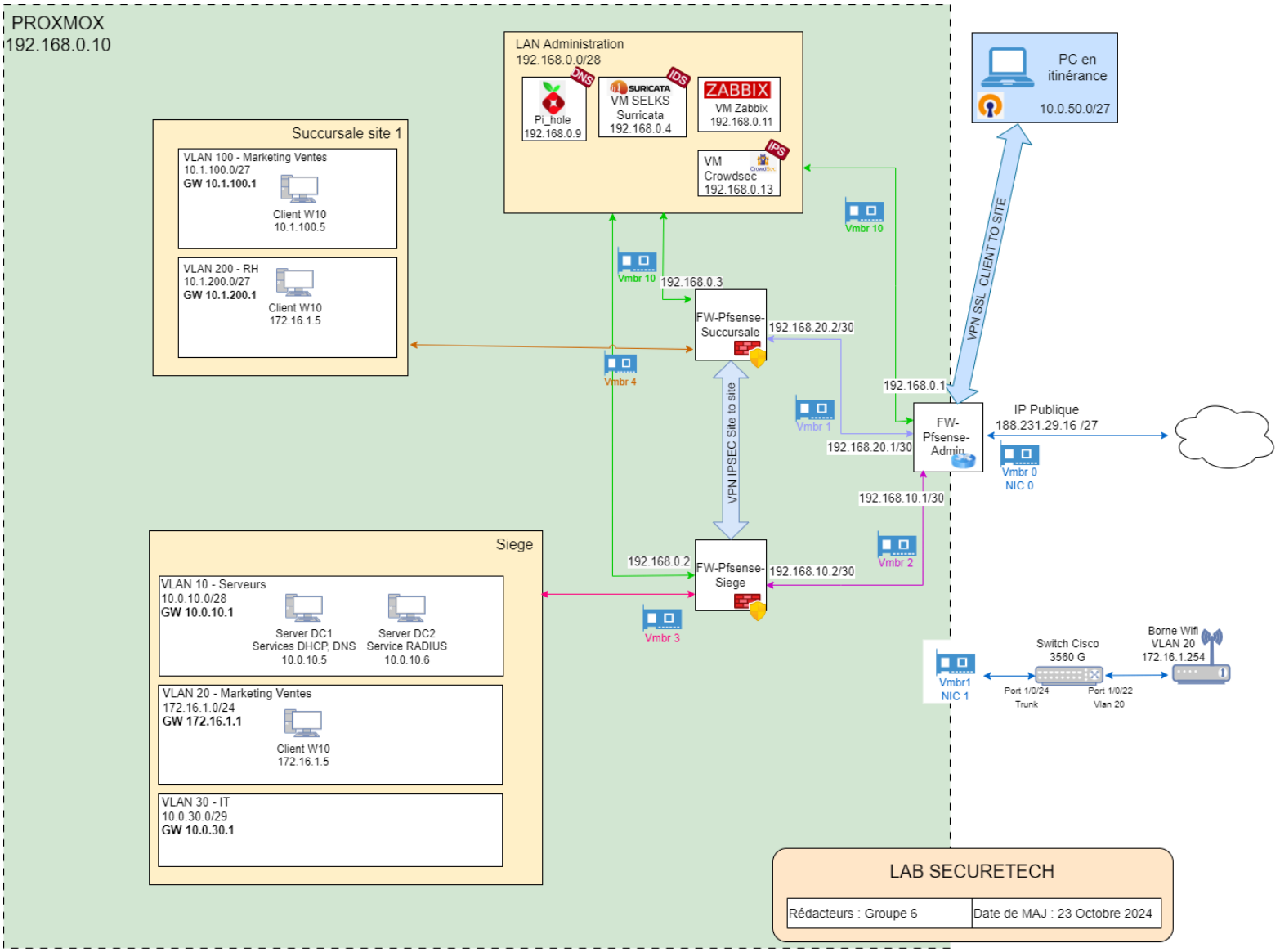
1. Interconnexion entre site Principal et site Succursale
   => VPN Site à Site ✅
2. Accès sécurisé pour les commerciaux itinérants
   =>VPN SSL ✅
3. Segmenter le réseau pour isoler la production du département de management et des autres services
   => VLAN ✅
4. Solutions d'authentification forte pour les commerciaux itinérants.
   => RADIUS pour l'authentification sur le WIFI 🟠

Mise en place de pare-feux, IDS/IPS pour détecter et prévenir les menaces.
   => Surricata/Crowdsec ✅

5. Configuration des listes de contrôle d'accès pour limiter l'accès aux ressources.
   => ACL
6. Mettre en œuvre des solutions de monitoring pour surveiller l'état et les performances du réseau.
   => Zabbix ✅
7. Configuration de la qualité de service pour prioriser le trafic critique.
   => QoS (Plan de continuité de service)
8. Filtrage
   =>DNSBL avec Pi-Hole ✅
9. Plan de reprise informatique
   => NAS synology avec NFS ✅

Document de conception réseau

- **Description** : Un document exhaustif qui donne une vue d'ensemble de la conception du réseau proposé pour SecureTech Industries.



Matrice des flux

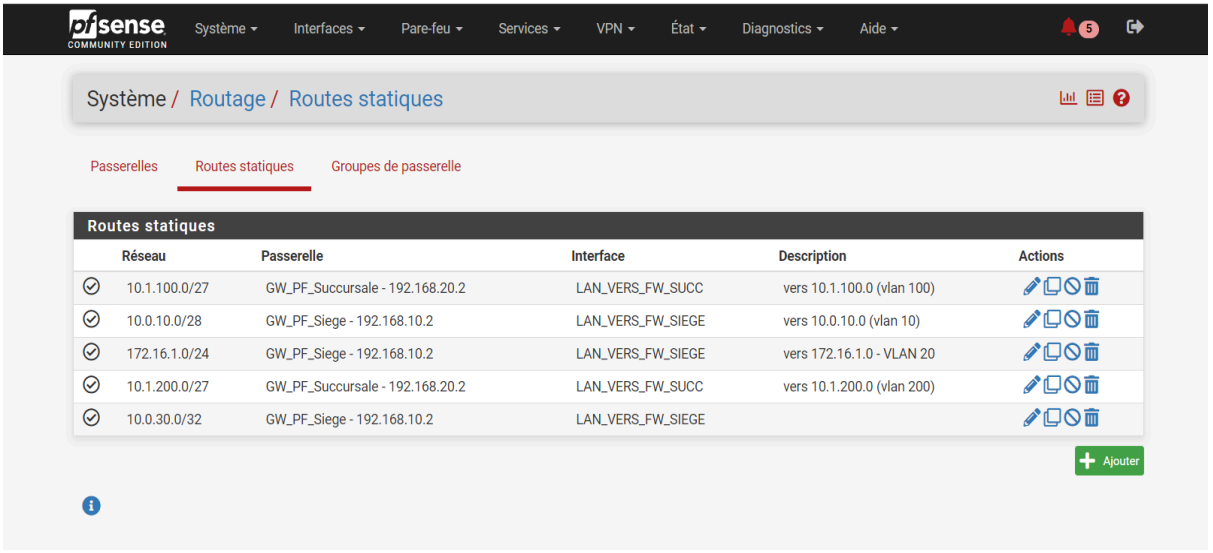
- **Description** : Une matrice qui détaille le flux de données entre les différents segments du réseau.
- **Contenu attendu** : Origine, destination, ports utilisés, protocoles, et toute règle de sécurité associée.
- **Importance** : Permet d'avoir une vue claire des communications attendues sur le réseau et est essentielle pour configurer correctement les pare-feux et autres dispositifs de sécurité.

Matrice

Lien [Matrice_des_flux_Securetech]

	DESTINATION	WAN	GW	AP	DC01	DC02	DHCP 1 AD	DHCP 2 FW	DNS PI HOLE	WWW	USERS	VPN	ADMINISTRATEURS	IDS SURICATA	ITS CROWDSEC	ZABBIX	NAS
SOURCE	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
WAN	/	/	X	X	X	X	X	X	X	HTTPS	X	X	X	X	X	X	X
GW	/	X	/	X	X	X	X	X	X	X	X	X	X	X	X	X	X
AP	/	X	X	/	DHCP	x	LDAP	LDAP	DNS	X	X	X	X	X	X	X	X
DC01	/	X	WEB	X	/	Replica	DHCP	X	Redirection DNS	UPDATE HTTPS	X	X	X	X	X	X	X
DC02	/	X	WEB	X	Replica	/	DHCP	X	Redirection DNS	UPDATE HTTPS	X	X	X	X	X	X	X
DHCP AD	/	X	X			X	/	X	Redirection DNS	X		X	X	X	X	X	X
DHCP FW	/	X	x	x	X	X	X	/		X		PAR VPN CLIENT TO SITE		X	X	X	X
DNS PI-HOLE	/	X	DNS	X	X	X	X	X	/	WEB DNS	X	X	X	DNS	DNS	DNS	DNS
WWW	/	X	X	X	X	X	X	X	X		X	X	X	XX	X	X	X
USERS	/	WEB	x		DNS LDAP	DNS LDAP	DHCP AD	DHCP FW sur site succursale	DNS	HTTPS	/		X	X	X	X	NFS SMB
VPN	/	VPN CLIENT TO SITE		X	LDAP	LDAP	X	DHCP	DNS	X	X	/	HTTPS	HTTPS	HTTP	HTTP HTTPS	NFS SMB
ADMINISTRATEURS	/	WEB	X		LDAP	LDAP	DHCP AD	DHCP	HTTPS	HTTPS	PMAD		/	HTTPS	HTTP	HTTP HTTPS	NFS SMB
IDS SURICATA	/	X	Sonde Pfsense	X	X	X	X	X	DNS	SONDE	X	SONDE interfaces	X	/	x	xx	X
ITS CROWDSEC	/	X					x	x	DNS	Interfaces	Interfaces	Interfaces	x	x	/	x	x
ZABBIX	/	X		X	Monitoring	Monitoring	x	x	DNS		x	X	X	Monitoring	Monitoring	Monitoring	Monitoring
NAS	/	X	X	X	SMB	SMB	X	X	X	X		X	X	X	X	X	/

Règles de routages

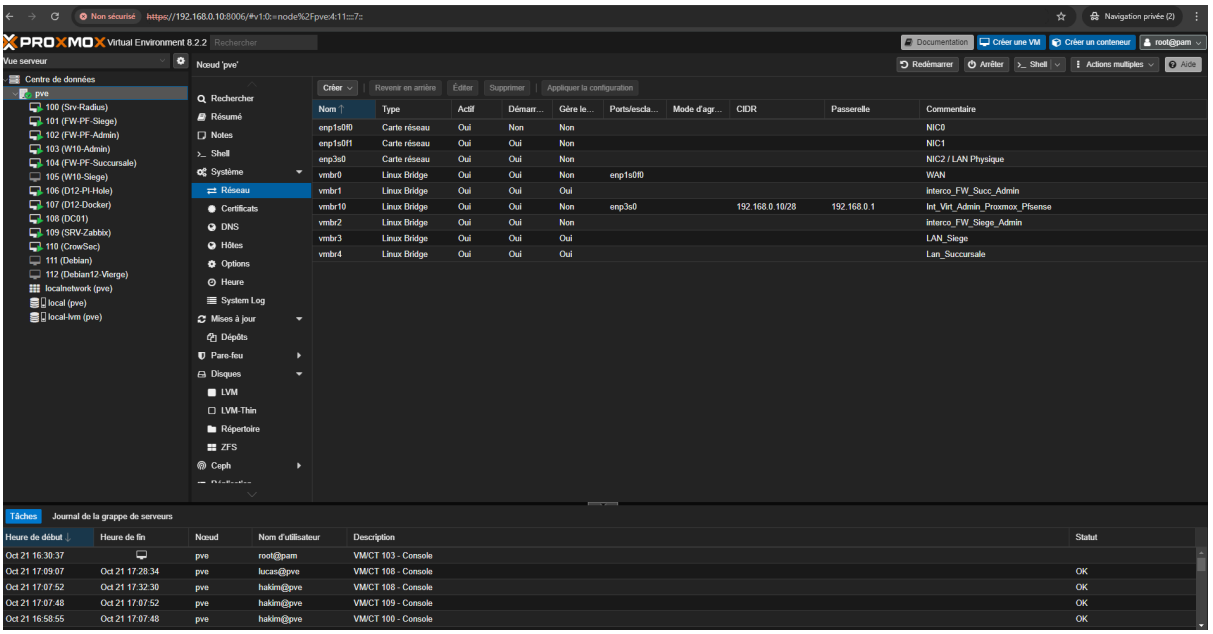


Document de Configuration des Équipements

- **Description** : Un guide qui détaille la configuration de chaque équipement réseau déployé.
- **Contenu attendu** : Configurations pas à pas pour les routeurs, commutateurs, pare-feux, etc. Chaque configuration doit inclure des commentaires pour expliquer le raisonnement derrière les choix.
- **Importance** : Assure la cohérence et la reproductibilité des configurations. Essentiel pour le dépannage et les audits de sécurité.

Proxmox

Vmbr2 : Admin
auto vmbr2
iface vmbr2 inet static
address 192.168.0.10/27
gateway 192.168.0.1
bridge-ports enp3s0
bridge-stp off
bridge-fd 0



Configuration Switch Cisco Catalyst 3560 G

Configuration trunk :

Switch<en
Switch#conf t
Switch(config)#int GigaBitEthernet 0/24
Switch (config-if)#Switchport trunk encapsulation dot1q
Switch (config-if)#Exit
Switch (config)#Exit
Switch#copy running-config startup-config

Configuration hostname et domaine

```
Switch#conf t
Switch(config)#hostname S1
S1(config)#ip domain-name grp6.local
S1(config)#end
S1#wr
```

Configuration SSH

```
S1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: S1.grp6.local

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#ip ssh version 2
S1(config)#ip ssh logging events
S1(config)#ip ssh time-out 60
S1(config)#ip ssh authentication-retries 3
```

Configuration de l'authentification et ajout d'un compte administrateur

```
S1(config)#aaa new-model
S1(config)#aaa authentication login default local
S1(config)#aaa authorization exec default local
S1(config)#username admin secret Ais2024!
S1(config)#username admin2 privilege 15 password Ais2024!
```

Configuration de l'adresse du switch

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.5 255.255.255.248
S1(config-if)# no shutdown
```

Configuration du port mirroring

```
S1(config)#monitor session 2 source interface gi0/1 - 23 both
S1(config)#monitor session 2 destination interface gi0/24
S1(config)#exit
S1#sh monitor session 2
Session 2
---------
Type                : Local Session
```

Source Ports :
Both : Gi0/1-23
Destination Ports : Gi0/24
Encapsulation : Native
Ingress : Disabled

Configuration ARP

S1#conf t
S1(config)# int gigabitEthernet 0/22
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security mac-address 28ee.522d.efea (MAC ADDRESS ACCESS POINT)
S1(config-if)#switchport port-security violation protect
S1(config-if)#exit
S1(config)#exit
S1#show port-security address
S1#copy running-config startup-config

```
Vlan    Mac Address       Type                        Ports   Remaining Age
                                                                 (mins)
----    -----------       ----                        -----   -------------
   1    28ee.522d.efea    SecureDynamic               Gi0/22        -
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 6144
S1#
```

Zabbix

wget
https://repo.zabbix.com/zabbix/7.0/debian/pool/main/z/zabbix-release/zabbix-release_latest+debian12_all.deb
dpkg -i zabbix-release_latest+debian12_all.deb
apt update

apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent

mysql -uroot -p
password
mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
mysql> create user zabbix@localhost identified by 'password';
mysql> grant all privileges on zabbix.* to zabbix@localhost;

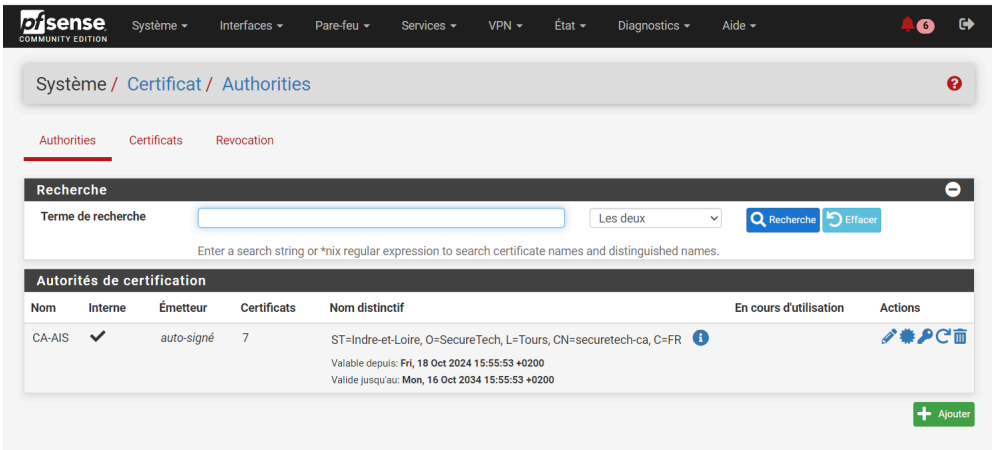
```
mysql> set global log_bin_trust_function_creators = 1;
mysql> quit;

# zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql
--default-character-set=utf8mb4 -uzabbix -p zabbix

# mysql -uroot -p
password
mysql> set global log_bin_trust_function_creators = 0;
mysql> quit;

Dans /etc/zabbix/zabbix_server.conf
DBPassword=password

# systemctl restart zabbix-server zabbix-agent apache2
# systemctl enable zabbix-server zabbix-agent apache2
```

PfSense

Configuration du VPN Client to Site (PFSENSE ADMIN)

L'objectif est de créer un lien virtuel entre un PC client et un réseau d'entreprise. Au sein de ce lien, les données seront sécurisées et isolées du reste du trafic, c'est là tout l'intérêt du VPN et cette notion de "privé". Le VPN permet de créer une extension virtuelle de votre réseau local jusqu'à un autre réseau (site) ou jusqu'à un poste de travail distant.

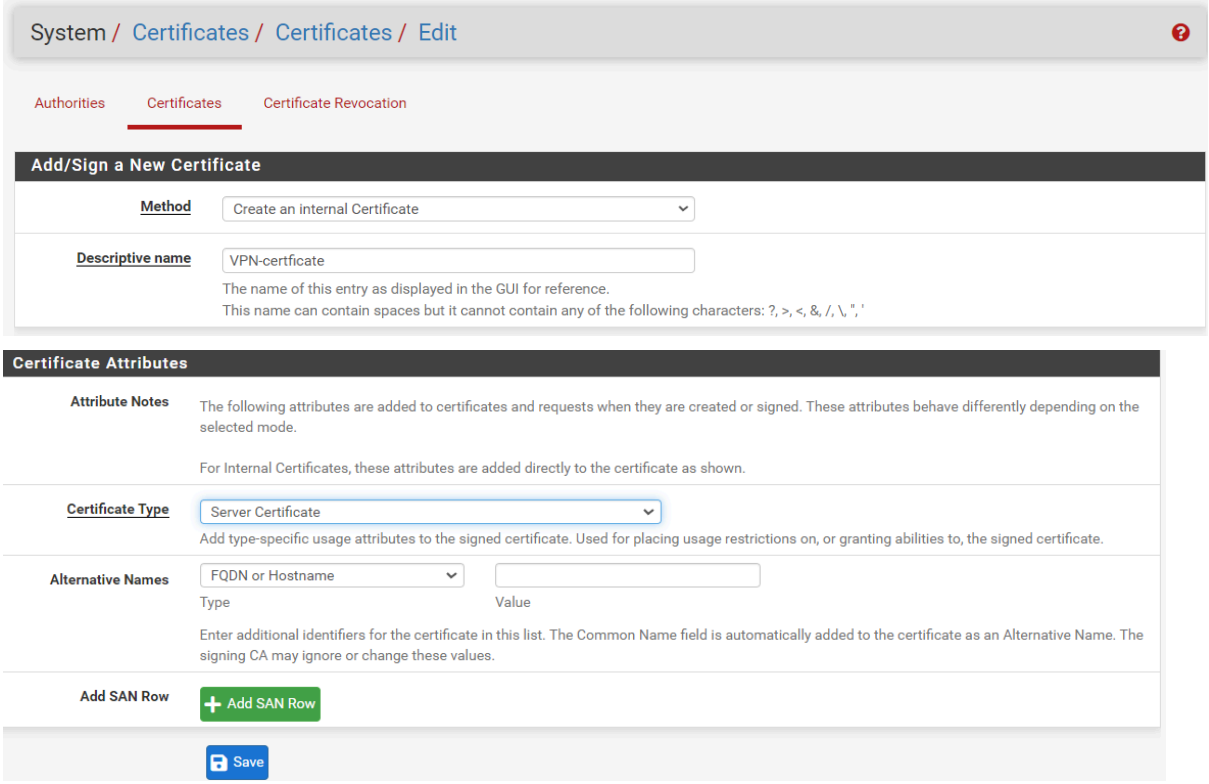
1. **Créer le certificat d'autorité**

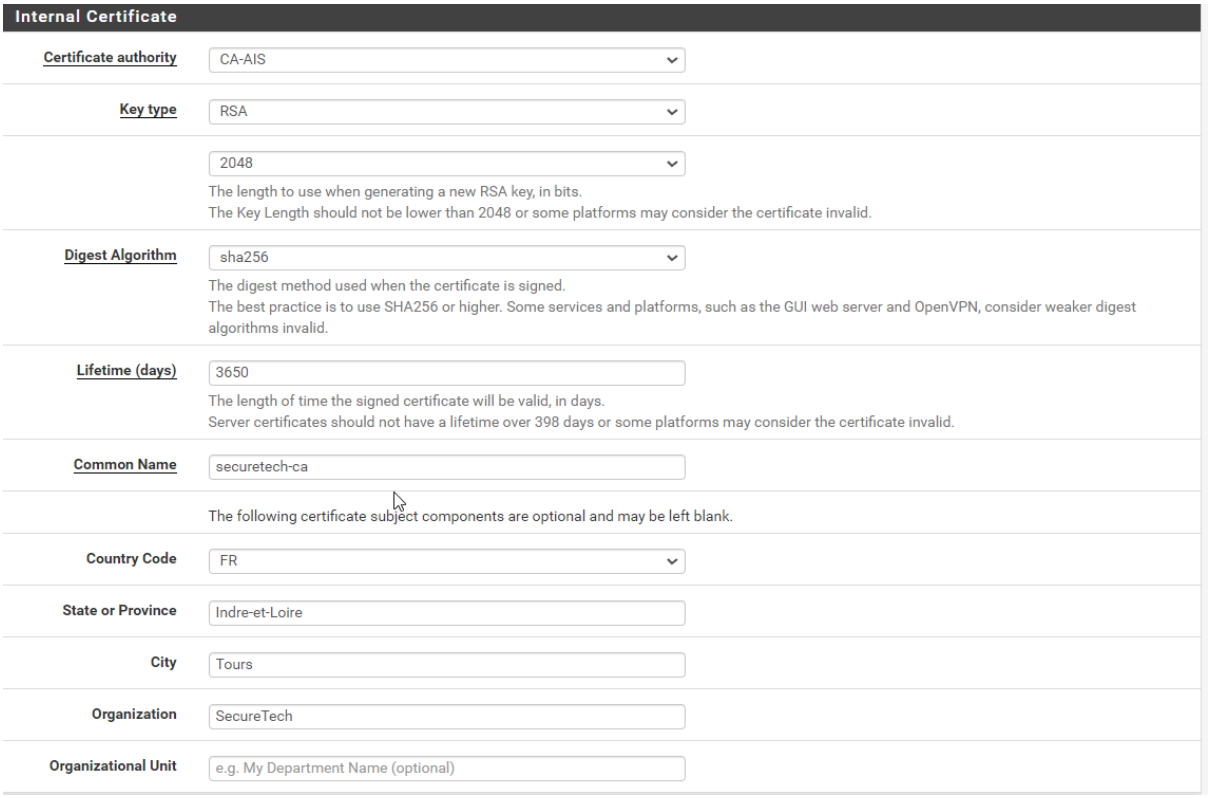


2. **Créer le certificat Server**

Création d'un certificat de type "Server" en nous basant sur notre nouvelle autorité de certification. Toujours dans "Certificate Manager", cette fois-ci dans l'onglet "Certificates", cliquez sur le bouton "Add/Sign".

Choisissez la méthode "Create an Internal Certificate" puisqu'il s'agit d'une création, donnez-lui un nom (VPN-Certficate) et sélectionnez l'autorité de certification au niveau du paramètre "Certificate authority". Par défaut, la validité du certificat est fixée à 3650 jours soit 10 ans. Le "Common Name" correspond là aussi au nom intégré dans le certificat (securetech-ca), si vous souhaitez établir une connexion VPN basée sur un nom de domaine, il est préférable d'indiquer cette valeur ici.

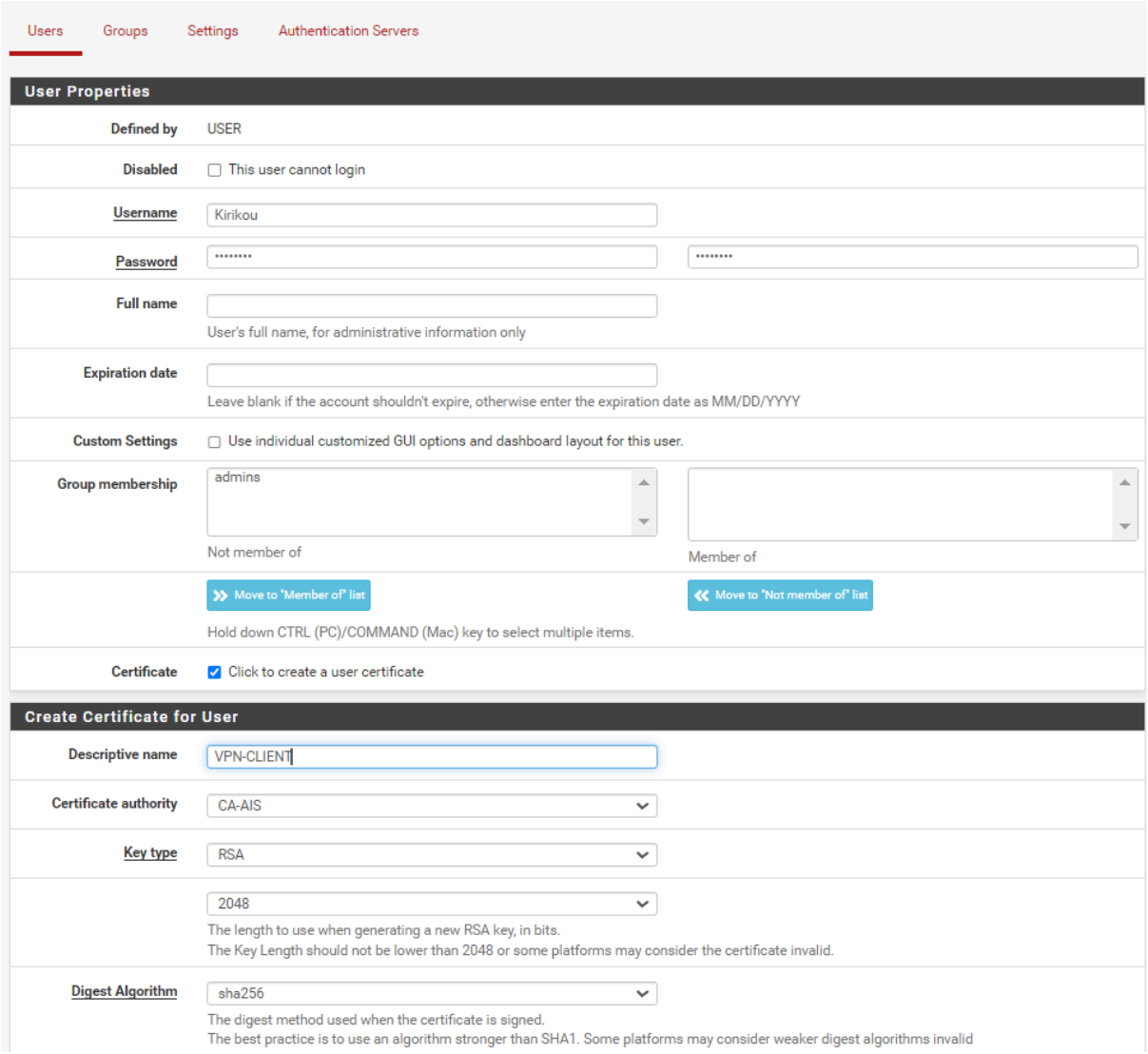




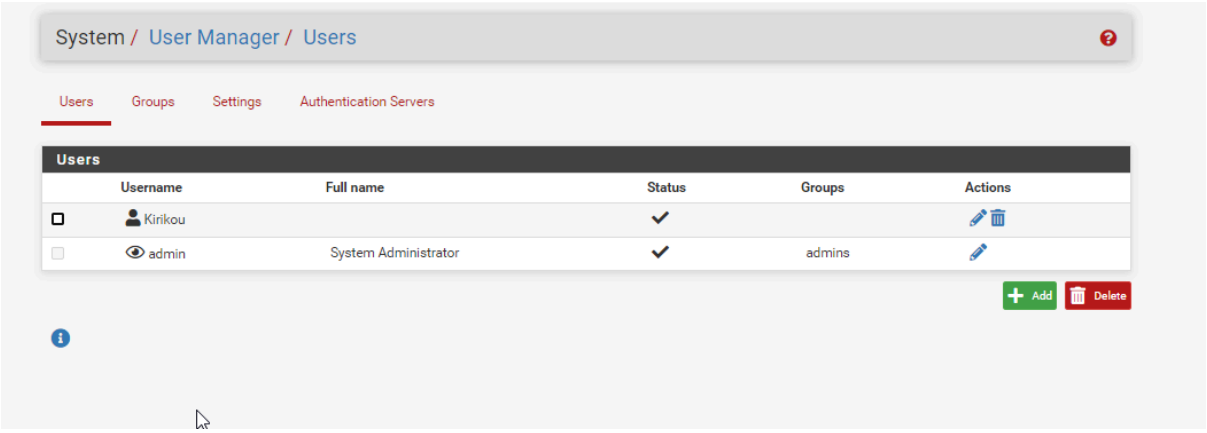
Créer les utilisateurs locaux

On créer un utilisateur ainsi qu'un certificat de type "User" pour l'authentification VPN. Pour créer l'utilisateur, il faut indiquer un identifiant, un mot de passe... Ainsi que cocher l'option "Click to create a user certificate" : cela va ajouter le formulaire de création du certificat juste en dessous. Pour créer le certificat, on se base sur notre autorité de certification.

Username : Kirikou Password : Ais2024!

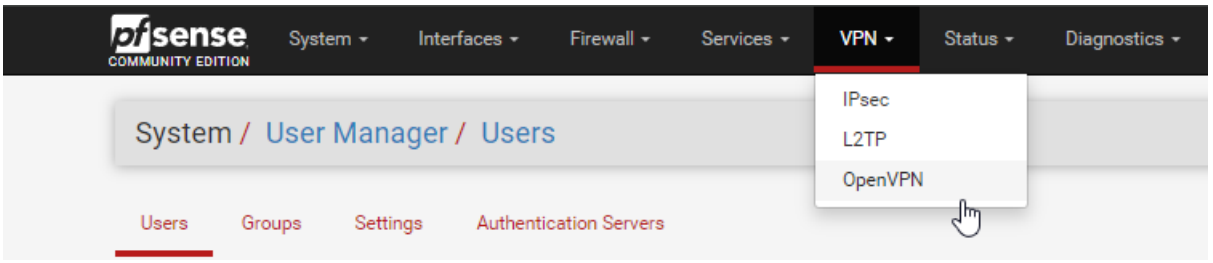


Lorsque l'utilisateur est créé, il apparaît bien dans la base locale.

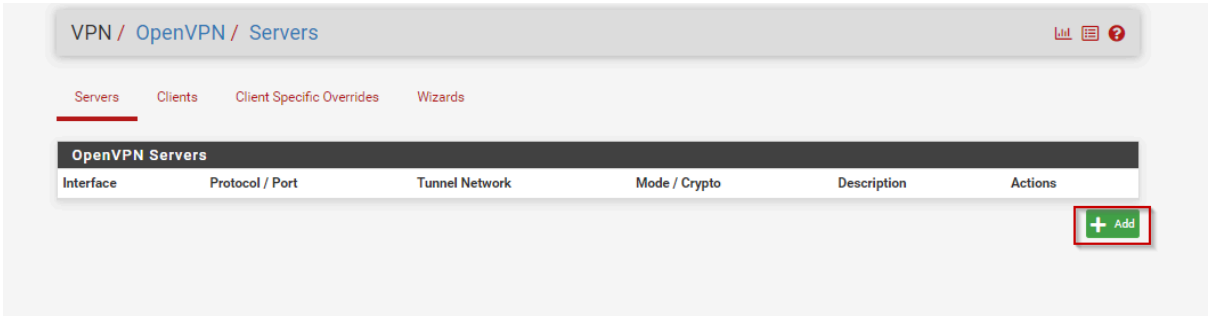


Configurer le serveur OpenVPN

Maintenant que la partie certificat est opérationnelle et que nous disposons d'un compte utilisateur, on peut s'attaquer à la configuration du VPN.
Cliquez sur le menu "VPN" puis "OpenVPN"

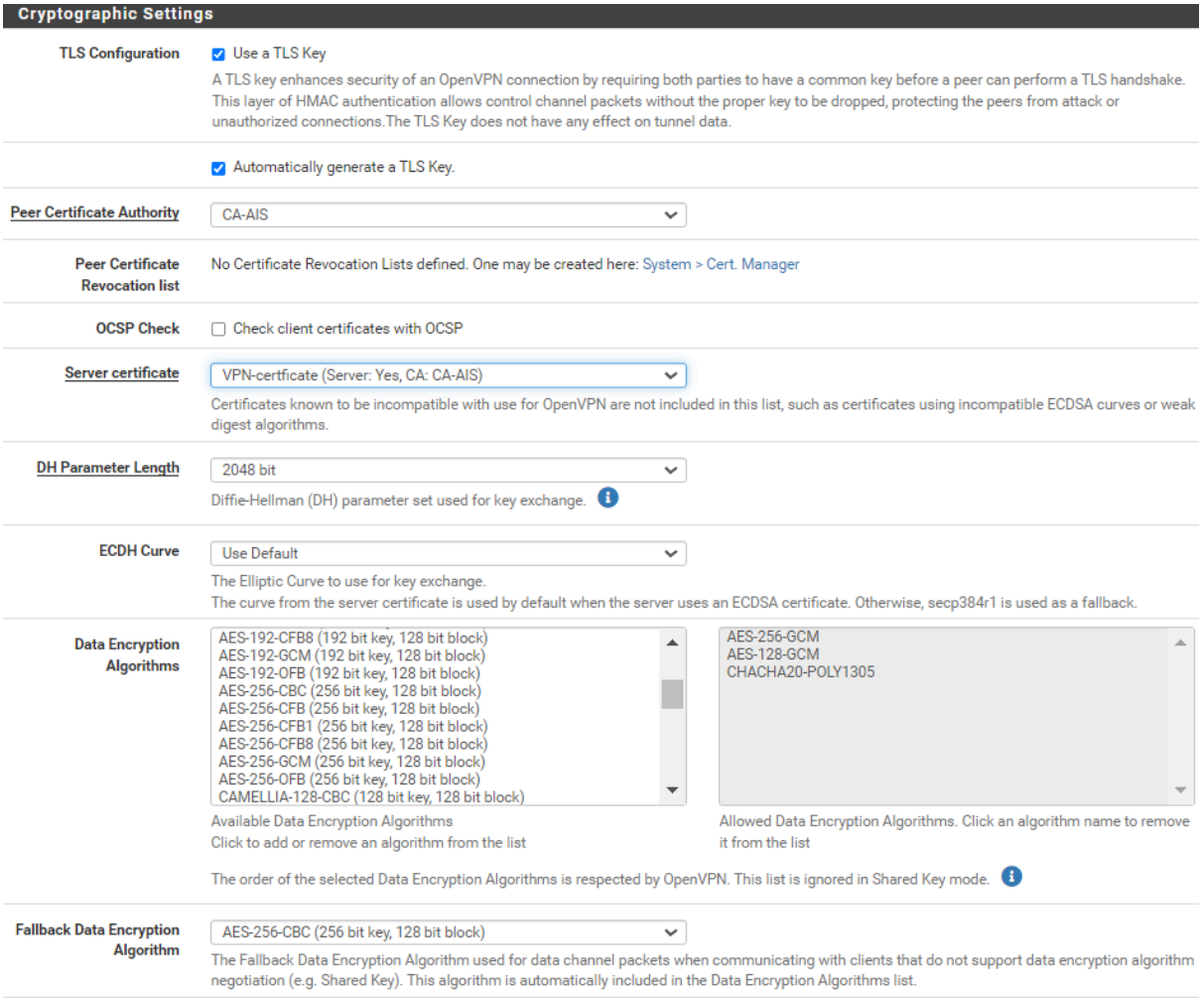


Dans l'onglet "Servers", cliquez sur "Add" pour créer une nouvelle configuration.



La première chose à faire, c'est de choisir le "Server Mode" suivant : Remote Access (SSL/TLS + User Auth). Pour le VPN, le protocole s'appuie sur de l'UDP, avec le port 1194 par défaut : je vous recommande d'utiliser un port différent. Pour l'interface, nous allons conserver "WAN" puisque c'est bien par cette interface que l'on va se connecter en accès distant.

Au niveau de la partie chiffrement, un peu plus bas dans la page, vous devez sélectionner votre autorité de certification au niveau du champ "Peer Certificate Authority". En complément, sélectionnez le certificat Server au niveau du champ "Server certificate".



Pour l'algorithme de chiffrement (Encryption Algorithm), nous pouvons passer sur de l'AES-256- CBC plutôt que de l'AES-128-CBC. La sécurité sera renforcée, mais cela impact légèrement les performances, car le processus de chiffrement est alourdi : il sera toujours possible de modifier cette valeur. Il n'est pas nécessaire de modifier les autres options liées au chiffrement.

Configuration du Tunnel :

Tunnel Settings

IPv4 Tunnel Network
10.0.50.0/27
This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.

IPv6 Tunnel Network
This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

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

Redirect IPv6 Gateway
Force all client-generated IPv6 traffic through the tunnel.

IPv4 Local network(s)
192.168.0.0/28
IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. 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.

IPv6 Local network(s)
IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. 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
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.
Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.

Asymmetric compression allows an easier transition when connecting with older peers.

Push Compression
Push the selected Compression setting to connecting clients.

Type-of-Service
Set the TOS IP header value of tunnel packets to match the encapsulated packet value.

Inter-client communication
Allow communication between clients connected to this server

Duplicate Connection
Allow multiple concurrent connections from the same user
When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.

Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.

Pour les paramètres des clients, je vous recommande de cocher l'option "Dynamic IP" : si l'adresse IP publique d'un client change, il pourra maintenir sa connexion VPN. C'est surtout utile si vous avez des personnes qui se connectent via une connexion 4G et en mobilité.

Client Settings

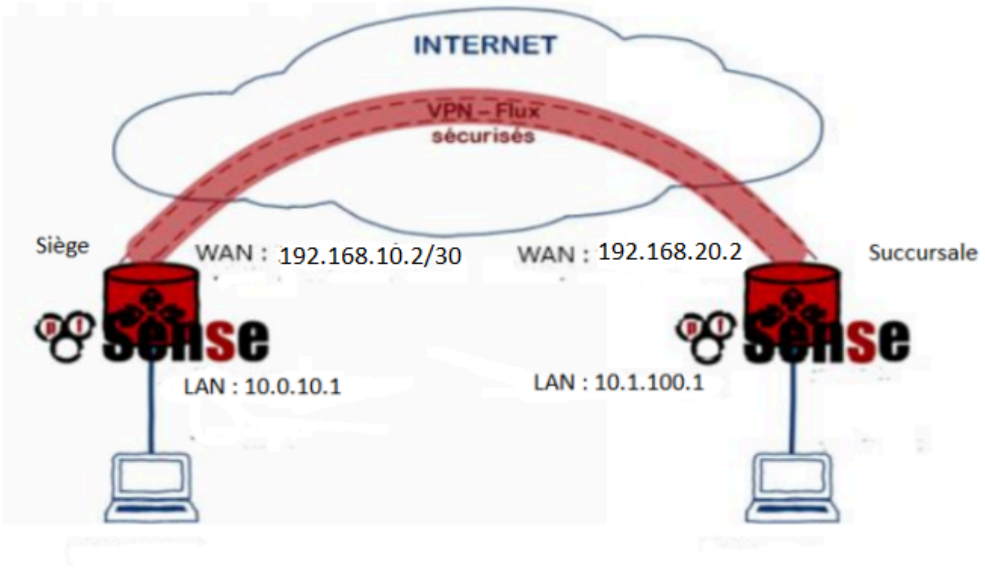
Dynamic IP
Allow connected clients to retain their connections if their IP address changes.

Topology
net30 -- Isolated /30 network per client
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".

Configuration du VPN Site to Site (PFSENSE SIEGE ET SUCCURSALE):

1. Présentation

Pour illustrer la mise en place de notre VPN Site-to-Site entre nos routeurs, nous allons utiliser le pare-feu PFSENSE et se baser sur le schéma de test suivant :

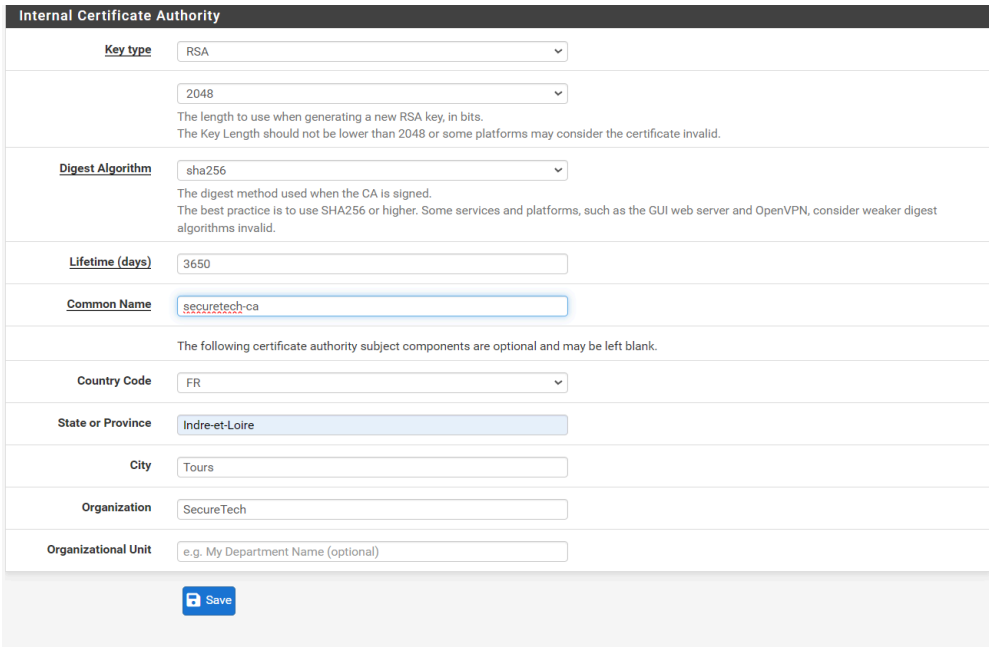


Nous aurons donc une interface WAN (192.168.X.0/30) et LAN (10.X.X.1/27) sur chacun de nos PFsense, le but final sera donc que nos clients puissent communiquer entre eux via ce tunnel.

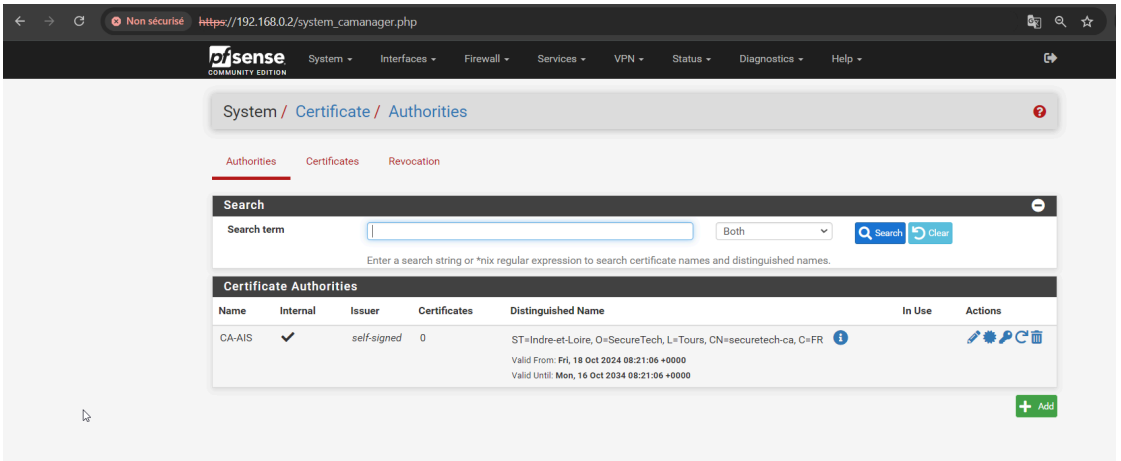
2. Reprise du meme certificat

Pour créer l'autorité de certification sur PFSENSE, vous devez accéder au menu : System > Authorities > Edit
Donnez un nom à l'autorité de certification, par exemple "CA-AIS", ce nom sera visible seulement dans PFSENSE. Choisissez la méthode "Create an internal Certificate Authority".

Concernant le nom qui sera affiché dans les certificats, il s'agit du champ "Common Name", nous indiquons "securetech-ca" pour notre part. Remplissez les autres valeurs : la région, la ville, etc... et cliquez sur "Save" pour créer la CA.

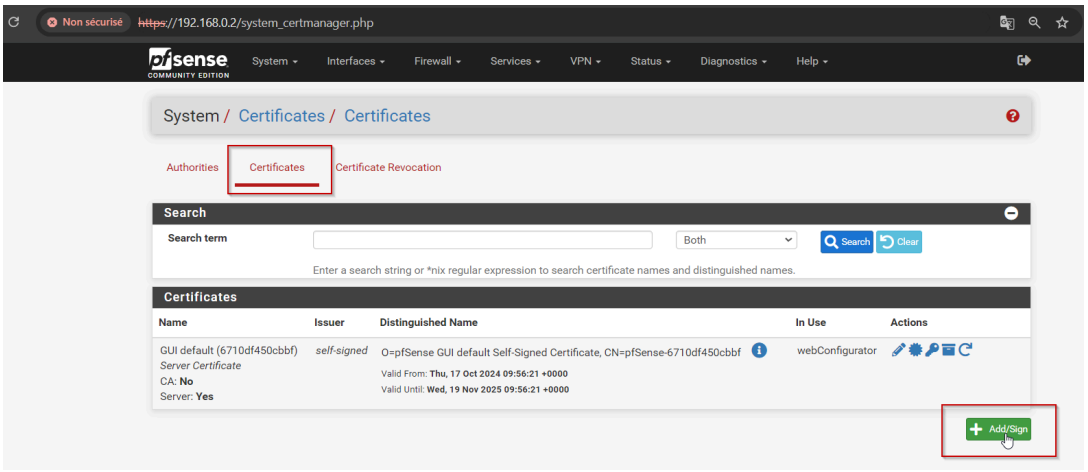


L'autorité de certification doit apparaître dans l'interface, comme ceci :

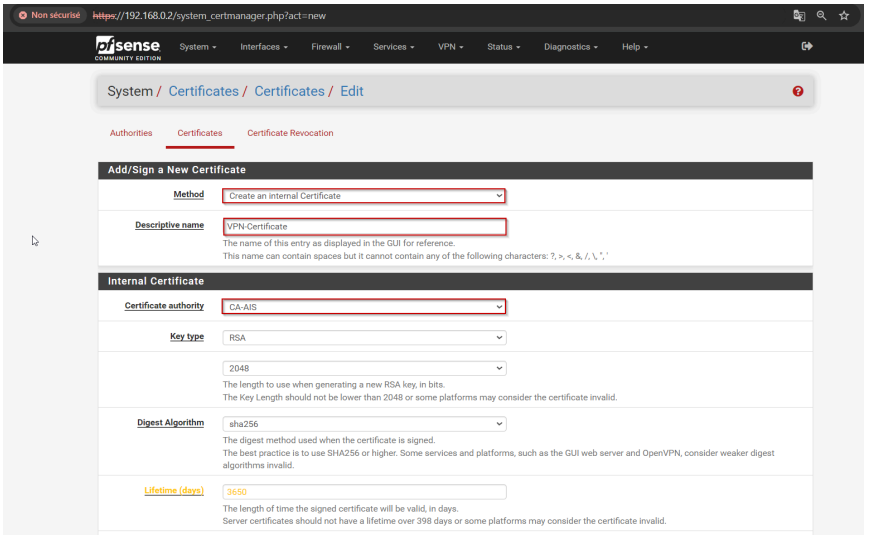


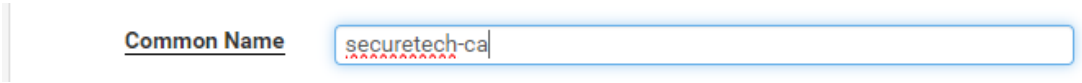
3. Créer le certificat Server

Nous devons créer un certificat de type "Server" en nous basant sur notre nouvelle autorité de
certification. Toujours dans "Certificate ", cette fois-ci dans l'onglet “Certificates", cliquez sur le bouton "Add/Sign".

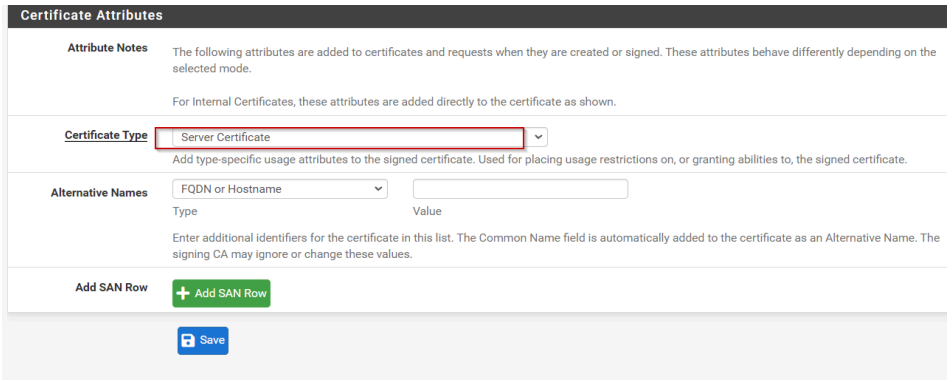


Choisissez la méthode "Create an Internal Certificate" puisqu'il s'agit d'une création, donnez-lui un nom (VPN-Certificate) et sélectionnez l'autorité de certification au niveau du paramètre "Certificate authority".
Par défaut, la validité du certificat est fixée à 3650 jours soit 10 ans. Le "Common Name" correspond là aussi au nom intégré dans le certificat (securetech-ca), si vous souhaitez établir une connexion VPN basée sur un nom de domaine, il est préférable d'indiquer cette valeur ici.

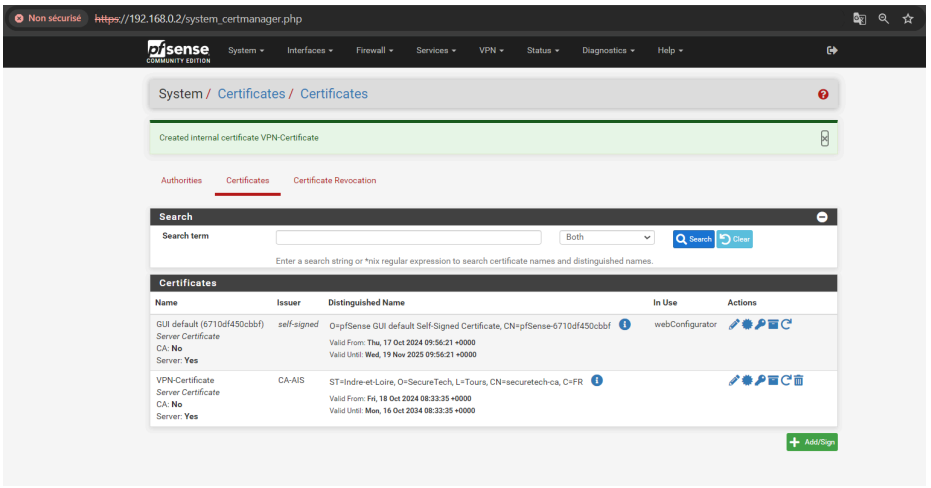




Choisissez bien le type de certificat (Certificate Type) suivant : **Server Certificate.**



Après avoir cliqué sur "Save" pour valider la création du certificat, il apparaît dans la liste des certificats du Pare-feu :

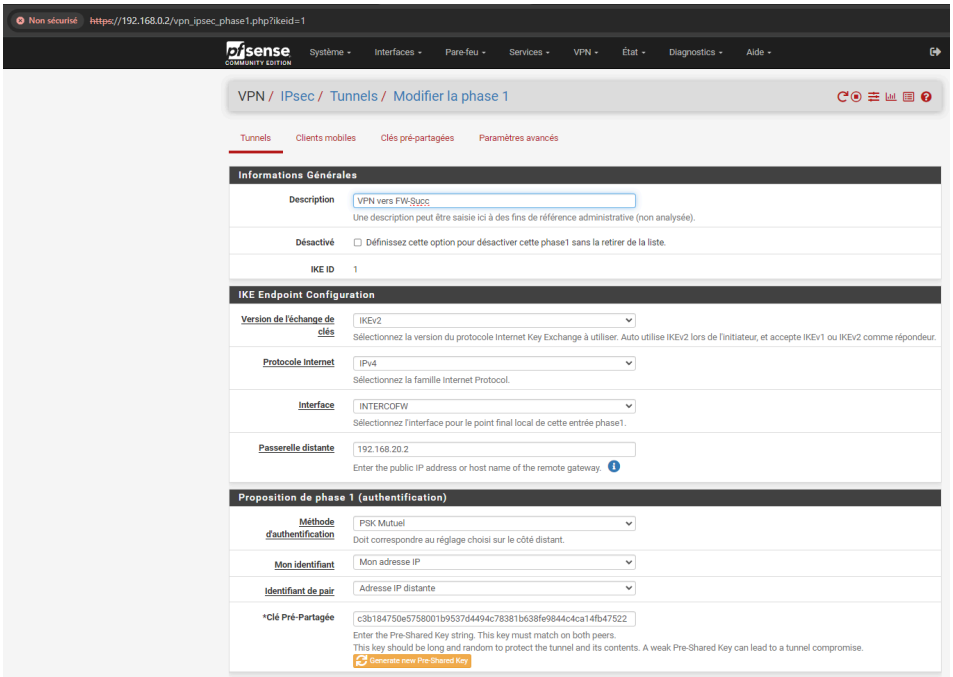


CONFIGURATION PFSENSE IPSEC PARTIE : SIÈGE

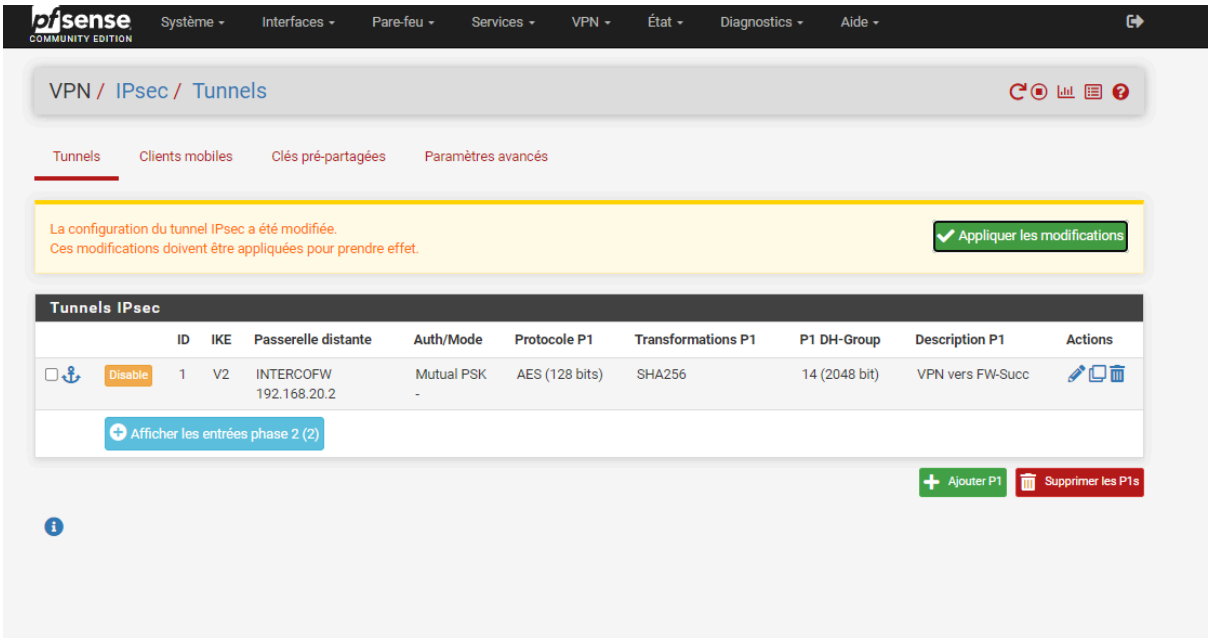
Partie SIEGE

On commence donc par accéder à l'interface d'administration dans le PfSense Siège. On se rend directement dans le menu "VPN" puis dans "IPsec" :

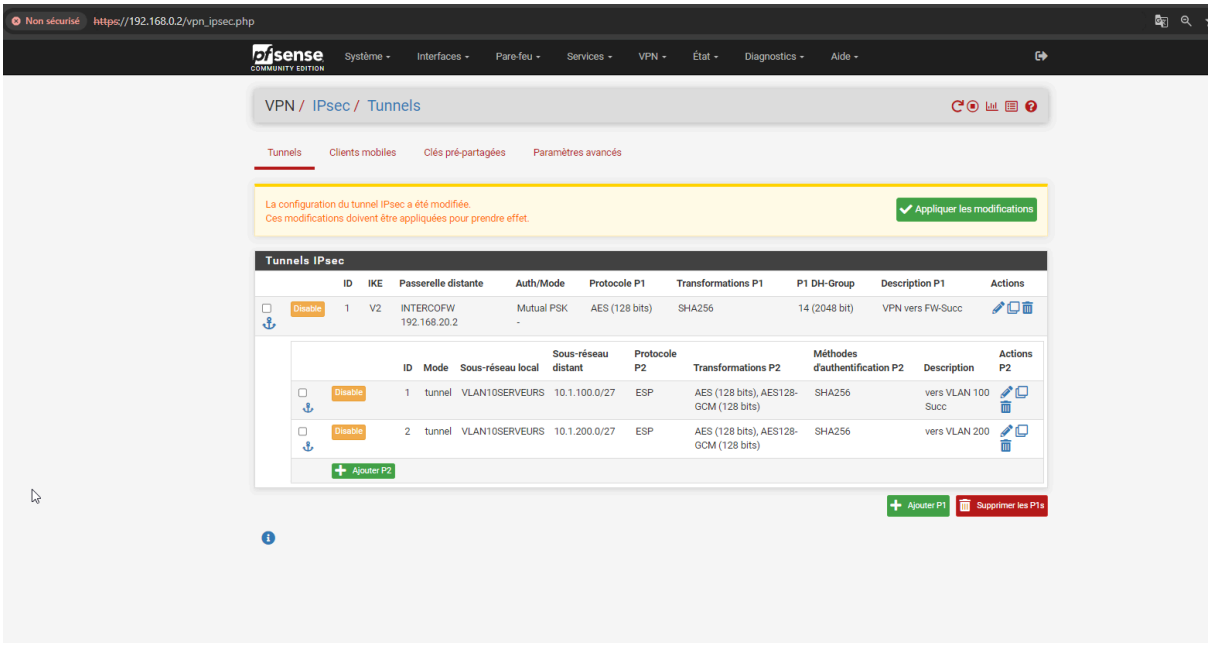
Dans le second cadre qui se nomme "Phase 1 proposal", on va remplir le champ "Pre-Shared Key" et ce parce que le champ "Authentication method" est positionné sur "Mutual PSK" :



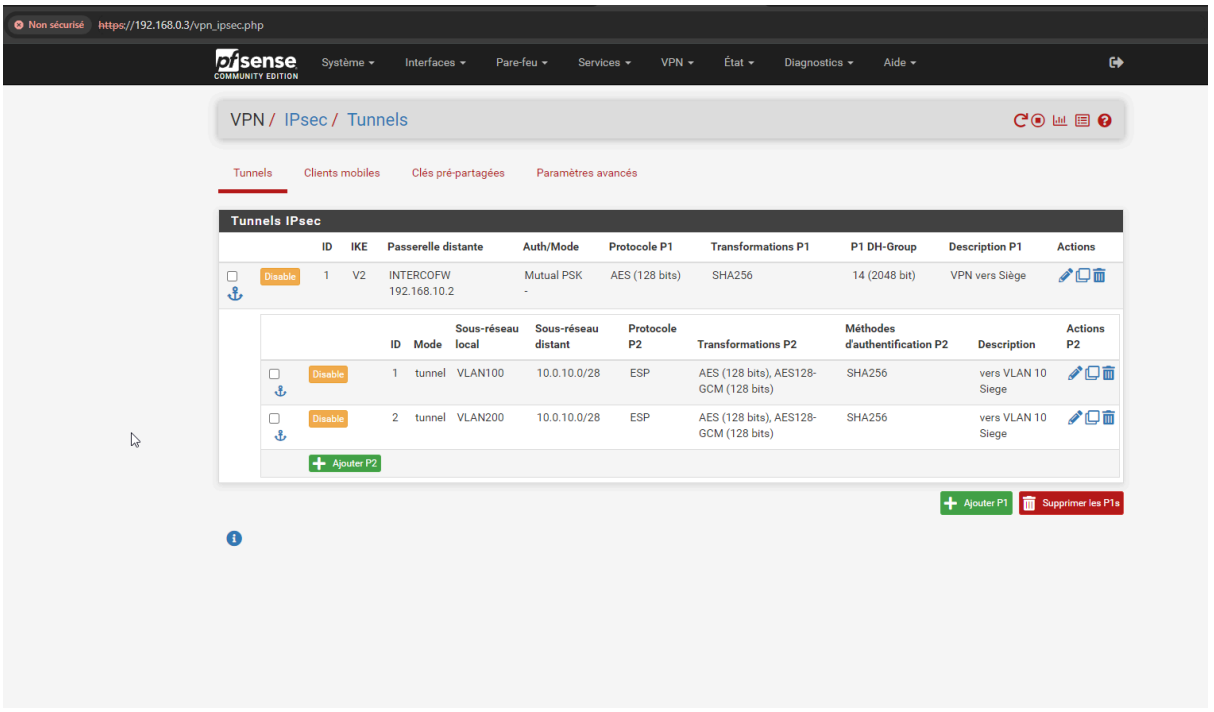
On finit par cliquer sur "Save" puis sur "Apply changes" sur la page suivante. On va alors cliquer sur le "+" présent en dessous de la première ligne du tableau qui se situe sur la page :



Voici les configurations des phases 2 de SIEGE :



Partie Succursale



La connexion est bien établie, les phases 1 et 2 sont montées et la connexion est en mode “established”

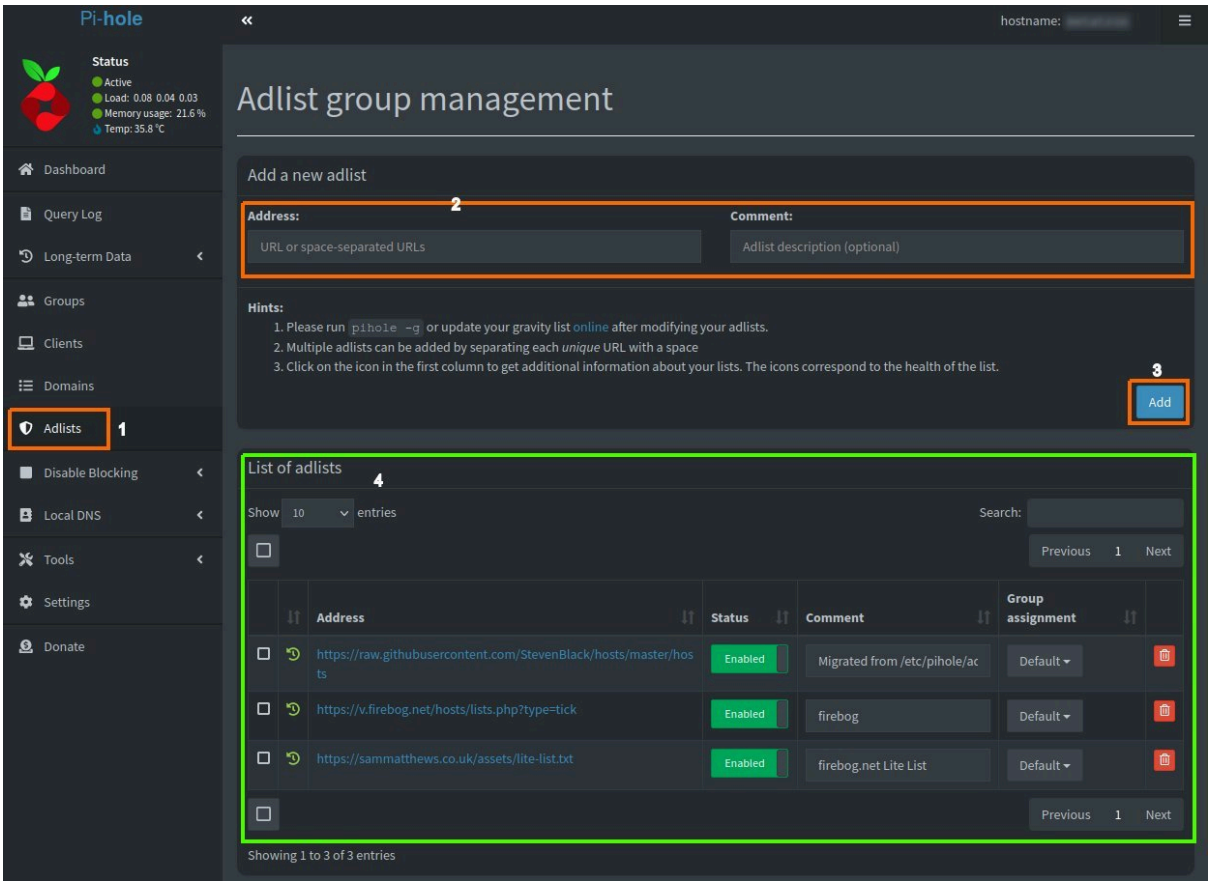
Pi-hole

Installation

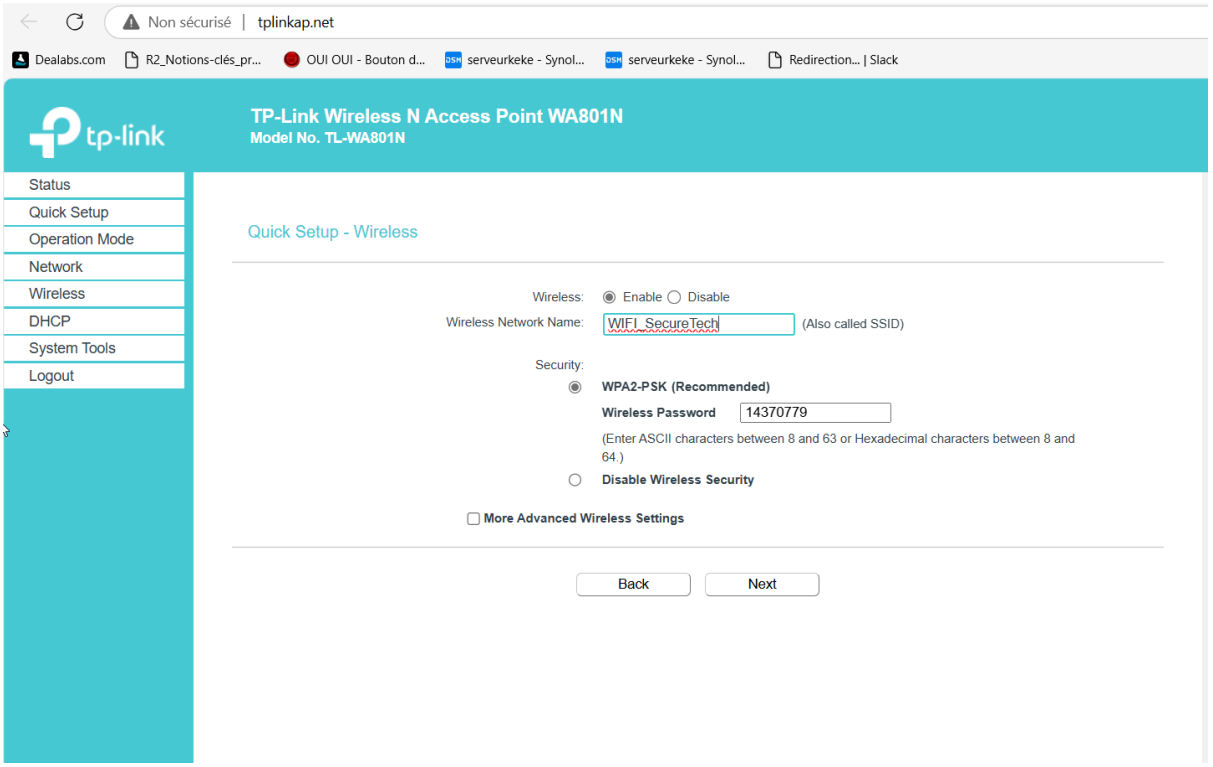
curl -sSL https://install.pi-hole.net | bash

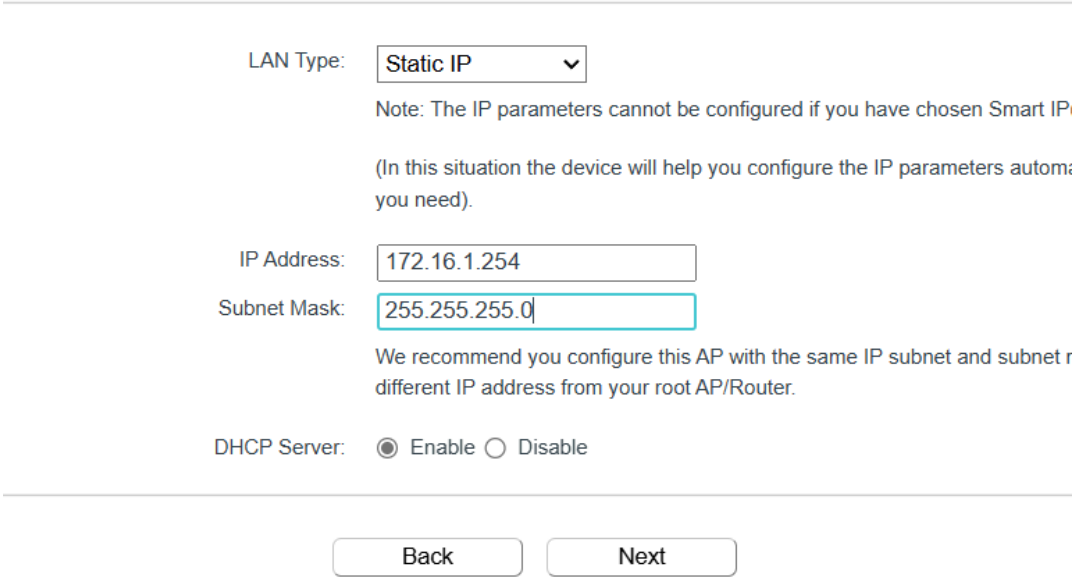
Ajout de nouvelles listes de blocage

1. Cliquez sur "Adlists" dans le menu de gauche
2. Ajoutez l'URL de la liste et éventuellement un commentaire pour vous y retrouver
3. Cliquez sur le bouton "Add" pour ajouter la liste
4. La nouvelle liste s'affiche maintenant en bas de l'écran dans "List of adlists" :



Configuration Point d'accès TP-Link





CrowdSec

Installation

curl -s https://packagecloud.io/install/repositories/crowdsec/crowdsec/script.deb.sh | sudo bash

sudo apt-get update
apt-get install crowdsec
systemctl reload crowdsec

wget https://github.com/crowdsecurity/cs-nginx-bouncer/releases/download/v0.0.4/cs-nginx-bouncer.tgz

tar -xzvf cs-nginx-bouncer.tg

cd cs-nginx-bouncer-v0.0.4/
./install.sh
systemctl restart nginx
cscli dashboard setup --listen 0.0.0.0

Plan de Sécurité du Réseau

- **Description** : Un document dédié à toutes les mesures de sécurité mises en œuvre.
- **Contenu attendu** : Détails sur les configurations de sécurité, les règles de pare-feu, les solutions IDS/IPS mises en œuvre, les stratégies d'authentification et tout autre mécanisme de sécurité.
- **Importance** : Souligne l'engagement à protéger les actifs de SecureTech Industries et donne une vue d'ensemble de toutes les mesures de sécurité en place.

Eléments de sécurité du réseau

Liste des logiciels choisis :

1. PfSense

Pfsense est un système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD.
Son but est simplement d'interconnecter plusieurs réseaux différents.

Mise en place d'un VPN TLS Client To Site sur PFSENSE à l'aide de OpenVPN afin de permettre à vos ordinateurs d'accéder à distance aux ressources de l'entreprise. Cette solution permet tout simplement de mettre en place du télétravail pour que vous puissiez effectuer votre activité professionnelle à distance.

Un VPN TLS est un type de réseau privé virtuel qui utilise le protocole TLS (Transport Layer Security) qui va permettre d'établir une connexion sécurisée d'accès à distance via une page WEB. Une connexion TLS va utiliser un algorithme de chiffrement pour protéger les données transmises entre le client et le serveur.

Mise en place d'un VPN IPSEC Site To Site afin de permettre de joindre deux réseaux LAN distants de manière à faire en sorte qu'ils puissent communiquer comme si ils étaient sur le même réseau et qu'un simple routeur les séparait.

Un VPN IPSEC (Internet Protocol Secure) va permettre de sécuriser les connexions entre les appareils en ajoutant une méthode de chiffrement et d'authentification.

2. Proxmox

Proxmox est une plateforme de virtualisation open-source qui combine la virtualisation basée sur des conteneurs (LXC) et la virtualisation de machines (KVM) dans une seule solution.

3. La solution de supervision Zabbix

Un logiciel libre permettant de surveiller l'état de divers services réseau, serveurs et autres matériels réseau et produisant des graphiques dynamiques de consommation des ressources.

4. Suricata

Un logiciel open source de détection d'intrusion, de prévention d'intrusion, et de supervision de sécurité réseau

5. CrowdSec

Un nouvel outil de prévention des intrusions conçu pour protéger les serveurs, les services, les conteneurs ou les machines virtuelles Linux exposés sur Internet.

6. RADIUS

(Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de centraliser des données d'authentification.

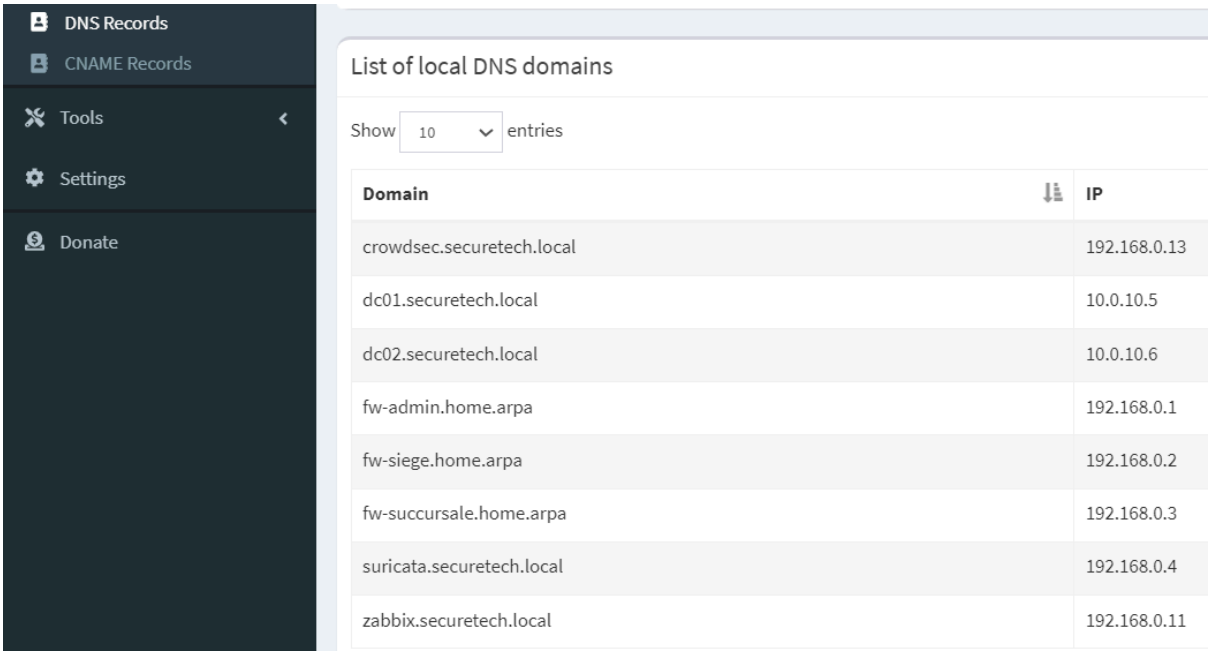
Stratégie d'authentifications (RADIUS SUR WIFI)

Règles de pare-feu

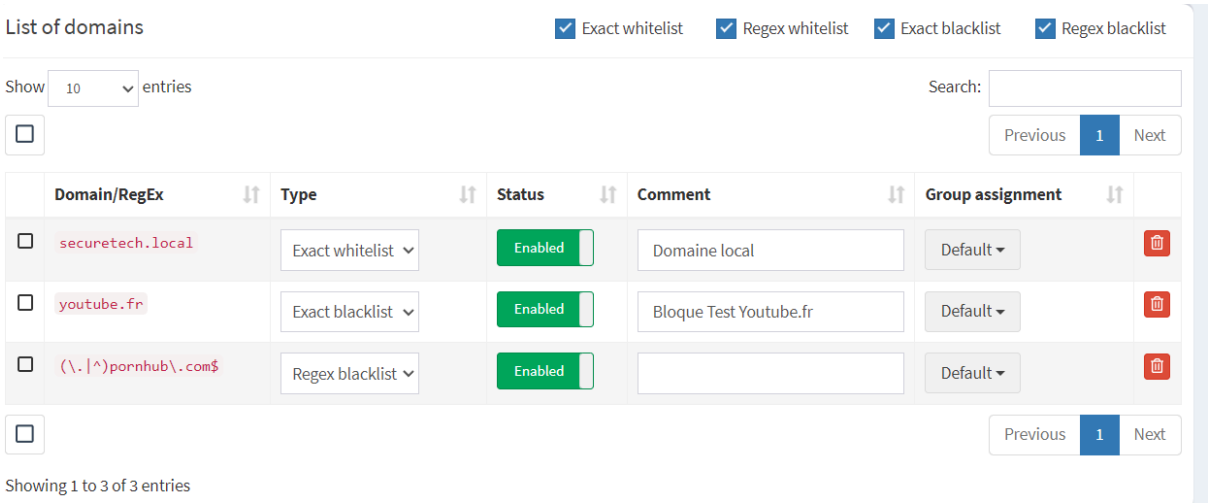
pi-Hole

Définition des noms de domaines

Enregistrement type A pour pouvoir se connecter aux interfaces web des serveurs par un FQDN et non une adresse IP



Blocage des noms de domaines des sites suivants :
youtube.fr
pornhub.com



Suricata

Recommandation ANSSI

Mot de passe :

Selon l'Agence Nationale des Systèmes d'Informations (ANSSI), les bonnes pratiques pour la création et la gestion d'un mot de passe sont entre 10 et 12 caractères pour un mot de passe utilisateur et 14 ou + pour un mot de passe administrateur.
Il faut également utiliser des majuscules, minuscules, des chiffres et des caractères spéciaux (@, #, -, _, &).

Il ne faut surtout pas communiquer son mot de passe à une autre personne, il ne faut pas écrire son mot de passe sur un papier ou un post-it.
Vous pouvez utiliser une phrase pour mémoriser vos mots de passe qui respectent les normes préconisées pour un mot de passe comme par exemple : J@1mE_L3s_Ch@T.

Vous avez notamment un logiciel préconisé par l'ANSSI pour la gestion des mots de passe chiffré et recommandé (Keepass). Attention, éviter d'utiliser le même mot de passe sur des comptes différents. Fixer un délai d'expiration sur des moyens d'authentification est une bonne mesure en général mais s'avère souvent contre-productif dans le cas des mots de passe. En effet, les utilisateurs ont tendance à ajouter un chiffre en + sur leurs mots de passe pour ne pas l'oublier.

En revanche pour les comptes administrateurs, conserver un délai d'expiration de mot de passe reste une bonne mesure à mettre en œuvre. Il est notamment important de mettre un historique de mots de passe pour faciliter la détection des comportements anormaux, les demandes de renouvellement de mots de passe.

<u>Authentification des utilisateurs :</u>
Selon Les règles d'hygiène informatiques de l'ANSSI, privilégier lorsque c'est possible une authentification forte.
En effet, il est vivement recommandé de mettre en œuvre une authentification forte nécessitant l'utilisation de deux facteurs d'authentification différents parmi les suivants :
- Application d'authentification mobile ;
- Un code unique SMS depuis le téléphone ;
- Un code utilisable pendant une période limitée (TOTP) ;

- Clé de sécurité ou cryptographique ;
- Empreinte biométrique
; - Reconnaissance faciale ;
- Reconnaissance Vocale ;

Gestion des droits

Selon les règles d'hygiène informatique de l'ANSSI, il est important d'avoir une gestion des utilisateurs afin d'attribuer les comptes aux utilisateurs de manière nominative et d'attribuer le moindre privilège, c'est-à-dire de ne pas donner des privilèges importants comme Administrateur mais seulement les droits dont ils sont besoin pour effectuer leurs tâches.

La sensibilisation

Selon le guide d'hygiène informatique de l'ANSSI, chaque utilisateur est un maillon à part entière de la chaîne des systèmes d'information.
A ce titre et dès son arrivée dans l'entité, il doit être informé des enjeux de sécurité, des règles à respecter et des bons comportements à adopter en matière de sécurité des systèmes d'information à travers des actions de sensibilisation.
Les sensibilisations doivent être régulières et adaptés aux utilisateurs ciblés sous différentes formes :

- Mails ;
- Réunions ;
- Espace Intranet ;
- Visioconférences ;

Vous devez notamment aborder au minimum les sujets suivants :

- Les objectifs et enjeux que rencontre l'entité en matière de sécurité des systèmes d'informations ;
- Les informations considérées comme données personnels ou données sensibles ;
- Les règlementations et obligations légales ;
- Les règles et consignes de sécurité régissant l'activité quotidienne, respect de la politique de sécurité, non connexion BYOD au réseau de l'entité, non divulgation de mots de passe à un tiers, non-réutilisation de mots de passe professionnels dans la sphère privée et inversement, signalement d'événements suspects.
- Les moyens disponibles en participant à la sécurité du système : verrouillage systématique de la session lorsque l'utilisateur quitte son poste, outil de protection des mots de passe…

Enfin, pour renforcer vivement ces mesures, l'élaboration et la signature d'une charte informatiques précisant les règles et consignes que doivent respecter les utilisateurs peut être envisagée.

Rapport de Monitoring et de Performance

- **Description** : Un rapport détaillant les outils et méthodes utilisés pour surveiller le réseau, ainsi que les performances observées.
- **Contenu attendu** : Outils utilisés, statistiques de performance, incidents détectés, et recommandations pour les améliorations futures.
- **Importance** : Démontre une compréhension approfondie de l'état actuel du réseau et souligne les domaines nécessitant une attention particulière.

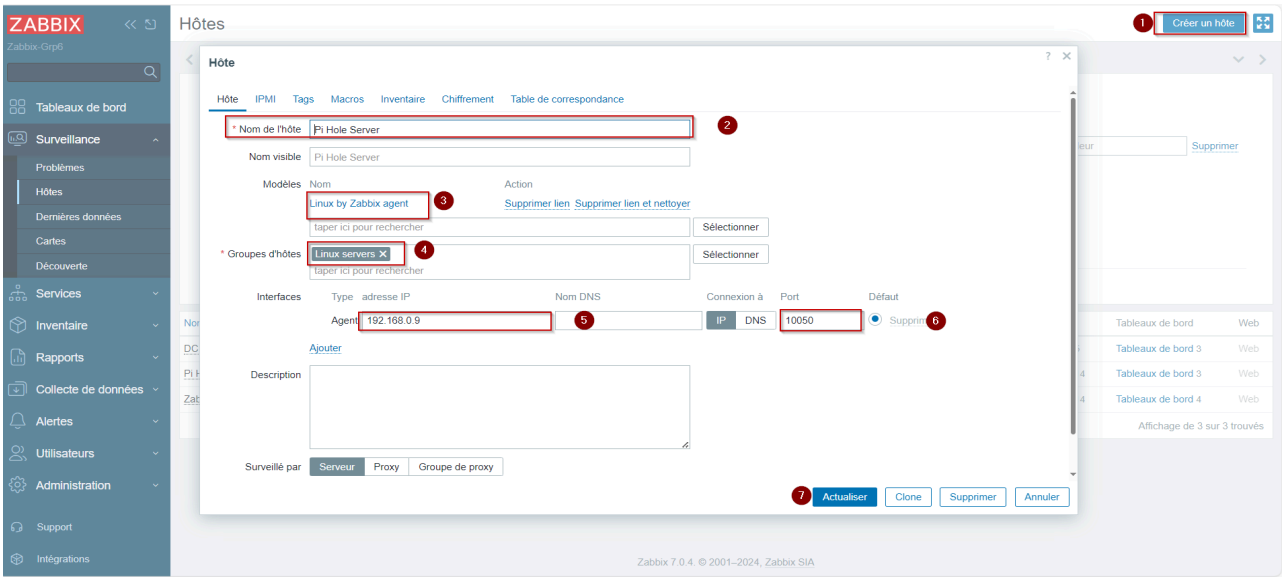
Supervision par Zabbix

Supervision sur les serveurs Linux afin de surveiller les performances du serveur.

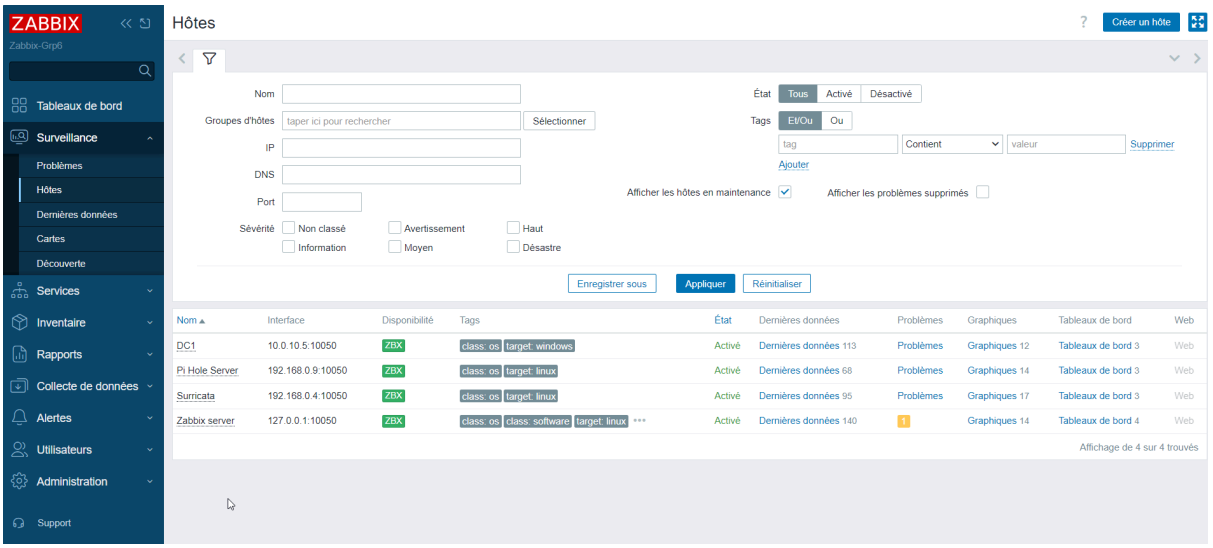
Installation d'agents Zabbix

Process d'installation sur les serveurs Pi-Hole & Surricata

apt install zabbix-agent
nano /etc/zabbix/zabbix_agentd.conf
Server=127.0.0.1,192.168.0.11
server-active=127.0.0.1,192.168.0.11
Listenport=10050
Hostname=zabbix
systemctl start zabbix-agent
systemctl enable zabbix-agent
systemctl status zabbix-agent

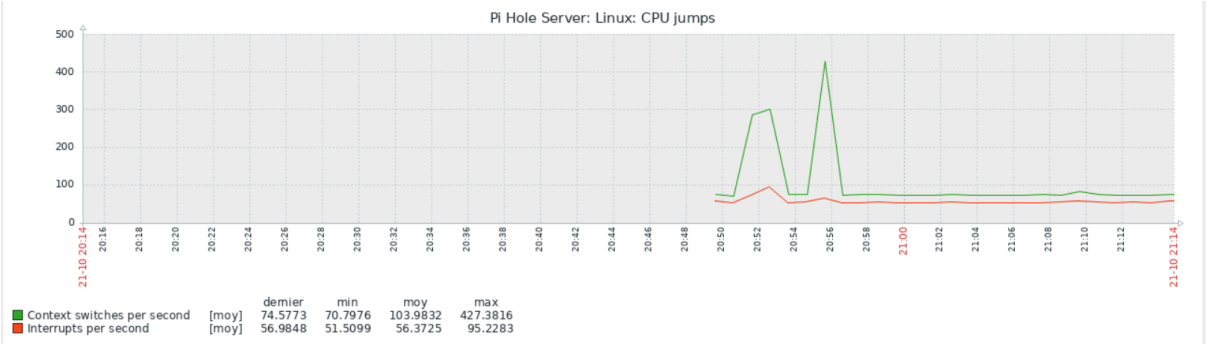


capture d'écran activation et bon fonctionnement des agents Zabbix



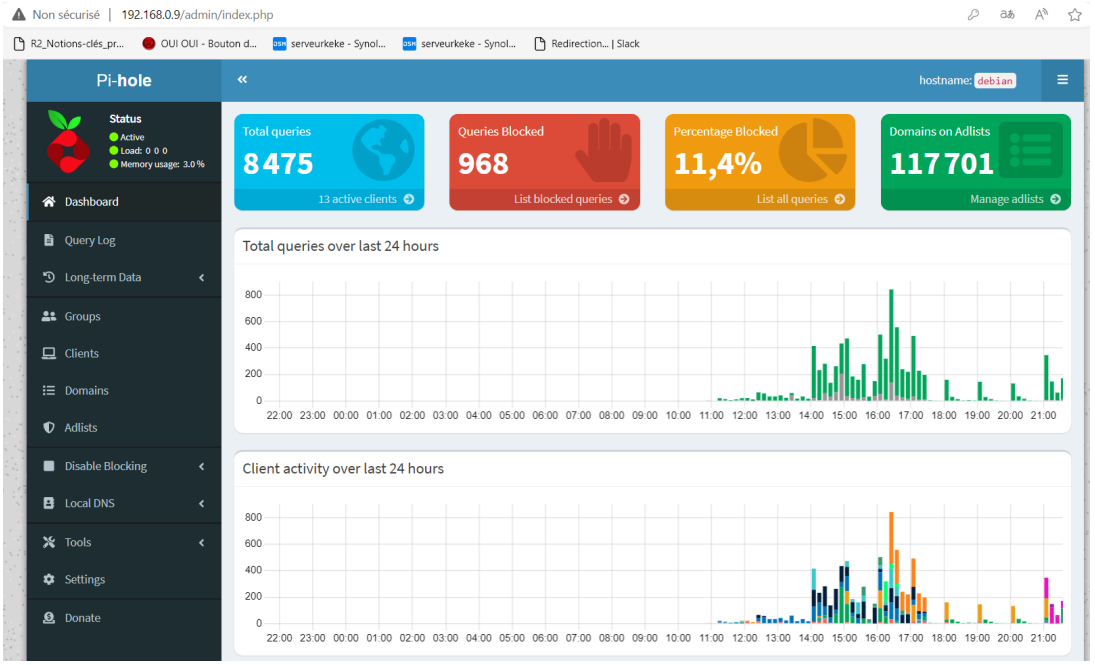
Lien installation zabbix agent Windows : [Download Zabbix agents]

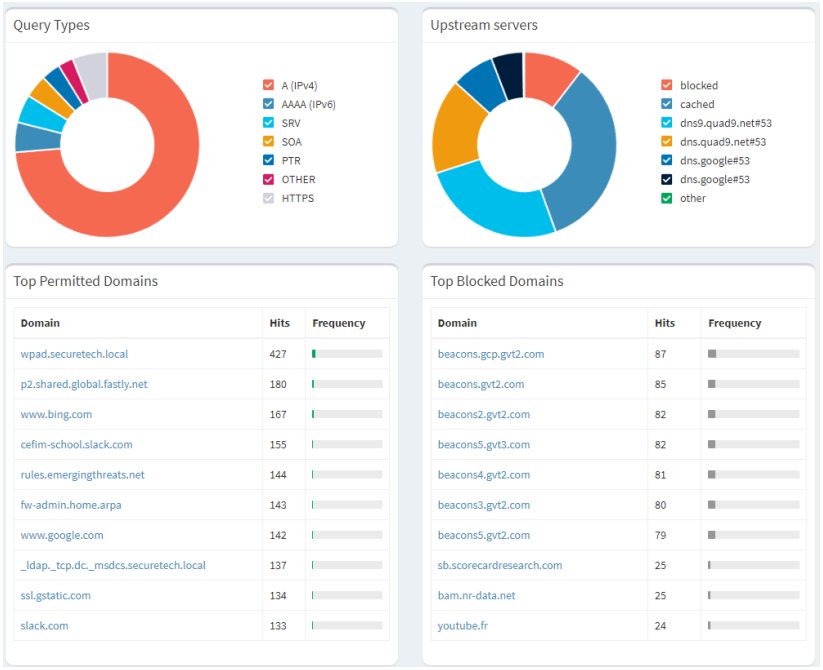
capture d'écran activité Zabbix



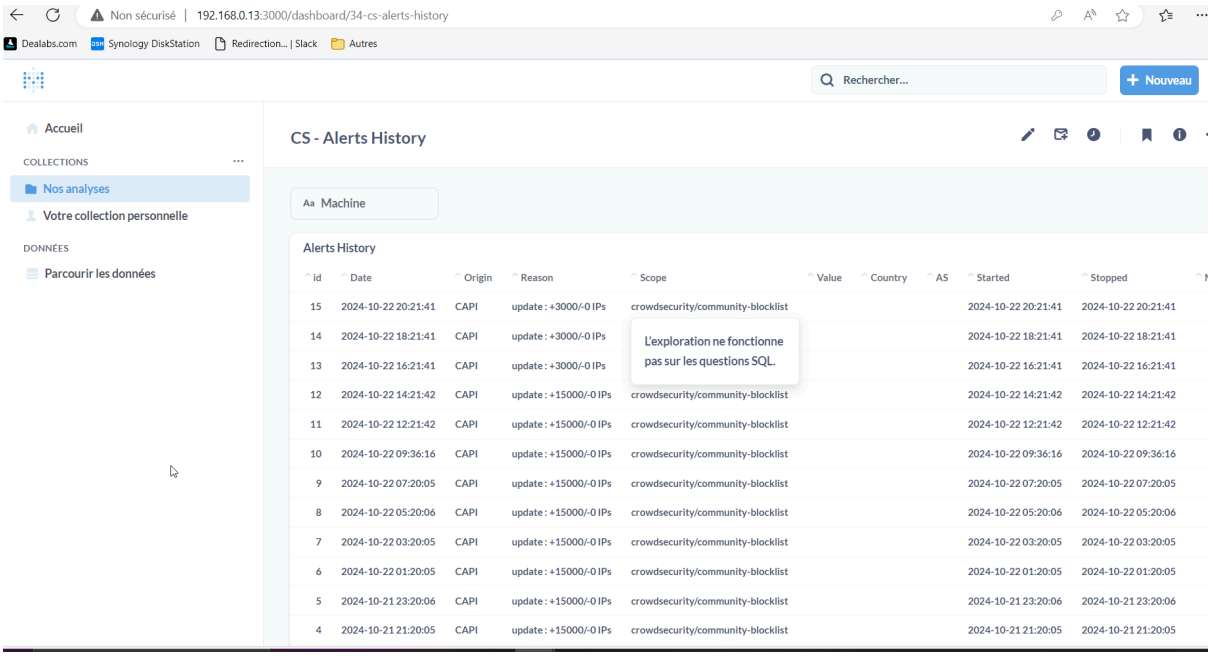
Pi-Hole

On peut constater que il y a eu plusieurs tentatives de connexions sur des sites bloqués :





CrowdSec

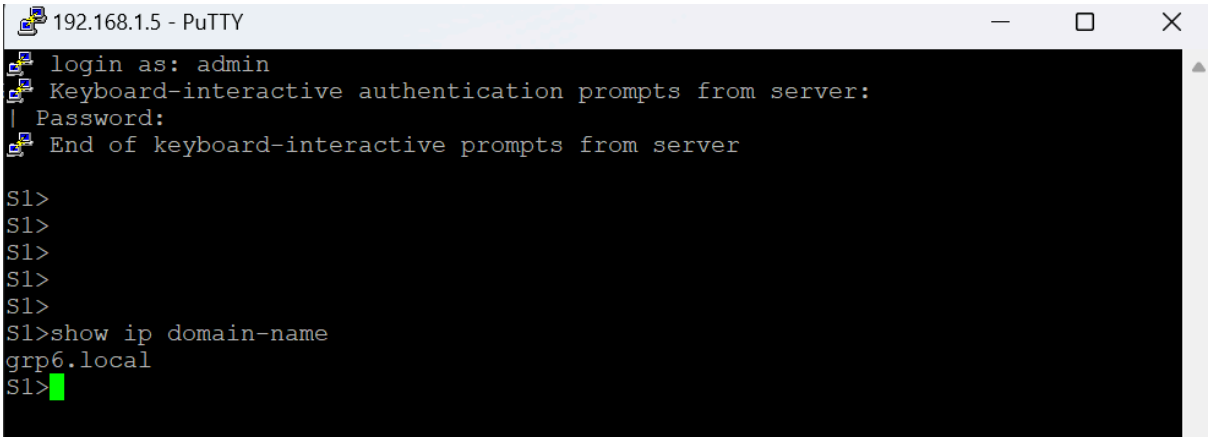


id	Date	Origin	Reason	Scope	Value	Country	AS	Started	Stopped
15	2024-10-22 20:21:41	CAPI	update : +3000/-0 IPs	crowdsecurity/community-blocklist				2024-10-22 20:21:41	2024-10-22 20:21:41
14	2024-10-22 18:21:41	CAPI	update : +3000/-0 IPs	crowdsecurity/community-blocklist				2024-10-22 18:21:41	2024-10-22 18:21:41
13	2024-10-22 16:21:41	CAPI	update : +3000/-0 IPs	crowdsecurity/community-blocklist				2024-10-22 16:21:41	2024-10-22 16:21:41
12	2024-10-22 14:21:42	CAPI	update : +15000/-0 IPs	crowdsecurity/community-blocklist				2024-10-22 14:21:42	2024-10-22 14:21:42
11	2024-10-22 12:21:42	CAPI	update : +15000/-0 IPs	crowdsecurity/community-blocklist				2024-10-22 12:21:42	2024-10-22 12:21:42
10	2024-10-22 09:36:16	CAPI	update : +15000/-0 IPs	crowdsecurity/community-blocklist				2024-10-22 09:36:16	2024-10-22 09:36:16
9	2024-10-22 07:20:05	CAPI	update : +15000/-0 IPs	crowdsecurity/community-blocklist				2024-10-22 07:20:05	2024-10-22 07:20:05
8	2024-10-22 05:20:06	CAPI	update : +15000/-0 IPs	crowdsecurity/community-blocklist				2024-10-22 05:20:06	2024-10-22 05:20:06
7	2024-10-22 03:20:05	CAPI	update : +15000/-0 IPs	crowdsecurity/community-blocklist				2024-10-22 03:20:05	2024-10-22 03:20:05
6	2024-10-22 01:20:05	CAPI	update : +15000/-0 IPs	crowdsecurity/community-blocklist				2024-10-22 01:20:05	2024-10-22 01:20:05
5	2024-10-21 23:20:06	CAPI	update : +15000/-0 IPs	crowdsecurity/community-blocklist				2024-10-21 23:20:06	2024-10-21 23:20:06
4	2024-10-21 21:20:05	CAPI	update : +15000/-0 IPs	crowdsecurity/community-blocklist				2024-10-21 21:20:05	2024-10-21 21:20:05

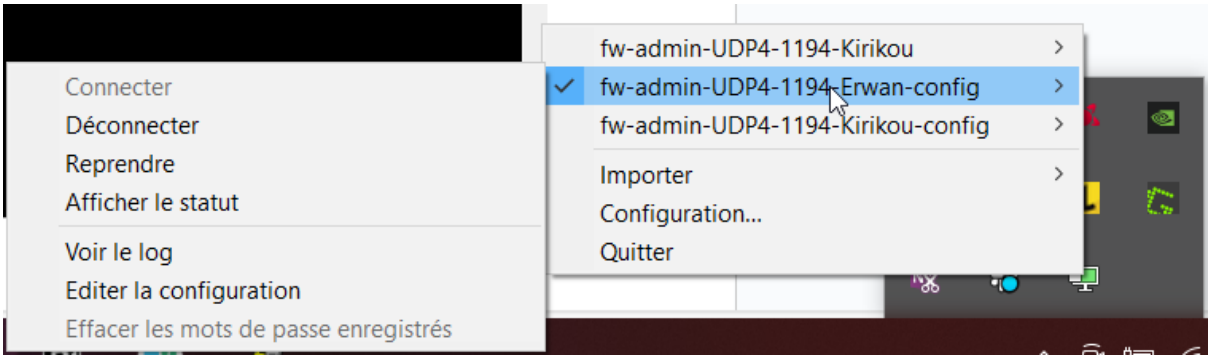
Document de Test

- **Description** : Un ensemble de tests conçus pour valider la fonctionnalité et la sécurité du réseau.
- **Contenu attendu** : Scénarios de test, méthodologies utilisées, résultats attendus et résultats observés.
- **Importance** : Valide que le réseau fonctionne comme prévu et que toutes les mesures de sécurité sont efficaces.

Switch connection en SSH

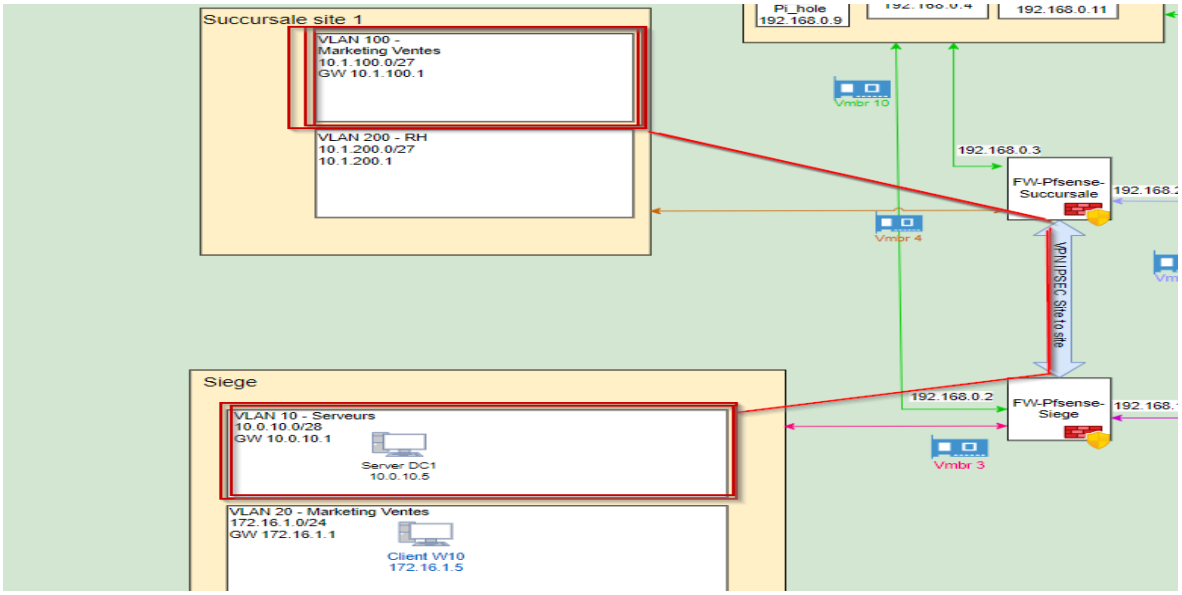


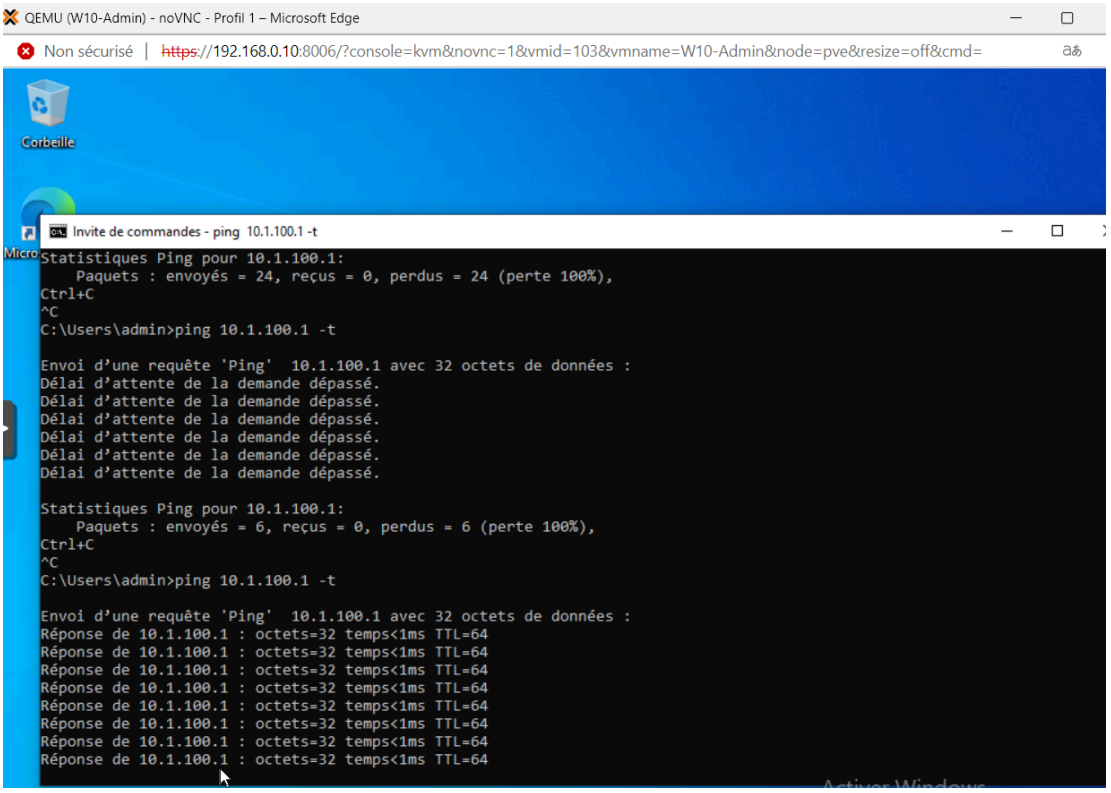
Connection VPN Client to Site



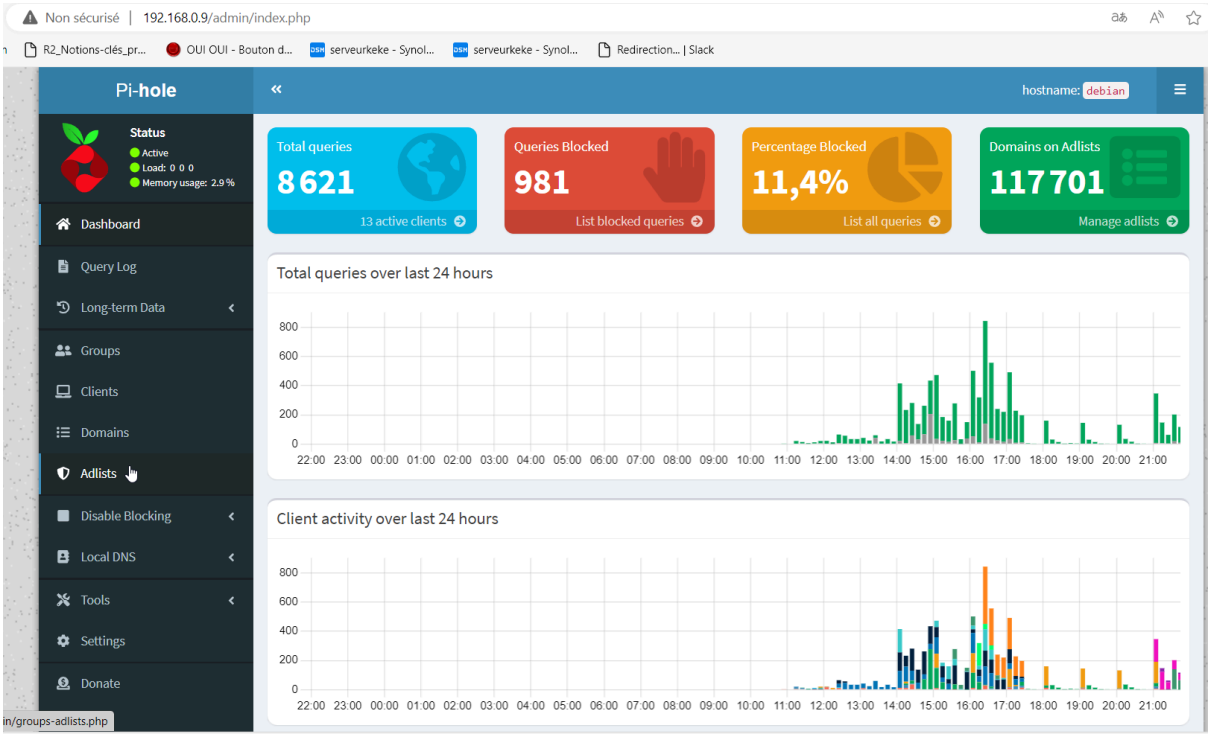
Connection VPN Site to Site :

Exemple avec un client Windows 10 de VLAN 100 Marketing Ventes du réseau Pfsense Succursale vers VLAN 10 Serveurs du réseau Pfsense Siège :


Succursale site 1
VLAN 100 - Marketing Ventes
10.1.100.0/27
GW 10.1.100.1
VLAN 200 - RH
10.1.200.0/27
10.1.200.1
Pi_hole
192.168.0.9
192.168.0.11
Vmbr 10
192.168.0.3
FW-Pfsense-Succursale
Vmbr 4
VPN IPSEC Site to site
Siege
VLAN 10 - Serveurs
10.0.10.0/28
GW 10.0.10.1
Server DC1
10.0.10.5
VLAN 20 - Marketing Ventes
172.16.1.0/24
GW 172.16.1.1
Client W10
172.16.1.5
192.168.0.2
FW-Pfsense-Siege
Vmbr 3


QEMU (W10-Admin) - noVNC - Profil 1 – Microsoft Edge
Non sécurisé | https://192.168.0.10:8006/?console=kvm&novnc=1&vmid=103&vmname=W10-Admin&node=pve&resize=off&cmd=
Corbeille
Invite de commandes - ping 10.1.100.1 -t
Statistiques Ping pour 10.1.100.1:
Paquets : envoyés = 24, reçus = 0, perdus = 24 (perte 100%),
Ctrl+C
^C
C:\Users\admin>ping 10.1.100.1 -t
Envoi d'une requête 'Ping' 10.1.100.1 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.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Statistiques Ping pour 10.1.100.1:
Paquets : envoyés = 6, reçus = 0, perdus = 6 (perte 100%),
Ctrl+C
^C
C:\Users\admin>ping 10.1.100.1 -t
Envoi d'une requête 'Ping' 10.1.100.1 avec 32 octets de données :
Réponse de 10.1.100.1 : octets=32 temps<1ms TTL=64
Réponse de 10.1.100.1 : octets=32 temps<1ms TTL=64
Réponse de 10.1.100.1 : octets=32 temps<1ms TTL=64
Réponse de 10.1.100.1 : octets=32 temps<1ms TTL=64
Réponse de 10.1.100.1 : octets=32 temps<1ms TTL=64
Réponse de 10.1.100.1 : octets=32 temps<1ms TTL=64
Réponse de 10.1.100.1 : octets=32 temps<1ms TTL=64
Réponse de 10.1.100.1 : octets=32 temps<1ms TTL=64

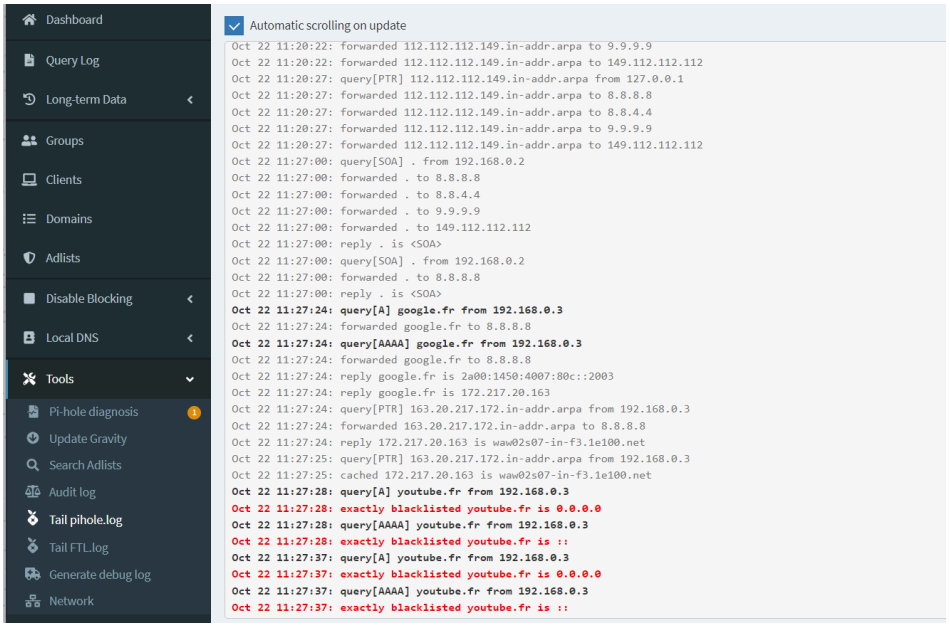
Remonté Pi-hole DNSBL



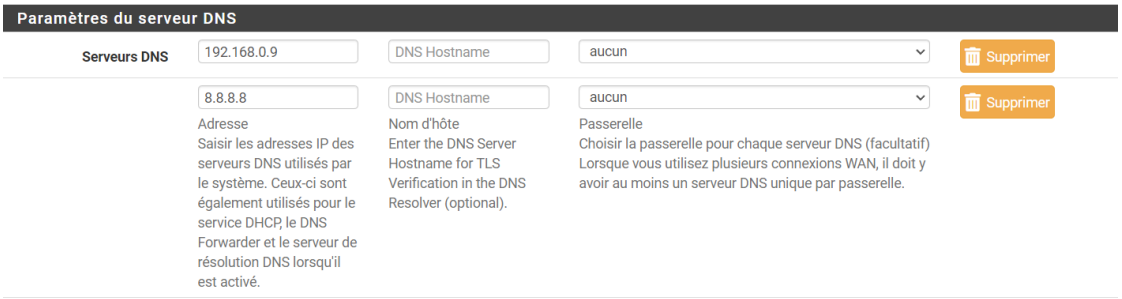
Pour tester nous avons Blacklister le nom de domaine “youtube.fr” et voici le résultat :
Depuis le serveur Zabbix :

```
root@debian:/etc# ping youtube.fr
PING youtube.fr (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.012 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.021 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.024 ms
64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.021 ms
64 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.016 ms
64 bytes from localhost (127.0.0.1): icmp_seq=6 ttl=64 time=0.018 ms
64 bytes from localhost (127.0.0.1): icmp_seq=7 ttl=64 time=0.011 ms
64 bytes from localhost (127.0.0.1): icmp_seq=8 ttl=64 time=0.014 ms
64 bytes from localhost (127.0.0.1): icmp_seq=9 ttl=64 time=0.013 ms
64 bytes from localhost (127.0.0.1): icmp_seq=10 ttl=64 time=0.017 ms
64 bytes from localhost (127.0.0.1): icmp_seq=11 ttl=64 time=0.019 ms
64 bytes from localhost (127.0.0.1): icmp_seq=12 ttl=64 time=0.017 ms
64 bytes from localhost (127.0.0.1): icmp_seq=13 ttl=64 time=0.017 ms
64 bytes from localhost (127.0.0.1): icmp_seq=14 ttl=64 time=0.016 ms
64 bytes from localhost (127.0.0.1): icmp_seq=15 ttl=64 time=0.017 ms
64 bytes from localhost (127.0.0.1): icmp_seq=16 ttl=64 time=0.020 ms
64 bytes from localhost (127.0.0.1): icmp_seq=17 ttl=64 time=0.018 ms
64 bytes from localhost (127.0.0.1): icmp_seq=18 ttl=64 time=0.019 ms
64 bytes from localhost (127.0.0.1): icmp_seq=19 ttl=64 time=0.019 ms
64 bytes from localhost (127.0.0.1): icmp_seq=20 ttl=64 time=0.019 ms
64 bytes from localhost (127.0.0.1): icmp_seq=21 ttl=64 time=0.018 ms
64 bytes from localhost (127.0.0.1): icmp_seq=22 ttl=64 time=0.015 ms
64 bytes from localhost (127.0.0.1): icmp_seq=23 ttl=64 time=0.018 ms
64 bytes from localhost (127.0.0.1): icmp_seq=24 ttl=64 time=0.018 ms
64 bytes from localhost (127.0.0.1): icmp_seq=25 ttl=64 time=0.019 ms
64 bytes from localhost (127.0.0.1): icmp_seq=26 ttl=64 time=0.020 ms
64 bytes from localhost (127.0.0.1): icmp_seq=27 ttl=64 time=0.019 ms
64 bytes from localhost (127.0.0.1): icmp_seq=28 ttl=64 time=0.019 ms
64 bytes from localhost (127.0.0.1): icmp_seq=29 ttl=64 time=0.019 ms
64 bytes from localhost (127.0.0.1): icmp_seq=30 ttl=64 time=0.020 ms
^C
--- youtube.fr ping statistics ---
30 packets transmitted, 30 received, 0% packet loss, time 29686ms
rtt min/avg/max/mdev = 0.011/0.017/0.024/0.002 ms
```

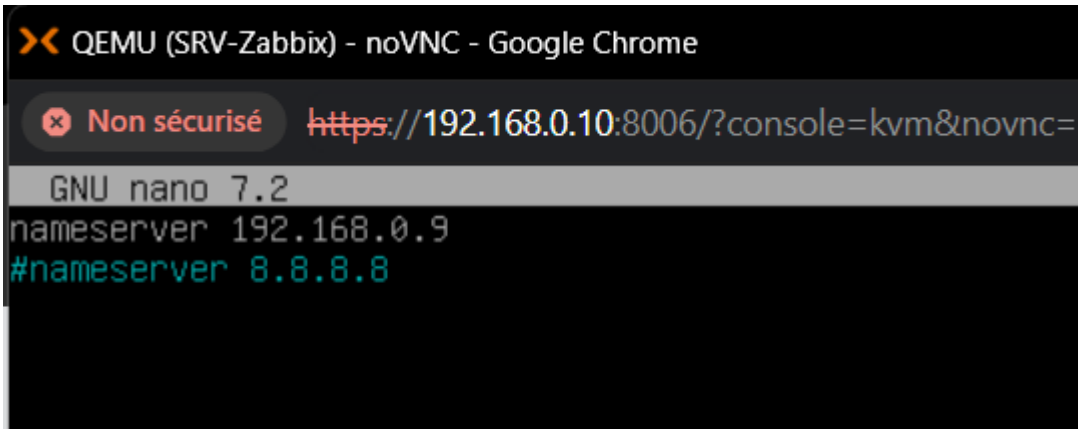
Depuis l’interface Pi_Hole :



Nous avons mis en DNS primaire sur les services, l’adresse IP du serveur Pi-Hole.
Sur les Pfsense : Admin, Succursale et Siège

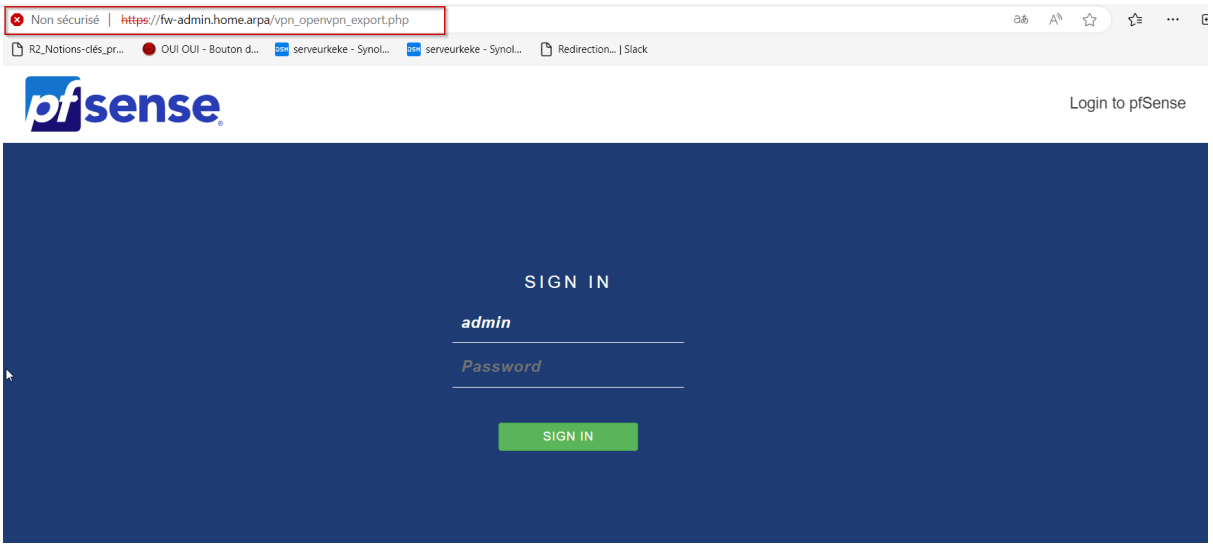


Sur les serveurs OS LINUX :



Pi-Hole - Nom de domaines

Les noms de domaines attribués à chacun de nos serveurs sont bien fonctionnels :



Crowdsec

Remonté d'alerte et autres : 192.168.0.13:3000