

	NetAdmin	Version : A
	[AIS2024]_Documentation_SecureTechIndustries	

Présentation Projet SecureTech

Introduction	1
Objectifs :.....	1

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 :

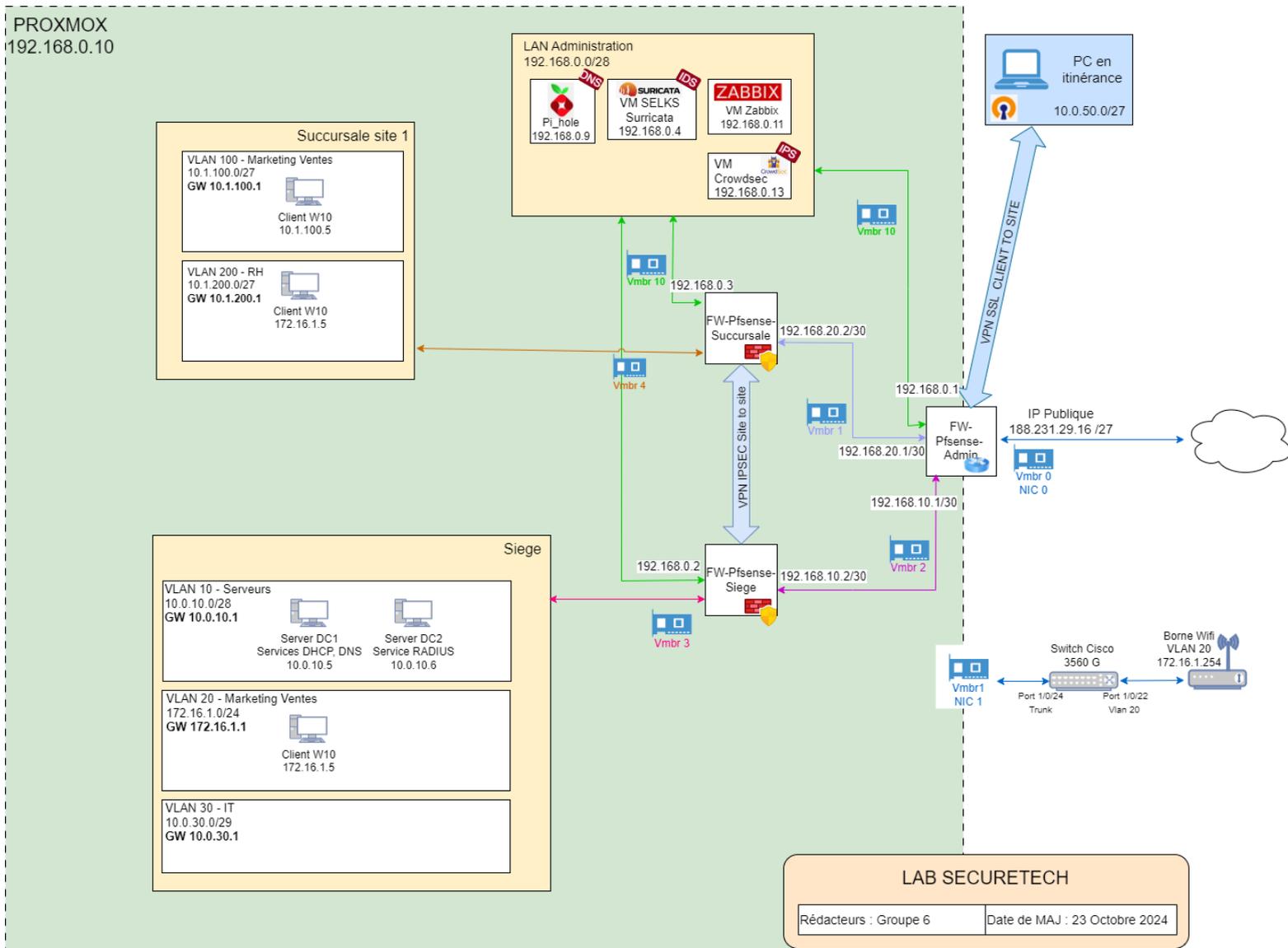
1. Interconnexion entre site Principal et site Succursale
=> VPN Site à Site
2. Accès sécurisé pour les commerciaux itinérants
=>VPN SSL
3. Segmenter le réseau pour isoler la production du département de management et des autres services
=> VLAN
4. Solutions d'authentification forte pour les commerciaux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



	NetAdmin	Version : A
	[AIS2024]_Matrice_des_flux	

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.....	2
Règles de routages.....	2



NetAdmin

[AIS2024]_Matrice_des_flux

Version : A

Matrice

Lien [Matrice des flux Securetech](#)

SOURCE	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
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	Redirection DNS	X			X	X	X	X	X
DHCP FW	/	X	x	x	X	X	X	/		X		PAR VPN CLIENT TO SITE	X	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	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 Interfaces	X		X	/	x	xx	X
ITS CROWDSEC	/	X			x	x	x	x	DNS	Interfaces	x		x	/	x	x	x
ZABBIX	/	X		X	Monitoring SMB	Monitoring SMB	x	x	DNS		x	X	X	Monitoring	Monitoring	Monitoring	Monitoring
NAS	/	X	X	X			X	X	X	X		X	X	X	X	X	/

Règles de routages

The screenshot shows the pfSense web interface for static routes. The breadcrumb navigation is "Système / Routage / Routes statiques". There are three tabs: "Passerelles", "Routes statiques" (selected), and "Groupes de passerelle".

Requête	Réseau	Passerelle	Interface	Description	Actions
<input checked="" type="checkbox"/>	10.1.100.0/27	GW_Pf_Succursale - 192.168.20.2	LAN_VERS_FW_SUCC	vers 10.1.100.0 (vlan 100)	
<input checked="" type="checkbox"/>	10.0.10.0/28	GW_Pf_Siege - 192.168.10.2	LAN_VERS_FW_SIEGE	vers 10.0.10.0 (vlan 10)	
<input checked="" type="checkbox"/>	172.16.1.0/24	GW_Pf_Siege - 192.168.10.2	LAN_VERS_FW_SIEGE	vers 172.16.1.0 - VLAN 20	
<input checked="" type="checkbox"/>	10.1.200.0/27	GW_Pf_Succursale - 192.168.20.2	LAN_VERS_FW_SUCC	vers 10.1.200.0 (vlan 200)	
<input checked="" type="checkbox"/>	10.0.30.0/32	GW_Pf_Siege - 192.168.10.2	LAN_VERS_FW_SIEGE		

At the bottom right, there is a green button labeled "Ajouter" with a plus sign icon.

 cefim <small>L'école du web et des réseaux</small>	NetAdmin	Version : A
	[AIS2024] Document de configuration des équipements	

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	2
Configuration Switch Cisco Catalyst 3560 G	2
Configuration trunk :	2
Configuration hostname et domaine.....	3
Configuration SSH.....	3
Configuration de l'authentification et ajout d'un compte administrateur.....	3
Configuration de l'adresse du switch.....	3
Configuration du port mirroring.....	3
Configuration ARP.....	4
Zabbix	4
PfSense	5
Configuration du VPN Client to Site (PFSENSE ADMIN).....	5
Configurer le serveur OpenVPN.....	9
Configuration du VPN Site to Site (PFSENSE SIEGE ET SUCCURSALE):.....	12
CONFIGURATION PFSENSE IPSEC PARTIE : SIÈGE.....	15
Partie SIEGE.....	15
Partie Succursale.....	17
Pi-hole	18
Installation.....	18
Ajout de nouvelles listes de blocage.....	18
Configuration Point d'accès TP-Link :	19
CrowdSec	20
Installation.....	20

Proxmox

Vmbr2 : Admin

auto vmbr2

iface **vmbr2** inet static

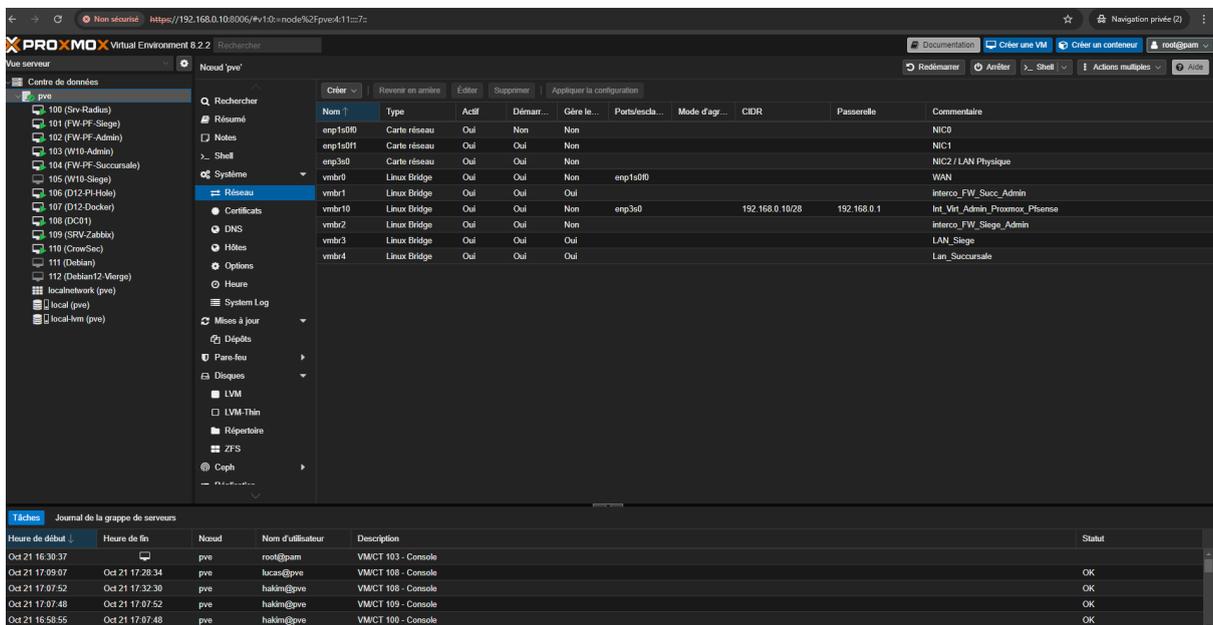
address 192.168.0.10/27

gateway 192.168.0.1

bridge-ports **enp3s0**

bridge-stp off

bridge-fd 0



The screenshot shows the Proxmox VE interface for a new VM named 'pve'. The 'Réseau' (Network) tab is selected, displaying a table of network interfaces:

Nom	Type	Actif	Démarr...	Gère le...	Ports/lescla...	Mode d'agr...	CIDR	Passerelle	Commentaire
emp1s00	Carte réseau	Oui	Non	Non					NIC0
emp1s01	Carte réseau	Oui	Oui	Non					NIC1
emp3s0	Carte réseau	Oui	Oui	Non					NIC2 / LAN Physique
vmbr0	Linux Bridge	Oui	Oui	Non	emp1s00				WAN
vmbr1	Linux Bridge	Oui	Oui	Oui					Interco_FW_Succ_Admin
vmbr10	Linux Bridge	Oui	Oui	Non	emp3s0		192.168.0.10/28	192.168.0.1	Int_Virt_Admin_Proxmox_PSense
vmbr2	Linux Bridge	Oui	Oui	Non					Interco_FW_Siege_Admin
vmbr3	Linux Bridge	Oui	Oui	Oui					LAN_Siege
vmbr4	Linux Bridge	Oui	Oui	Oui					Lan_Succursale

Below the network configuration, a 'Tâches' (Tasks) section shows a log of recent operations:

Heure de début	Heure de fin	Nœud	Nom d'utilisateur	Description	Statut
Oct 21 16:30:37		pve	root@pam	VM/CT 103 - Console	
Oct 21 17:09:07	Oct 21 17:28:34	pve	hacker@pve	VM/CT 100 - Console	OK
Oct 21 17:07:52	Oct 21 17:32:30	pve	hacker@pve	VM/CT 100 - Console	OK
Oct 21 17:07:48	Oct 21 17:07:52	pve	hacker@pve	VM/CT 109 - Console	OK
Oct 21 16:58:55	Oct 21 17:07:48	pve	hacker@pve	VM/CT 100 - Console	OK

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

	NetAdmin	Version : A
	[AIS2024] Document de configuration des équipements	

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
```

Rédacteur : Département DSI	Date de MAJ : 23 oct. 2024	Page 3 sur 20
-----------------------------	----------------------------	---------------

 cefim <small>L'école du web et des réseaux</small>	NetAdmin	Version : A
	[AIS2024] Document de configuration des équipements	

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
```

```
Secure Mac Address Table
-----
```

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;
```

Rédacteur : Département DSI	Date de MAJ : 23 oct. 2024	Page 4 sur 20
-----------------------------	----------------------------	---------------

```
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

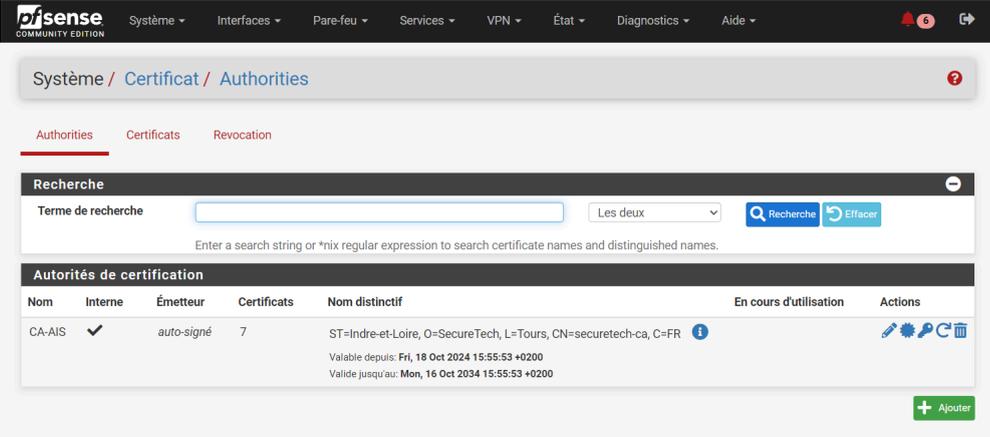
```
# systemctl restart zabbix-server zabbix-agent apache2
# systemctl enable zabbix-server zabbix-agent apache2
```

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

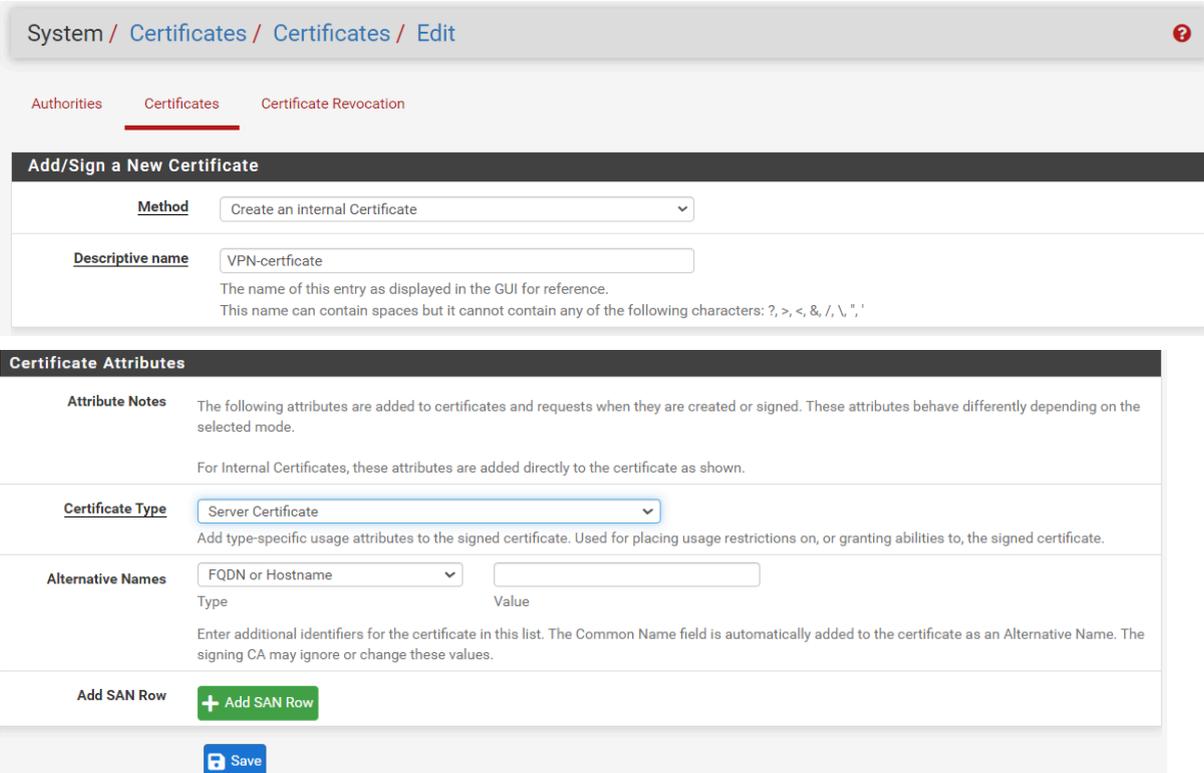


Nom	Interne	Émetteur	Certificats	Nom distinctif	En cours d'utilisation	Actions
CA-AIS	✓	auto-signé	7	ST=Indre-et-Loire, O=SecureTech, L=Tours, CN=securetech-ca, C=FR		  

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-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.



System / Certificates / Certificates / Edit

Authorities Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create an internal Certificate

Descriptive name VPN-certificate
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: ?, >, <, &, /, \, ", '.

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 SAN Row + Add SAN Row

Save

	NetAdmin	Version : A
	[AIS2024] Document de configuration des équipements	

Internal Certificate	
Certificate authority	CA-AIS
Key type	RSA
	2048
	<small>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.</small>
Digest Algorithm	sha256
	<small>The digest method used when the certificate is signed. The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.</small>
Lifetime (days)	3650
	<small>The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.</small>
Common Name	securetech-ca
	<small>The following certificate subject components are optional and may be left blank.</small>
Country Code	FR
State or Province	Indre-et-Loire
City	Tours
Organization	SecureTech
Organizational Unit	e.g. My Department Name (optional)

Créer les utilisateurs locaux

On crée 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!

Users Groups Settings Authentication Servers

User Properties

Defined by: USER

Disabled: This user cannot login

Username:

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:
Not member of: Member of

Certificate: Click to create a user certificate

Create Certificate for User

Descriptive name:

Certificate authority:

Key type:

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:
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

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

System / User Manager / Users

Users Groups Settings Authentication Servers

Users

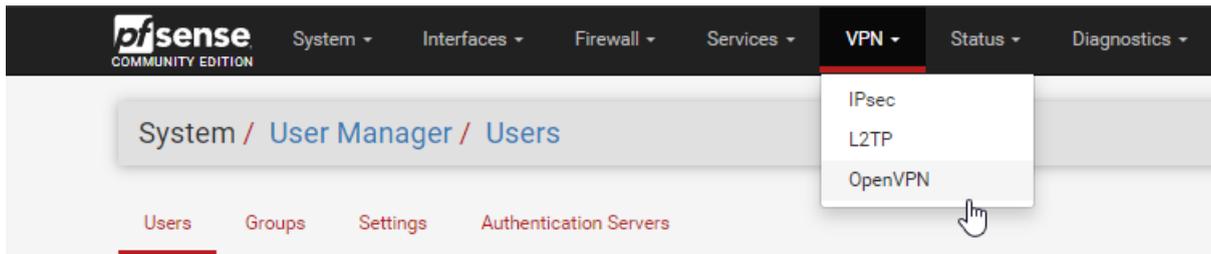
	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	 Kirikou		✓		 
<input type="checkbox"/>	 admin	System Administrator	✓	admins	



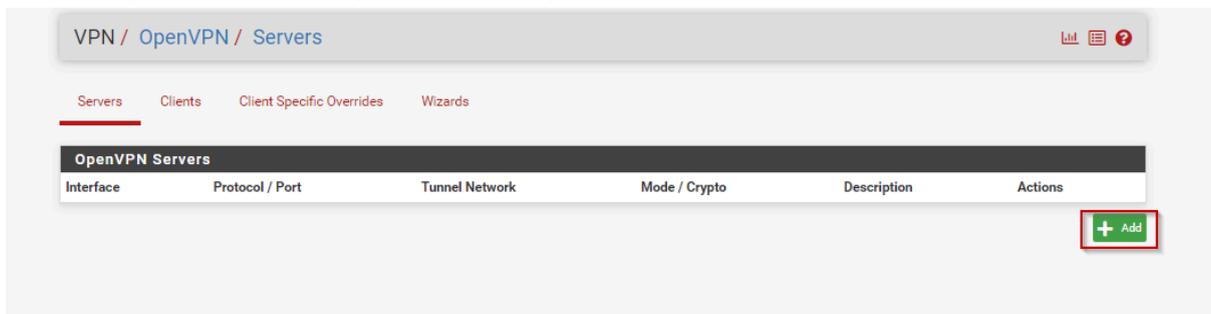
Configurer le serveur OpenVPN

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".

Cryptographic Settings

TLS Configuration Use a TLS Key
 A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.

Automatically generate a TLS Key.

Peer Certificate Authority

Peer Certificate Revocation list No Certificate Revocation Lists defined. One may be created here: [System > Cert. Manager](#)

OCSP Check Check client certificates with OCSP

Server certificate
 Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.

DH Parameter Length
 Diffie-Hellman (DH) parameter set used for key exchange. [i](#)

ECDH Curve
 The Elliptic Curve to use for key exchange.
 The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.

Data Encryption Algorithms

Available Data Encryption Algorithms Click to add or remove an algorithm from the list AES-192-CFB8 (192 bit key, 128 bit block) AES-192-GCM (192 bit key, 128 bit block) AES-192-OFB (192 bit key, 128 bit block) AES-256-CBC (256 bit key, 128 bit block) AES-256-CFB (256 bit key, 128 bit block) AES-256-CFB1 (256 bit key, 128 bit block) AES-256-CFB8 (256 bit key, 128 bit block) AES-256-GCM (256 bit key, 128 bit block) AES-256-OFB (256 bit key, 128 bit block) CAMELLIA-128-CBC (128 bit key, 128 bit block)	Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list AES-256-GCM AES-128-GCM CHACHA20-POLY1305
---	---

The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode. [i](#)

Fallback Data Encryption Algorithm
 The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.

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

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)

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

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

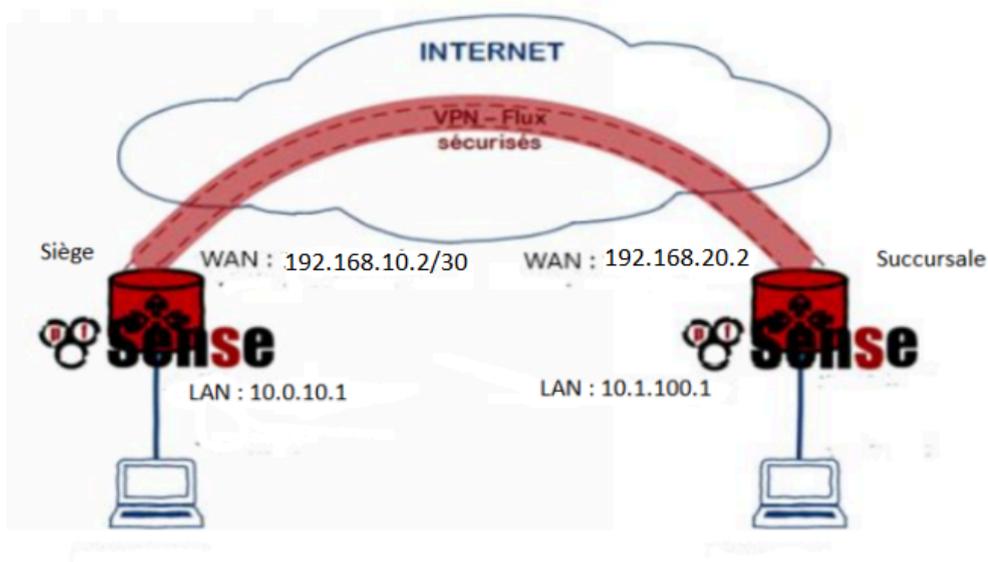
Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

	NetAdmin	Version : A
	[AIS2024] Document de configuration des équipements	

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 :



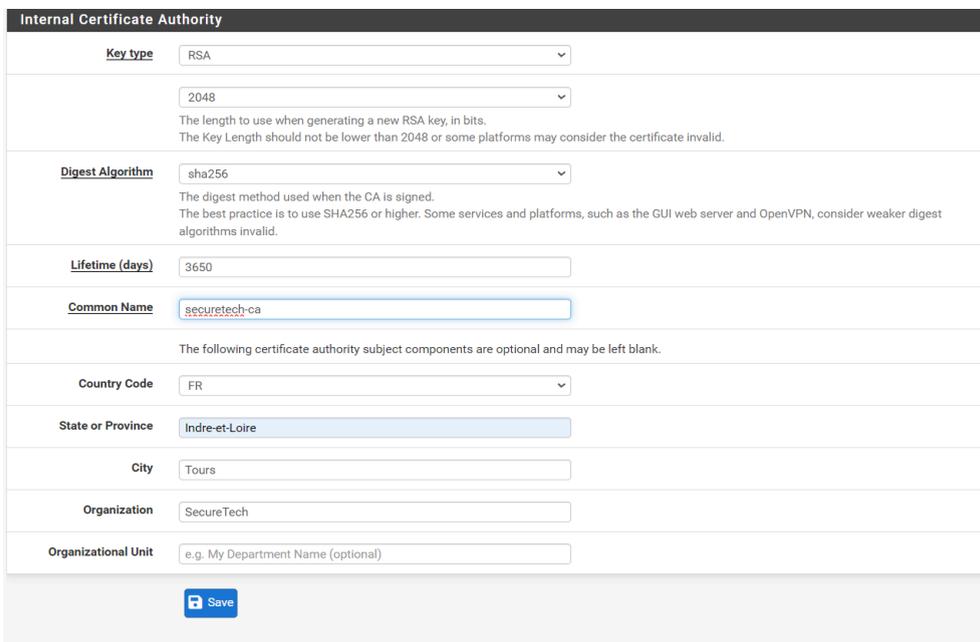
Nous aurons donc une interface WAN (192.168.X.0/30) et LAN (10.X.X.1/27) sur chacun de nos PfSense, le but final sera donc que nos clients puissent communiquer entre eux via ce tunnel.

2. Reprise du meme certificat

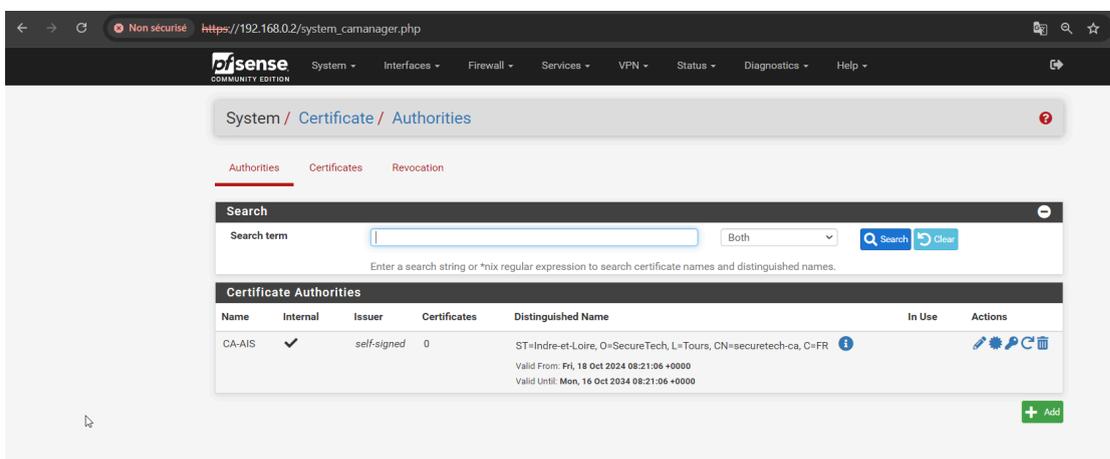
Pour créer l'autorité de certification sur PFSENSE, vous devez accéder au menu : System > Authorities > Edit

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.



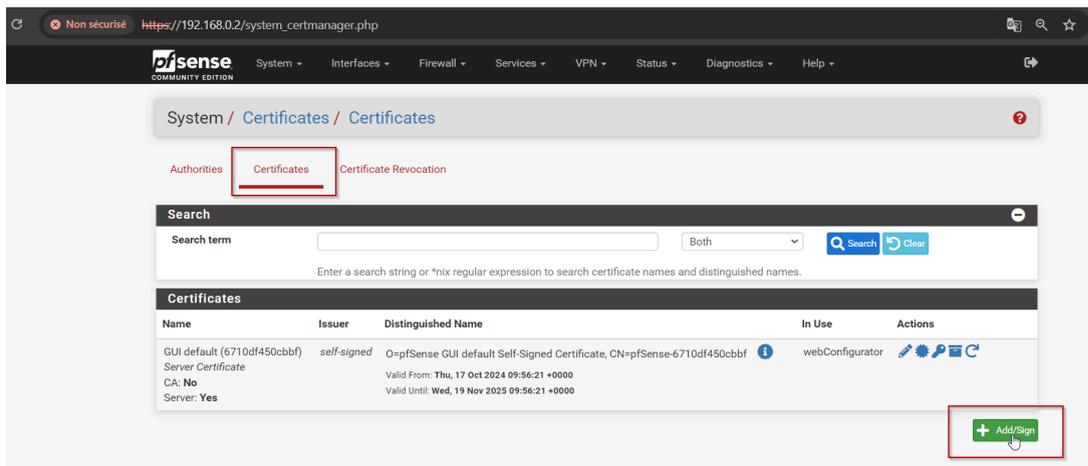
L'autorité de certification doit apparaître dans l'interface, comme ceci :



Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
CA-AIS	✓	self-signed	0	ST=Indre-et-Loire, O=SecureTech, L=Tours, CN=securetech-ca, C=FR		   

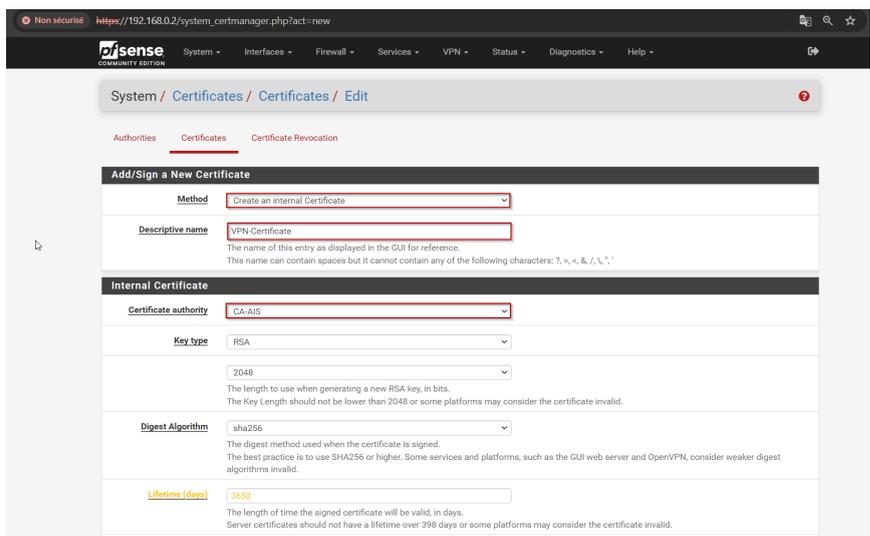
3. Créer le certificat Server

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.



Common Name

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

Certificate Attributes

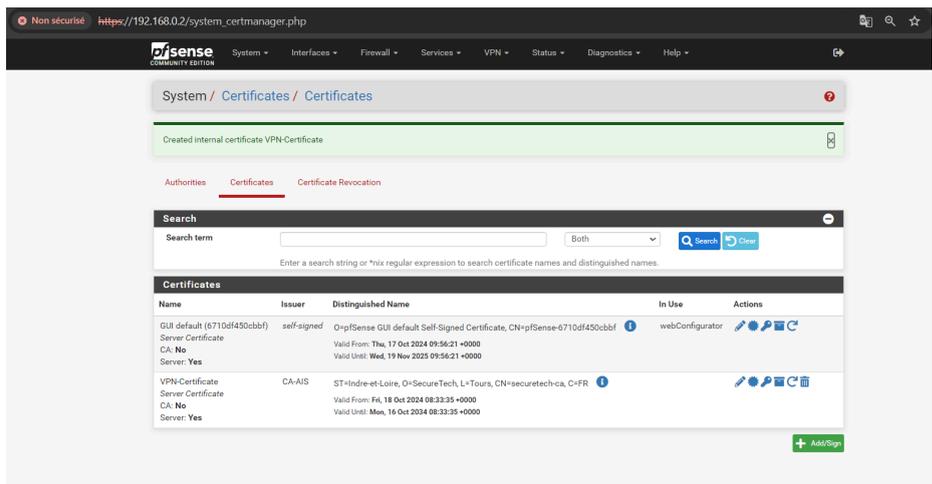
Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.
For Internal Certificates, these attributes are added directly to the certificate as shown.

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

Alternative Names
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 SAN Row

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

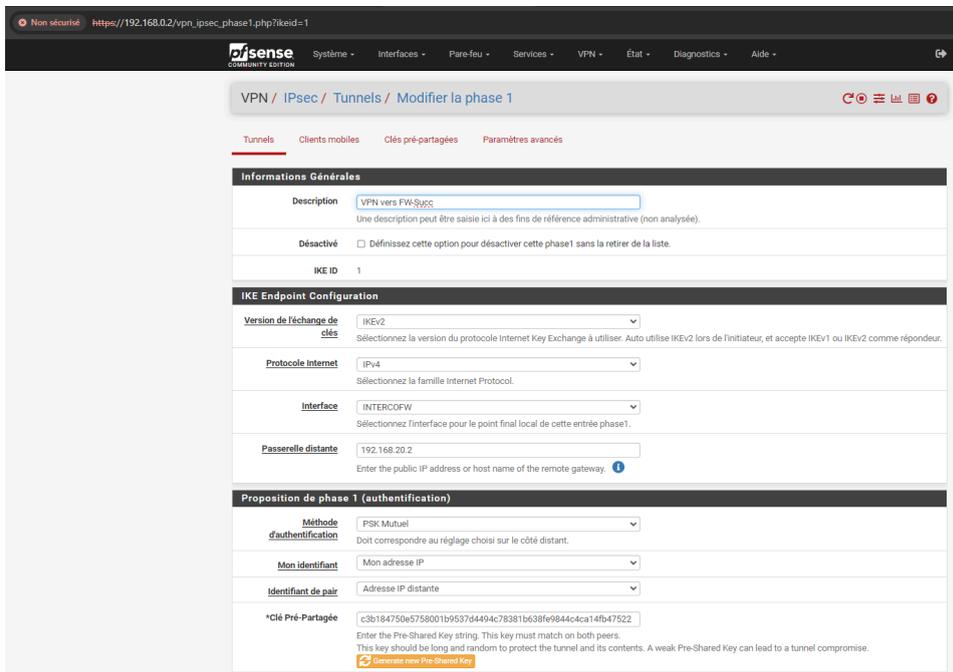


CONFIGURATION PFSENSE GUI IPSEC PARTIE : SIÈGE

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" :



VPN / IPsec / Tunnels / Modifier la phase 1

Tunnels Clients mobiles Clés pré-partagées Paramètres avancés

Informations Générales

Description: VPN vers FW-Succ
 Une description peut être saisie ici à des fins de référence administrative (non analysée).

Désactivé: Définissez cette option pour désactiver cette phase1 sans la retirer de la liste.

IKE ID: 1

IKE Endpoint Configuration

Version de l'échange de clés: IKEV2
 Sélectionnez la version du protocole Internet Key Exchange à utiliser. Auto utilise IKEV2 lors de l'initiateur, et accepte IKEV1 ou IKEV2 comme répondeur.

Protocole Internet: IPv4
 Sélectionnez la famille Internet Protocol.

Interface: INTERCOFW
 Sélectionnez l'interface pour le point final local de cette entrée phase1.

Passerelle distante: 192.168.20.2
 Enter the public IP address or host name of the remote gateway.

Proposition de phase 1 (authentification)

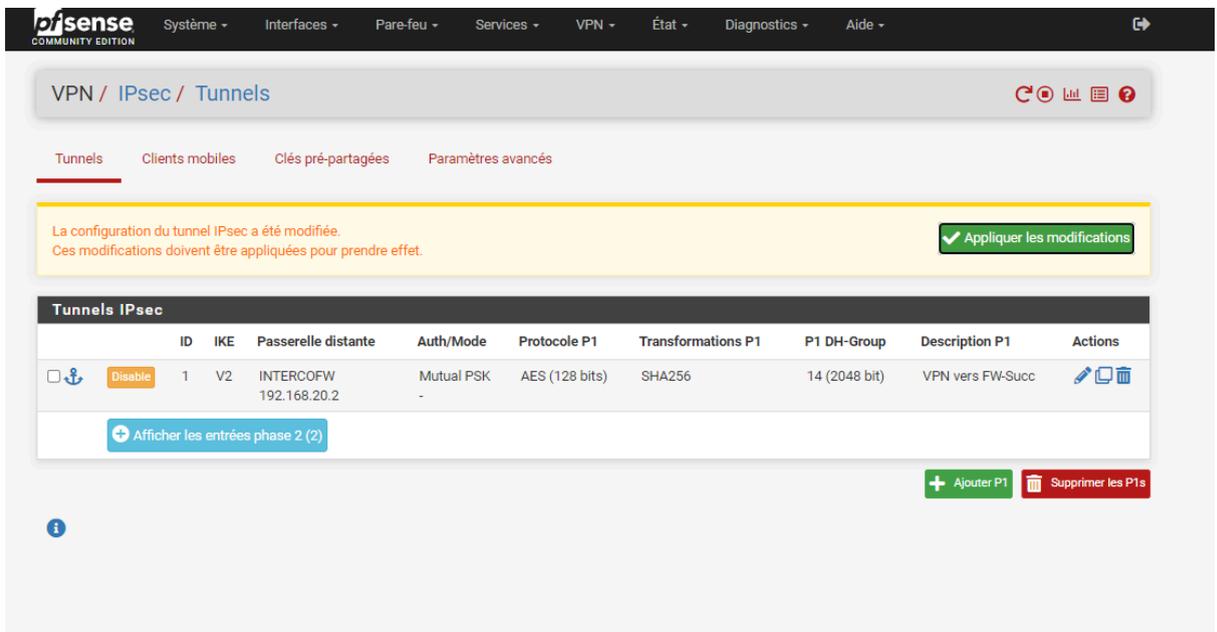
Méthode d'authentification: PSK Mutuel
 Doit correspondre au réglage choisi sur le côté distant.

Mon identifiant: Mon adresse IP

Identifiant de pair: Adresse IP distante

*Clé Pré-Partagée: c3b184750e5758001b9537d4494c78381b638fe9844c4ca14fb47522
 Enter the Pre-Shared Key string. This key must match on both peers. This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.

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 :



VPN / IPsec / Tunnels

Tunnels Clients mobiles Clés pré-partagées Paramètres avancés

La configuration du tunnel IPsec a été modifiée. Ces modifications doivent être appliquées pour prendre effet. [Appliquer les modifications](#)

Tunnels IPsec

ID	IKE	Passerelle distante	Auth/Mode	Protocole P1	Transformations P1	P1 DH-Group	Description P1	Actions
1	V2	INTERCOFW 192.168.20.2	Mutual PSK	AES (128 bits)	SHA256	14 (2048 bit)	VPN vers FW-Succ	+ - 🗑️

[+ Afficher les entrées phase 2 \(2\)](#)

[+ Ajouter P1](#) [Supprimer les P1s](#)

Voici les configurations des phases 2 de SIEGE :



NetAdmin

[AIS2024] Document de configuration des équipements

Version : A

VPN / IPsec / Tunnels

La configuration du tunnel IPsec a été modifiée.
Ces modifications doivent être appliquées pour prendre effet.

ID	IKE	Passerelle distante	Auth/Mode	Protocole P1	Transformations P1	P1 DH-Group	Description P1	Actions
1	V2	INTERCOFW 192.168.20.2	Mutual PSK	AES (128 bits)	SHA256	14 (2048 bit)	VPN vers FW-Succ	

ID	Mode	Sous-réseau local	Sous-réseau distant	Protocole P2	Transformations P2	Méthodes d'authentification P2	Description	Actions
1	tunnel	VLANT0SERVEURS	10.1.100.0/27	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256	vers VLAN 100 Succ	
2	tunnel	VLANT0SERVEURS	10.1.200.0/27	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256	vers VLAN 200	

+ Ajouter P2

+ Ajouter P1 | Supprimer les P1s

Partie Succursale

VPN / IPsec / Tunnels

ID	IKE	Passerelle distante	Auth/Mode	Protocole P1	Transformations P1	P1 DH-Group	Description P1	Actions
1	V2	INTERCOFW 192.168.10.2	Mutual PSK	AES (128 bits)	SHA256	14 (2048 bit)	VPN vers Siège	

ID	Mode	Sous-réseau local	Sous-réseau distant	Protocole P2	Transformations P2	Méthodes d'authentification P2	Description	Actions
1	tunnel	VLAN100	10.0.10.0/28	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256	vers VLAN 10 Siege	
2	tunnel	VLAN200	10.0.10.0/28	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256	vers VLAN 10 Siege	

+ Ajouter P2

+ Ajouter P1 | Supprimer les P1s

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

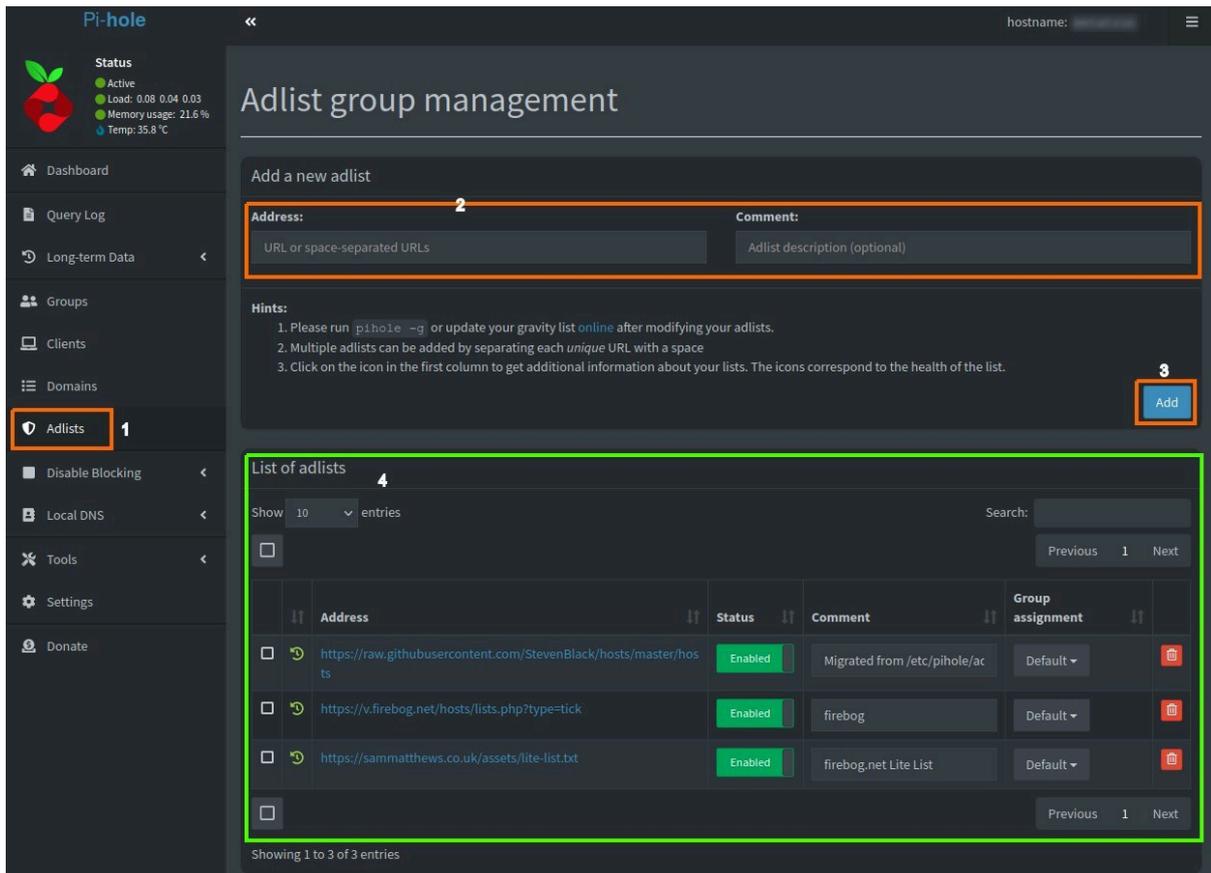
Pi-hole

Installation

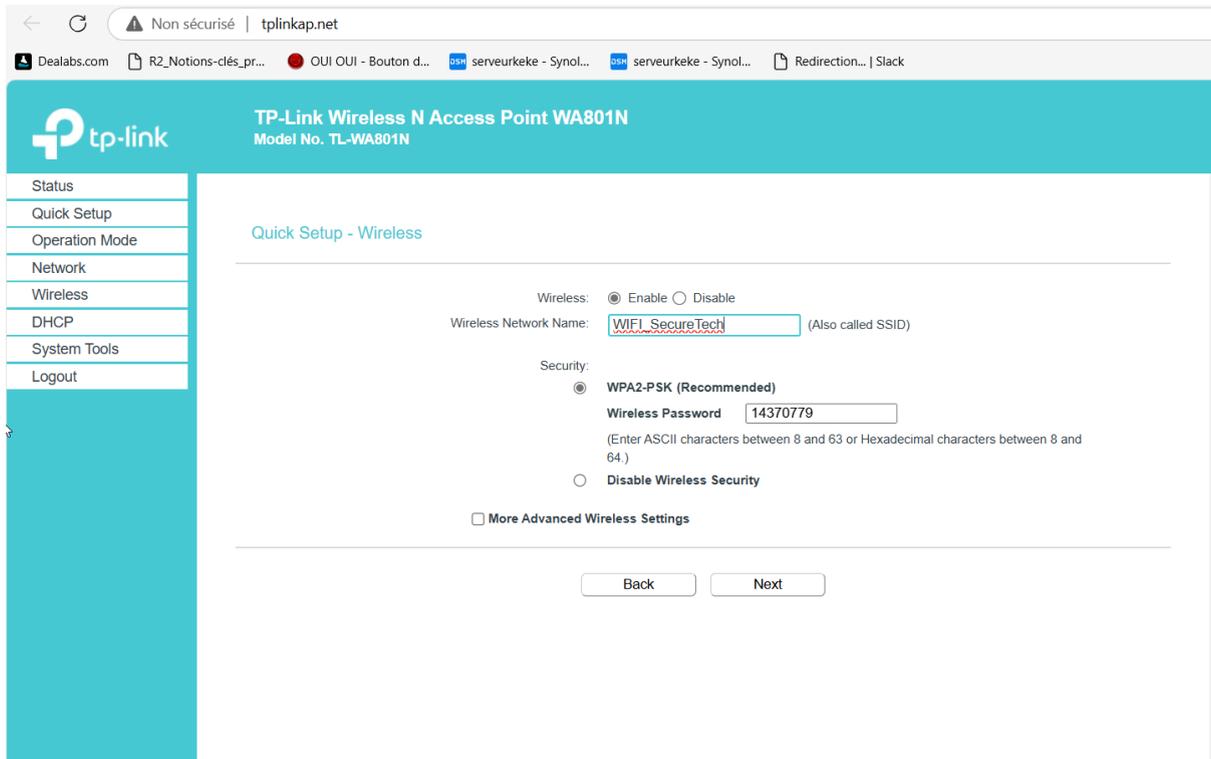
```
# curl -sSL https://install.pi-hole.net | bash
```

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



Non sécurisé | tplinkap.net

Dealabs.com R2_Notions-clés_pr... OUI OUI - Bouton d... serveurkeke - Synol... serveurkeke - Synol... Redirection... | Slack

tp-link TP-Link Wireless N Access Point WA801N
Model No. TL-WA801N

Status
Quick Setup
Operation Mode
Network
Wireless
DHCP
System Tools
Logout

Quick Setup - Wireless

Wireless: Enable Disable

Wireless Network Name: (Also called SSID)

Security:

WPA2-PSK (Recommended)

Wireless Password:
(Enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Disable Wireless Security

More Advanced Wireless Settings

Back Next

LAN Type:

Note: The IP parameters cannot be configured if you have chosen Smart IP.

(In this situation the device will help you configure the IP parameters automatically you need).

IP Address:

Subnet Mask:

We recommend you configure this AP with the same IP subnet and subnet mask and a different IP address from your root AP/Router.

DHCP Server: Enable Disable

Back

Next

	NetAdmin	Version : A
	[AIS2024] Document de configuration des équipements	

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 -xzf cs-nginx-bouncer.tgz
```

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

	NetAdmin	Version : A
	[AIS2024]_Plan_de_sécurité_du_réseau	

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.....	2
Stratégie d'authentications (RADIUS SUR WIFI).....	3
Règles de pare-feu.....	3
pi-Hole.....	3
Suricata.....	5
Recommandation ANSSI.....	5

	NetAdmin	Version : A
	[AIS2024]_Plan_de_sécurité_du_réseau	

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 sépareit.

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.

 cefim L'école du web et des réseaux	NetAdmin	Version : A
	[AIS2024]_Plan_de_sécurité_du_réseau	

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'authentications (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

- [DNS Records](#)
- [CNAME Records](#)
- [Tools](#)
- [Settings](#)
- [Donate](#)

List of local DNS domains

Show entries

Domain	IP
crowdsec.securetech.local	192.168.0.13
dc01.securetech.local	10.0.10.5
dc02.securetech.local	10.0.10.6
fw-admin.home.arpa	192.168.0.1
fw-siege.home.arpa	192.168.0.2
fw-succursale.home.arpa	192.168.0.3
suricata.securetech.local	192.168.0.4
zabbix.securetech.local	192.168.0.11

Blocage des noms de domaines des sites suivants :

youtube.fr
 pornhub.com

List of domains

 Exact whitelist
 Regex whitelist
 Exact blacklist
 Regex blacklist

Show entries Search:

Previous
1
Next

<input type="checkbox"/>	Domain/RegEx	Type	Status	Comment	Group assignment	<input type="checkbox"/>
<input type="checkbox"/>	securetech.local	Exact whitelist	Enabled	Domaine local	Default	<input type="checkbox"/>
<input type="checkbox"/>	youtube.fr	Exact blacklist	Enabled	Bloque Test Youtube.fr	Default	<input type="checkbox"/>
<input type="checkbox"/>	(\. ^).pornhub\.com\$	Regex blacklist	Enabled		Default	<input type="checkbox"/>

Previous
1
Next

Showing 1 to 3 of 3 entries

	NetAdmin	Version : A
	[AIS2024]_Plan_de_sécurité_du_réseau	

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.

Authentification des utilisateurs :

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) ;

	NetAdmin	Version : A
	[AIS2024]_Plan_de_sécurité_du_réseau	

- 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 ont 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 personnelles ou données sensibles ;
- Les réglementations 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.

Rédacteur : Département DSI	Date de MAJ : 16 oct. 2024	Page 6 sur 6
-----------------------------	----------------------------	--------------

	NetAdmin	Version : A
	[AIS2024]_Rapport_Monitoring_et_Performance	

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** : Démonstre une compréhension approfondie de l'état actuel du réseau et souligne les domaines nécessitant une attention particulière.

Supervision par Zabbix.....	2
Installation d'agents Zabbix.....	2
Pi-Hole.....	4
CrowdSec.....	5

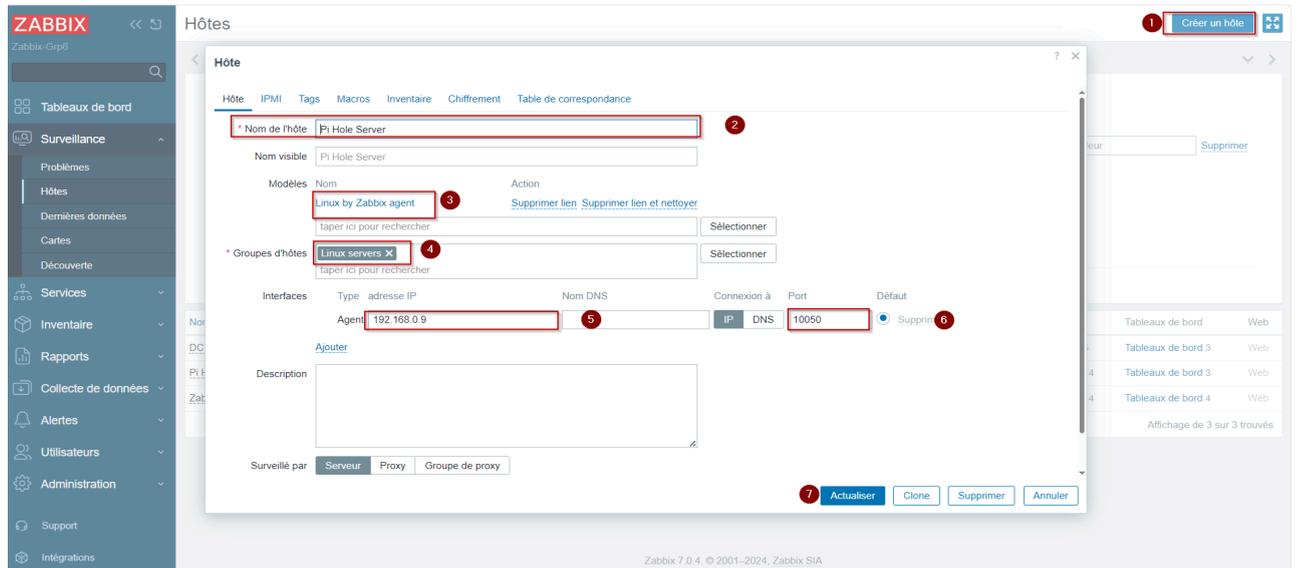
Supervision par Zabbix

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

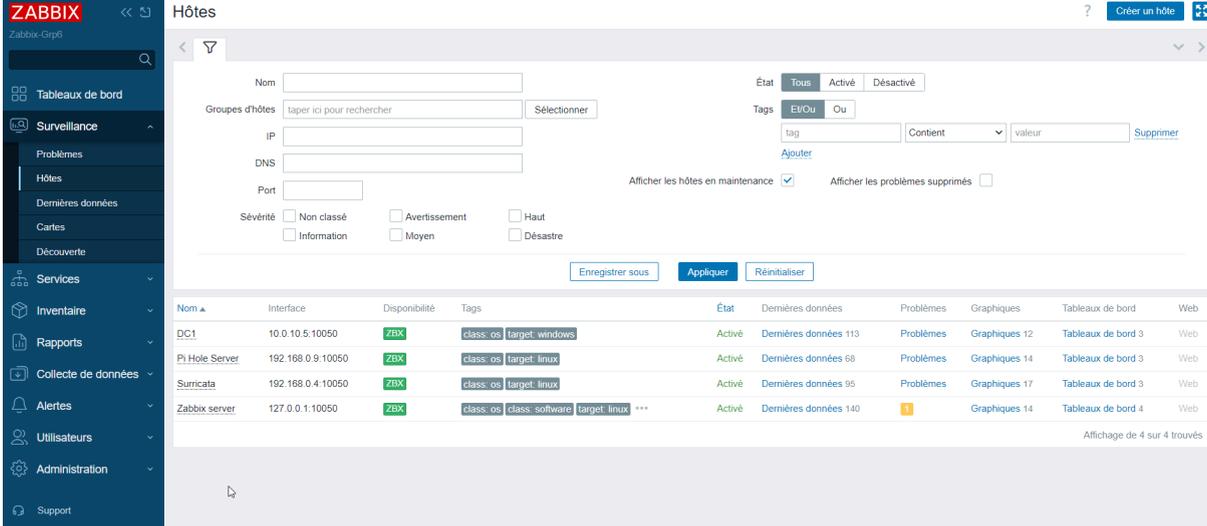
Installation d'agents Zabbix

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

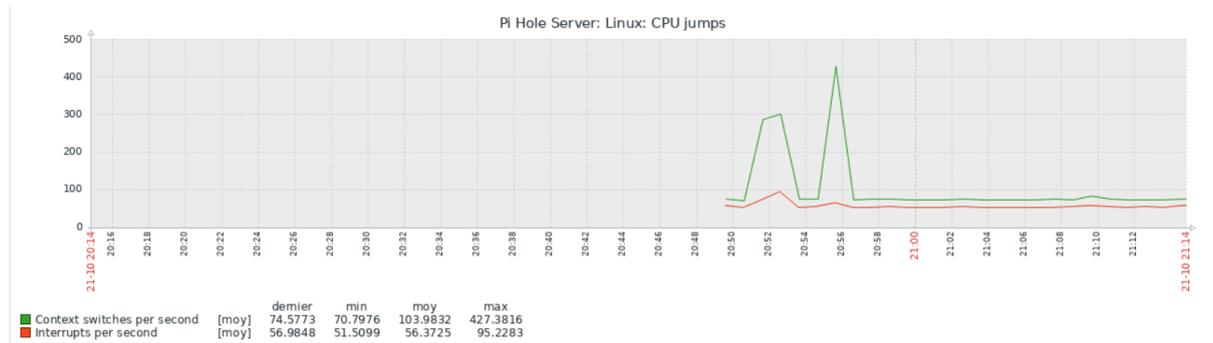


The screenshot shows the Zabbix web interface. On the left is a navigation menu with options like 'Tableaux de bord', 'Surveillance', 'Problèmes', 'Hôtes', 'Dernières données', 'Cartes', 'Découverte', 'Services', 'Inventaire', 'Rapports', 'Collecte de données', 'Alertes', 'Utilisateurs', 'Administration', and 'Support'. The main area is titled 'Hôtes' and contains a form for adding a new host with fields for Name, Groups, IP, DNS, Port, and Severity. Below the form is a table of existing hosts:

Nom	Interface	Disponibilité	Tags	État	Dernières données	Problèmes	Graphiques	Tableaux de bord	Web
DC1	10.0.10.5:10050	ZBX	class:os target:windows	Activé	Dernières données 113	Problèmes	Graphiques 12	Tableaux de bord 3	Web
Pi Hole Server	192.168.0.9:10050	ZBX	class:os target:linux	Activé	Dernières données 68	Problèmes	Graphiques 14	Tableaux de bord 3	Web
Surricata	192.168.0.4:10050	ZBX	class:os target:linux	Activé	Dernières données 95	Problèmes	Graphiques 17	Tableaux de bord 3	Web
Zabbix server	127.0.0.1:10050	ZBX	class:os class:software target:linux ***	Activé	Dernières données 140		Graphiques 14	Tableaux de bord 4	Web

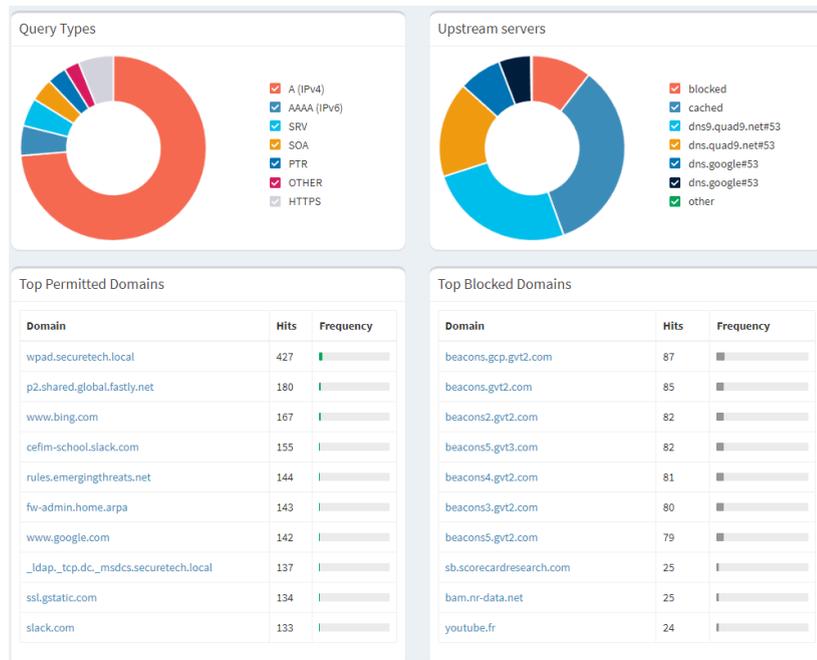
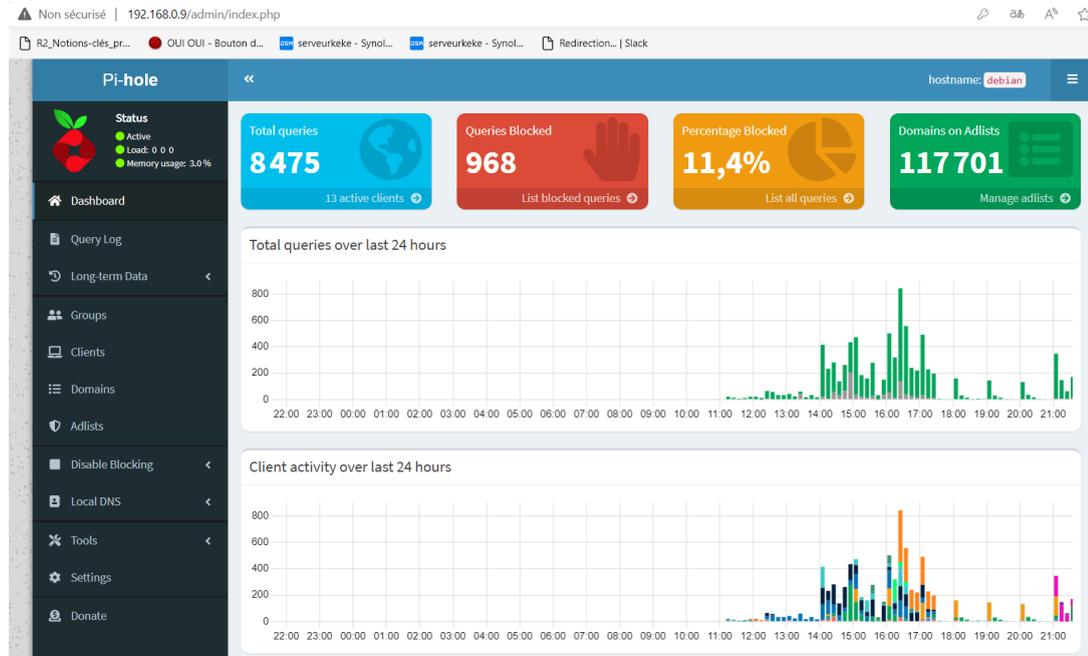
Lien installation zabbix agent Windows : [Download Zabbix agents](#)

capture d'écran activité Zabbix



Pi-Hole

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





CrowdSec

192.168.0.13:3000/dashboard/34-cs-alerts-history

Dealabs.com | Synology DiskStation | Redirection... | Slack | Autres

Rechercher... + Nouveau

CS - Alerts History

Aa Machine

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	Exploration ne fonctionne pas sur les questions SQL.			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

	NetAdmin	Version : A
	[AIS2024]_Document_de_Test	

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.....	2
Connection VPN Client to Site.....	2
Connection VPN Site to Site :.....	2
Remonté Pi-hole DNSBL.....	4
Pi-Hole - Nom de domaines.....	6
Crowdsec.....	7

Switch connection en SSH

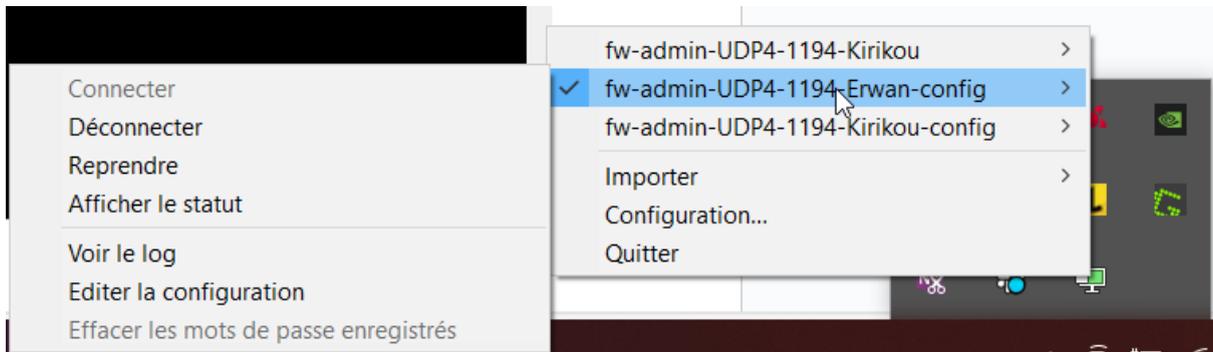
```

192.168.1.5 - PuTTY
login as: admin
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server

S1>
S1>
S1>
S1>
S1>
S1>show ip domain-name
grp6.local
S1>

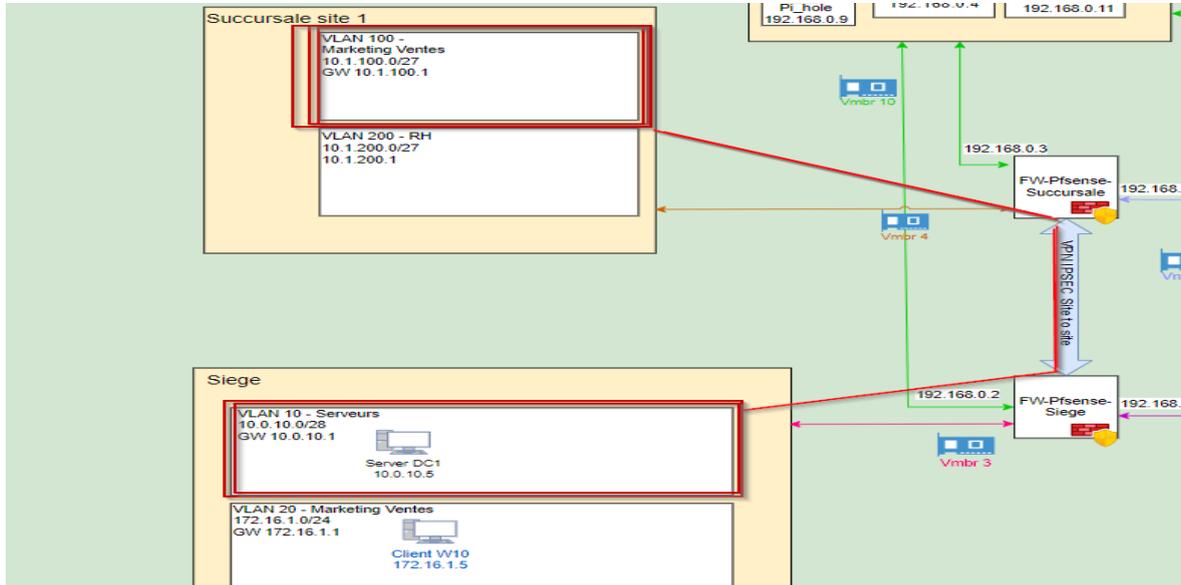
```

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 :



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=>

```

C:\Users\admin>ping 10.1.100.1 -t

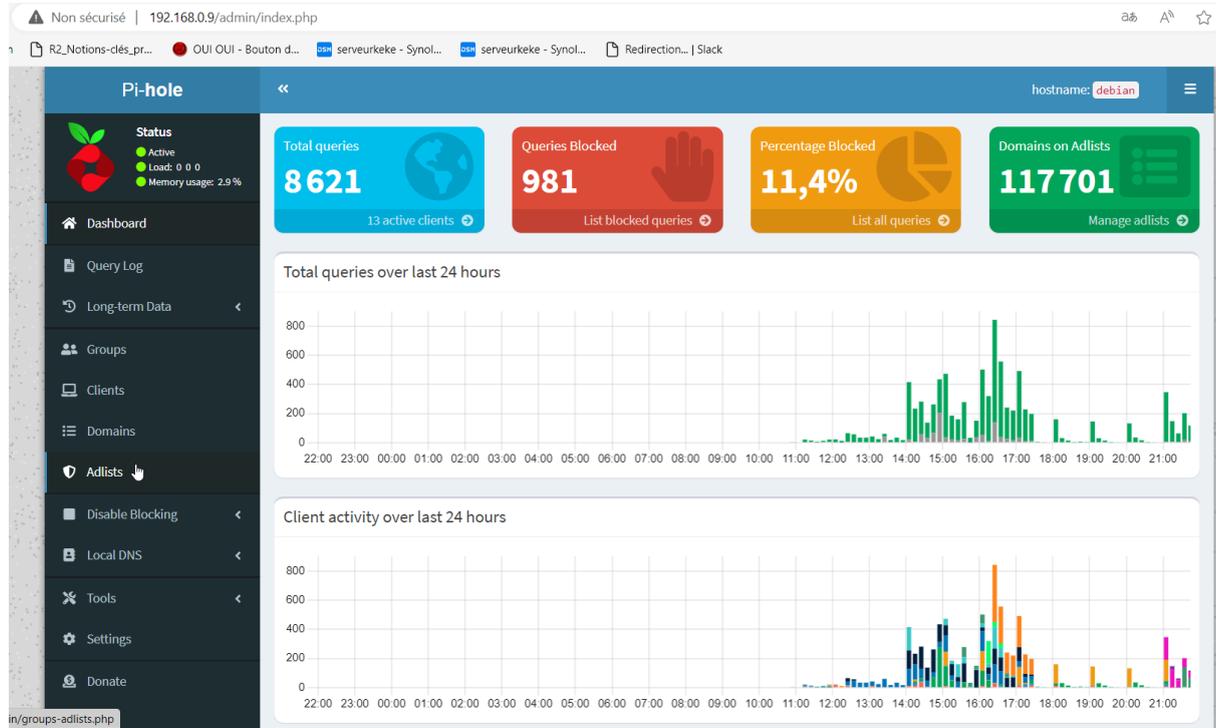
Statistiques Ping pour 10.1.100.1:
    Paquets : envoyés = 24, reçus = 0, perdus = 24 (perte 100%),
Ctrl+C
^C
C:\Users\admin>ping 10.1.100.1 -t

Envoi d'une requête 'Ping' 10.1.100.1 avec 32 octets de données :
Délai d'attente de la demande dépassé.

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
  
```

Remonté Pi-hole DNSBL

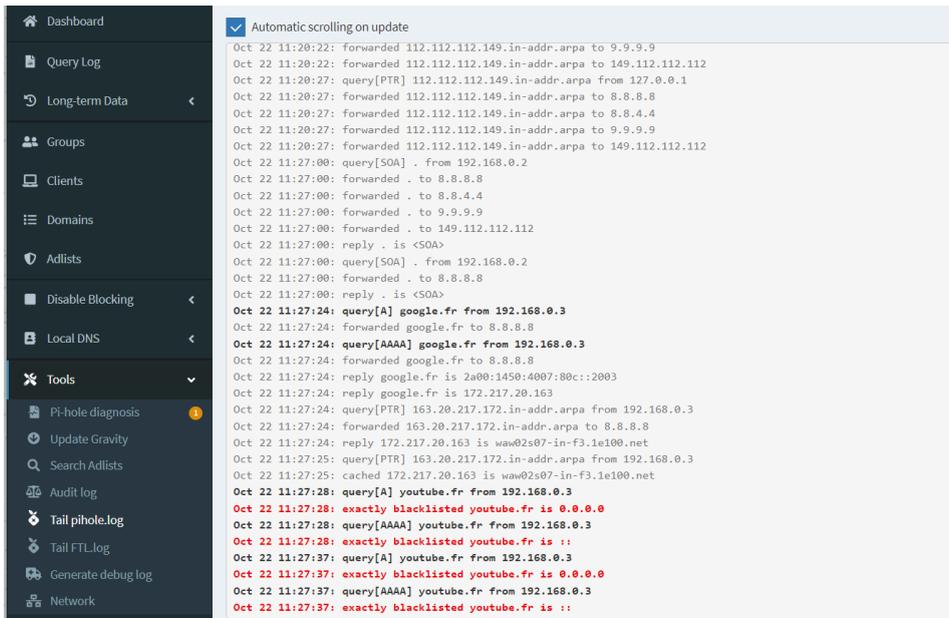


Pour tester nous avons Blacklister le nom de domaine "youtube.fr" et voici le résultat :
 Depuis le serveur Zabbix :

```

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 :



The screenshot shows the Pi-hole dashboard interface. On the left is a navigation menu with options like Dashboard, Query Log, Long-term Data, Groups, Clients, Domains, Adlists, Disable Blocking, Local DNS, Tools, Pi-hole diagnosis, Update Gravity, Search Adlists, Audit log, Tail pihole.log, Tail FTL.log, Generate debug log, and Network. The main area displays a log of DNS queries. Several entries are highlighted in red, indicating they are blocked. Key entries include:

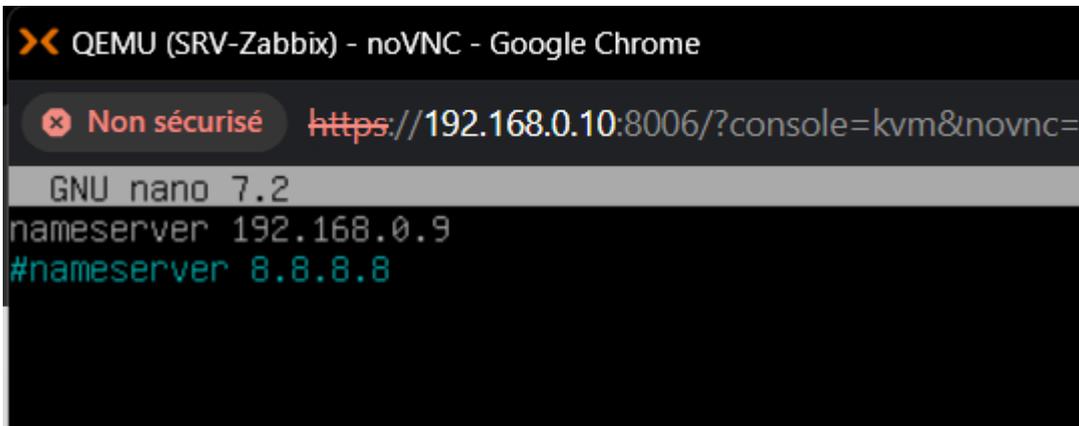
- Oct 22 11:27:24: query[A] google.fr from 192.168.0.3
- Oct 22 11:27:24: query[AAAA] google.fr from 192.168.0.3
- Oct 22 11:27:28: query[A] youtube.fr from 192.168.0.3
- Oct 22 11:27:28: exactly blacklisted youtube.fr is 0.0.0.0
- Oct 22 11:27:28: query[AAAA] youtube.fr from 192.168.0.3
- Oct 22 11:27:28: exactly blacklisted youtube.fr is ::
- Oct 22 11:27:37: query[A] youtube.fr from 192.168.0.3
- Oct 22 11:27:37: exactly blacklisted youtube.fr is 0.0.0.0
- Oct 22 11:27:37: query[AAAA] youtube.fr from 192.168.0.3
- Oct 22 11:27:37: exactly blacklisted youtube.fr is ::

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

Paramètres du serveur DNS

Serveurs DNS	192.168.0.9	DNS Hostname	aucun	Supprimer
	8.8.8.8	DNS Hostname	aucun	Supprimer
Adresse	Nom d'hôte		Passerelle	
Saisir les adresses IP des serveurs DNS utilisés par le système. Ceux-ci sont également utilisés pour le service DHCP, le DNS Forwarder et le serveur de résolution DNS lorsqu'il est activé.	Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).		Choisir la passerelle pour chaque serveur DNS (facultatif) Lorsque vous utilisez plusieurs connexions WAN, il doit y avoir au moins un serveur DNS unique par passerelle.	

Sur les serveurs OS LINUX :

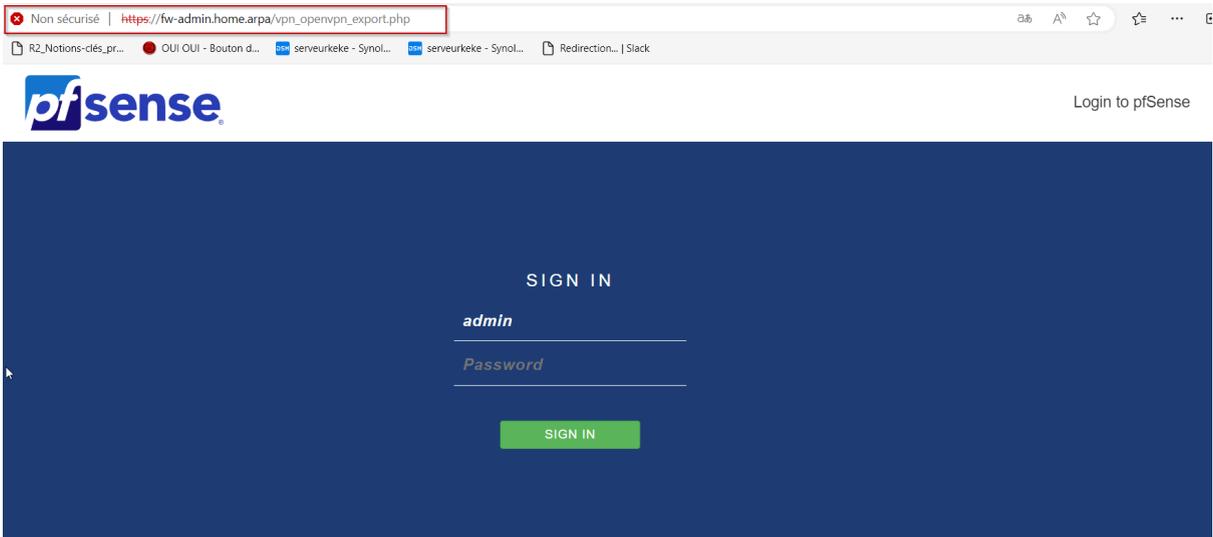


```

QEMU (SRV-Zabbix) - noVNC - Google Chrome
Non sécurisé https://192.168.0.10:8006/?console=kvm&novnc=
GNU nano 7.2
nameserver 192.168.0.9
#nameserver 8.8.8.8
  
```

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

