



Mise en place d'un VPN
site à site





Sommaire :

- I. Présentation du VPN site à site
- II. Objectif du projet
- III. Mise en place du VPN site à site avec pfSense
- IV. Tests de connectivité et vérifications
- V. Compétences mises en œuvre
- VI. Problèmes rencontrés et solutions



I. Présentation du VPN site à site :

Le VPN (Virtual Private Network) site à site est une technologie permettant d'interconnecter de manière sécurisée deux réseaux locaux (LAN) géographiquement séparés, en utilisant une infrastructure réseau publique comme Internet.

Contrairement à un VPN d'accès distant, qui connecte un utilisateur à un réseau d'entreprise, le VPN site à site relie directement deux sites entiers.

Cette solution est couramment utilisée par les entreprises possédant plusieurs agences ou filiales. Elle permet un échange sécurisé des données comme si les machines distantes appartenaient au même réseau local, tout en évitant les frais liés à l'installation d'un réseau privé physique.

Le VPN site à site repose sur des protocoles de tunneling et de chiffrement, tels qu'IPsec, afin de garantir la confidentialité, l'intégrité et l'authenticité des données échangées entre les sites. Il est généralement mis en œuvre à l'aide de pare-feux ou de routeurs compatibles, comme **pfSense**, qui sera utilisé dans ce projet.



II. Objectif du projet :

Le but de ce projet est de connecter deux sites distants entre eux en utilisant un VPN site à site. Pour cela, j'utiliserai pfSense sur chaque site, qui servira à établir et gérer le tunnel VPN.

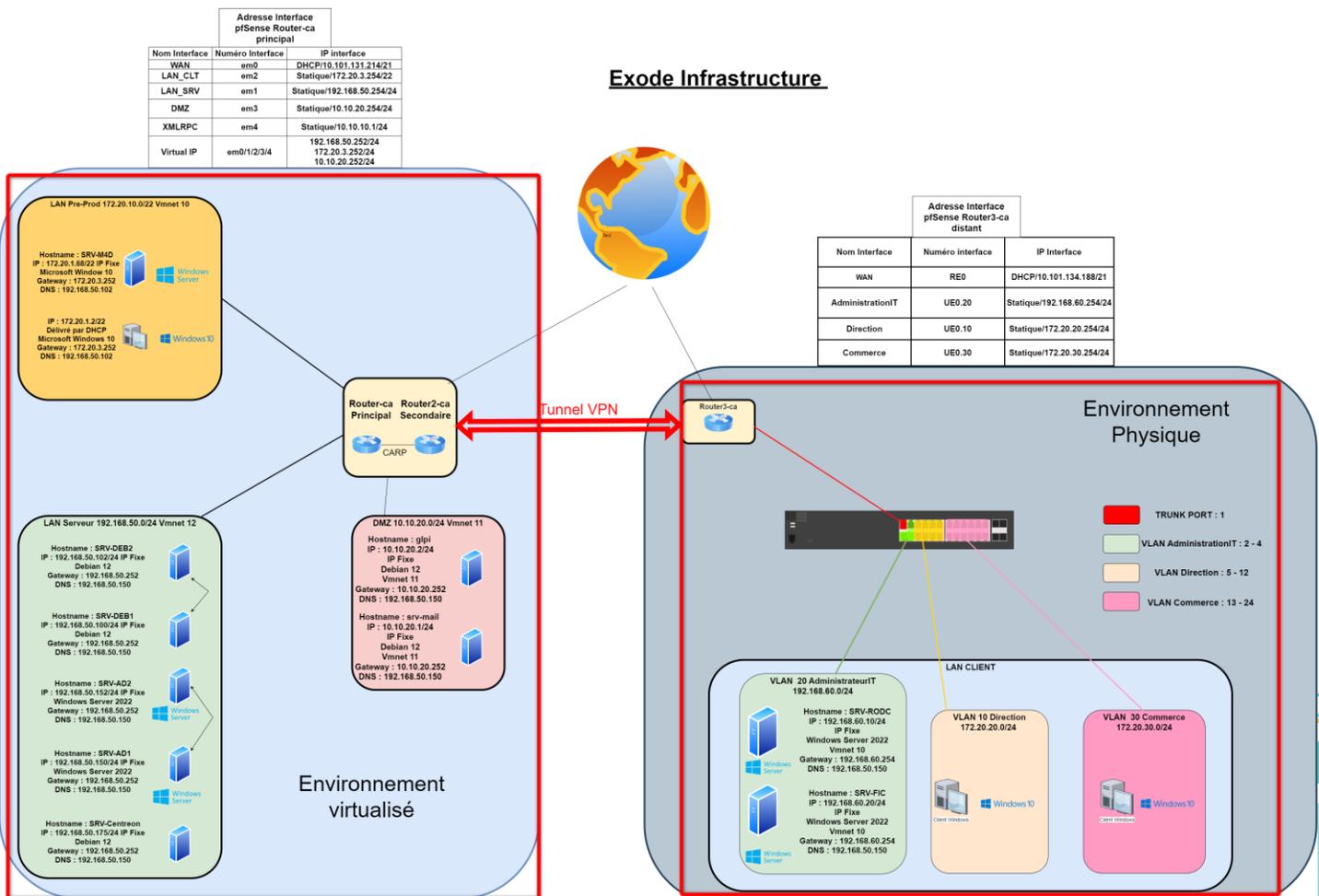
Un VPN (Virtual Private Network) est une technologie qui permet de créer une connexion sécurisée à travers un réseau non sécurisé, comme Internet. Il garantit la confidentialité et la sécurité des échanges de données entre deux points.

Dans ce projet, le protocole utilisé sera IPsec (Internet Protocol Security). IPsec est un protocole de sécurité conçu pour chiffrer et authentifier les paquets IP. Il est particulièrement adapté aux connexions VPN site à site, car il est stable, sécurisé, et largement compatible avec les équipements réseau professionnels comme pfSense. IPsec est plus adapté qu'un protocole comme OpenVPN pour ce type d'architecture, car il est directement pris en charge au niveau du système et des équipements réseau, ce qui en fait un choix privilégié dans les infrastructures professionnelles pour interconnecter plusieurs sites de façon permanente et fiable.

Grâce à cette configuration, les deux sites pourront communiquer comme s'ils faisaient partie d'un même réseau local, tout en passant par une connexion chiffrée sur Internet.

III. Mise en place du VPN site à site avec pfSense :

Comme vu précédemment IPsec est utilisé lors d'une interconnexion entre deux sites distants. Dans mon cas et suivant ce schéma réseau, IPsec répond donc parfaitement à mon besoin de VPN site à site.

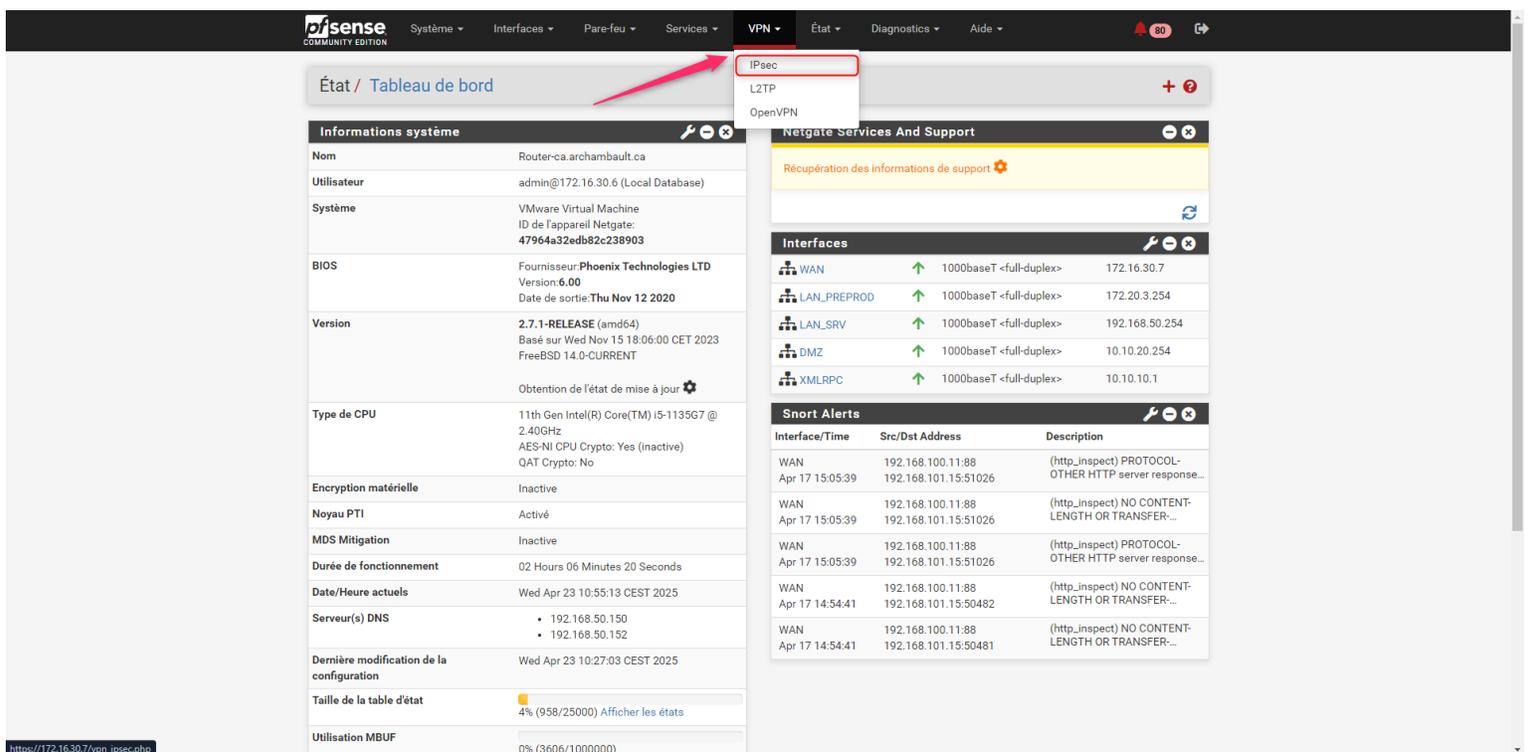


Dans cette configuration, il faut commencer par la configuration de VPN IPsec sur le site principal, en bleu clair.

1- Configuration du VPN IPsec sur le site principal :

Dans un premier temps, connectez vous sur l'interface pfSense du site principal.

Il faut ensuite aller dans l'onglet VPN > IPsec



The screenshot shows the pfSense web interface. The top navigation bar includes 'Système', 'Interfaces', 'Pare-feu', 'Services', 'VPN', 'État', 'Diagnostics', and 'Aide'. The 'VPN' menu is expanded, showing 'IPsec', 'L2TP', and 'OpenVPN'. A red arrow points to the 'IPsec' option. The main content area is divided into two panels: 'Informations système' on the left and 'Netgate Services And Support' on the right. The 'Informations système' panel displays system details such as 'Router-ca.archambault.ca', 'admin@172.16.30.6', and hardware information. The 'Netgate Services And Support' panel shows a 'Récupération des informations de support' button and a table of 'Interfaces' with columns for name, status, speed, and IP address. Below the interfaces is a 'Snort Alerts' table with columns for interface, time, source/destination address, and description.

Interface	Time	Src/Dst Address	Description
WAN	Apr 17 15:05:39	192.168.100.11:88 192.168.101.15:51026	(http_inspect) PROTOCOL-OTHER HTTP server response...
WAN	Apr 17 15:05:39	192.168.100.11:88 192.168.101.15:51026	(http_inspect) NO CONTENT-LENGTH OR TRANSFER...
WAN	Apr 17 15:05:39	192.168.100.11:88 192.168.101.15:51026	(http_inspect) PROTOCOL-OTHER HTTP server response...
WAN	Apr 17 14:54:41	192.168.100.11:88 192.168.101.15:50482	(http_inspect) NO CONTENT-LENGTH OR TRANSFER...
WAN	Apr 17 14:54:41	192.168.100.11:88 192.168.101.15:50481	(http_inspect) NO CONTENT-LENGTH OR TRANSFER...

Une fois dans la section de configuration IPsec de pfSense, la première étape consiste à configurer la Phase 1. Cette phase permet d'établir une connexion sécurisée initiale entre les deux sites, en s'appuyant sur le protocole IKE (Internet Key Exchange). IKE est utilisé pour négocier et établir une association de sécurité (Security Association - SA) entre les deux pare-feux pfSense.

Voici les paramètres importants à définir dans la phase 1 :

- Key Exchange version : IKEv2 (recommandé pour sa robustesse et sa compatibilité)
- Remote Gateway : Adresse IP publique du site distant
- Authentication Method : Pre-Shared Key (clé partagée, plus simple pour un environnement de test)
- My identifier / Peer identifier : Généralement configuré avec les adresses IP ou FQDN
- Encryption Algorithm : AES (256 bits recommandé)
- Hash Algorithm : SHA256
- DH Group : 14 ou 19 (selon le niveau de sécurité souhaité)
- Lifetime : 28800 secondes (valeur par défaut généralement conservée)

Informations Générales					
Description	Tunnel VPN Site à Site <small>Une description peut être saisie ici à des fins de référence administrative (non analysée).</small>				
Désactivé	<input type="checkbox"/> 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 <small>Sélectionnez la version du protocole Internet Key Exchange à utiliser. Auto utilise IKEv2 lors de l'initiateur, et accepte IKEv1 ou IKEv2 comme répondeur.</small>				
Protocole Internet	IPv4 <small>Sélectionnez la famille Internet Protocol.</small>				
Interface	WAN <small>Sélectionnez l'interface pour le point final local de cette entrée phase1.</small>				
Passerelle distante	172.16.30.4 <small>Enter the public IP address or host name of the remote gateway.</small>				
Proposition de phase 1 (authentification)					
Méthode d'authentification	PSK Mutuel <small>Doit correspondre au réglage choisi sur le côté distant.</small>				
Mon identifiant	Mon adresse IP				
Identifiant de pair	Adresse IP distante				
*Clé Pré-Partagée	2490e995897d1a09168c0e4897257b40c36ef4f62b5e5ebab63b9e99 <small>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.</small> Generate new Pre-Shared Key				
Phase 1 Proposal (Encryption Algorithm)					
Algorithme de chiffrement	AES Longueur de la clé	256 bits	SHA256 Hash	14 (2048 bit) DH Group	Supprimer

Expiration and Replacement	
Life Time	28800 <small>Hard IKE SA life time, in seconds, after which the IKE SA will be expired. Must be larger than Rekey Time and Reauth Time. Cannot be set to the same value as Rekey Time or Reauth Time. If left empty, defaults to 110% of whichever timer is higher (reauth or rekey)</small>
Rekey Time	25920 <small>Time, in seconds, before an IKE SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Only supported by IKEV2, and is recommended for use with IKEV2. Leave blank to use a default value of 90% Life Time when using IKEV2. Enter a value of 0 to disable.</small>
Reauth Time	0 <small>Time, in seconds, before an IKE SA is torn down and recreated from scratch, including authentication. This can be disruptive unless both sides support make-before-break and overlapping IKE SA entries. Cannot be set to the same value as Life Time. Supported by IKEv1 and IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv1. Enter a value of 0 to disable.</small>
Rand Time	2880 <small>A random value up to this amount will be subtracted from Rekey Time/Reauth Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.</small>
Options Avancées	
Child SA Start Action	Par défaut <small>Set this option to force specific initiation/responder behavior for child SA (P2) entries</small>
Child SA Close Action	Par défaut <small>Set this option to control the behavior when the remote peer unexpectedly closes a child SA (P2)</small>
NAT Traversal	Auto <small>Définissez cette option pour permettre l'utilisation de NAT-T (c'est-à-dire l'encapsulation d'ESP dans les paquets UDP) si nécessaire, ce qui peut aider les clients derrière des pare-feu restrictifs.</small>
MOBIKE	Désactiver <small>Définissez cette option pour contrôler l'utilisation de MOBIKE</small>
Gateway duplicates	<input type="checkbox"/> Enable this to allow multiple phase 1 configurations with the same endpoint. When enabled, pfSense does not manage routing to the remote gateway and traffic will follow the default route without regard for the chosen interface. Static routes can override this behavior.
Connexions partagées	<input type="checkbox"/> Activez ceci pour fractionner les entrées de connexion avec plusieurs configurations de phase 2. Obligatoire pour les points distants qui ne prennent en charge qu'un seul sélecteur de trafic par enfant SA.
PRF Selection	<input type="checkbox"/> Enable manual Pseudo-Random Function (PRF) selection

Une fois tous les champs correctement remplis, il suffit d'enregistrer la phase 1, puis de passer à la configuration de la phase 2, qui permettra de définir les réseaux autorisés à communiquer à travers le tunnel.

Toujours dans VPN > IPsec, cliquez sur Show Phase 2 Entries sous la configuration de la phase 1.

Cliquez sur Add P2.

Et remplir les informations suivantes :

- Mode : Tunnel IPv4
- Local Network : Réseau LAN du site principal
- Remote Network : Réseau LAN du site distant

Informations Générales

Description	LAN SERVEUR <small>Une description peut être saisie ici à des fins de référence administrative (non analysée).</small>
Désactivé	<input type="checkbox"/> Désactivez cette phase 2 sans la supprimer de la liste.
Mode	Tunnel IPv4
Phase 1	Tunnel VPN Site à Site (IKE ID 1)
P2 reqid	1

Réseaux

Réseau local	Réseau Type	192.168.50.0 Adresse	/ 24
<small>Local network component of this IPsec security association.</small>			
Traduction NAT/BINAT	Aucun Type		/ 0
<small>Si NAT/BINAT est requis sur ce réseau, spécifiez l'adresse à traduire</small>			
Réseau distant	Réseau Type	192.168.60.0 Adresse	/ 24
<small>Remote network component of this IPsec security association.</small>			

- Protocol : ESP
- Encryption Algorithms : AES 256
- Hash Algorithms : SHA256
- PFS Key Group : 14 (2048-bit)
- Lifetime : 3600 (par défaut)

Proposition de phase 2 (SA/Key Exchange)

Protocole	ESP
<small>Encapsulating Security Payload (ESP) performs encryption and authentication, Authentication Header (AH) is authentication only.</small>	
Algorithmes de chiffrement	<input checked="" type="checkbox"/> AES Auto
	<input type="checkbox"/> AES128-GCM Auto
	<input type="checkbox"/> AES192-GCM Auto
	<input checked="" type="checkbox"/> AES256-GCM 128 bits
	<input type="checkbox"/> CHACHA20-POLY1305
Algorithmes de hachage	<input type="checkbox"/> SHA1 <input checked="" type="checkbox"/> SHA256 <input type="checkbox"/> SHA384 <input type="checkbox"/> SHA512 <input type="checkbox"/> AES-XCBC
<small>Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be avoided.</small>	
Groupe de clés PFS	14 (2048 bit)
<small>Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.</small>	

Expiration and Replacement

Life Time	3600
<small>Hard Child SA life time, in seconds, after which the Child SA will be expired. Must be larger than Rekey Time. Cannot be set to the same value as Rekey Time. If left empty, defaults to 110% of Rekey Time. If both Life Time and Rekey Time are empty, defaults to 3600.</small>	
Rekey Time	3240
<small>Time, in seconds, before a Child SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Leave blank to use a default value of 90% Life Time. If both Life Time and Rekey Time are empty, defaults to 3600. Enter a value of 0 to disable, but be aware that when rekey is disabled, connections can be interrupted while new Child SA entries are negotiated.</small>	
Rand Time	360
<small>A random value up to this amount will be subtracted from Rekey Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.</small>	

Sauvegarder et appliquer.

Une fois la configuration terminée, la configuration devrait ressembler à ça :

The screenshot shows the pSense VPN/IPsec configuration interface. The main menu includes 'Système', 'Interfaces', 'Pare-feu', 'Services', 'VPN', 'État', 'Diagnostics', and 'Aide'. The current page is 'VPN / IPsec / Tunnels'. Below the navigation tabs, there are sections for 'Tunnels IPsec' and 'Tunnels'. The 'Tunnels IPsec' section contains a table with the following data:

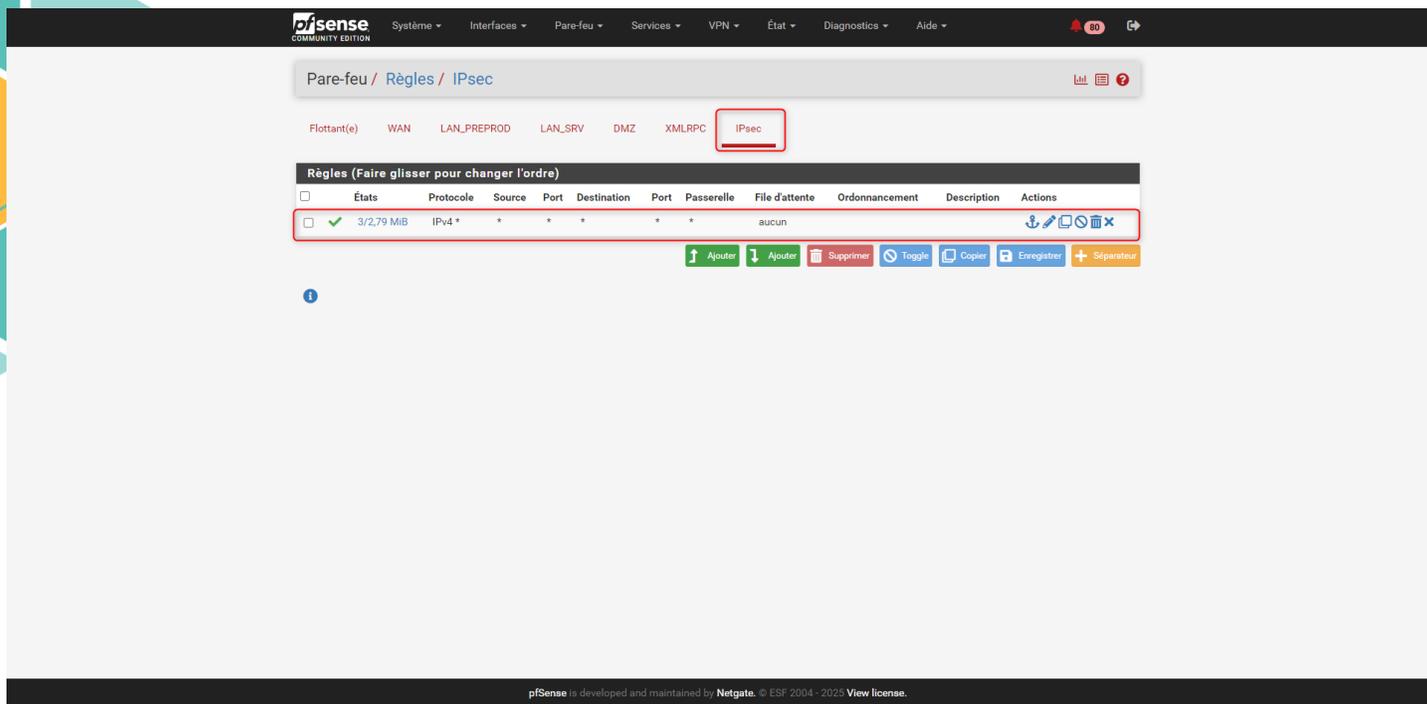
ID	IKE	Passerelle distante	Auth/Mode	Protocole P1	Transformations P1	P1 DH-Group	Description P1	Actions
1	V2	WAN 172.16.30.4	Mutual PSK	AES (256 bits)	SHA256	14 (2048 bit)	Tunnel VPN Site à Site	[Edit] [Copy] [Delete]

Below this table is a detailed view of the selected tunnel (ID 1), showing its phases:

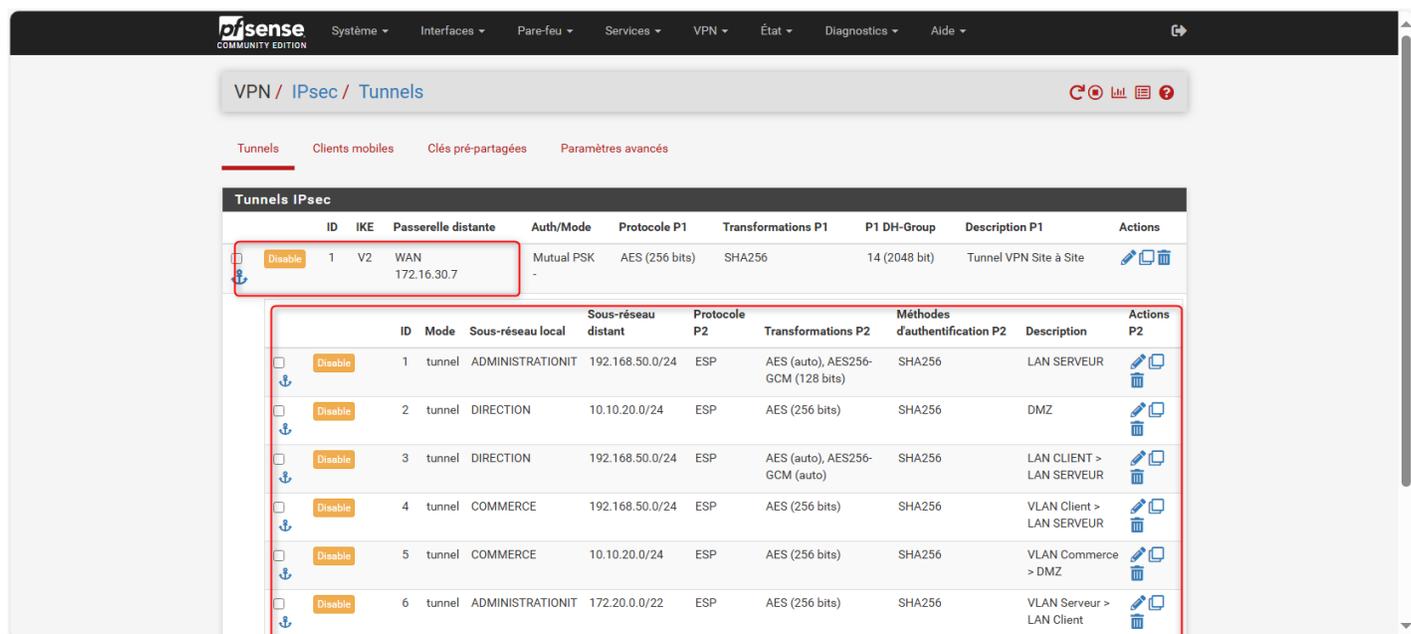
ID	Mode	Sous-réseau local	Sous-réseau distant	Protocole P2	Transformations P2	Méthodes d'authentification P2	Description	Actions
1	tunnel	192.168.50.0/24	192.168.60.0/24	ESP	AES (auto), AES256-GCM (128 bits)	SHA256	LAN SERVEUR	[Edit] [Copy] [Delete]
2	tunnel	10.10.20.0/24	192.168.60.0/24	ESP	AES (auto), AES256-GCM (128 bits)	SHA256	DMZ	[Edit] [Copy] [Delete]
3	tunnel	LAN_SRV	172.20.20.0/24	ESP	AES (auto), AES256-GCM (128 bits)	SHA256	LAN SERVEUR > LAN CLIENT	[Edit] [Copy] [Delete]
4	tunnel	LAN_SRV	172.20.30.0/24	ESP	AES (256 bits)	SHA256	LAN SERVEUR > VLAN COMMERCE	[Edit] [Copy] [Delete]
5	tunnel	DMZ	172.20.30.0/24	ESP	AES (128 bits), AES128-GCM (128 bits)	SHA256	DMZ > VLAN Commerce	[Edit] [Copy] [Delete]
6	tunnel	LAN_PREPROD	192.168.60.20	ESP	AES (256 bits)	SHA256	LAN Client > VLAN Server	[Edit] [Copy] [Delete]

Buttons for '+ Ajouter P2', '+ Ajouter P1', and 'Supprimer les P1s' are visible at the bottom of the configuration area.

Une fois la phase 1 et la phase 2 configurées, allez dans les règles de pare-feu IPsec pour ajouter une règle permettant la communication. Ici nous allons tout ouvrir puisque les règles spécifiques s'appliqueront sur les interfaces des différents réseaux.



Une fois la configuration sur le site principal faites, allez sur l'interface web du pfSense distant et rentré l'identique configuration, mais avec les adresses inverses.



Ici sur l'interface web du pfSense distant on retrouve bien la phase 1, avec comme passerelle distante l'IP WAN du site principal.

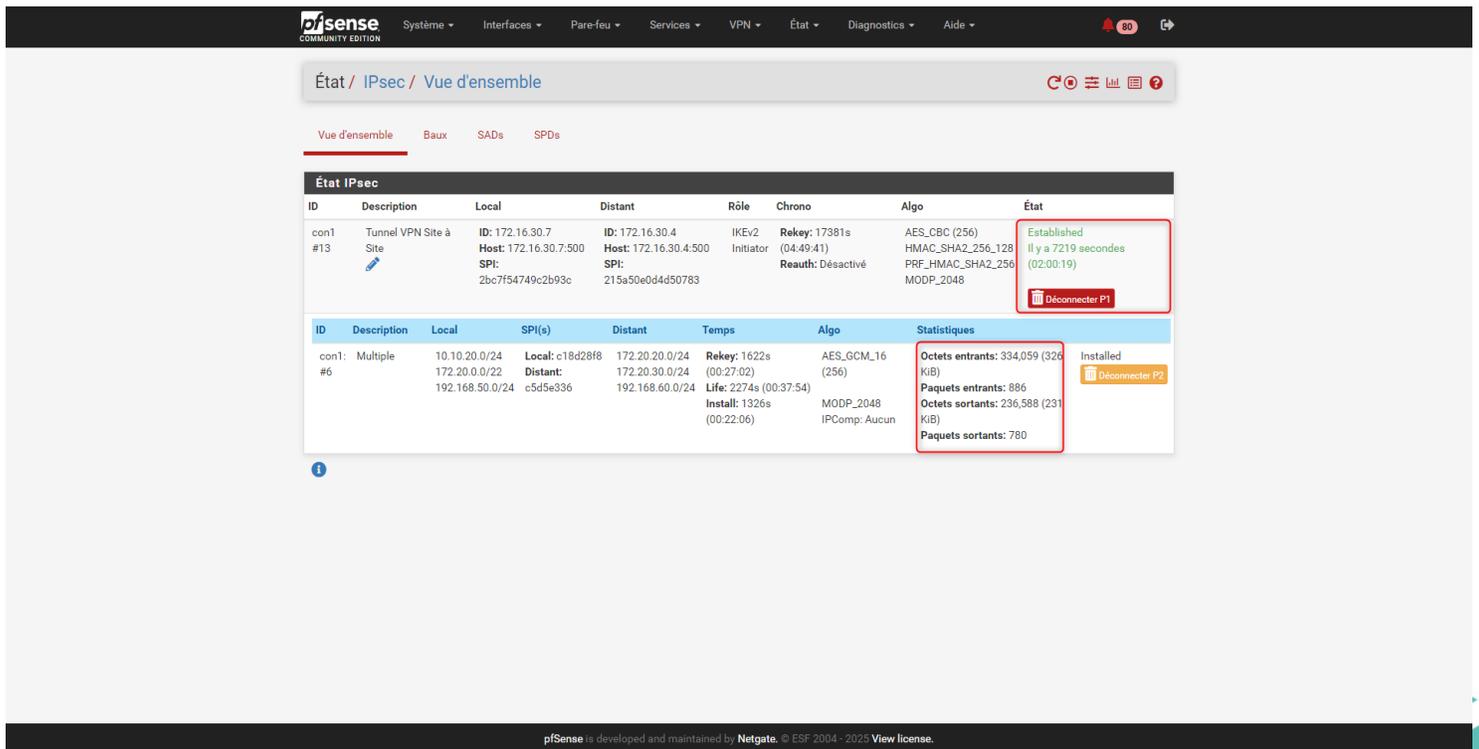


Ainsi que toutes les phases 2 permettant aux VLANs du site distant de communiquer avec les différents services présents sur le site principal.

IV. Tests de connectivité et vérifications :

Une fois les deux configurations terminées, allez dans sur l'interface pfSense d'un des deux routeurs dans la partie Etat > IPsec.

Connecter les phases 1 et 2 et vérifier si la connexion est établie avec une indication « ESTABLISHED ».



The screenshot shows the pfSense web interface with the following data:

ID	Description	Local	Distant	Rôle	Chrono	Algo	État
con1 #13	Tunnel VPN Site à Site	ID: 172.16.30.7 Host: 172.16.30.7:500 SPI: 2bc7f54749c2b93c	ID: 172.16.30.4 Host: 172.16.30.4:500 SPI: 215a50e0d4d50783	IKEv2 Initiator	Rekey: 17381s (04:49:41) Reauth: Désactivé	AES_CBC (256) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	Established Il y a 7219 secondes (02:00:19) Déconnecter P1

ID	Description	Local	SPI(s)	Distant	Temps	Algo	Statistiques
con1 #6	Multiple	10.10.20.0/24 172.20.0.0/22 192.168.50.0/24	Local: c18d28f8 Distant: c5d5e336	172.20.20.0/24 172.20.30.0/24 192.168.60.0/24	Rekey: 1622s (00:27:02) Life: 2274s (00:37:54) Install: 1326s (00:22:06)	AES_GCM_16 (256) MODP_2048 IPComp: Aucun	Oclets entrants: 334,059 (326 KIB) Paquets entrants: 886 Oclets sortants: 236,588 (231 KIB) Paquets sortants: 780 Installed Déconnecter P2

Il est possible maintenant d'effectuer un test de ping entre différentes machines présentes sur les réseaux distant.

Ici je vais vérifier que mon SRV-FIC (serveur fichier) situé dans le VLAN serveur sur le site secondaire peut communiquer avec mon serveur de fichier SRV-M4D (serveur application métier) situé dans le LAN_PREPROD sur le site distant.

```
C:\Windows\system32\cmd.exe
C:\Users\c.archambault>ping 172.20.1.68

Envoi d'une requête 'Ping' 172.20.1.68 avec 32 octets de données :
Réponse de 172.20.1.68 : octets=32 temps=3 ms TTL=126
Réponse de 172.20.1.68 : octets=32 temps=4 ms TTL=126
Réponse de 172.20.1.68 : octets=32 temps=2 ms TTL=126
Réponse de 172.20.1.68 : octets=32 temps=3 ms TTL=126

Statistiques Ping pour 172.20.1.68:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 4ms, Moyenne = 3ms

C:\Users\c.archambault>
C:\Users\c.archambault>
```

Le test de connectivité est donc bien fonctionnel.

V. Compétences mises en œuvre :

Compétence du référentiel	Mise en œuvre dans le projet
Gérer le patrimoine informatique	Recherche des ressources disponibles sur l'infrastructure pour la création du VPN. Configuration du matériel sur les deux sites.
Répondre aux incidents et aux demandes d'assistance et d'évolution	Rattachement du site étendu à l'infrastructure initiale (site principale).
Mettre à disposition des utilisateurs un service informatique	Mise en place d'un tunnel VPN entre les deux sites pour garantir l'accès aux services pour les utilisateurs du site distant.

VI. Problèmes rencontrés et solutions :

Lors de la mise en place du VPN site-à-site avec pfSense, plusieurs difficultés ont été rencontrées, dont une erreur importante liée à la configuration de la Phase 2 du tunnel IPsec.

Problème :

Lors de l'établissement du tunnel VPN, la Phase 2 a été mal configurée. Plus précisément, les réseaux définis ne correspondaient pas correctement aux réseaux LAN à interconnecter, notamment le LAN_PREPROD qui n'arrivait pas à communiquer avec les VLANs distants du site opposé. Cette mauvaise configuration empêchait tout échange de paquets entre les deux sites malgré un tunnel apparemment actif en Phase 1.

Solution :

Après analyse des logs et tests de connectivité, il a été constaté que la Phase 2 devait être recréée proprement, avec une définition correcte des réseaux locaux et distants. Une fois les bons réseaux renseignés dans la configuration de la Phase 2, la communication entre les VLANs a été rétablie et le LAN Préproduction a pu accéder aux ressources distantes comme prévu.

Cette erreur a mis en évidence l'importance de bien définir les correspondances réseau dans la Phase 2 d'un VPN IPsec, car une Phase 1 établie sans Phase 2 fonctionnelle bloque complètement le trafic inter-sites.