



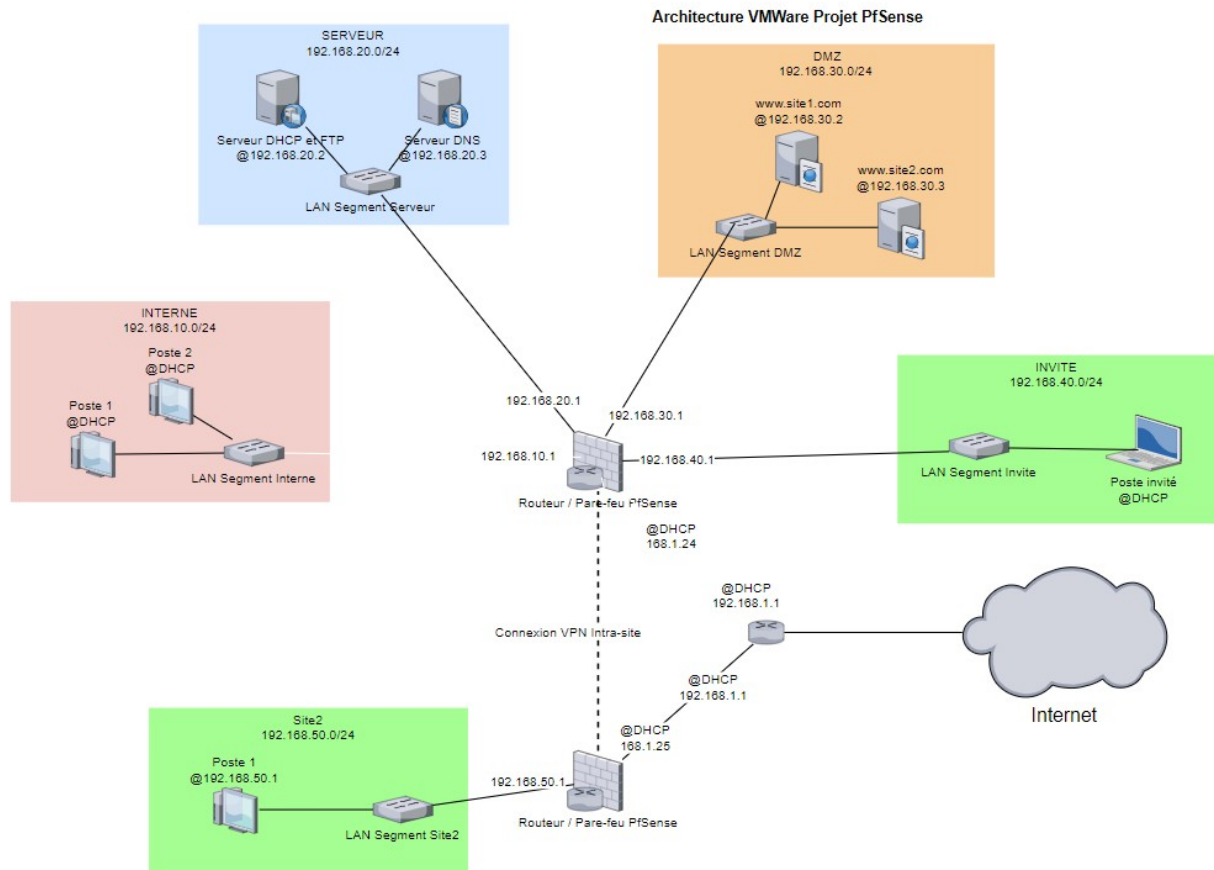
Configuration d'un réseau sécurisé multi-sites avec « pfSense »

Livrable 3 : Configuration d'un VPN site à site – Documentation technique

Table des matières

Configuration topologique du réseau.....	3
Pré-requis.....	4
Installer pfSense sur VMware Workstation Pro.....	4
Configurer la machine virtuelle et ses interfaces réseaux.....	4
Installer pfSense sur la machine virtuelle.....	5
Premier démarrage de pfSense.....	5
Première connexion à l'interface d'administration pfSense.....	6
Se connecter à l'interface web de pfSense.....	6
L'assistant de configuration Web.....	7
pfSense : Ajouter une interface.....	8
La mise en place d'un VPN site à site.....	8
Configuration du routeur PF-Sense2.....	9
Les règles de pare-feu du VPN du routeur PF-Sense2.....	10
Configuration du routeur PF-Sense1.....	12
Les règles de pare-feu du VPN du routeur PF-Sense1.....	13
Problèmes techniques.....	16
DHCP.....	16
DNS.....	16
Pour aller plus loin.....	17
OpenVPN.....	17
WireGuard.....	17
L2TP/IPsec.....	17

Configuration topologique du réseau



Pré-requis

Pour réaliser ce réseau virtuel, nous aurons besoin :

- Un hôte sur lequel VMWare Workstation Pro est installé,
- Le fichier d'installation de pfSense,
- L'image de disque Fedora-Workstation-Live 'Gnome',
- Plusieurs machines virtuelles depuis lesquelles nous testerons notre configuration, sous l'environnement de notre choix,
- Une machine virtuelle sous Windows Serveur 2022,
- La configuration du réseau présentée dans le livrable 2.

Installer pfSense sur Vmware Workstation Pro

Configurer la machine virtuelle et ses interfaces réseaux

Dans la machine VMWare Workstation Pro, ouvrez l'assistant de création d'une machine virtuelle depuis le menu **"File > New Virtual Machine"**. Une fois l'assistant lancé, nous allons sélectionner le mode de création **"Typical"** et cliquer sur **"Suivant"**.

À cette étape, nous allons sélectionner l'option d'installation depuis l'image ISO et renseigner l'emplacement de l'image. Ensuite, nous allons nommer notre machine virtuelle et définir l'emplacement où stocker les données de la machine virtuelle (fichier de configuration, disque dur virtuel, etc.).

Nous allons pouvoir configurer le disque dur virtuel de la machine virtuelle. Dans notre cas, nous sommes dans un réseau virtuel, donc nous allons conserver les paramètres par défaut proposés par l'assistant de création de machine virtuelle et cliquer sur **"Suivant"**. Finaliser la création de la machine virtuelle.

Nous allons maintenant créer un **"LAN Segment"** qui va permettre d'avoir plusieurs réseaux virtuels au sein de VMWare Workstation distincts les uns des autres. Pour ce faire, lorsque vous êtes sur les paramètres d'une interface réseau, cliquez sur **"LAN Segment"**. Ensuite, cliquez sur **"Add"** et nommez-le. Ensuite, il faut modifier le type de connexion au réseau de la première interface afin de s'assurer qu'elle soit sur **"Bridge"**.

La configuration du **"LAN Segment"** est la suivante :

- Network Adapter 2 → **Site2**.

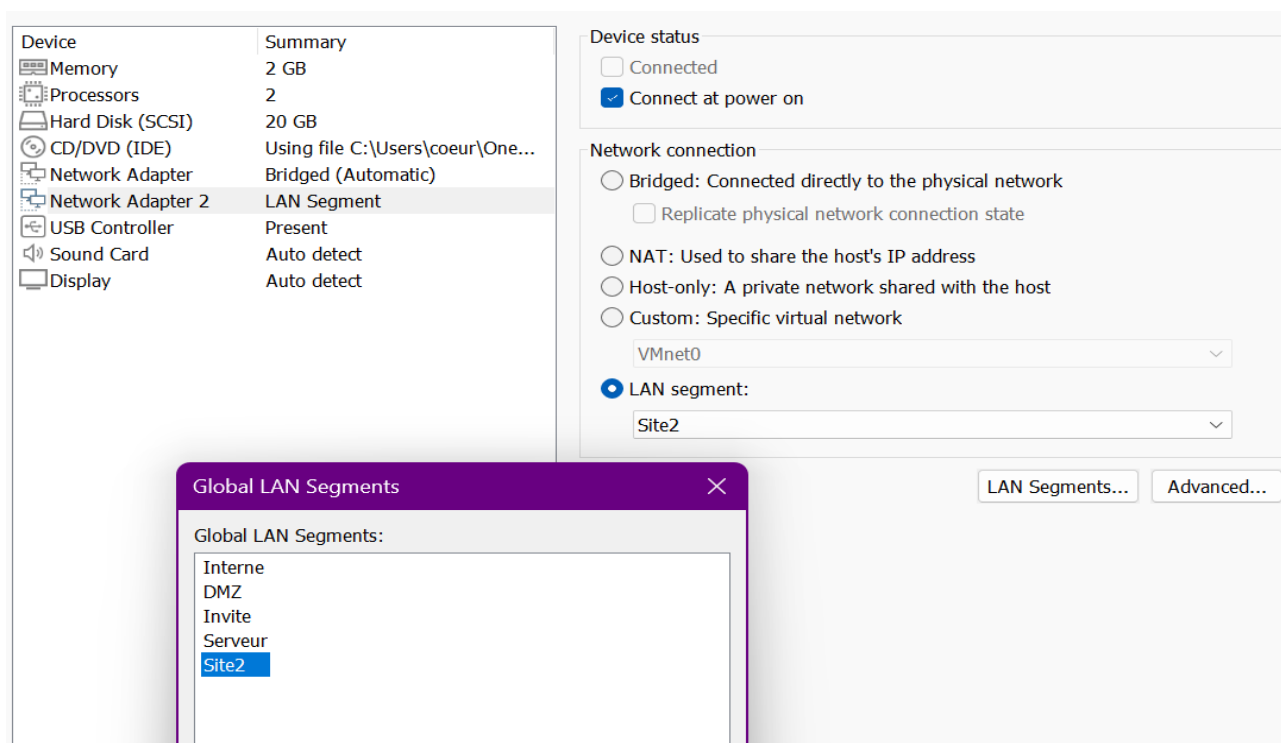


Figure 1: Configuration du LAN segment

Installer pfSense sur la machine virtuelle

Maintenant que notre machine virtuelle est configurée selon notre besoin, nous allons pouvoir la démarrer. Cliquer sur "**Power on this virtual machine**". La machine virtuelle va automatiquement débiter sur le fichier d'installation ISO de pfSense. L'installateur de pfSense va d'abord analyser la configuration matérielle de la machine virtuelle et charger l'assistant d'installation.

Une fois le chargement terminé, veuillez accepter le contrat d'utilisation de pfSense (tapez sur Entrée). Pour poursuivre l'installation, sélectionnez "**Install pfSense**" et appuyez sur Entrée. À l'étape de partitionnement du disque, nous allons utiliser le mode "**Auto (ZFS)**" présélectionné et appuyer sur "Entrée".

À cette étape, un récapitulatif du partitionnement automatique ZFS est présenté. Appuyez sur "Entrée" pour valider.

Dans notre cas, nous allons faire une installation sans redondance (mode stripe). Appuyez sur "Entrée". Pour sélectionner le disque dur virtuel, appuyez sur Espace puis sur Entrée et sélectionnez "**Yes**" (flèche gauche et Entrée). Une fois l'installation achevée, validez le redémarrage de la machine virtuelle.

Premier démarrage de pfSense

Nous allons maintenant modifier les différentes configurations IP de notre réseau, nous allons procéder comme suit :

- Choisissez l'option 2,
- Nous allons sélectionner l'interface WAN en entrant l'option 1 et indiquer que nous n'allons pas configurer l'interface via DHCP,
 - L'adresse IP de l'interface WAN : **192.168.1.26/24**,

- Pas de passerelle, configuration IPV6 ou DHCP IPv4.
- Nous allons sélectionner l'interface LAN en entrant l'option 2 et indiquer que nous n'allons pas configurer l'interface via DHCP,
 - L'adresse IP de l'interface LAN : **192.168.50.1/24**,
 - Pas de passerelle, configuration IPV6 ou DHCP IPv4.

Une fois terminé, l'URL pour accéder à l'interface Web d'administration de pfSense s'affiche et faire "**Entrée**" pour terminer.

```
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.26/24
LAN (lan)      -> em1      -> v4: 192.168.50.1/24
```

Figure 2: Configuration des interfaces via pfSense

Première connexion à l'interface d'administration pfSense

Se connecter à l'interface web de pfSense

Depuis le poste client (c'est-à-dire depuis notre réseau LAN virtuel), nous allons nous connecter à l'interface Web d'administration de pfSense à l'adresse IP "**https://192.168.50.1/**".

Au préalable, il est nécessaire de configurer l'interface réseau de la machine virtuelle cliente comme suit :

- Adresse IPv4 : **192.168.50.2**
- Masque : **255.255.255.0**
- Passerelle : **192.168.50.1**
- Serveur DNS : **1.1.1.1**

Cancel Wired Apply

Details Identity IPv4 IPv6 Security

IPv4 Method

☐ Automatic (DHCP) ☐ Link-Local Only

☒ Manual ☐ Disable

☐ Shared to other computers

Addresses

Address	Netmask	Gateway	
192.168.50.2	255.255.255.0	192.168.50.1	⊗
			⊗

DNS Automatic ☐

1.1.1.1

Separate IP addresses with commas

Figure 3: Configuration du réseau du poste client

Pour vous connecter à l'interface Web d'administration, il est nécessaire de saisir l'identifiant et le mot de passe prédéfinis à l'installation. Voici les identifiants par défaut :

- Identifiant : **admin**,
- Mot de passe : **pfSense** (à modifier par la suite).

L'assistant de configuration Web

Une fois connecté, l'assistant de configuration Web s'ouvrira. Cliquez sur "**Next**".

Nous allons préciser les serveurs DNS de notre firewall pfSense, à savoir "**1.1.1.1**" et "**8.8.8.8**", et cliquer sur "**Next**". Nous allons configurer le serveur de temps qui est important pour bénéficier de logs à jour. Sélectionnez le fuseau horaire correspondant à votre emplacement, puis cliquez sur "**Next**".

À l'étape 4, conservez les paramètres prédéfinis par pfSense pour la configuration de l'interface WAN en veillant à décocher les deux options suivantes : "**Block private networks form entering via WAN**" et "**Block non-internet routed networks from entering via WAN**". Ces deux paramètres, lorsque pfSense est installé dans un réseau local existant, permettent de ne pas bloquer le trafic reposant sur des adresses IP privées. Ici, entre notre box internet et pfSense.

À l'étape 5 de l'assistant, conservez la configuration de l'interface LAN que nous avons faite en amont.

À l'étape 6 de l'assistant, définissez un nouveau mot de passe et cliquez sur "**Next**". Dans notre cas, nous avons :

- Identifiant : **admin**,
- Mot de passe : **admin**.

À l'étape 7, cliquez sur "**Reload**" afin de recharger la configuration de pfSense avec les informations que nous venons de définir.

Après quelques secondes, nous arrivons à la fin de l'assistant de configuration. Nous pouvons cliquer sur "**Finish**" pour accéder au tableau de bord.

pfSense : Ajouter une interface

Nous allons accéder au menu « Interfaces » puis « Assignent ». On constate que l'interface "em2" peut être ajoutée : cliquez sur "Add" puis "Save".




Interface	Network port
WAN	em0 (00:0c:29:15:74:46) 
Interne	em1 (00:0c:29:15:74:50)  

Figure 4: Association des cartes réseaux aux interfaces

La mise en place d'un VPN site à site

Pour configurer un Virtual Private Network (VPN) site à site qui permet de connecter plusieurs sites à distance de manière sécurisée, nous allons devoir configurer le routeur PF-Sense précédemment créé et ce nouveau routeur PF-Sense.

Ici, nous allons configurer un VPN Internet Protocol Security (IPsec).

IPSec (Internet Protocol Security) est un protocole de sécurité utilisé pour protéger les échanges de données sur des réseaux IP. Il permet de sécuriser la communication en cryptant les données et en garantissant leur intégrité et leur authenticité. IPSec peut être utilisé pour établir des réseaux privés virtuels (VPN), permettant ainsi de sécuriser les connexions à distance entre des appareils ou des réseaux.

Il fonctionne à travers deux modes :

- Mode transport : seuls les paquets de données sont cryptés, l'en-tête IP reste inchangé. Ce mode est souvent utilisé pour la sécurisation de la communication entre deux hôtes.
- Mode tunnel : l'intégralité du paquet IP est cryptée, y compris l'en-tête. Ce mode est typiquement utilisé pour créer des tunnels VPN entre des réseaux distants.

IPSec repose sur deux protocoles principaux :

- AH (Authentication Header) : pour garantir l'intégrité et l'authenticité des données sans les chiffrer.
- ESP (Encapsulating Security Payload) : pour assurer à la fois le chiffrement, l'intégrité et l'authentification des données.

Les VPN IPSec peuvent être configurés pour offrir différents niveaux de sécurité, en fonction des besoins spécifiques du réseau et des utilisateurs. Ils sont largement utilisés dans les entreprises pour sécuriser l'accès à distance et les communications inter-sites.

Configuration du routeur PF-Sense2

À partir du nouveau poste créé dans le site 1, nous accédons à l'interface graphique de pfSense à partir de l'adresse « **192.168.50.1** ».

Nous nous rendons ensuite dans « **VPN > IPSec** ».

Cliquer sur « **Add P1** » et suivre la configuration suivante :

- Description : **VPN test 1 phase 1**,
- Key Exchange version : **IKEv2**,
- Internet Protocol : **IPv4**,
- Interface : **WAN**,
- Remote Gateway : **192.168.1.25**,

La « **Remote Gateway** » doit correspondre à l'adresse de l'interface WAN du routeur PfSense auquel vous allez vous relier, qui a donc été distribuée par votre box internet. Ici, le routeur PfSense-1 est donc en « **192.168.1.25** ».

The screenshot displays the pfSense configuration interface for a new Phase 1 Proposal. The 'General Information' section is at the top, followed by the 'IKE Endpoint Configuration' section. The 'Phase 1 Proposal (Authentication)' section is currently active. In this section, the 'Authentication Method' is set to 'Mutual PSK', 'My identifier' is 'My IP address', 'Peer identifier' is 'Peer IP address', and the 'Pre-Shared Key' is 'password'. A 'Generate new Pre-Shared Key' button is visible below the key field. The interface includes descriptive text for each field and a status bar at the bottom right.

General Information	
Description	VPN test 1 phase 1 <small>A description may be entered here for administrative reference (not parsed).</small>
Disabled	<input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.
IKE ID	1

IKE Endpoint Configuration	
Key Exchange version	IKEv2 <small>Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.</small>
Internet Protocol	IPv4 <small>Select the Internet Protocol family.</small>
Interface	WAN <small>Select the interface for the local endpoint of this phase1 entry.</small>
Remote Gateway	192.168.1.25 <small>Enter the public IP address or host name of the remote gateway.</small>

Phase 1 Proposal (Authentication)	
Authentication Method	Mutual PSK <small>Must match the setting chosen on the remote side.</small>
My identifier	My IP address
Peer identifier	Peer IP address
Pre-Shared Key	password <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

Figure 5: Configuration de la phase 1 du routeur PfSense2

Nous allons ensuite poursuivre en cliquant sur « **Show Phase 2 entries** » puis « **Add P2** ».

On suit la configuration suivante :

- Description : **Tunnel de Site2 vers Interne**,

- Mode : **Tunnel IPv4**,
- Local Network : **Site2 subnet**,
- NAT/BINAT translation : **None**,
- Remote Network :
 - Type : **Network**,
 - Adress : **192.168.10.0**,
- Automatically ping host : **192.168.10.1**.

General Information

Description

tunnel de Site2 vers Interne

A description may be entered here for administrative reference (not parsed).

Disabled

☐ Disable this phase 2 entry without removing it from the list.

Mode

Tunnel IPv4

Phase 1

VPN test 1 phase 1 (IKE ID 1)

P2 reqid

1

Networks

Local Network

SITE2 subnet

Type

Address

Local network component of this IPsec security association.

NAT/BINAT translation

None

Type

Address

If NAT/BINAT is required on this network specify the address to be translated

Remote Network

Network

Type

Address

Remote network component of this IPsec security association.

Figure 6: Configuration de la phase 2 du routeur PfSense2

Nous avons donc créé un tunnel vers le LAN Interne de notre site 1.

Il faudra refaire cette configuration pour tout autre LAN que l’on souhaite connecter en ajoutant une phase 2 et en modifiant « **Remote Network** » avec l’adresse réseau du LAN concerné.

Les règles de pare-feu du VPN du routeur PF-Sense2

Nous allons créer les règles de flux suivantes, dont certaines ont déjà été créées :

FloatingWANSITE2IPsec

Rules (Drag to Change Order)






<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	3/1.06 MiB	IPv4 *	*	*	*	*	none			    

Illustration 1: Règles de pare-feu du WAN

Floating

WAN

SITE2

IPsec

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	*	*	*	SITE2 Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 *	SITE2 net	*	192.168.20.2	*	*	none		Autorise les échanges de Site2 vers le serveur de Partage FTP	
<input type="checkbox"/>	0/8 KiB	IPv4 UDP	*	*	*	67 - 68	*	none		Autorisation des échanges broadcast pour DHCP	
<input type="checkbox"/>	0/109 KiB	IPv4 UDP	SITE2 net	*	192.168.20.0/24	53 (DNS)	*	none		Autorise les échanges depuis Site2 vers lan Serveurs sur le port 53	
<input type="checkbox"/>	0/323 KiB	IPv4 TCP	SITE2 net	*	192.168.30.0/24	80 (HTTP)	*	none		Autorise les échanges de Site vers Serveurs sur le port 80	
<input type="checkbox"/>	0/0 B	IPv4 TCP	SITE2 net	*	192.168.30.0/24	443 (HTTPS)	*	none		Autorise les échanges de Site vers Serveurs sur le port 443	
<input type="checkbox"/>	0/0 B	IPv4 *	SITE2 net	*	192.168.30.0/24	*	*	none		Interdit Site2 vers DMZ	
<input type="checkbox"/>	0/336 B	IPv4 *	SITE2 net	*	192.168.10.0/24	*	*	none		Interdit Site2 vers Interne	
<input type="checkbox"/>	0/0 B	IPv4 *	SITE2 net	*	192.168.20.0/24	*	*	none		Interdit Site2 vers Serveurs	
<input type="checkbox"/>	0/0 B	IPv4 *	SITE2 net	*	192.168.40.0/24	*	*	none		Interdit Site2 vers Invite	
<input type="checkbox"/>	0/3.69 MiB	IPv4 *	SITE2 net	*	*	*	*	none		Default allow LAN to any rule	

Illustration 2: Règles de pare-feu du LAN Site2

Floating

WAN

SITE2

IPsec

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<div><div>✓</div><div>0/22 KiB</div></div>	IPv4 *	192.168.10.0/24	*	192.168.50.0/24	*	*	none			<div><div></div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div>✓</div><div>0/22 KiB</div></div>	IPv4 *	192.168.20.0/24	*	192.168.50.0/24	*	*	none			<div><div></div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div>✓</div><div>0/22 KiB</div></div>	IPv4 *	192.168.30.0/24	*	192.168.50.0/24	*	*	none			<div><div></div><div></div><div></div><div></div><div></div></div>
<input type="checkbox"/>	<div><div>✓</div><div>0/22 KiB</div></div>	IPv4 *	192.168.40.0/24	*	192.168.50.0/24	*	*	none			<div><div></div><div></div><div></div><div></div><div></div></div>

Illustration 3: Règles de pare-feu de IPsec

Pour ajouter les ACL rendez-vous dans Firewall > Rules :

Sur l'interface IPsec :

Ajoutez une acl en cliquant sur add en bas à droite.

On va se baser sur la première règle de l'interface IPsec pour faire un exemple.

Choisissez l'action de l'acl, pour la première règle du IPsec c'est Pass

Dans Protocol, choisissez celui que vous voulez filtrer, par exemple pour la première règle du IPsec c'est IPv4*.

Dans Source, choisissez Network et mettez l'adresse 192.168.10.0 et /24.

Dans Destination, choisissez Network et mettez l'adresse 192.168.50.4 et /24.

Répétez ensuite pour le reste des règles à instaurer.

Configuration du routeur PF-Sense1

À partir du poste créé dans le réseau Interne, nous accédons à l'interface graphique de pfSense à partir de l'adresse « **192.168.10.1** ».

Nous nous rendons ensuite dans « **VPN > IPsec** ».

Cliquer sur « **Add P1** » et suivre la configuration suivante :

- Description : **phase 1 VPN test 1 pfsense1**,
- Key Exchange version : **IKEv2**,
- Internet Protocol : **IPv4**,
- Interface : **WAN**,
- Remote Gateway : **192.168.1.26**,

La « **Remote Gateway** » doit correspondre à l'adresse de l'interface WAN du routeur PfSense auquel vous allez vous relier, qui a donc été distribuée par votre box internet. Ici, le routeur PfSense-1 est donc en « **192.168.1.26** ».

The screenshot displays the pfSense VPN configuration interface, organized into three main sections:

- General Information:** Contains fields for Description (set to "phase 1 VPN test 1 pfsense1"), a Disabled checkbox, and IKE ID (set to 1).
- IKE Endpoint Configuration:** Contains dropdown menus for Key Exchange version (IKEv2), Internet Protocol (IPv4), and Interface (WAN). It also has a text field for Remote Gateway (192.168.1.26).
- Phase 1 Proposal (Authentication):** Contains dropdown menus for Authentication Method (Mutual PSK), My identifier (My IP address), and Peer identifier (Peer IP address). It also has a text field for Pre-Shared Key (password) and a "Generate new Pre-Shared Key" button.

Figure 7: Configuration de la phase 1 du routeur PfSense1

Nous allons ensuite poursuivre en cliquant sur « **Show Phase 2 entries** » puis « **Add P2** ».

On suit la configuration suivante :

- Description : **Tunnel de Interne vers Site2**,

- Mode : **Tunnel IPv4**,
- Local Network : **INTERNE subnet**,
- NAT/BINAT translation : **None**,
- Remote Network :
 - Type : **Network**,
 - Address : **192.168.50.0**,
- Automatically ping host : **192.168.50.1**.

General Information

Description

tunnel de Site2 vers Interne

A description may be entered here for administrative reference (not parsed).

Disabled

☐ Disable this phase 2 entry without removing it from the list.

Mode

Tunnel IPv4

Phase 1

VPN test 1 phase 1 (IKE ID 1)

P2 reqid

1

Networks

Local Network

SITE2 subnet

Type

Address

Local network component of this IPsec security association.

NAT/BINAT translation

None

Type

Address

If NAT/BINAT is required on this network specify the address to be translated

Remote Network

Network

192.168.10.0

24

Type

Address

Remote network component of this IPsec security association.

Figure 8: Configuration de la phase 2 du routeur PfSense1

Nous avons donc créé un tunnel vers le LAN Interne de notre site 1.

Il faudra refaire cette configuration pour tout autre LAN que l’on souhaite connecter en ajoutant une phase 2 et en modifiant « **Local Network** » avec l’adresse réseau du LAN concerné.

Les règles de pare-feu du VPN du routeur PF-Sense1

Nous allons créer les règles de flux suivantes, dont certaines ont déjà été créées :

Floating	WAN	INTERNE	DMZ	INVITE	SERVEUR	IPsec					
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	*	*	192.168.20.4	21 (FTP)	*	none		Bloque tous le trafic vers le Serveur-Partage sur le port 21 (ftp)	
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	*	*	192.168.20.4	*	*	none		Bloque tous le trafic vers le Serveur-Partage	
<input type="checkbox"/>	✓ 4/4.51 MiB	IPv4 *	*	*	*	*	*	none			

Illustration 4: Règles de pare-feu du WAN

Floating	WAN	INTERNE	DMZ	INVITE	SERVEUR	IPsec					
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0/0 B	*	*	*	INTERNE Address	443 80	*	*		Anti-Logout Rule	
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	INTERNE net	*	192.168.20.2	*	*	none		Autorise Interne vers host Serveur-DNS-Partage	
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	*	*	*	67 - 68	*	none		Autorise tout du port 67 vers le port 68 (bootpc vers bootps)	
<input type="checkbox"/>	✓ 0/18 KiB	IPv4 UDP	INTERNE net	*	SERVEUR net	53 (DNS)	*	none		Autorise Interne vers Serveur sur le port 53 (DNS)	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	192.168.10.0/24	*	192.168.30.0/24	80 (HTTP)	*	none		Autorise Interne vers Serveur sur le port 80 (http)	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	192.168.10.0/24	*	192.168.30.0/24	443 (HTTPS)	*	none		Autorise Interne vers Serveur sur le port 443 (https)	
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	INTERNE net	*	SERVEUR net	*	*	none		Interdit Interne vers Serveur	
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	INTERNE net	*	DMZ net	*	*	none		Interdit Interne vers DMZ	
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	INTERNE net	*	INVITE net	*	*	none		Interdit Interne vers invite	
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	INTERNE net	*	192.168.50.0/24	*	*	none		Interdit Interne vers Site2	
<input type="checkbox"/>	✓ 0/63 KiB	IPv4 *	INTERNE net	*	*	*	*	none		Autorise tout vers tous	

Illustration 5: Règles de pare-feu du LAN Interne

Floating	WAN	INTERNE	DMZ	INVITE	SERVEUR	IPsec					
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 TCP	192.168.30.0/24	*	*	80 (HTTP)	*	none		Autorise DMZ vers tous sur le port 80 (http)	
<input type="checkbox"/>	0/0 B	IPv4 TCP	192.168.30.0/24	*	*	443 (HTTPS)	*	none		Autorise DMZ vers tous sur le port 443 (https)	
<input type="checkbox"/>	0/1 KiB	IPv4 TCP	192.168.30.0/24	*	*	*	*	none		Autorise DMZ vers tous sortant et incluant les connexions déjà établis	
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	*	*	*	none		Interdit tous vers tous	

Illustration 6: Règles de pare-feu du LAN DMZ





































Floating	WAN	INTERNE	DMZ	INVITE	SERVEUR	IPsec					
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	*	*	*	67 - 68	*	none	Autorise tout du port 67 vers le port 68 (bootpc vers bootps)	   
<input type="checkbox"/>	✓	0/0 B	IPv4 UDP	192.168.40.0/24	*	192.168.30.0/24	53 (DNS)	*	none	Autorise Invite vers Serveur sur le port 53 (DNS)	   
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	192.168.40.0/24	*	192.168.30.0/24	80 (HTTP)	*	none	Autorise Invite vers DMZ sur le port 80 (http)	   
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	192.168.40.0/24	*	192.168.30.0/24	443 (HTTPS)	*	none	Autorise Invite vers DMZ sur le port 443 (https)	   
<input type="checkbox"/>	✗	0/0 B	IPv4 TCP	INVITE net	*	INTERNE net	*	*	none	Interdit Invite vers Interne	   
<input type="checkbox"/>	✗	0/0 B	IPv4 TCP	INVITE net	*	SERVEUR net	*	*	none	Interdit Invite vers Serveur	   
<input type="checkbox"/>	✗	0/0 B	IPv4 TCP	INVITE net	*	DMZ net	*	*	none	Interdit Invite vers DMZ	   
<input type="checkbox"/>	✗	0/0 B	IPv4 TCP	INVITE net	*	192.168.50.0/24	*	*	none	Interdit Invite vers Site2	   
<input type="checkbox"/>	✓	0/0 B	IPv4 *	INVITE net	*	*	*	*	none	Autorise Invite vers tout	   

Illustration 7: Règles de pare-feu du LAN Invité

Floating

WAN

INTERNE

DMZ

INVITE

SERVEUR

IPsec

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 TCP	192.168.20.2	*	*	*	*	none		Autorise tous le trafic partant du Serveur-DHCP-Partage	
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	21 (FTP)	*	*	*	none		Autorise tous le trafic avec le port 21	
<input type="checkbox"/>	2/194 KiB	IPv4 UDP	*	*	*	53 (DNS)	*	none		Autorise tous le trafic sur le port 53 (DNS)	
<input type="checkbox"/>	0/3 KiB	IPv4 UDP	*	*	*	67 - 68	*	none		Autorise tous le trafic avec le port 67 (bootpc)	
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none		Autorise tous le trafic avec le port 80 (http)	
<input type="checkbox"/>	0/0 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		Autorise tous le trafic avec le port 443 (https)	
<input type="checkbox"/>	0/8 KiB	IPv4 *	*	*	*	*	*	none		Bloquer tous le trafic	

Illustration 8: Règles de pare-feu du LAN Serveur

















Floating	WAN	INTERNE	DMZ	INVITE	SERVEUR	IPsec					
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/22 KiB	IPv4 *	192.168.50.0/24	*	192.168.10.0/24	*	*	none	Autorisation des échanges venant du LAN Site2 via VPN vers Interne	   
<input type="checkbox"/>	✓	0/131 KiB	IPv4 *	192.168.50.0/24	*	192.168.20.0/24	*	*	none	Autorisation des échanges venant du LAN Site2 via VPN vers Serveurs	   
<input type="checkbox"/>	✓	0/345 KiB	IPv4 *	192.168.50.0/24	*	192.168.30.0/24	*	*	none	Autorisation des échanges venant du LAN Site2 via VPN vers DMZ	   
<input type="checkbox"/>	✓	0/22 KiB	IPv4 *	192.168.50.0/24	*	192.168.40.0/24	*	*	none	Autorisation des échanges venant du LAN Site2 via VPN vers Invite	   

Illustration 9: Règles de pare-feu de IPsec

Pour ajouter les ACL rendez-vous dans Firewall > Rules :

Sur l'interface IPsec :

Ajoutez une acl en cliquant sur add en bas à droite.

On va se baser sur la première règle de l'interface IPsec pour faire un exemple.

Choisissez l'action de l'acl, pour la première règle du IPsec c'est Pass

Dans Protocol, choisissez celui que vous voulez filtrer, par exemple pour la première règle du IPsec c'est IPv4.

Dans Source, choisissez Network et mettez l'adresse 192.168.50.0 et /24.

Dans Destination, choisissez Network et mettez l'adresse 192.168.10.4 et /24.

Répétez ensuite pour le reste des règles à instaurer. Répétez ensuite pour le reste des règles à instaurer.

Problèmes techniques

Dans ce dernier livrable, nous n'avons rencontré que peu de problèmes lors de la configuration d'un VPN site à site avec le VPN IPsec.

DHCP

La remarque qui est nécessaire à apporter est le choix de ne pas utiliser le DHCP du pfSense du site 1 pour ce nouveau site. En effet, ceci n'est pas recommandé, car si le VPN tombe en panne ou que le DHCP du site 1 tombe en panne, nous n'aurions plus d'adresse pour le site 2.

On pourrait éventuellement le gérer en rajoutant un serveur DHCP du côté du site 2.

DNS

Parfois, le DNS ne fonctionne pas sur le site 2, car les communications sont bloquées par des règles de pare-feu de pfSense du site 1.

Mais cela ne devrait pas être le cas comme les règles autorisent leur trafic.

Last 500 Firewall Log Entries. (Maximum 500)						
Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Jan 10 10:45:56	DMZ	Default deny rule IPv4 (1000000103)	192.168.30.2:53896	1.1.1.1:53	UDP
✗	Jan 10 10:45:56	DMZ	Default deny rule IPv4 (1000000103)	192.168.30.2:53896	192.168.20.3:53	UDP

Figure 9: Image du problème DNS présent dans les logs

Pour y remédier, nous devons redémarrer l'ensemble du projet dans l'ordre suivant :

- Les routeurs,
- Le serveur DHCP,
- Les serveurs Internet,
- Le serveur DNS,
- Les postes.

Pour aller plus loin

Nous avons remarqué plusieurs autres solutions que IPsec pour la configuration d'un tunnel site-à-site.

OpenVPN

OpenVPN est une solution VPN open source qui prend en charge à la fois les connexions site-à-site et client-à-site.

Il est plus flexible, plus facile à configurer, et bien adapté à des environnements variés et à des situations où traverser des NAT ou gérer des configurations complexes est important. Bien qu'il puisse avoir une légère surcharge de performance par rapport à IPsec, il reste une option solide pour la majorité des configurations VPN site-à-site, avec une bonne prise en charge des technologies modernes et une maintenance rapide.

Si la facilité de gestion, la flexibilité et la prise en charge des différents types de connexion sont cruciaux pour votre infrastructure, OpenVPN est souvent le meilleur choix. Si vous recherchez une solution robuste, standardisée et compatible avec des équipements spécialisés, alors IPsec pourrait être plus approprié.

WireGuard

WireGuard est un VPN relativement nouveau, il est intégré dans pfSense depuis la version 2.5.0. Il devient de plus en plus populaire en raison de sa simplicité, de sa rapidité, et de son efficacité.

C'est une solution plus moderne, plus rapide, plus simple à configurer et à maintenir. Il est parfait pour des environnements plus petits ou des connexions simples où la performance et la facilité d'utilisation sont les priorités. Cependant, il peut ne pas être aussi flexible qu'IPsec pour des configurations très spécifiques.

Si vous avez besoin d'une solution VPN simple, rapide et moderne, WireGuard est probablement le meilleur choix. Si vous avez des exigences complexes en matière de sécurité, d'interopérabilité et de personnalisation, IPsec reste une valeur sûre.

À noter : WireGuard n'est pas un VPN natif de PfSense. Il est apparu sur PfSense une première fois en 2021, mais il a rapidement été retiré de la plateforme pour des problèmes de fiabilité et de sécurité. Il figure à nouveau depuis 2022 en tant qu'extension. Il faut donc le télécharger au travers de 'System > Packages > Available Packages'.

L2TP/IPsec

L2TP est souvent utilisé conjointement avec IPsec pour fournir une solution VPN sécurisée. L2TP est plus simple à configurer que l'IPsec seul.

C'est une solution plus simple à déployer lorsque vous avez besoin d'un tunneling supplémentaire et d'une compatibilité NAT plus robuste. Il est généralement préféré pour des environnements dans lesquels la simplicité et la prise en charge de différents périphériques sont les priorités.

Si vous recherchez flexibilité et personnalisation dans la sécurité, choisissez IPsec.

Si vous avez besoin d'une solution VPN simple avec un bon support NAT, L2TP/IPsec peut être plus adapté