

Introduction

Pour résumer IPsec va permettre de chiffrer les données avant de les envoyer dans le tunnel qui sera mis en place par L2TP.

Avec cette forme de vpn nous avons **deux phase** :

La sécurité IPsec est divisée en deux phases. La première phase est la phase de négociation de la sécurité, qui établit une connexion sécurisée entre les deux extrémités d'une communication VPN. La deuxième phase est la phase de transfert de données, qui permet le transfert de données chiffrées entre les deux extrémités ¹.

La phase 1 de IPsec est utilisée pour établir une connexion sécurisée entre les deux extrémités d'une communication VPN. Elle utilise le protocole IKE (Internet Key Exchange) pour négocier les paramètres de sécurité nécessaires à la communication

L2TP est un protocole de tunneling qui permet de créer un tunnel sécurisé entre deux réseaux. Il est souvent utilisé en combinaison avec IPsec pour fournir une sécurité supplémentaire

La phase 2 de IPsec est utilisée pour transférer des données chiffrées entre les deux extrémités d'une communication VPN. Elle utilise le protocole ESP (Encapsulating Security Payload) pour chiffrer les données en transit

En résumé, la phase 1 de IPsec est utilisée pour établir une connexion sécurisée entre les deux extrémités d'une communication VPN, tandis que la phase 2 est utilisée pour transférer des données chiffrées entre les deux extrémités. L2TP est souvent utilisé en combinaison avec IPsec pour fournir une sécurité supplémentaire

Topologie

Les deux firewall sur leur pates WAN sont dans le même réseau 10.0.0.0/24

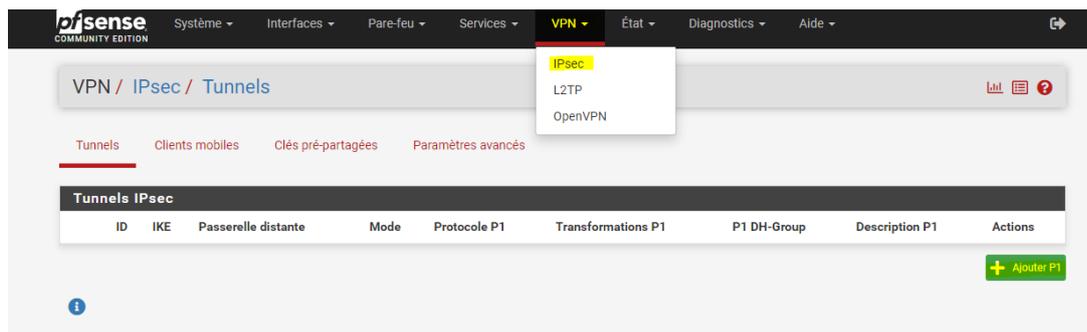
WAN PFSense 1 : 10.0.0.253, LAN : 172.16.0.0 /24

WAN PFSense 2 : 10.0.0.254, LAN : 172.20.0.0 /24

Objectif pour notre labo créer un VPN ipsec entre les deux pfsense pour faire communiquer nos deux LAN de manière transparente.

Activation IPSEC + phase 1

On se rend directement dans le menu "VPN" puis dans "IPsec" :



Ensuite on clique sur ajouter P1

Informations Générales	
Description	VERS PFSENSE 2 <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 Endpoint Configuration	
Version de l'échange de clés	IKEV2 <small>Sélectionnez la version du protocole Internet Key Exchange à utiliser. Auto utilise IKEV1 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	10.0.0.252 <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	12345678 <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

Du coup on a pas beaucoup de choses à modifier au niveau des algorithmes laissez par défaut car ipsec est très sensible.

Je définis quel interface je vais utiliser pour communiquer avec l'autre pare-feu je renseigne ensuite son IP.

Et je choisis une authentification via clé pré partagé je mets un mot de passe simple pour l'exercice !

Ensuite je modifie rien d'autre

Expiration and Replacement

Life Time	<input type="text" value="28800"/>	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)
Rekey Time	<input type="text" value="25920"/>	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.
Reauth Time	<input type="text" value="0"/>	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.
Rand Time	<input type="text" value="2880"/>	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.

Options Avancées

Child SA Start Action	<input type="text" value="Par défaut"/>	Set this option to force specific initiation/responder behavior for child SA (P2) entries
Child SA Close Action	<input type="text" value="Par défaut"/>	Set this option to control the behavior when the remote peer unexpectedly closes a child SA (P2)
NAT Traversal	<input type="text" value="Auto"/>	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.
MOBIKE	<input type="text" value="Désactiver"/>	Définissez cette option pour contrôler l'utilisation de MOBIKE
Gateway duplicates	<input type="checkbox"/>	Enable this to allow multiple phase 1 configurations with the same endpoint. When enabled, pSense 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 Manual PRF selection is typically not required, but can be useful in combination with AEAD Encryption Algorithms such as AES-GCM
Custom IKE/NAT-T Ports	<input type="text" value="Remote IKE Port"/>	<input type="text" value="Remote NAT-T Port"/>
	UDP port for IKE on the remote gateway. Leave empty for default automatic behavior (500/4500).	UDP port for NAT-T on the remote gateway. i
Détection des pairs morts	<input checked="" type="checkbox"/>	Activer DPD Check the liveness of a peer by using IKEv2 INFORMATIONAL exchanges or IKEv1 R_U_THERE messages. Active DPD checking is only enforced if no IKE or ESP/AH packet has been received for the configured DPD delay.
Délai	<input type="text" value="10"/>	Delay between sending peer acknowledgement messages. In IKEv2, a value of 0 sends no additional messages and only standard messages (such as those to rekey) are used to detect dead peers.
Échecs maxi	<input type="text" value="5"/>	Number of consecutive failures allowed before disconnecting. This only applies to IKEv1; in IKEv2 the retransmission timeout is used instead.

Enregistrer

Ensuite on valide et on affiche les entrée pour la P2 que l'on va devoir modifier

Ensuite on ajoute P2

	ID	Mode	Sous-réseau local	Sous-réseau distant	Protocole P2	Transformations P2	Méthodes d'authentification P2	Description	Actions P2
	+ Ajouter P2								

Pas grand-chose à modifier ici juste l'ip du LAN derrière le second routeur

VPN / IPsec / Tunnels / Modifier la phase 2

Tunnels Clients mobiles Clés pré-partagées Paramètres avancés

Informations Générales

Description VERS PFSENSE 2
 Une description peut être saisie ici à des fins de référence administrative (non analysée).

Désactivé Désactivez cette la phase 2 sans la supprimer de la liste.

Mode Tunnel IPv4

Phase 1 VERS PFSENSE 2 (IKE ID 1)

Réseaux

Réseau local LAN subnet / 0
 Type Adresse
 Local network component of this IPsec security association.

Traduction NAT/BINAT Aucun / 0
 Type Adresse
 Si NAT/BINAT est requis sur ce réseau, spécifiez l'adresse à traduire

Réseau distant Réseau 172.20.0.0 / 24
 Type Adresse
 Remote network component of this IPsec security association.

Proposition de phase 2 (SA/Key Exchange)

Protocole ESP
 Encapsulating Security Payload (ESP) performs encryption and authentication, Authentication Header (AH) is authentication only.

Algorithmes de chiffrement

- AES 128 bits
- AES128-GCM 128 bits
- AES192-GCM Auto
- AES256-GCM Auto

Algorithmes de hachage SHA1 SHA256 SHA384 SHA512 AES-XCBC

Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be avoided.

Groupe de clés PFS 14 (2048 bit)
 Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Expiration and Replacement

Life Time 3600
 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 3960.

Rekey Time 3240
 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.

Rand Time 360
 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.

Keep Alive

Pinger automatiquement l'hôte
 Sends an ICMP echo request inside the tunnel to the specified IP Address. Can trigger initiation of a tunnel mode P2, but does not trigger initiation of a VTI mode P2.

Keep Alive Enable periodic keep alive check
 Periodically checks to see if the P2 is disconnected and initiates when it is down. Does not send traffic inside the tunnel. Works for VTI and tunnel mode P2 entries. For IKEv2 without split connections, this only needs enabled on one P2.

[Enregistrer](#)

Ensuite on refait exactement la même config de l'autre coté en inversant certains parametre

Coter second routeur :

[Tunnels](#) [Mobile Clients](#) [Pre-Shared Keys](#) [Advanced Settings](#)**General Information**

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

Disabled Set this option to disable this phase1 without removing it from the list.

IKE Endpoint Configuration

Key Exchange version
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.

Internet Protocol
Select the Internet Protocol family.

Interface
Select the interface for the local endpoint of this phase1 entry.

Remote Gateway
Enter the public IP address or host name of the remote gateway. 

Phase 1 Proposal (Authentication)

Authentication Method
Must match the setting chosen on the remote side.

My identifier

Peer identifier

Pre-Shared Key
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.
[Generate new Pre-Shared Key](#)

Expiration and Replacement	
Life Time	<input type="text" value="28800"/> 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)
Rekey Time	<input type="text" value="25920"/> 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.
Reauth Time	<input type="text" value="0"/> 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.
Rand Time	<input type="text" value="2880"/> 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.
Advanced Options	
Child SA Start Action	<input type="text" value="Default"/> Set this option to force specific initiation/responder behavior for child SA (P2) entries
Child SA Close Action	<input type="text" value="Default"/> Set this option to control the behavior when the remote peer unexpectedly closes a child SA (P2)
NAT Traversal	<input type="text" value="Auto"/> Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls.
MOBIKE	<input type="text" value="Disable"/> Set this option to control the use of MOBIKE
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.
Split connections	<input type="checkbox"/> Enable this to split connection entries with multiple phase 2 configurations. Required for remote endpoints that support only a single traffic selector per child SA.
PRF Selection	<input type="checkbox"/> Enable manual Pseudo-Random Function (PRF) selection Manual PRF selection is typically not required, but can be useful in combination with AEAD Encryption Algorithms such as AES-GCM
Custom IKE/NAT-T Ports	<input type="text" value="Remote IKE Port"/> <input type="text" value="Remote NAT-T Port"/> UDP port for IKE on the remote gateway. Leave empty for default automatic behavior (500/4500). UDP port for NAT-T on the remote gateway. ⓘ
Dead Peer Detection	<input checked="" type="checkbox"/> Enable DPD Check the liveness of a peer by using IKEv2 INFORMATIONAL exchanges or IKEv1 R_U_THERE messages. Active DPD checking is only enforced if no IKE or ESP/AH packet has been received for the configured DPD delay.
Delay	<input type="text" value="10"/> Delay between sending peer acknowledgement messages. In IKEv2, a value of 0 sends no additional messages and only standard messages (such as those to rekey) are used to detect dead peers.
Max failures	<input type="text" value="5"/> Number of consecutive failures allowed before disconnecting. This only applies to IKEv1; in IKEv2 the retransmission timeout is used instead.
<input type="button" value="Save"/>	

P2:

VPN / IPsec / Tunnels / Edit Phase 2

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

General Information

Description PFSense 2 VERS PFSense 1
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 VERS PFSense 1 (IKE ID 1)

Networks

Local Network LAN subnet / 0
Type Address
Local network component of this IPsec security association.

NAT/BINAT translation None / 0
Type Address
If NAT/BINAT is required on this network specify the address to be translated

Remote Network Network 172.16.0.0 / 24
Type Address
Remote network component of this IPsec security association.

Phase 2 Proposal (SA/Key Exchange)

Même conf que l'autre pfsense

Protocol ESP
Encapsulating Security Payload (ESP) performs encryption and authentication, Authentication Header (AH) is authentication only.

Encryption Algorithms

- AES 128 bits
- AES128-GCM 128 bits
- AES192-GCM Auto
- AES256-GCM Auto
- CHACHA20-POLY1305

Hash Algorithms

- SHA1
- SHA256
- SHA384
- SHA512
- AES-XCBC

Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be avoided.

PFS key group 14 (2048 bit)
Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Expiration and Replacement

Life Time 3600
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 3960.

Rekey Time 3240
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.

Rand Time 360
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.

Keep Alive

Automatically ping host
Sends an ICMP echo request inside the tunnel to the specified IP Address. Can trigger initiation of a tunnel mode P2, but does not trigger initiation of a VTI mode P2.

Keep Alive Enable periodic keep alive check
Periodically checks to see if the P2 is disconnected and initiates when it is down. Does not send traffic inside the tunnel. Works for VTI and tunnel mode P2 entries. For IKEv2 without split connections, this only needs enabled on one P2.

Règles pare-feu

Il faut mettre en place des règles sur l'interface IPsec pour que le trafic puisse correctement passer car par défaut il est bloqué.

J'autorise tout en restreindra plus tard

PFSENSE 1

Pare-feu / Règles / Modifier

Modifier la règle de Pare-Feu

Action	Autoriser
<small>Choisissez que faire des paquets qui correspondent aux critères ci-dessous. Aide : La différence entre bloquer et rejeter est qu'avec 'Rejeter', un paquet (TCP, RST ou ICMP port unreachable pour UDP) est retourné à l'expéditeur, alors qu'avec 'Bloquer', le paquet est supprimé silencieusement. Dans tous les cas, le paquet est supprimé.</small>	
Désactivé	<input type="checkbox"/> Désactiver cette règle <small>Choisissez cette option pour désactiver cette règle sans la supprimer de la liste.</small>
Interface	IPsec <small>Choisissez l'interface d'où les paquets doivent provenir pour correspondre à cette règle.</small>
Famille d'adresse	IPv4 <small>Choisissez la version du protocole IP à laquelle cette règle s'applique.</small>
Protocole	Tous <small>Choisissez quel protocole IP cette règle devrait correspondre.</small>

Source

Source	<input type="checkbox"/> Invert match	tout	Source Address	/	
---------------	---------------------------------------	------	----------------	---	--

Destination

Destination	<input type="checkbox"/> Invert match	tout	Destination Address	/	
--------------------	---------------------------------------	------	---------------------	---	--

Options additionnelles

Journalise	<input type="checkbox"/> Journaliser les paquets gérés par cette règle <small>Suggestion : Le pare-feu a un espace de journalisation limité. N'activez pas la journalisation de tout. Si vous faites beaucoup de journalisation considérez l'utilisation d'un serveur syslog distant (voir la page Statut: Journaux système : Paramètres).</small>
Description	<input type="text"/> <small>Une description est proposée ici pour aider l'administrateur. Un maximum de 52 caractères sera utilisé dans l'ensemble de règles et affiché dans le journal du pare-feu.</small>

Options Avancées

PFSENSE 2

Firewall / Rules / Edit

Edit Firewall Rule

Action
 Choose what to do with packets that match the criteria specified below.
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

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

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

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

Protocol
 Choose which IP protocol this rule should match.

Source
 Invert match / /

Destination
 Invert match / /

Extra Options

Log Log packets that are handled by this rule
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Ensuite ne pas appuyer sur Disable pour passer en Enable car sa désactive s'active rien.

VPN / IPsec / Tunnels

Tunnels Clients mobiles Clés pré-partagées Paramètres avancés

Tunnels IPsec

ID	IKE	Passerelle distante	Mode	Protocole P1	Transformations P1	P1 DH-Group	Description P1	Actions
<input type="checkbox"/> <input type="button" value="Disable"/>	1	V2 WAN 10.0.0.252		AES (128 bits)	SHA256	14 (2048 bit)	VERS PFSENSE 2	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Ensuite pour vérifier que le VPN fonctionne correctement.

pfSense COMMUNITY EDITION

Système Interfaces Pare-feu Services VPN État Diagnostics Aide

État / IPsec / Vue d'ensemble

Vue d'ensemble Baux SADs SPDs

État IPsec

ID	Description	Local	Distant	Règle	Algo	État
				IPsec		

Ensuite on doit voir que les phases fonctionnent

ID	Description	Local	Distant	Rôle	Chrono	Algo	État
con1 #3	VERS PFSENSE 2	ID: 10.0.0.253 Host: 10.0.0.253:500 SPI: 23c2c482d6290d38	ID: 10.0.0.252 Host: 10.0.0.252:500 SPI: 91d4e3eb28cb5a08	IKEv2 Responder	Rekey: 23454s (06:30:54) Reauth: Désactivé	AES_CBC (128) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	Established Il y a 113 secondes (00:01:53) Déconnecter P1
ID	Description	Local	SPI(s)	Distant	Temps	Algo	Statistiques
con1: #2	VERS PFSENSE 2	172.16.0.0/24	Local: ce580bef Distant: c8d0baa3	172.20.0.0/24	Rekey: 2852s (00:47:32) Life: 3564s (00:59:24) Install: 36s (00:00:36)	AES_GCM_16 (128) MODP_2048 IPComp: Aucun	Octets entrants: 180 (180 B) Paquets entrants: 3 Octets sortants: 348 (348 B) Paquets sortants: 3 Installed Déconnecter P2

Si la une fonctionne sans la deux peut être d'un côté ou l'autre elle est désactivé ou il y'a un soucis dans la conf mais si les deux machine sur leur interfaces WAN ce ping et que la conf est correct il n'ya pas de raison que ça ne fonctionne pas.

Test

Ping depuis 172.20.0.0 vers 172.16.0.0

```
C:\windows\system32>ping 172.16.0.250

Envoi d'une requête 'Ping' 172.16.0.250 avec 32 octets de données :
Réponse de 172.16.0.250 : octets=32 temps=1 ms TTL=126
Réponse de 172.16.0.250 : octets=32 temps=1 ms TTL=126
Réponse de 172.16.0.250 : octets=32 temps<1ms TTL=126

Statistiques Ping pour 172.16.0.250:
    Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

Depuis 172.16.0.0 vers 172.20.0.0

```
C:\Users\Administrateur>ping 172.20.0.1

Envoi d'une requête 'Ping' 172.20.0.1 avec 32 octets de données :
Réponse de 172.20.0.1 : octets=32 temps=1 ms TTL=126
Réponse de 172.20.0.1 : octets=32 temps<1ms TTL=126
Réponse de 172.20.0.1 : octets=32 temps<1ms TTL=126
Réponse de 172.20.0.1 : octets=32 temps=1 ms TTL=126

Statistiques Ping pour 172.20.0.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
```

+ tracert

```
C:\Users\Administrateur>tracert 172.20.0.1
Détermination de l'itinéraire vers 172.20.0.1 avec un maximum de 30 sauts.

 1  <1 ms  <1 ms  <1 ms  172.16.0.254
 2  *      *      *      Délai d'attente de la demande dépassé.
 3  <1 ms  <1 ms  <1 ms  172.20.0.1

Itinéraire déterminé.
```

Voilà maintenant nous savons comment mettre en place IPsec entre deux firewall pfsense.