# VPN de site à site IPsec avec clés pré-partagées

## Introduction

Un tunnel IPsec de site à site interconnecte deux réseaux comme s'ils **étaient directement connectés par une paserelle telle qu’un routeur**.   
Les systèmes du site A peuvent atteindre des serveurs ou d'autres systèmes du site B, et vice versa.

Ce **trafic peut également être régulé à l’aide de règles de pare-feu**, comme pour toute autre interface réseau.

Si plusieurs clients se connectent à un autre site à partir du même emplacement contrôlé, un **tunnel de site à site sera** **probablement plus efficace**, sans parler de **plus pratique** et **plus facile à prendre en charge**.

Avec un tunnel de site à site, les **systèmes de l'un ou l'autre réseau n'ont pas besoin de savoir qu'un VPN existe**.   
**Aucun logiciel client n'est nécessaire** et tout le **travail du tunnel est géré par les points de terminaison du tunnel**.

C'est également une bonne solution pour les ap**pareils qui prennent en charge le réseau mais ne gèrent pas les connexions VPN** telles que les **imprimantes**, les **caméras** et autres **matériels intégrés**.

### IPsec

IPsec est souvent un composant de VPN, il est à l'origine de son aspect sécurité (canal sécurisé ou *tunneling*).  
La mise en place d'une architecture sécurisée à base d'IPsec est détaillée dans la RFC 43012.

IPSec présente en outre l'intérêt d'être une solution évolutive puisque les algorithmes de chiffrement et d'authentification à proprement parler sont spécifiés séparément du protocole lui-même.

* IPSec peut être **indépendant des algorithmes de chiffrement** ;
* IPSec doit être **indépendant des mécanismes d’échange de** clés ;
* IPSec doit **supporter les différents mécanismes d’authentification déjà utilisés** (comme Kerberos).

IPSec est un donc gabarit où on insère …

* des **algorithmes de chiffrement**
* et
* des **mécanismes d’échange de clés**.

Il offre également une conformité au contexte légaux particuliers.

IPSec possède cependant l'inconvénient inhérent à sa flexibilité : sa grande complexité rend son implémentation délicate.   
Il propose plusieurs options de configuration, affectant les performances et la sécurité des connexions IPsec.

#### Modes IPSec

Une communication entre deux hôtes protégée par IPSec est susceptible de **fonctionner suivant deux modes différents** …

* le **mode transport**Communication IPSec bout en bout  
  et
* le **mode tunne**l  
  Communication IPSec au moyen d’une passerelle de sécurité.

Le mode transport offre essentiellement une **protection aux protocoles de niveau supérieur**.   
Il est utilisé par les **stations et par les serveurs pour sécuriser les flux de bout en bout**.   
Dans le mode transport, l’**entête** **du paquet IP sécurisé n’est pas modifié** et est **expédié en clair sur le réseau**.

Dans le mode transport, ce sont **uniquement les données transférées** (la partie payload du paquet IP) **qui sont chiffrées** **et/ou authentifiées**. Le **reste du paquet IP demeure intact** et de ce fait le routage des paquets n'est pas modifié. Néanmoins, les **adresses IP ne pouvant pas être modifiées par le NAT sans corrompre le condensé** (hash) de l'en-tête AH généré par IPsec, **AH ne peux pas être utilisé** dans un **environnement nécessitant ces modifications** d'en-tête.

Le mode transport est utilisé pour les **communications dites hôte à hôte** (*Host-to-Host*).

Le mode tunnel permet quant à lui d'**encapsuler** **des datagrammes IP dans d'autres datagrammes IP** dont le **contenu** **est protégé**.

L'intérêt majeur du mode tunnel est qu'il rend la **mise en place de passerelles de sécurité** qui …

* traitent toute la partie IPSec d'une communication  
  **et**
* transmettent les datagrammes épurés de leur partie IPSec à leur destinataire réel.

En mode tunnel, c'est la **totalité du paquet IP qui est chiffré et/ou authentifié**.   
Le paquet est ensuite **encapsulé dans un nouveau paquet IP avec un nouvel en-tête IP**.

Au contraire du mode transport, ce mode **supporte donc bien la traversée de NAT** quand le protocole ESP est utilisé.

Le mode tunnel est **utilisé pour créer des réseaux privés virtuels** (VPN) permettant la **communication de réseau à** **réseau** (c.a.d. entre deux sites distants), d'**hôte** **à réseau** (accès à distance d'un utilisateur) ou bien d'**hôte à hôte** (messagerie privée.)

Le mode tunnel, surtout utilisé par les **équipements de base de réseau**, va permettre de faire du *tunneling*.   
Le **paquet d’origine est complètement encapsulé dans un nouveau paquet IP.**   
Les données du paquet IPSec sont en fait le paquet d’origine en entier et non pas les données du paquet d’origine.

Il est également **possible d'encapsuler une communication IPsec en mode tunnel ou transport** dans une **autre** **communication IPsec en mode tunnel**, elle-même traitée par une passerelle de sécurité, qui transmet les datagrammes après suppression de leur première enveloppe à un hôte traitant à son tour les protections restantes ou à une seconde passerelle de sécurité.

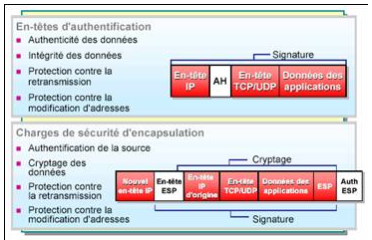
#### Protocoles AH et ESP

IPSec fournit deux protocoles de base …

* **AH** (*Authentication Header*)

et

* **ESP** (*Encapsulation Security Paylod*)



*AH et ESP*

**AH (*Authentication Header*)**AH est le premier et le plus simple des protocoles de protection des données qui font partie de la spécification IPsec.   
Il est détaillé dans la **RFC 2402**.

Il a pour vocation de garantir …

* l’**authentification** ;
* l’**unicité** (optionnelle, à la discrétion du récepteur)   
  et
* l’**intégrité**

Ce mode permet **uniquement de réaliser l’authentification et la vérification de l’intégrité des paquets**.   
**Aucune confidentialité** dans les données n’est assurée.

Les **services fournis** **par** AH sont les suivants …

* **Authentification de l’émetteur des paquets** ;
* **Intégrité des données** ;
* **Détection d’intrusion dans un flux**.

Le mode AH est **moins consommateur de ressources** **machine** que le mode ESP dont le rôle est de chiffrer les données.

**ESP (*Encapsulation Security Paylod*)**

ESP est le second protocole de protection des données qui fait partie de la spécification IPsec.   
Il est détaillé dans la **RFC 2406**.

Contrairement à AH, **ESP ne protège pas les entêtes des datagrammes IP utilisés** pour transmettre la communication. **Seules les données sont protégées**.

ESP assure …

* la **confidentialité des données** (optionnelle)
* l’**authentification** (optionnelle, mais obligatoire en l’absence de confidentialité)
* l’**unicité** (optionnelle, à la discrétion du récepteur).
* l’**integrité**

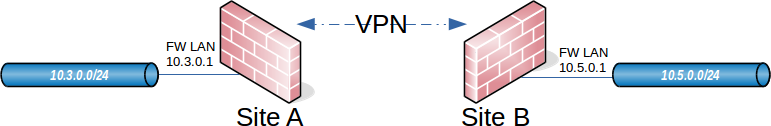
## Configuration de site à site

La clé pour créer un tunnel IPsec fonctionnel est de **s'assurer que les deux côtés ont des paramètres correspondants** **pour l'authentification**, le **chiffrement**, **...**

Avant de débuter, on doit **noter les adresses IP WAN locales et distantes**, ainsi que les sous**-réseaux internes locaux et distants** qui seront acheminés à travers le tunnel.   
Hormis certaines descriptions du tunnel, ces informations et **les autres** **paramètres de connexion seront identiques**.

Les paramètres suivants seront pris en charge …

* Installation de **2 pfSense** (2 interfaces - WAN et LAN) ;
* Installation de **2 hôtes clients DHCP** (avec interfaces graphiques).
* **Hôte01** (Interface graphique)  
  Client DHCP dans le **réseau 10.3.0.0/24** Segment réseau – **Montréal**
* **Hôte02** (Interface graphique)  
  Client DHCP dans le **réseau 10.5.0.0/24** Segment réseau – **Québec**
* **pfSense01 (Site A)**   
  Interface WAN DHCP - Par pont (*bridge ou NAT*)  
  Interface LAN 10.3.0.1/24 Segment réseau – **Montréal**
* **pfSense02 (site B)**   
  Interface WAN DHCP - Par pont (*bridge ou NAT*)  
  Interface LAN 10.5.0.1/24 Segment réseau – **Québec**



La configuration d’un tunnel IPsec site à site de fait en deux phases …

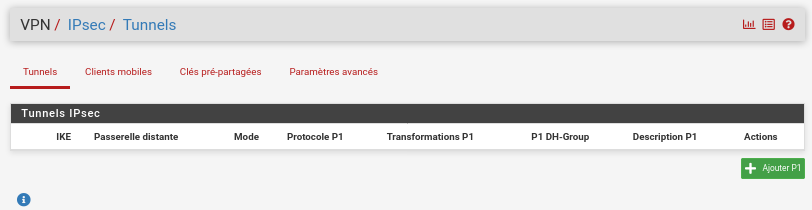
* **Phase 1**Configuration des deux extrémités du tunnel ;
* **Phase 2**  
  Configuration des algorithmes de chiffrement et de hachage ainsi que les données de temporisation.

## Configuration du Site A

On débute par configurer le tunnel et ses paramètres associés sur le pare-feu du site A.

### Phase 1 Configuration des deux extrémités du tunnel

Pour ajouter une nouvelle phase IPsec 1 …  
**>> VPN > IPsec > Ajouter P1** …



On complète les paramètres suivants de la fenêtre suivante.

#### Section – Informations générales

Une image contenant texte

Description générée automatiquement

La section **Informations générales** contient les informations générales de la phase 1.  
Les éléments en gras sont obligatoires.

**Désactivée** (*Disabled*)  
Indication si le tunnel est opérationnel ou non ;

**Version d'échange de clés** (*Key Exchange version*)  
Spécification de l’utilisation d’IKEv2 ou d’IKEv1.   
IKEv2 est une meilleure pratique lorsqu'il est pris en charge par les deux points de terminaison du tunnel ;

**Protocole Internet** (*Internet Protocol*)  
Choix de la version du protocole IP.  
IPv4 dans la plupart des cas, sauf si les deux WAN ont IPv6, auquel cas l'un ou l'autre type peut être utilisé ;

**Interface**  
Cette option permet de déterminer l’interface de sortie vers la passerelle distante.  
Habituellement, elle est définie sur WAN ;

**Passerelle distante** (*Remote Gateway*) \*Précision de l’adresse IP ou le nom DNS de la passerelle distante.  
Habituellement, on retrouve ici l'adresse WAN du site distant ;

**Description**  
Texte décrivant l'objet ou l'identité du tunnel.   
La meilleure pratique consiste à mettre le nom du site distant dans cette case.  
Il peut être également pratique d’ajouter de brefs détails sur le but du tunnel pour fins de documentations.

\* La valeur du point de terminaison distant (Passerelle distante) varie selon le contexte.

#### Section – Proposition de phase 1 (Authentification)

Une image contenant texte

Description générée automatiquement

Cette section contrôle les paramètres IPsec de la phase d’authentification.   
Les valeurs par défaut sont celles recommandées pour la plupart de ces paramètres car elles simplifient le processus.

**Méthode d'authentification** (*Authentification Method*)  
Indication du choix de l’authentification par mot de passe ou par certificat.  
La valeur par défaut, Mutual PSK, exige la création d’un mot de passe partagé pour les deux sites.  
Il est également possible d’utiliser des certificats comme mécanique d’authentification ;

**Identifiant de l’hôte local** (*My identifier*)  
Identification du point de terminaison distant.  
Les choix peuvent être une identification LDAP, DNS, …  
De manière générale, on utilise l’adresse IP ;

**Identifiant du pair** (*Peer Identifier*)Identification du point de terminaison distant.  
Les choix peuvent être une identification LDAP, DNS, …  
De manière générale, on utilise l’adresse IP ;

**Clé Pré-Partagée** (Pre-shared Key)  
Définition de la clé (mot ou phrase de passe) qui sera partagé entre les deux points de terminaison du tunnel.  
Il est préférable d’utiliser une clé complexe, d'au moins 10 caractères contenant un mélange de lettres majuscules et minuscules, de chiffres et de symboles.   
Il est également possible de générer une nouvelle clé pré-partagée afin de remplir automatiquement le champ avec une longue chaîne aléatoire pouvant être utilisée comme clé pré-partagée   
  
**Avertissement** …  
C'est le paramètre le plus important de la configuration.   
IPsec utilise des clés pré-partagées et le tunnel peut être rompu si ce dernier utilise une clé faible.  
La même clé (exacte) doit être saisie dans la configuration du tunnel pour le site distant lors de sa configuration.

#### Section – Proposition de phase 1 (Algorithmes de chiffrement)

Une image contenant texte

Description générée automatiquement

Il existe de nombreuses options pour les algorithmes de chiffrement sur la phase 1 (et la phase 2).

Le choix de l’algorithme de chiffrement dépend du périphérique auquel le tunnel se connectera et de son matériel.   
De manière générale, AES-GCM est le chiffrement le plus souhaitable.   
Lors de la connexion à des appareils tiers, AES avec une longueur de clé de 128 bits est un choix courant sur les points de terminaison qui ne prennent pas en charge AES-GCM.

Plusieurs combinaisons de ces options peuvent être définies à l'aide du bouton **Ajouter** **un algorithme**.

**Algorithme de chiffrement** (*Encryption Algorithm*)  
**Longueur de la clé** (*Key Lenght*)  
Sélection de l’algorithme de chiffrement ainsi que la longueur de la clé pour l’établissement de la connexion entre les deux points de terminaison du tunnel.   
Si les deux côtés prennent en charge AES-GCM, il est préférable d’utiliser AES128-GCM avec une longueur de clé de 128 bits. Ce choix combine un chiffrement fort et un hachage suffisant ;

**Algorithme de hachage** (*Hash*)  
Sélection de l’algorithme de hachage qui est utilisé avec IPsec afin de vérifier l'authenticité des données de paquets et en tant que fonction pseudo-aléatoire (PRF).   
Le meilleur choix pour une utilisation avec AES-GCM est AES-XCBC ;

**Groupe de clés DH** (*DH Group*)  
Sélection des groupes Diffie-Hellman (DH).  
Les groupes DH déterminent la force de la clé utilisée dans le processus d'échange de clé.  
La meilleure pratique consiste à utiliser le groupe DH 14 (2048 bits) ou supérieur si les deux côtés le prennent en charge. Évitez d'utiliser les groupes 1, 2, 22, 23 et 24 car ils n'offrent pas une sécurité suffisante.

#### Section – délais d’expiration de de remplacement

Une image contenant table

Description générée automatiquement

La durée de vie totale pour la phase 1 définit la fréquence à laquelle la connexion sera valide ou authentifiée par le démon IPsec, en secondes.

**Avertissement** …  
Il faut être prudent pour la définition de ces valeurs.   
Des valeurs incorrectes ou non optimales peuvent entraîner des problèmes tels que l'échec de la renégociation des tunnels ou dupliquer des associations de sécurité en double.

Les valeurs spécifiques de ces champs dépendent du mode IKE et des mécanismes pris en charge par les deux points de terminaison du tunnel, mais dans la plupart des cas, la définition de la valeur de durée de vie permettra au pare-feu de choisir la meilleure option.

**Durée de vie** (*Life Time*)  
Définition de la durée de vie de l'IKE SA, en secondes, et après laquelle elle expirera.   
Cette valeur doit être supérieure à ***Rekey Time*** et ***Reauth Time*** et ne peut pas être définie sur la même valeur.  
Le nombre total de secondes (28 800) qui est la valeur proposée par défaut est un bon équilibre entre des ressaisies fréquentes sans être trop agressif.  
**Conseil** …  
On définit un point de terminaison sur cette valeur recommandée, mais il est préférable de spécifier une durée de vie plus élevée sur l'autre point de terminaison d'au moins 10 % (par exemple 31680) pour éviter les chevauchements.  
Si elle est laissée vide, la valeur par défaut est 110 % de Rekey Time ou Reauth Time , selon la valeur la plus élevée.

**Temps de recléage** (*Rekey Time*)  
Définition du temps, en secondes, avant que le démon IPsec ne tente d'établir un nouveau jeu de clés pour l'association de sécurité IKE.   
Cette option est uniquement prise en charge par IKEv2, et constitue le meilleur choix pour une utilisation avec IKEv2.  
Rekey fonctionne sans interruption et permet aux deux points de terminaison du tunnel de passer de manière transparente à de nouvelles clés à la volée.   
On laisse ce champ vide afin de calculer automatiquement la valeur en fonction de 90 % de la durée de vie.  
On peut également choisir la valeur 0 pour désactiver la nouvelle saisie.

**Heure de Réauth** (*Reauth Time*)Définition du temps, en secondes, avant qu'une SA IKE ne soit détruite et recréée à partir de zéro par le démon IPsec, y compris l'authentification.   
On laisse ce champ vide afin de calculer automatiquement la valeur en fonction de 90 % de la durée de vie.  
On peut également choisir la valeur 0 pour désactiver la réauthentification.

**Temps de randomisation** (*Rand Time*)  
Spécification de l’introduction d’un un caractère aléatoire dans le processus de renouvellement de clé ou de réauthentification pour éviter que les deux points de terminaison tentent de renégocier simultanément.  
Une valeur aléatoire jusqu'à ce montant sera soustraite de Rekey Time ou Reauth Time pour chaque renégociation programmée afin de réduire les risques de collisions.  
Si elle est laissée vide, la valeur par défaut est 10 % de la durée de vie.  
On peut également choisir la valeur 0 pour désactiver le caractère aléatoire.

**Avertissement** …  
La désactivation de Rand Time augmente la probabilité d'une renégociation simultanée, ce qui peut entraîner des associations de sécurité en double.

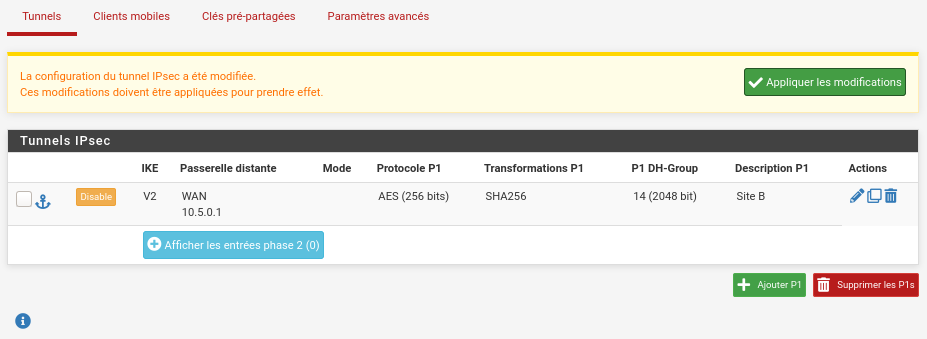
Comme dernière étape de la phase 1, on clique sur **Enregistrer** afin de terminer la configuration de la phase 1.

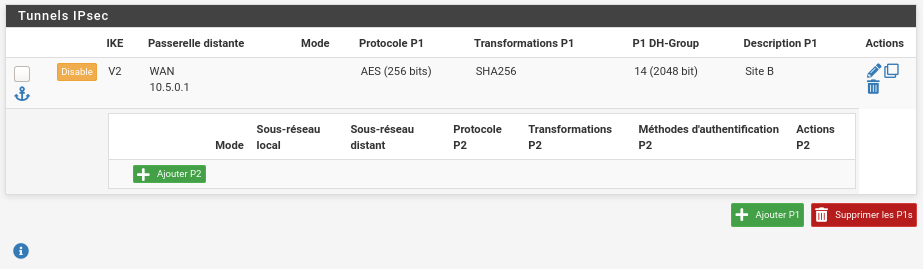
### Phase 2 Configuration des algorithmes de chiffrement et de hachage ainsi que les données de temporisation

Avec la phase 1 terminée, on doit créer une nouvelle définition de phase 2 pour le VPN.

Les paramètres de phase 2 d'un tunnel IPsec régissent la façon dont le tunnel gère le trafic (par exemple, basé sur une politique ou sur un itinéraire) ainsi que le chiffrement de ce trafic.

Afin de compléter la phase 2 …  
On clique sur **Afficher les entrées de la phase** **2**.  
On clique sur **Ajouter P2** pour ajouter une nouvelle entrée de phase 2.





#### Section Information générale

Une image contenant texte

Description générée automatiquement

**Remarque** …  
Les paramètres de la phase 2 peuvent varier davantage que ceux de la phase 1.

**Désactivée**  
Interrupteur marche/arrêt pour cette entrée de phase 2 uniquement.  
Indique si le tunnel est opérationnel ou non ;

**Mode**  
Le mode IPsec contrôle la façon dont le tunnel gère le trafic.   
**Tunnel IPv4**Tunnel basé sur des règles qui acheminera le trafic entre les réseaux IPv4 correspondant au réseau local et au réseau distant spécifiés ;  
**Tunnel IPv6**Tunnel basé sur des règles qui acheminera le trafic entre les réseaux IPv6 correspondant au réseau local et au réseau distant spécifiés ;  
**Transport**  
Mode qui chiffre tout le trafic entre les points de terminaison.   
Le réseau local et le réseau distant ne sont pas définis pour le mode de transport, ils assument les adresses en fonction des paramètres de la phase 1 ;  
**Routé (VTI)**  
IPsec routé à l'aide d'interfaces de tunnel virtuel.   
Le réseau local et le réseau distant définissent les adresses utilisées par le pare-feu pour l'interface VTI.

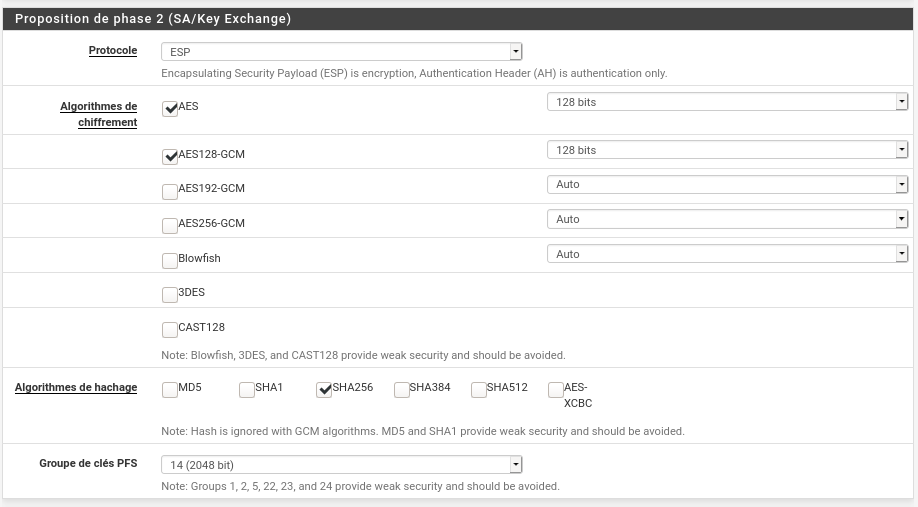
**Réseau local**Il est possible de définir quel sous-réseau ou hôte est accessible de l'autre côté du tunnel VPN.   
Il s'agit généralement du réseau local ou d'un autre sous-réseau interne pour le VPN, mais il peut également s'agir d'une seule adresse IP si un seul client a besoin d'utiliser le tunnel.   
Le plus souvent, cela est défini sur LAN subnet , ce qui signifie que l'ensemble du LAN sera accessible à partir du réseau distant.

**NAT/BINAT**Cette option est utilisé si on doit utiliser la fonctionnalité de translation d’adresse ;

* **Réseau à distance**Le réseau à distance est l’autre extrémité du tunnel.  
  On règle la valeur sur le réseau du site B (selon l’adresse IP WAN) ;
* **Description**  
  Une brève description du ou des réseaux impliqués dans cette entrée de phase 2.

#### Section – Proposition de phase 2 (SA/Key Exchange)

Le reste des paramètres de la phase 2 concernent le chiffrement du trafic.



Les algorithmes de chiffrement et les algorithmes de hachage peuvent tous deux être configurés afin d’autoriser plusieurs options dans la phase 2, et les deux parties négocieront et s'accorderont sur les paramètres tant que chaque partie possède au moins une de chacune en commun.

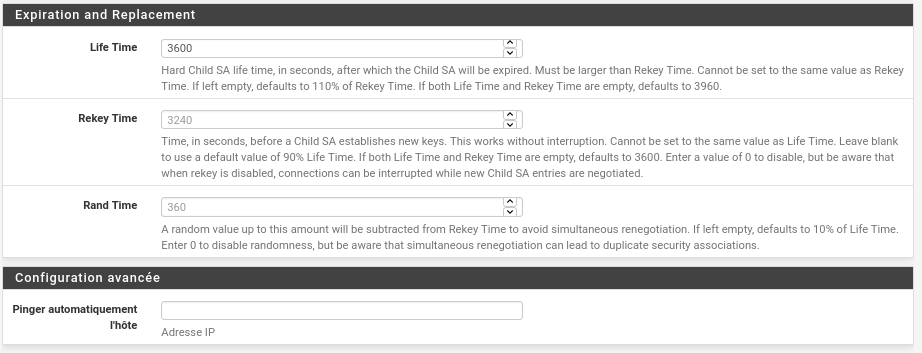
Dans certains cas, cela peut être une bonne chose, mais il est généralement préférable de limiter cela aux seules options spécifiques souhaitées des deux côtés.

* **Protocole**  
  Choix du protocole Ipsec.  
  On fait référence aux protocole ESP (Encapsulating Security Payload) ou AH (Authentification Header)  
  Contrôle la façon dont IPsec protège son trafic.  
  ESP chiffre le trafic avant de l'envoyer à l'homologue. Dans presque toutes les circonstances, l'ESP est le bon choix. Il est plus sécure, quoique plus onéreux en ressources machine, d’utiliser ESP pour le chiffrement.  
  AH fournit l'assurance que le trafic provient d'une source fiable mais ne fournit pas de cryptage. Il est rarement utilisé en pratique.  
  Des algorithmes de hachage sont utilisés avec IPsec afin de vérifier l'authenticité des données de paquets et en tant que fonction pseudo-aléatoire (PRF) ;
* **Algorithme de chiffrement**  
  La meilleure pratique consiste à utiliser un chiffrement tel que AES-GCM s'il est pris en charge par les deux points de terminaison. On sélectionne AES256-GCM avec une longueur de clé de 128 bits.   
  Sinon, utilisez AES 256 ou le chiffrement le plus puissant pris en charge par les deux points de terminaison.
* **Algorithme de hachage**Si AES-GCM est sélectionné pour Encryption Algorithm, on ne sélectionne aucun hachage.  
  Sinon, utilisez SHA256 ou le hachage pris en charge par les deux côtés est le plus puissant.
* **PFS**  
  *Perfect Forward Secrecy* peut aider à protéger contre certaines attaques clés.  
  Il est toutefois facultatif.

#### Section Proposition de l’échange des clés

Les derniers paramètres sont ceux de la durée de vie des différents paramètres du tunner.

* **Durée de vie  
  Rekey Time  
  Rand Time**Similaire aux valeurs de la phase 1, de manière générale, on laisse ces paramètres tels quels.



Comme dernière étape, on clique sur **Enregistrer** afin de terminer la configuration de la phase 1.

Il faut également **Appliquer les nouvelles règles** comme habituellement.

Ajouter la notion de ping

#### Règles de pare-feu

Le tunnel du site A terminé, il faut par la suite définir des règles de pare-feu afin de permettre au trafic du réseau du site B d'entrer à l’aide du tunnel IPsec.

Pour ce faire …

**>> Pare-feu > Règles > IPsec**   
On ajoute des règles afin de transmettre le trafic du côté distant du VPN.

Les règles peuvent être aussi permissives que souhaité (autoriser n'importe quel protocole de n'importe où vers n'importe où) ou restrictives (autoriser TCP d'un certain hôte sur le site B à un certain hôte sur le site A sur un certain port).

Comme pour les autres règles de pare-feu, les connexions sont vérifiées lors de l'entrée dans le pare-feu, de sorte que la source de tout le trafic sur les règles de l'onglet IPsec sera les réseaux VPN distants, tels que ceux du site B.

On doit s’assurer que les adresses source sur les règles de pare-feu correspondent aux adresses du site B, telles que 10.5.0.0/24. Les adresses de destination seront sur le site A, telles que 10.3.0.0/24.



Source .. LanNEt

Destination Network autre network

Protocole any

### Configuration du Site B

Maintenant que le site A est configuré, il est temps de configurer le site B.   
On répété simplement le processus sur le point de terminaison du site B pour ajouter un tunnel.

Seules quelques parties de cette configuration seront différentes du site A.  
Il s’agit des paramètres de phase 1 pour l'adresse WAN, la description, la durée de vie, l'action de démarrage de la SA enfant et l'action de fermeture de la SA enfant.

On ajoute une entrée de phase 1 au pare-feu du site B en utilisant les mêmes paramètres que ceux utilisés sur le site A mais avec les différences suivantes …

* **Passerelle distante**L'adresse WAN du site A (selon l’adresse du WAN)
* **Description**  
  Site A ;
* **Durée de vie**Au moins 10 % plus élevé que le site A, soit 31680 ;
* **Action de démarrage de l'enfant SA**On définit cette option sur Aucun (répondeur uniquement) afin que ce point de terminaison ne démarre pas tout seul, mais attende que le site A se lance.
* **Action de fermeture de l'enfant SA**On définit ce point de terminaison sur Fermer la connexion et on efface SA afin que la phase 2 ne se reconnecte pas automatiquement, car c’est le site A qui va gérer cette étape.

Comme dernière étape, on clique sur **Enregistrer** afin de terminer la configuration de la phase 1.

On ajoute par la suite une entrée de phase 2 au pare-feu du site B en utilisant les mêmes paramètres que ceux utilisés sur le site A mais avec les différences suivantes …

* **Sous-réseau distant**Le réseau du site A, dans ce cas 10.3.0.0/24;
* **Description**  
  Connexion au Site B ;
* **Durée de vie**Au moins 10 % plus élevé que le site A, soit 5400

On sauvegarde la configuration de la phase 2.

On s’assure d’appliquer les modifications au tunnels IPsec.

Comme pour le site A, des règles de pare-feu doivent également être ajoutées afin de permettre au trafic sur le tunnel de passer du site A au site B …  
**>> Pare-feu > Règles > IPsec**   
On ajoute des règles afin de transmettre le trafic du côté distant du VPN.

Les règles peuvent être aussi permissives que souhaité (autoriser n'importe quel protocole de n'importe où vers n'importe où) ou restrictives (autoriser TCP d'un certain hôte sur le site B à un certain hôte sur le site A sur un certain port).

Comme pour les autres règles de pare-feu, les connexions sont vérifiées lors de l'entrée dans le pare-feu, de sorte que la source de tout le trafic sur les règles de l'onglet IPsec sera les réseaux VPN distants, tels que ceux du site B.

Cette fois, la source du trafic serait le site A, destination le site B.

## Vérification de l'état du tunnel

Les deux tunnels sont maintenant configurés et actifs.   
On peut vérifier l'état IPsec …

**>> État > IPsec**   
Une description du tunnel s'affiche ainsi que son état.  
Il est donc alors possible d’établir la connexion avec le bouton …



Une confirmation de la connexion devrait indiquer le bon fonctionnement du tunnel ...

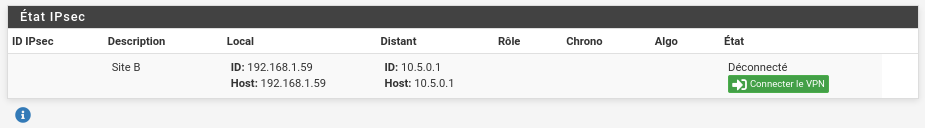
Une image contenant texte

Description générée automatiquement

**Remarque** …  
La connexion doit être demandée par les deux bouts du tunnel.

Si le tunnel n'est pas répertorié comme **Établi**, il peut y avoir un problème d'établissement du tunnel.   
La raison la plus probable est qu'aucun trafic n'a tenté de traverser le tunnel.

Un bouton de connexion est proposé sur cet écran qui tentera d'initier le tunnel.   
On clique sur le bouton Connect VPN afin de tenter d'ouvrir le tunnel.



Si le bouton de connexion n'apparaît pas, on peut essayer d'envoyer une requête ping à un système du sous-réseau distant sur le site B à partir d'un périphérique à l'intérieur du réseau local de phase 2 sur le site A (ou vice versa).  
On peut alors vérifier si le tunnel s'établit.

En cas de non-fonctionnement, les journaux IPsec offrent généralement une explication.   
On peut les retrouver …  
**>> État > Journaux système** **> IPsec**.

On doit vérifier l'état et les journaux sur les deux sites.

## En résumé

**Phase 01  
pfSense 01**Établissement du tunnel WAN (b.b.b.b -a.a.a.a)  
**pfSense02**Établissement du tunnel WAN (a.a.a.a - b.b.b.b)

**Phase 02  
pfSense 01**Établissement du tunnel LAN (10.3.0.0)  
**pfSense02**Établissement du tunnel LAN (10.5.0.0)

Vérification des règles de pare-feu  
Vérification à l'aide d’un ping si la communication passe  
Vérification si une requête HTTP passe d'un hôte à l'autre

Bonne référence

https://www.provya.net/?d=2020/02/11/08/22/01-pfsense-configurer-un-vpn-ipsec-site-a-site