Tunnel IPSEC Pfsense

Introduction

Dans le cadre de la sécurisation des échanges inter-sites, la mise en place d'un tunnel IPsec sur pfSense permet de chiffrer et d'authentifier le trafic réseau entre deux réseaux distants. IPsec (Internet Protocol Security) est un ensemble de protocoles garantissant la confidentialité, l'intégrité et l'authenticité des données transitant sur des réseaux non sécurisés, comme Internet. Grâce à pfSense, une solution pare-feu open source, il est possible de configurer et d'administrer facilement ce tunnel sécurisé. La procédure ci-dessous détaille les étapes de création et de paramétrage d'une nouvelle connexion IPsec, depuis l'accès à l'interface d'administration jusqu'à la configuration des phases 1 et 2, afin d'établir une liaison fiable et sécurisée entre vos différents sites.

Présentation du VPN IPSec

Les VPN de type IPSec permettent d'établir un tunnel sécurisé entre des sites distants, assurant ainsi la confidentialité et l'intégrité des échanges de données sur des réseaux non sécurisés. Les principales caractéristiques de ce type de VPN sont :

- **Chiffrement et Confidentialité :**
  L'utilisation d'algorithmes robustes (comme AES ou 3DES) garantit que les données transitant par le tunnel sont protégées contre toute interception.
- **Intégrité et Authentification :**
  Grâce à des mécanismes de hachage (SHA-1, SHA-256, etc.) et à l'authentification par clés pré-partagées ou certificats numériques, le VPN IPSec vérifie que les données n'ont pas été altérées et que les entités communiquant sont bien légitimes.
- **Négociation des Clés (IKE) :**
  Le protocole IKE (Internet Key Exchange) permet d'établir de manière sécurisée les paramètres de chiffrement et d'authentification, facilitant ainsi l'établissement du tunnel.
- **Modes de Fonctionnement :**
  En mode transport, seul le contenu du paquet IP est chiffré, tandis qu'en mode tunnel, l'intégralité du paquet est encapsulée. Ce dernier mode est particulièrement adapté aux connexions inter-sites.

Thomas Kireche

- **Interopérabilité et Flexibilité :**
  IPSec est une norme largement adoptée, compatible avec une grande diversité de systèmes d'exploitation et d'appareils réseau, ce qui en fait une solution idéale pour des infrastructures hétérogènes.

Usage du VPN IPSec

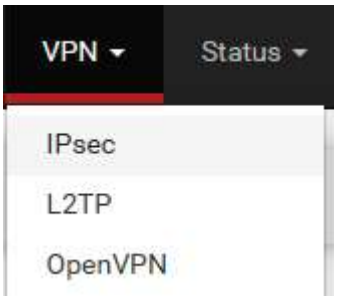
L'usage du VPN IPSec s'inscrit dans une démarche de sécurisation des communications entre des sites géographiquement dispersés ou pour offrir un accès sécurisé aux utilisateurs distants. Ses applications incluent :

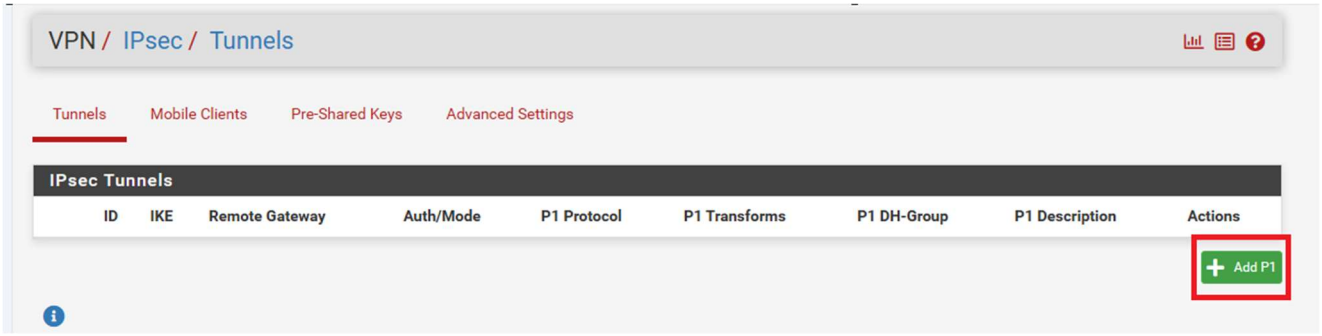
- **Sécurisation des échanges inter-sites :**
  En chiffrant le trafic entre les différents sites, le VPN IPSec assure la continuité des opérations tout en protégeant les informations sensibles de l'entreprise.
- **Accès distant sécurisé :**
  Les employés ou partenaires externes peuvent accéder aux ressources internes via un tunnel VPN sécurisé, garantissant une connexion fiable même sur des réseaux publics.
- **Protection contre les intrusions :**
  La combinaison de chiffrement, d'authentification et de vérification d'intégrité réduit considérablement les risques d'interception et de manipulation des données.

Configuration Tunnel Ipsec

1.1. Accéder à l'interface d'administration

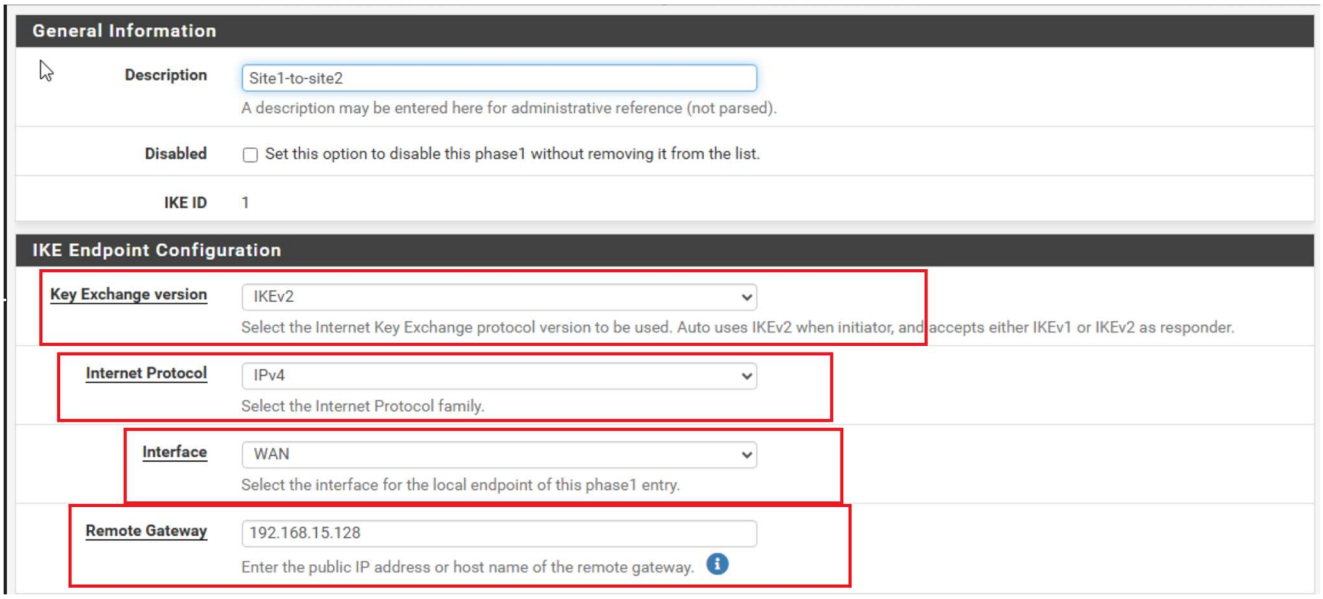
1. Connectez-vous à l'interface web de pfSense.
2. Allez dans **VPN > IPsec**.
3. Cliquez sur **Ajouter une nouvelle connexion**.

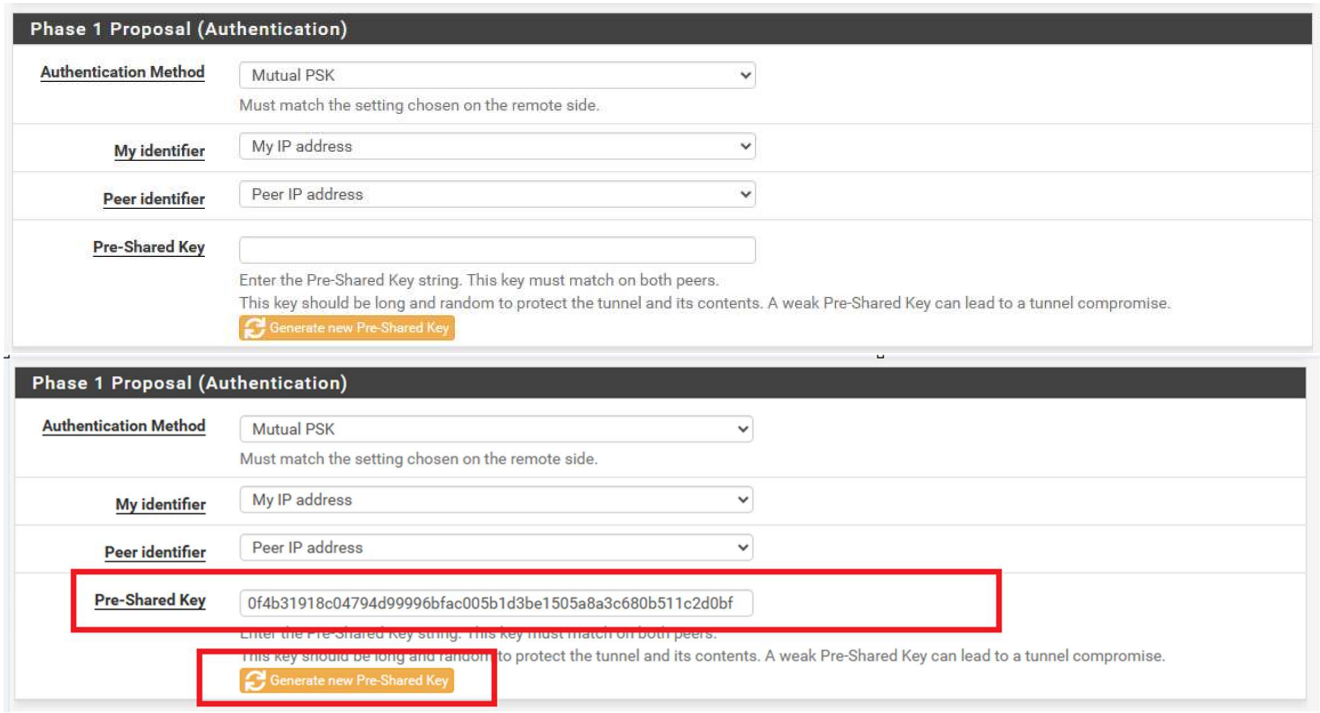




1.2. Paramétrage de la phase 1

1. **Activer la connexion** : cochez **Enable IPsec**.
2. **Interface** : WAN.
3. **Type de tunnel** : Site-to-Site.
4. **Adresse IP du pair distant** : entrez l'adresse publique de l'autre pfSense.
5. **Identifiant local** : Adresse IP publique locale.
6. **Identifiant distant** : Adresse IP publique du pair.



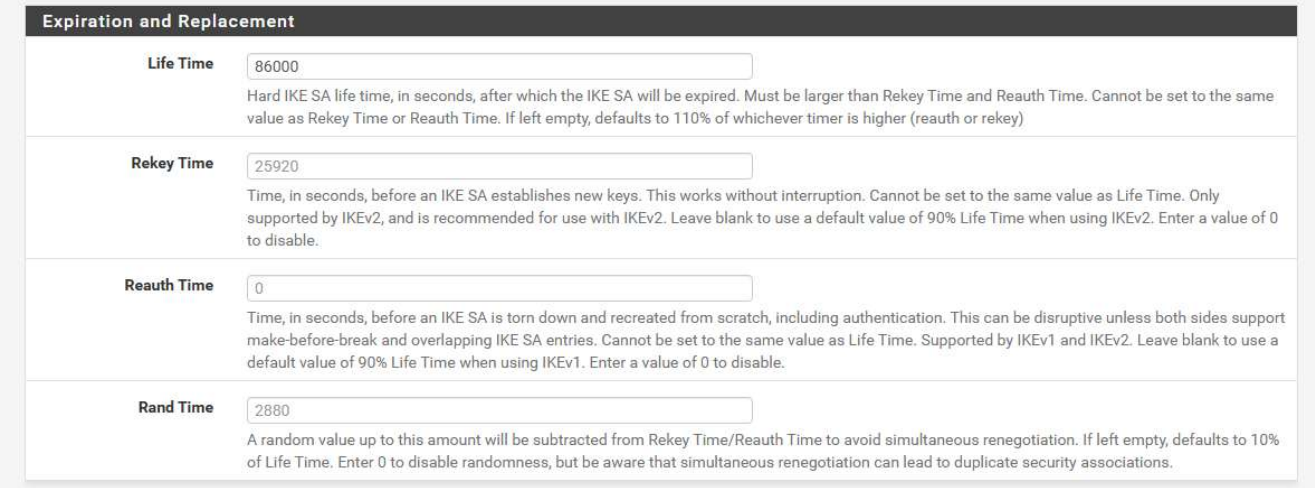
1. **Méthode d'authentification** : Choisissez **Pre-Shared Key**.
2. **Saisissez la clé partagée** (ex : SuperSecretKey123).
3. 

Chiffrement et authentification :

- Algorithme de chiffrement : AES 256

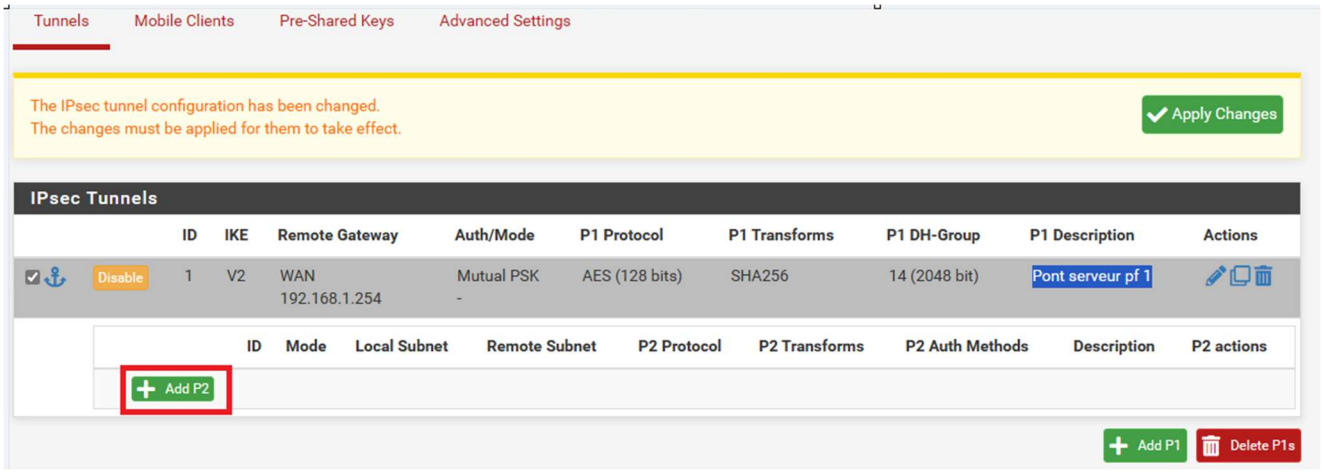
- Algorithme d'authentification : SHA256
- Groupe DH : 14 (2048 bits)

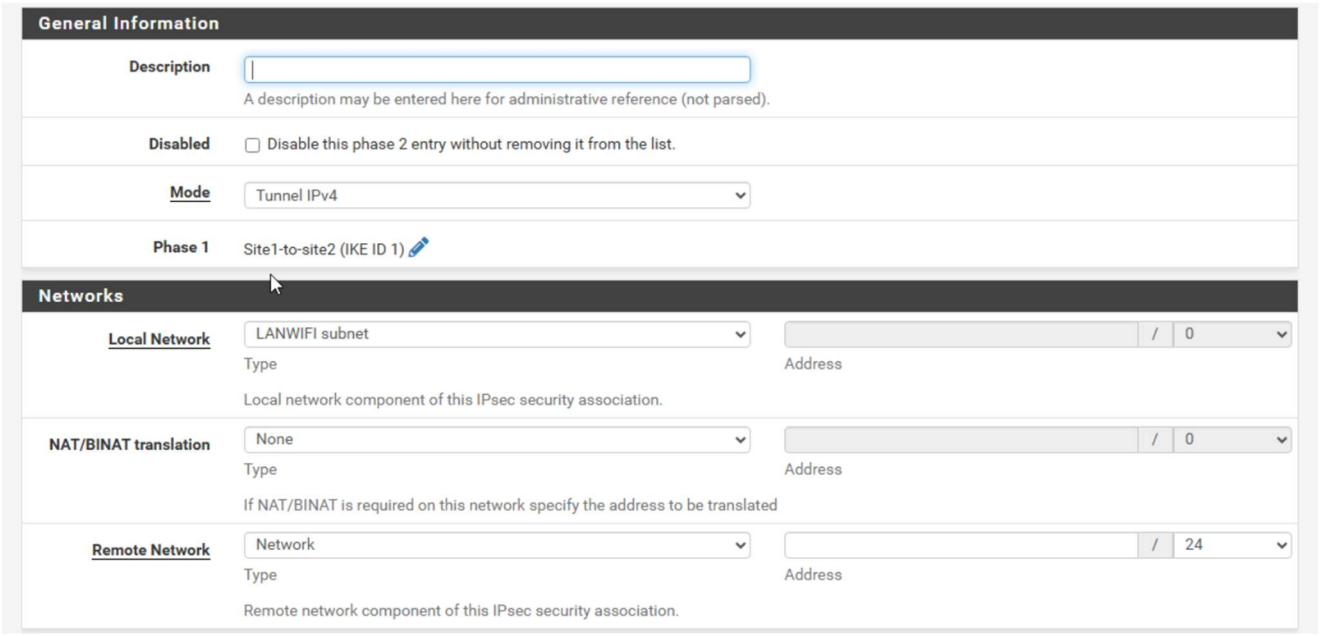
4. **Durée de vie de la SA** : 3600 secondes.
5. **Enregistrer et appliquer**.

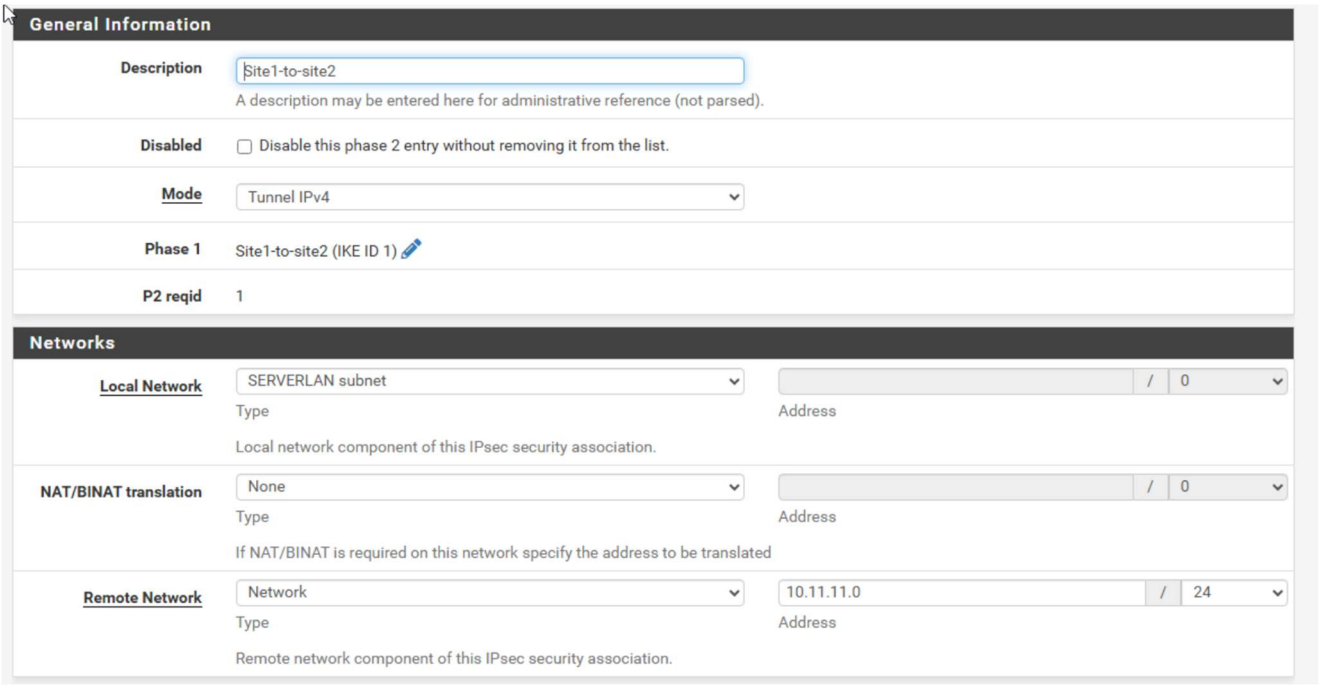


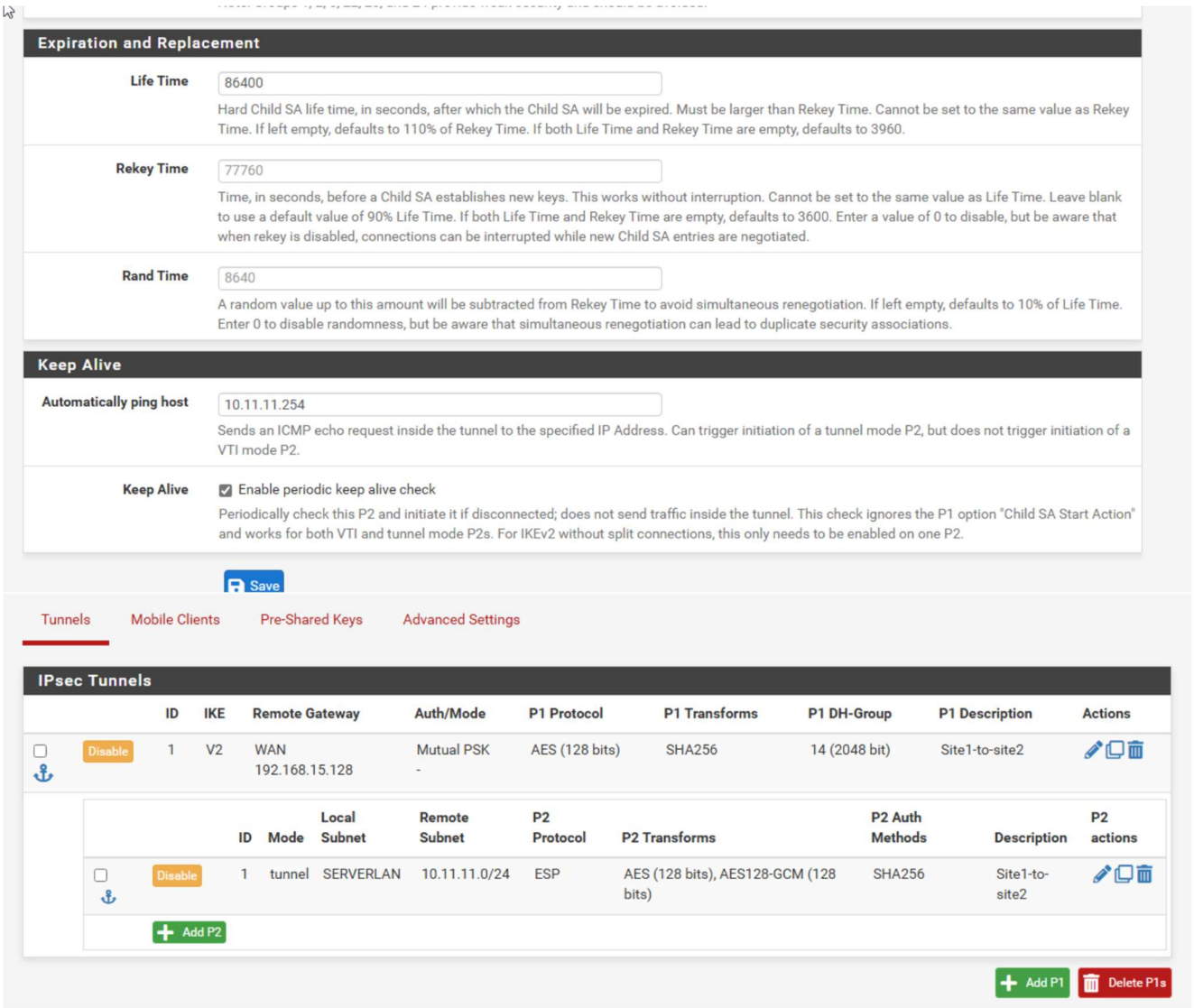
1.3. Paramétrage de la phase 2

1. **Mode** : Tunnel.
2. **Réseau local** : 192.168.1.0/24 (exemple de réseau local).
3. **Réseau distant** : 192.168.2.0/24 (réseau du second site).
4. **Protocole ESP** :
   - Chiffrement : AES 256
   - Authentification : SHA256
   - Groupe PFS : 14
5. **Durée de vie de la SA** : 3600 secondes.
6. **Enregistrer et appliquer**.

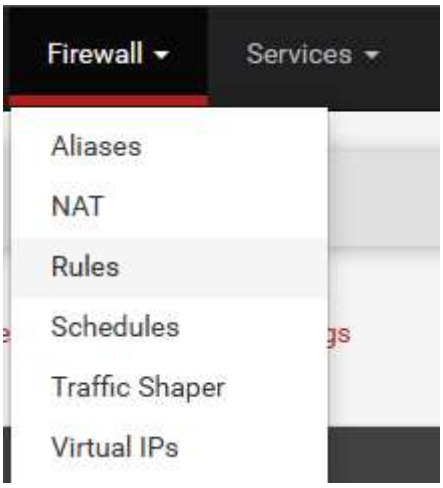

Tunnels
Mobile Clients
Pre-Shared Keys
Advanced Settings
The IPsec tunnel configuration has been changed.
The changes must be applied for them to take effect.
Apply Changes
IPsec Tunnels
ID
IKE
Remote Gateway
Auth/Mode
P1 Protocol
P1 Transforms
P1 DH-Group
P1 Description
Actions
Disable
1
V2
WAN
192.168.1.254
Mutual PSK
-
AES (128 bits)
SHA256
14 (2048 bit)
Pont serveur pf 1
ID
Mode
Local Subnet
Remote Subnet
P2 Protocol
P2 Transforms
P2 Auth Methods
Description
P2 actions
Add P2
Add P1
Delete P1s

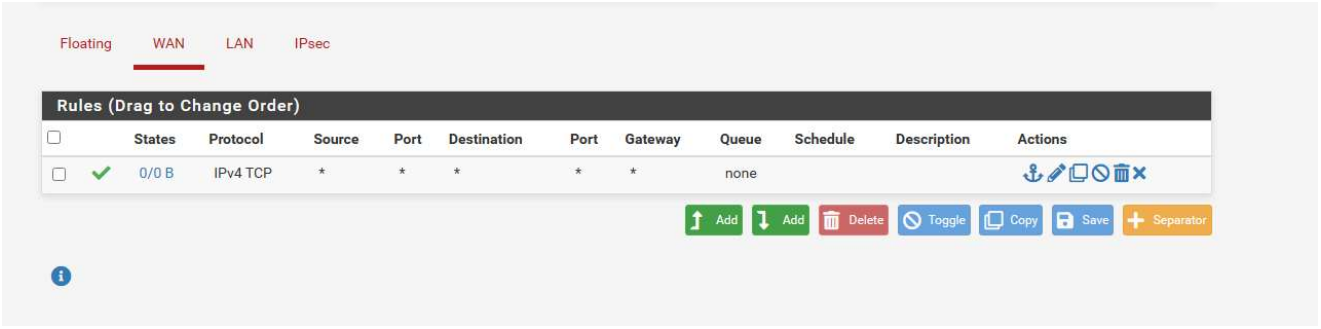

General Information
Description
A description may be entered here for administrative reference (not parsed).
Disabled
Disable this phase 2 entry without removing it from the list.
Mode
Tunnel IPv4
Phase 1
Site1-to-site2 (IKE ID 1)
Networks
Local Network
LANWIFI subnet
Type
Address
Local network component 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
24
Remote network component of this IPsec security association.

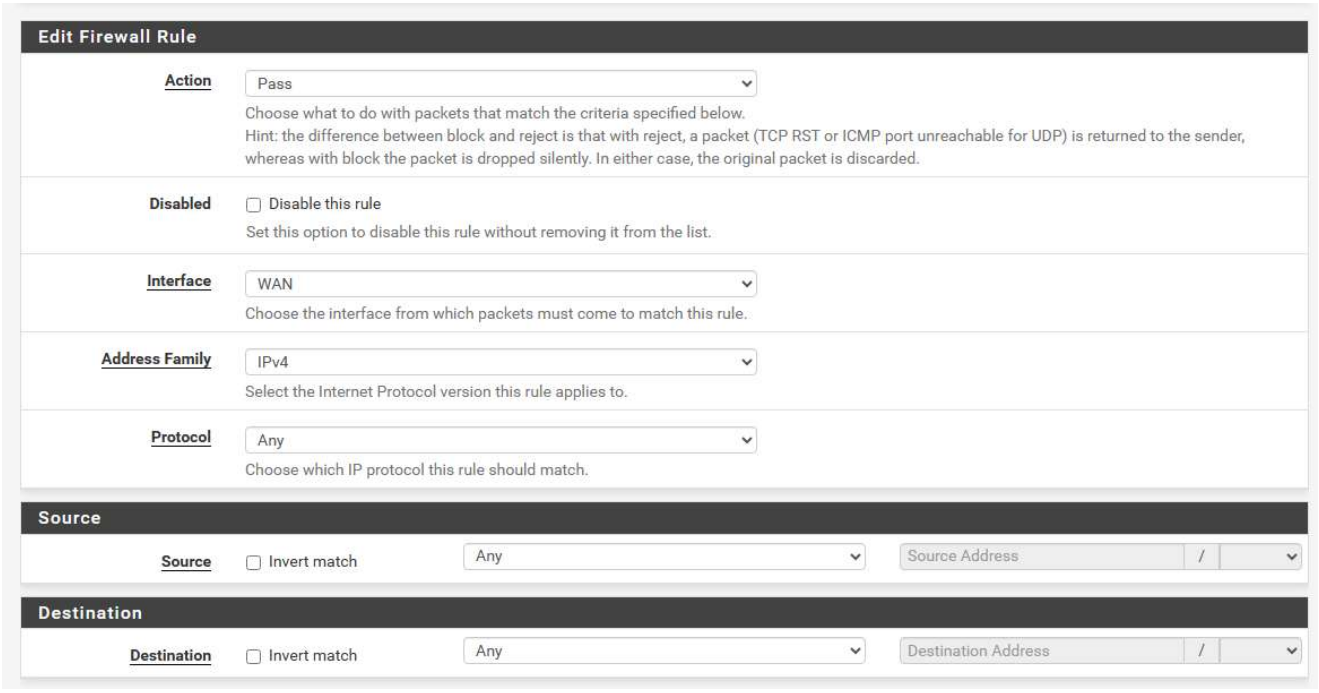

General Information
Description
Site1-to-site2
A description may be entered here for administrative reference (not parsed).
Disabled
Disable this phase 2 entry without removing it from the list.
Mode
Tunnel IPv4
Phase 1
Site1-to-site2 (IKE ID 1)
P2 reqid
1
Networks
Local Network
SERVERLAN subnet
Type
Address
0
Local network component of this IPsec security association.
NAT/BINAT translation
None
Type
Address
0
If NAT/BINAT is required on this network specify the address to be translated
Remote Network
Network
Type
10.11.11.0
Address
24
Remote network component of this IPsec security association.


Expiration and Replacement
Life Time
86400
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
77760
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
8640
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
10.11.11.254
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 check this P2 and initiate it if disconnected; does not send traffic inside the tunnel. This check ignores the P1 option "Child SA Start Action" and works for both VTI and tunnel mode P2s. For IKEv2 without split connections, this only needs to be enabled on one P2.
Save
Tunnels
Mobile Clients
Pre-Shared Keys
Advanced Settings
IPsec Tunnels
ID
IKE
Remote Gateway
Auth/Mode
P1 Protocol
P1 Transforms
P1 DH-Group
P1 Description
Actions
Disable
1
V2
WAN
192.168.15.128
Mutual PSK
-
AES (128 bits)
SHA256
14 (2048 bit)
Site1-to-site2
ID
Mode
Local Subnet
Remote Subnet
P2 Protocol
P2 Transforms
P2 Auth Methods
Description
P2 actions
Disable
1
tunnel
SERVERLAN
10.11.11.0/24
ESP
AES (128 bits), AES128-GCM (128 bits)
SHA256
Site1-to-site2
Add P2
Add P1
Delete P1s

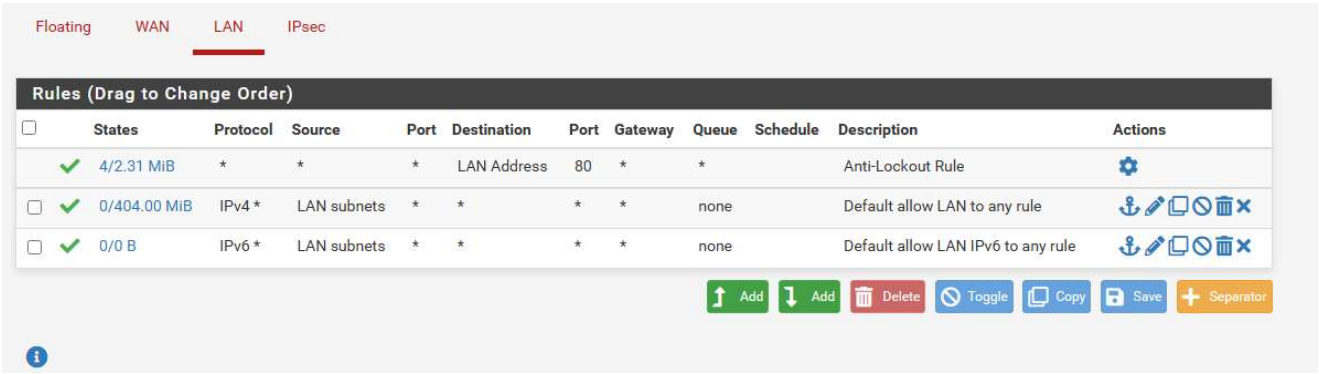
1. **Appliquer les règles et tester la connexion.**

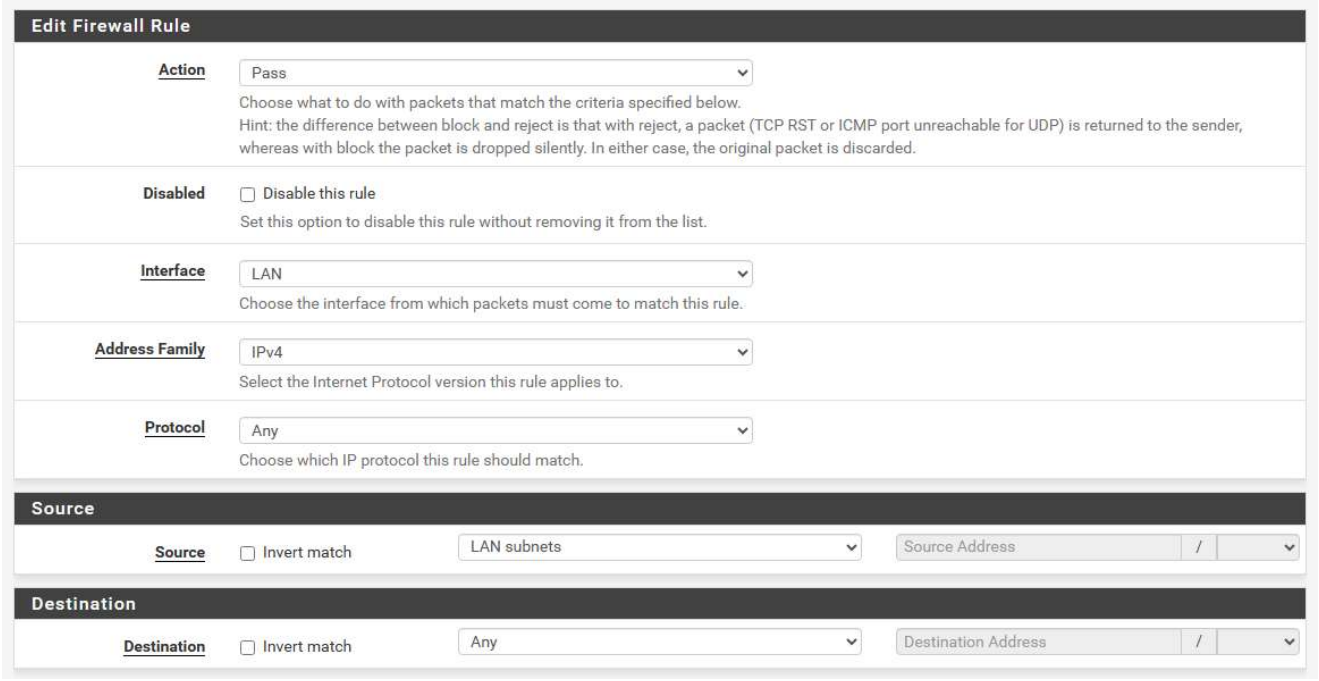


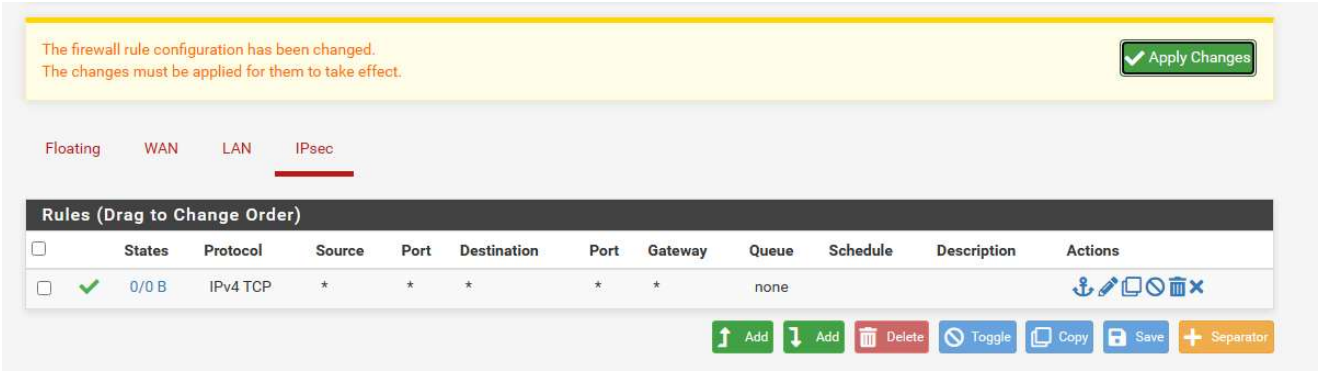


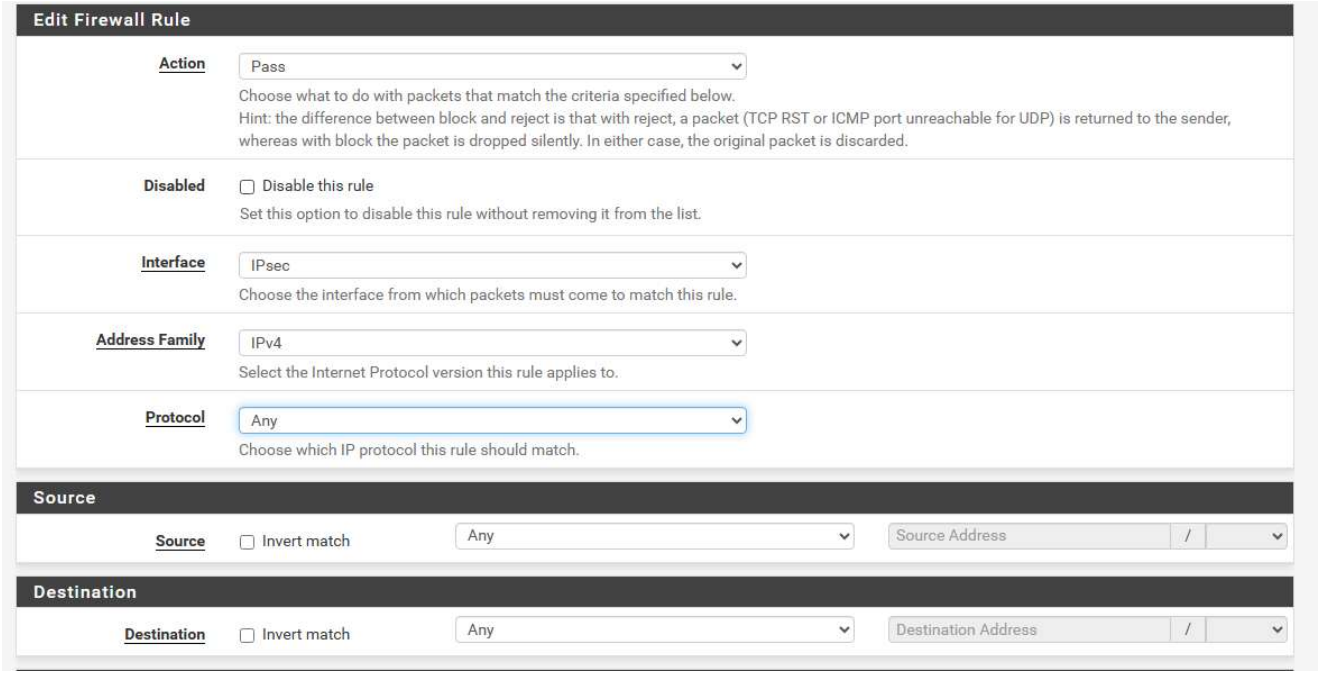

Edit Firewall Rule
Action
Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In 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
WAN
Choose the interface from which packets must come to match this rule.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
Any
Choose which IP protocol this rule should match.
Source
Source
Invert match
Any
Source Address
Destination
Destination
Invert match
Any
Destination Address

+


Floating
WAN
LAN
IPsec
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
4/2.31 MiB * * * LAN Address 80 * * Anti-Lockout Rule
0/404.00 MiB IPv4 * LAN subnets * * * * none Default allow LAN to any rule
0/0 B IPv6 * LAN subnets * * * * none Default allow LAN IPv6 to any rule
Add
Add
Delete
Toggle
Copy
Save
Separator

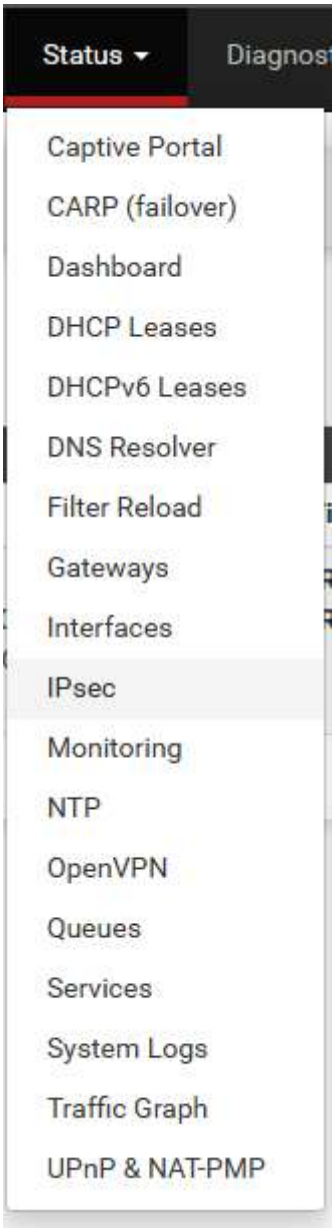

Edit Firewall Rule
Action
Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In 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
LAN
Choose the interface from which packets must come to match this rule.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
Any
Choose which IP protocol this rule should match.
Source
Source
Invert match
LAN subnets
Source Address
Destination
Destination
Invert match
Any
Destination Address

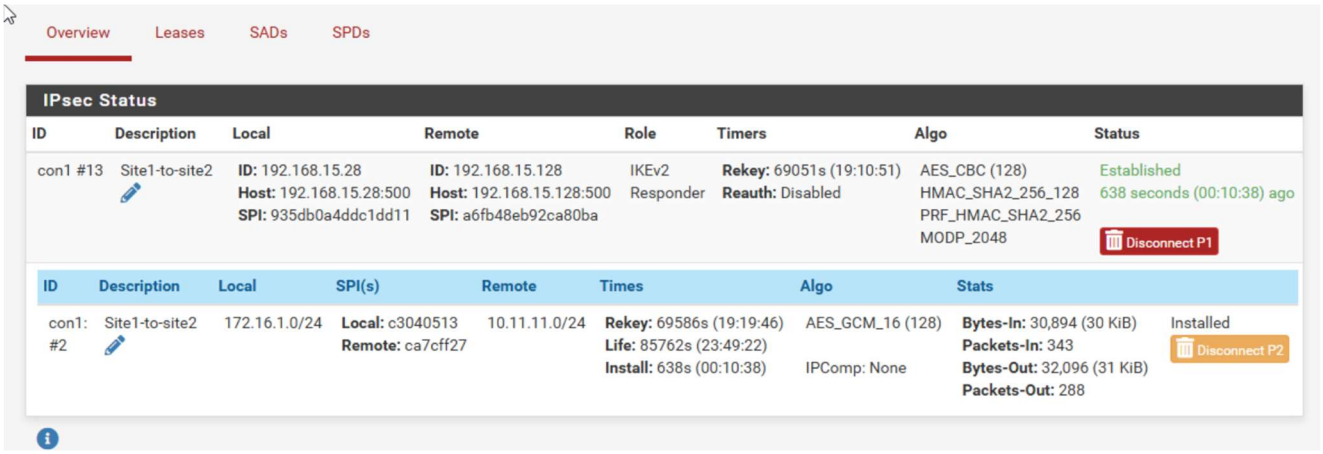

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.
Apply Changes
Floating
WAN
LAN
IPsec
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
0/0 B
IPv4 TCP
*
*
*
*
*
none
Add
Add
Delete
Toggle
Copy
Save
Separator


Edit Firewall Rule
Action
Pass
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
IPsec
Choose the interface from which packets must come to match this rule.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
Any
Choose which IP protocol this rule should match.
Source
Source
Invert match
Any
Source Address
Destination
Destination
Invert match
Any
Destination Address

Vérification du tunnel IPsec

1. Allez dans **Status > IPsec**.
2. Vérifiez que le tunnel est **établi** et que les sessions sont actives.
3. Testez la connectivité en effectuant un **ping** entre les deux réseaux (ex: serveur site 2 : 10.11.11.200)






```
C:\Users\Administrateur>ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv4. . . . . . . . . . . . . .: 172.16.1.1
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 172.16.1.252

C:\Users\Administrateur>ping 10.11.11.200

Envoi d'une requête 'Ping'  10.11.11.200 avec 32 octets de données :
Réponse de 10.11.11.200 : octets=32 temps<1ms TTL=126
Réponse de 10.11.11.200 : octets=32 temps=1 ms TTL=126
Réponse de 10.11.11.200 : octets=32 temps=1 ms TTL=126
Réponse de 10.11.11.200 : octets=32 temps=1 ms TTL=126

Statistiques Ping pour 10.11.11.200:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms

C:\Users\Administrateur>
```