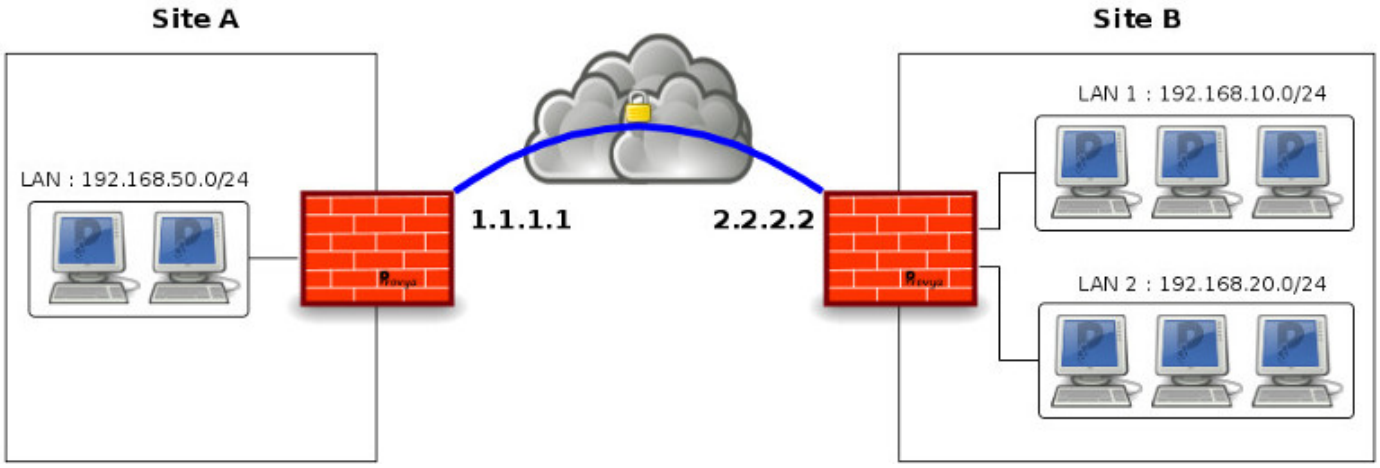
[pfSense] Configurer un VPN IPsec site à site

Dans cet article nous traitons de la configuration d'un VPN IPsec entre deux firewall.
La configuration porte sur un firewall pfSense, mais les grandes lignes de configuration sont applicables à tous les équipements du marché supportant IPsec.

1/4. Schéma de mise en œuvre

Nous suivrons la configuration présentée sur le schéma suivant :



Pour le site A :

- Adresse IP publique : 1.1.1.1
- Réseau local : 192.168.50.0/24

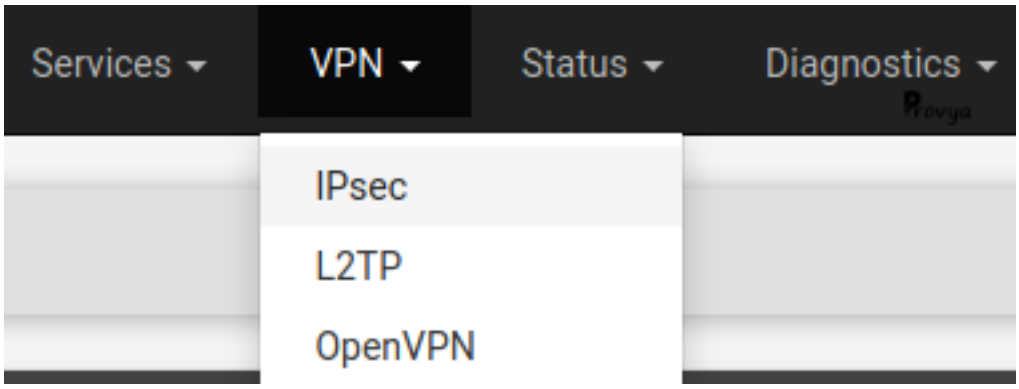
Pour le site B :

- Adresse IP publique : 2.2.2.2
- Réseaux locaux : 192.168.10.0/24 et 192.168.20.0/24

Nous présenterons la configuration pour le site A uniquement. La configuration pour le site B étant facilement déductible à partir de celle du site A.

2/4. Configuration de la Phase 1

Se rendre dans le menu VPN > IPsec

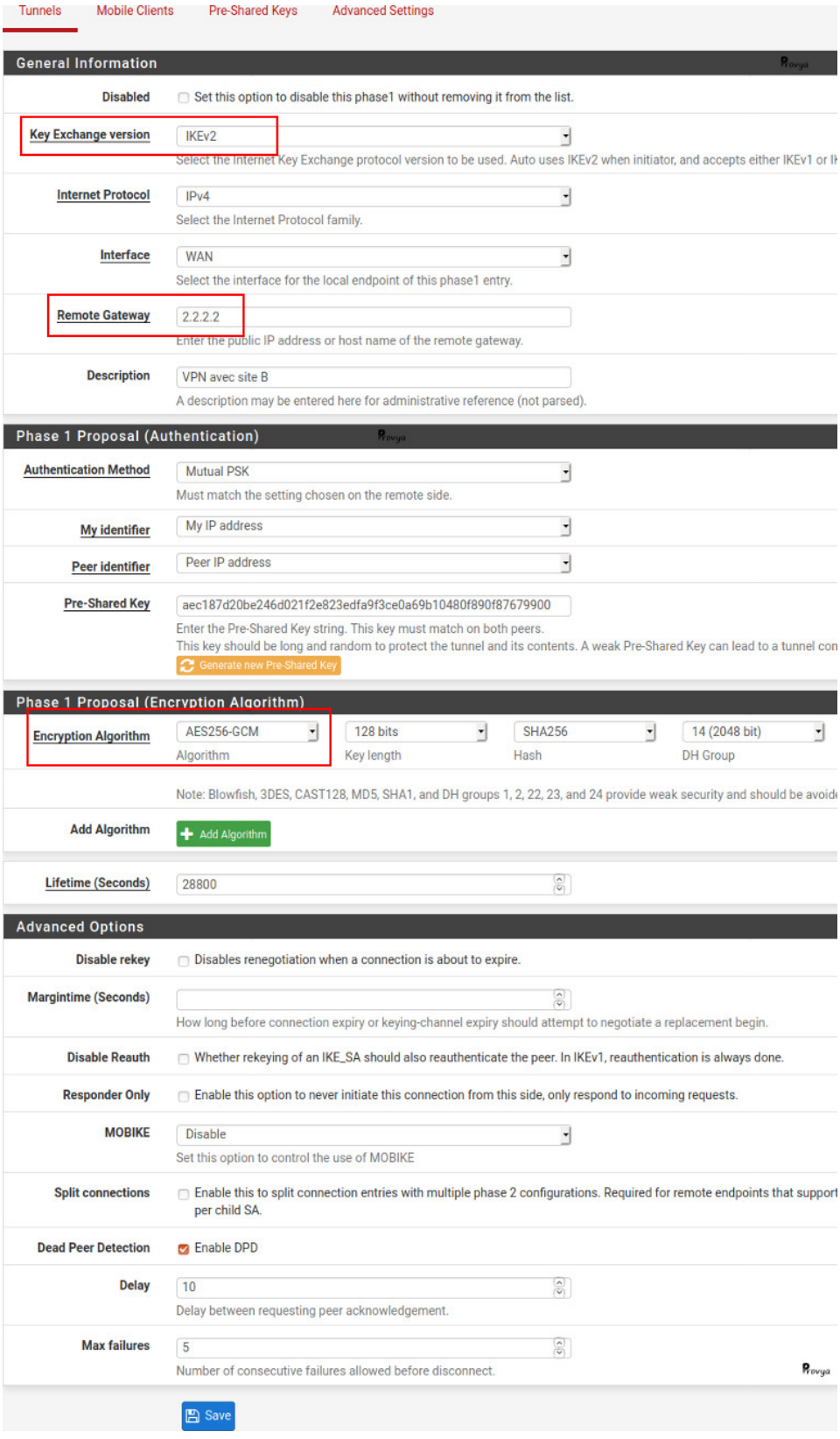


Cliquer sur le bouton "+ Add P1". Les éléments à configurer sont les suivants :

- **Disabled** : cocher cette case permet de désactiver la phase 1 du VPN IPsec (et donc de désactiver le VPN IPsec)
- **Key Exchange version** : permet de choisir la version du protocole IKE (Internet Key Exchange). Nous choisissons "IKEv2". Si l'autre pair ne support par l'IKEv2 ou si un doute subsiste, il est recommandé de choisir "Auto".
- **Internet Protocol** : IPv4 ou IPv6 ; dans notre cas, nous choisissons IPv4
- **Interface** : l'interface sur laquelle nous souhaitons monter notre tunnel VPN IPsec. Nous choisissons WAN
- **Remote Gateway** : l'adresse IP publique du site distant. Dans notre cas : 2.2.2.2
- **Description** : champ facultatif de commentaire (mais que nous conseillons de remplir pour une meilleure lisibilité)
- **Authentication Method** : la méthode d'authentification des deux pairs. Deux choix sont possibles : authentification par clé pré-partagée (PSK) ou par certificat (RSA). Le plus simple et le plus courant est de choisir "Mutual PSK" ; ce que nous faisons.
- **My identifier** : notre identifiant unique. Par défaut, il s'agit de l'adresse IP publique. Nous laissons donc la valeur "My IP address".
- **Peer identifier** : l'identifiant unique de l'autre pair. Par défaut, il s'agit de son adresse IP publique. Nous laissons la valeur "Peer IP address"

- **Pre-Shared Key** : la clé pré-partagée. Nous laissons pfSense la générer et cliquons pour cela sur "Generate new Pre-Shared Key". Cette clé pré-partagée devra être saisie sur l'autre firewall lors de sa configuration.
- **Encryption Algorithm** : l'algorithme de chiffrement. Si les deux parties supportent l'AES-GCM, nous recommandons l'utilisation d'AES256-GCM ou d'AES128GCM ; ce qui permettra de bénéficier d'un bon niveau de chiffrement et sera compatible avec l'accélération cryptographique offert par AES-NI. Autrement, choisir AES avec une longueur de clé de 256 bits dans l'idéal. Enfin, nous conservons SHA256 pour fonction de hachage et 14 ou 16 pour la valeur du groupe Diffie-Hellman (DH group - utilisé pour l'échange de clés).
- **Lifetime (Seconds)** : permet de définir la fréquence de renouvellement de la connexion. La valeur par défaut, 28800 secondes, reste un bon choix
- **Advanced Options** : nous laissons les valeurs par défaut

Exemple de résultat obtenu :


Tunnels
Mobile Clients
Pre-Shared Keys
Advanced Settings
General Information
Disabled
Set this option to disable this phase1 without removing it from the list.
Key Exchange version
IKEv2
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or I
Internet Protocol
IPv4
Select the Internet Protocol family.
Interface
WAN
Select the interface for the local endpoint of this phase1 entry.
Remote Gateway
2.2.2.2
Enter the public IP address or host name of the remote gateway.
Description
VPN avec site B
A description may be entered here for administrative reference (not parsed).
Phase 1 Proposal (Authentication)
Authentication Method
Mutual PSK
Must match the setting chosen on the remote side.
My identifier
My IP address
Peer identifier
Peer IP address
Pre-Shared Key
aec187d20be246d021f2e823edfa9f3ce0a69b10480f890f87679900
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 con
Generate new Pre-Shared Key
Phase 1 Proposal (Encryption Algorithm)
Encryption Algorithm
AES256-GCM
Algorithm
128 bits
Key length
SHA256
Hash
14 (2048 bit)
DH Group
Note: Blowfish, 3DES, CAST128, MD5, SHA1, and DH groups 1, 2, 22, 23, and 24 provide weak security and should be avoid
Add Algorithm
Add Algorithm
Lifetime (Seconds)
28800
Advanced Options
Disable rekey
Disables renegotiation when a connection is about to expire.
Margintime (Seconds)
How long before connection expiry or keying-channel expiry should attempt to negotiate a replacement begin.
Disable Reauth
Whether rekeying of an IKE_SA should also reauthenticate the peer. In IKEv1, reauthentication is always done.
Responder Only
Enable this option to never initiate this connection from this side, only respond to incoming requests.
MOBIKE
Disable
Set this option to control the use of MOBIKE
Split connections
Enable this to split connection entries with multiple phase 2 configurations. Required for remote endpoints that support
per child SA.
Dead Peer Detection
Enable DPD
Delay
10
Delay between requesting peer acknowledgement.
Max failures
5
Number of consecutive failures allowed before disconnect.
Save

Nous cliquons sur le bouton "Save" pour enregistrer les changements.

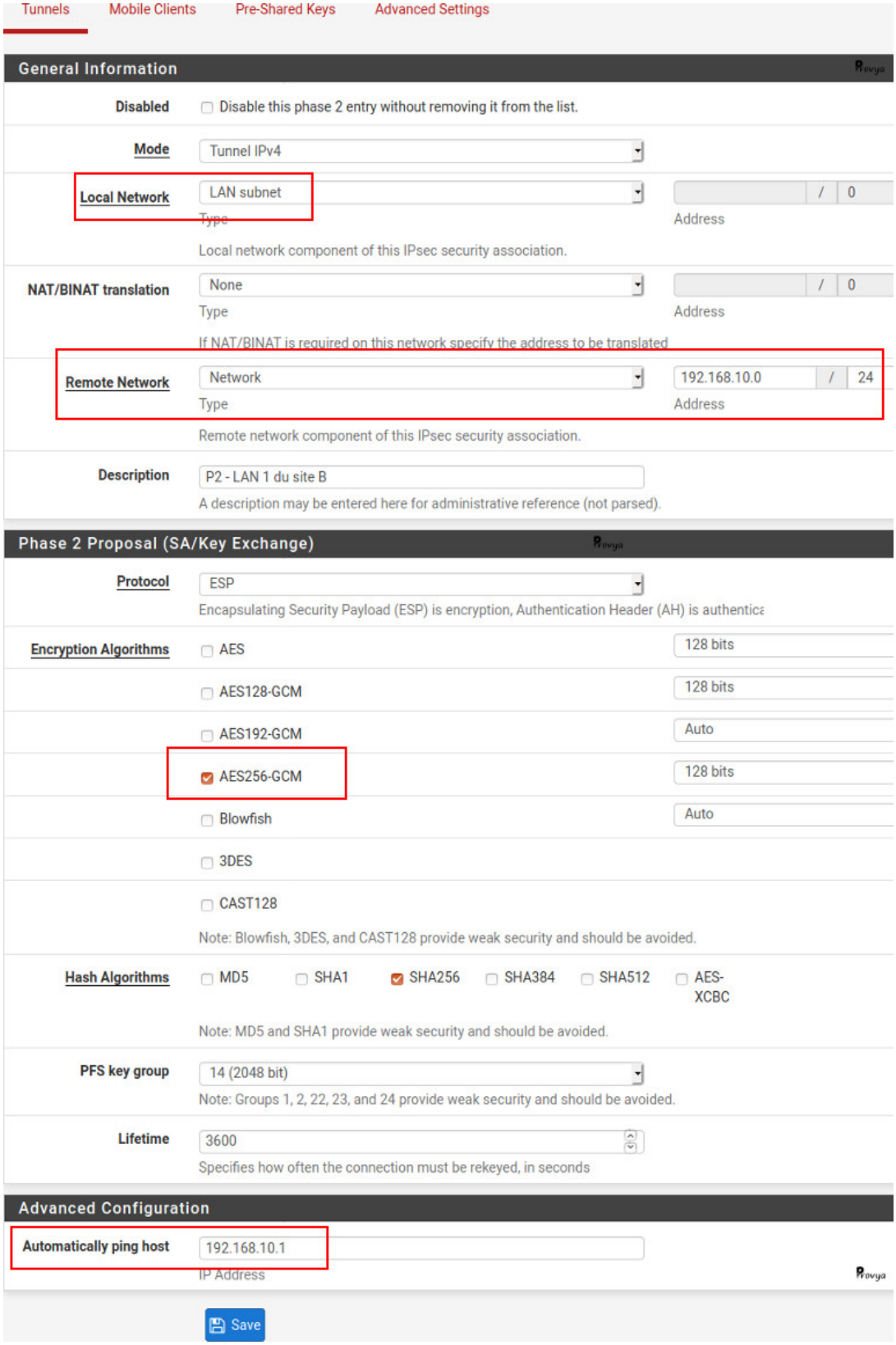
3/4. Configuration des Phases 2

Sur la page des tunnels VPN IPsec (sur laquelle vous devez être actuellement), pour notre entrée P1 que nous venons de créer, nous cliquons successivement sur les boutons "Show Phase 2 Entries (0)", puis sur "+ Add P2".

Les éléments à configurer sont les suivants :

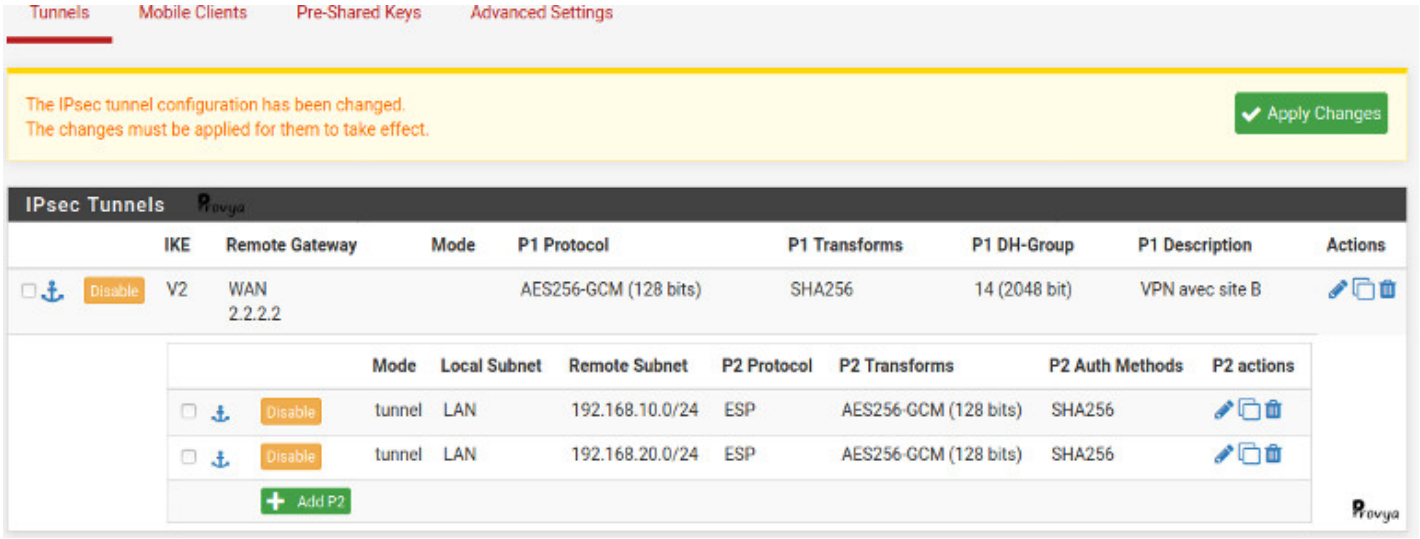
- **Disabled** : cocher cette case permet de désactiver cette phase 2 du VPN IPsec
- **Mode** : nous laissons le mode par défaut "Tunnel IPv4"
- **Local Network** : le réseau-local joignable par l'hôte distant sur ce VPN IPsec. Dans notre cas, nous choisissons "LAN subnet".
- **NAT/BINAT translation** : si l'on souhaite configurer du NAT sur le tunnel IPsec. Ceci peut être très utile si le plan d'adressage est le même sur les deux sites distants que nous souhaitons interconnecter. Ce n'est pas notre cas dans notre exemple. Nous laissons donc la valeur à "None".
- **Remote Network** : l'adresse IP ou le sous-réseau du site distant. Dans notre cas, nous renseignons ici le premier sous-réseau, soit 192.168.10.0/24 ; puis nous créerons une seconde phase 2 en précisant cette fois le second sous-réseau du site distant (192.168.20.0/24).
- **Description** : champ facultatif de commentaire (mais que nous conseillons de remplir pour une meilleure lisibilité)
- **Protocol** : nous choisissons ESP. AH est rarement utilisé en pratique. Techniquement, le protocole ESP permet de chiffrer l'intégralité des paquets échangés, tandis qu'AH ne travaille que sur l'entête du paque IP sans offrir la confidentialité des données échangées.
- **Encryption Algorithms** : Algorithmes de chiffrement. Comme pour la phase 1, si les deux parties supportent l'AES-GCM, nous recommandons l'utilisation d'AES256-GCM ou d'AES128GCM ; ce qui permettra de bénéficier d'un bon niveau de chiffrement et sera compatible avec l'accélération cryptographique offert par AES-NI. Autrement, choisir AES avec une longueur de clé de 256 bits dans l'idéal. Enfin, nous conservons SHA256 pour fonction de hachage et 14 ou 16 pour la valeur du groupe Diffie-Hellman (PFS key group).
- **Lifetime** : nous laissons la valeur par défaut, soit 3600 secondes
- **Automatically ping host** : une adresse IP à *pinguer* sur le site distant afin de conserver le tunnel actif. Ce peut être l'adresse IP du firewall sur le site distant par exemple ; nous indiquons 192.168.10.1 dans notre cas.

Exemple de résultat obtenu :



Nous cliquons sur le bouton "Save" pour sauvegarder notre configuration. Puis nous créeons une nouvelle phase 2 en indiquant cette fois, pour le champ "Remote Network", le second sous-réseau du site B (LAN 2 : 192.168.20.0/24) et choisissons, bien sûr, une adresse IP dans ce sous-réseau pour le champ "Automatically ping host".

Une fois ces configurations effectuées, nous obtenons le résultat suivant :



Il ne nous reste plus qu'à cliquer sur le bouton "Apply Changes" pour appliquer nos configurations.

À ce stade, le VPN IPsec doit être monté. Il ne nous reste plus qu'à configurer nos règle de filtrage afin d'autoriser le trafic.

4/4. Règles de filtrage

Il y a au moins deux règles de filtrage à implémenter : celles autorisant le trafic depuis le LAN vers les réseaux du site distant ; et celles autorisant le trafic depuis les deux sous-réseaux du site distant vers le LAN.

Soit, pour l'interface LAN, voici un exemple de règles :

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✔	0 /0 B	*	*	*	LAN Address	443 80 35190	*	*		Anti-Lockout Rule
✔	0 /0 B	IPv4 *	LAN net	*	192.168.10.0/24	*	*	none		LAN vers LAN 1 du site B
✔	0 /0 B	IPv4 *	LAN net	*	192.168.20.0/24	*	*	none		LAN vers LAN 2 du site B

Et pour l'interface IPsec, voici un exemple de règles :

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
✔	0 /0 B	IPv4 *	192.168.10.0/24	*	LAN net	*	*	none		LAN 1 du site B vers LAN local
✔	0 /0 B	IPv4 *	192.168.20.0/24	*	LAN net	*	*	none		LAN 2 du site B vers LAN local

Ces règles sont, en l'état, très permissives. Nous vous recommandons de les affiner afin qu'elles apportent une meilleure sécurité et qu'elles soient en conformité avec votre politique de filtrage.

Dernier élément, si vous avez modifié les options avancées accessibles depuis le menu System > Advanced, onglet Firewall/NAT et que vous avez coché la case "Disable all auto-added VPN rules", alors vous devrez créer des règles de filtrage sur l'interface WAN afin d'autoriser le trafic IPsec avec l'hôte distant. IPsec utilise les ports UDP 500 et 4500, ainsi que le protocole ESP (ou AH, le cas échéant).

La configuration est terminée et doit être fonctionnelle. Pour visualiser les logs associés au VPN IPsec, cela se passe dans le menu Status > System Logs, onglet Firewall.