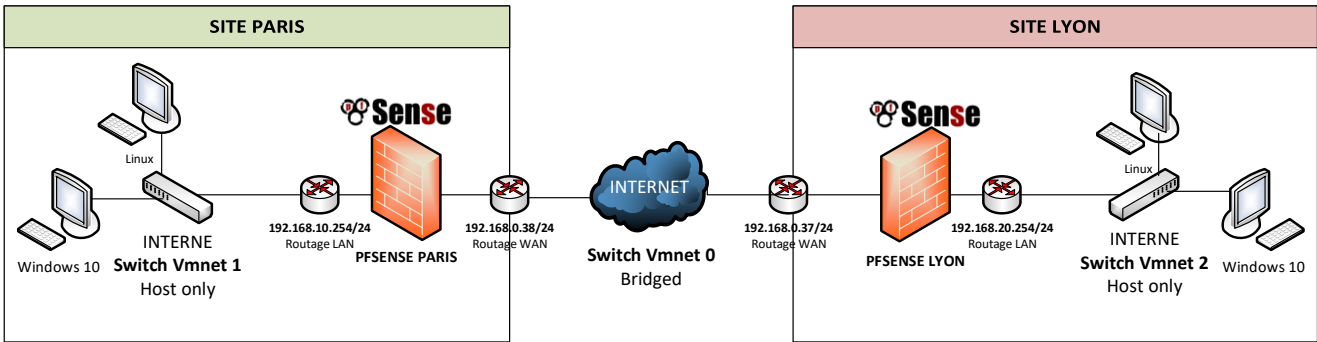

Objectifs traités

Mise en place du Tunnel VPN IPSEC SERVEUR 15-3

Mise en place du Tunnel VPN IPSEC SERVEUR 25-7

VPN site to Site via IPSEC

Le VPN site to site va permettre de relier deux réseaux LAN entre une connexion WAN en toute sécurité en permanence.
Les sites pourront communiquer de manière transparente comme s'ils avaient qu'un simple routeur entre eux.
IPSEC utilise IKE qui négocie la connexion pour une authentification les deux extrémités du tunnel en échangeant des clés partagées

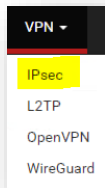


Voici la configuration pour chaque serveur.

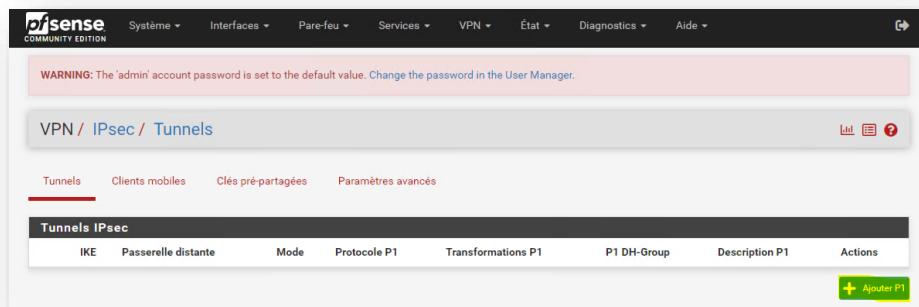
SITE PARIS	SITE LYON
FreeBSD/amd64 (pfSense-Paris.formation.local) (ttyv0) VMware Virtual Machine - Netgate Device ID: 8ef8df9f301d89c215bf *** Welcome to pfSense 2.5.0-RELEASE (amd64) on pfSense-Paris *** WAN (wan) -> em0 -> v4/DHCP4: 192.168.0.38/24 v6/DHCP6: 2a01:e0a:936:d560:20c:29ff:fe40:f6d1 /64 LAN (lan) -> em1 -> v4: 192.168.10.254/24	FreeBSD/amd64 (pfSense-Lyon.formation.local) (ttyv0) VMware Virtual Machine - Netgate Device ID: d62bcb36f259e3c6c167 *** Welcome to pfSense 2.5.0-RELEASE (amd64) on pfSense-Lyon *** WAN (wan) -> em0 -> v4/DHCP4: 192.168.0.37/24 v6/DHCP6: 2a01:e0a:936:d560:20c:29ff:fe02:ba67 /64 LAN (lan) -> em1 -> v4: 192.168.20.254/24

Mise en place du VPN en IPSEC

Aller dans le menu **VPN** puis choisir **IPSEC**



Cliquer ensuite sur **+Ajouter P1**



Taper l'IP de la **passerelle distante** ici **192.168.0.37** qui doit correspondre à celle de LYON

Définir une description ici **IPSEC vers LYON**

Mettre nom unique dans **mon identifiant** et affecter le nom du serveur, faire la même chose sur **identifiant de pair** et générer une clé partagée.

Cette clé doit être reporter sur le deuxième serveur puis enregistrer

Informations Générales

☒ Désactivé Définissez cette option pour désactiver cette phase1 sans la retirer de la liste.

Version de l'échange de clés
Sélectionnez la version du protocole Internet Key Exchange à utiliser. Auto utilise IKEv2 lors de l'initiateur, et accepte IKEv1 ou IKEv2 comme répondeur.

Protocole Internet
Sélectionnez la famille Internet Protocol.

Interface
Sélectionnez l'interface pour le point final local de cette entrée phase1.

Passerelle distante
Enter the public IP address or host name of the remote gateway. ? 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. ?

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

Proposition de phase 1 (authentification)

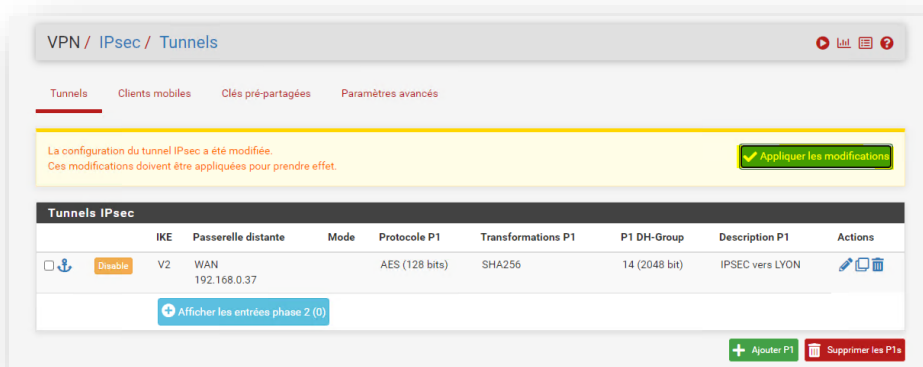
Méthode d'authentification
Doit correspondre au réglage choisi sur le côté distant.

Mon identifiant

Identifiant de pair

***Clé Pré-Partagée**
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](#)

Appliquer les modifications



Cliquez sur **Afficher les entrées phase 2** puis **+ajouter P2**
Réseau distant donner l'adresse du réseau IP local du serveur distant (pfsense-lyon)

Sélectionner **AES256-GCM** avec **128 bits**

IP de l'hôte à pinger constamment, ici la passerelle du réseau local de Lyon puis **enregistrer**
N'oublier pas **d'appliquer les modifications**

Configuration avancée

Pinger automatiquement l'hôte

192.168.20.254

Adresse IP

Enregistrer

Voici le résultat pour le serveur Pfsense-Paris

VPN / IPsec / Tunnels

Tunnels

Clients mobiles

Clés pré-partagées

Paramètres avancés

Les modifications ont été appliquées avec succès.

Tunnels IPsec

	IKE	Passerelle distante	Mode	Protocole P1	Transformations P1	P1 DH-Group	Description P1	Actions
<input type="checkbox"/> 	Disable V2	WAN 192.168.0.37		AES256-GCM (128 bits)	SHA256	14 (2048 bit)	IPSEC vers LYON	

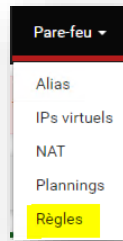
	Mode	Sous-réseau local	Sous-réseau distant	Protocole P2	Transformations P2	Méthodes d'authentification P2	Actions
<input type="checkbox"/> 	Disable tunnel	LAN	192.168.20.0/24	ESP	AES256-GCM (128 bits)		

Ajouter P2

Ajouter P1

Supprimer les P1s

Il faut aller dans le pare-feu pour créer des règles de filtrage.



Aller dans pare-feu puis règles

Il faut ajouter 2 règles, une pour l'ICMP et l'autre pour tout le Traffic.

Sélectionner **Interface IPsec** puis le protocole **ICMP**

Le sous type sera **tout**

Dans **Sources** choisir **Réseau** avec une IP réseau **192.168.20.0/24** (**réseau LAN LYON**)

Dans **Destination** choisir **WAN-net**

Puis Enregistrer

Sélectionner **Interface IPsec** puis le protocole **TCP/UDP**

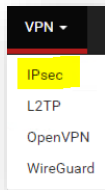
Dans **Sources** choisir **Réseau** avec une IP réseau **192.168.20.0/24** (**réseau LAN LYON**)

Dans **Destination** choisir **LAN-net** avec une page **tout**

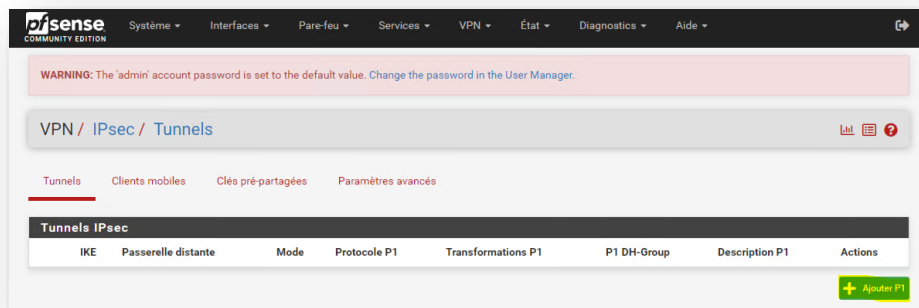
Puis Enregistrer

L'opération doit aussi se répéter sur le deuxième serveur donc il faut reprendre depuis le début.

Aller dans le menu **VPN** puis choisir **IPSEC**



Cliquer ensuite sur **+Ajouter P1**



Taper l'IP de la **passerelle distante** ici **192.168.0.38** qui doit correspondre à celle de PARIS

Définir une description ici **IPSEC vers PARIS**

Mettre nom unique dans **mon identifiant** et affecter le nom du serveur, faire la même chose sur **identifiant de pair**

Reprenez la clé générer du serveur PARIS pour l'appliquer ici puis enregistrer

Informations Générales

☐ Désactivé Définissez cette option pour désactiver cette phase1 sans la retirer de la liste.

Version de l'échange de clés IKEv2
Sélectionnez la version du protocole Internet Key Exchange à utiliser. Auto utilise IKEv1 ou IKEv2 comme répondeur.

Protocole Internet IPv4
Sélectionnez la famille Internet Protocol.

Interface WAN
Sélectionnez l'interface pour le point final local de cette entrée phase1.

Passerelle distante 192.168.0.38
Enter the public IP address or host name of the remote gateway. Remote IKE Port: UDP port for IKE on the remote gateway. Leave empty for default automatic behavior (500/4500). Remote NAT-T Port: UDP port for NAT-T on the remote gateway.

Description IPSEC vers PARIS
Une description peut être saisie ici à des fins de référence administrative (non analysée).

Proposition de phase 1 (authentification)

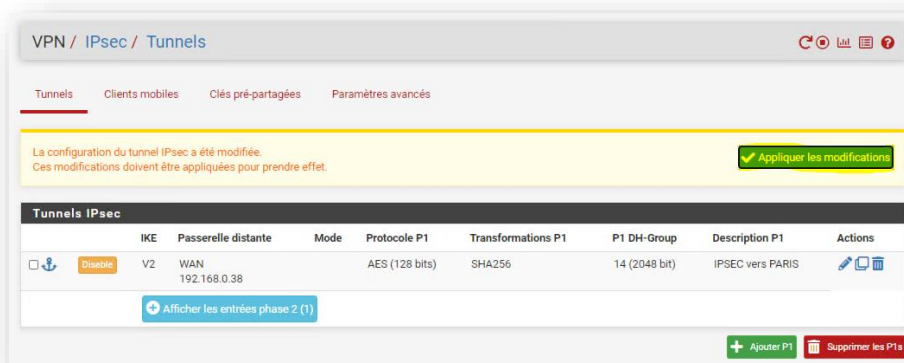
Méthode d'authentification PSK Mutuel
Doit correspondre au réglage choisi sur le côté distant.

Mon identifiant mon unique

Identifiant de pair pair unique

***Clé Pré-Partagée** 2ae40fbd384de6b12d39be6d482bca979b72e7c5e939c37ca0558e8
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 now Pre-Shared Key](#)

Appliquer les modifications



Cliquez sur **Afficher les entrées phase 2** puis **+ajouter P2**
Réseau distant donner l'adresse du réseau IP local du serveur distant (pfsense-lyon)

Informations Générales

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

Mode: Tunnel IPv4

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 192.168.10.0 / 24

Type: Adresse

Remote network component of this IPsec security association.

Description: IPSEC vers PARIS

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

Sélectionner **AES256-GCM** avec **128 bits**

Proposition de phase 2 (SA/Key Exchange)

Protocole: ESP

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

Algorithme de chiffrement: AES256-GCM 128 bits

Algorithme de hachage: MD5

Groupe de clés PFS: 14 (2048 bit)

Note: Blowfish, 3DES, and CAST128 provide weak security and should be avoided.

Note: Hash is ignored with GCM algorithms. MD5 and SHA1 provide weak security and should be avoided.

Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.


IP de l'hôte à pinger constamment, ici la passerelle du réseau local de Lyon puis **enregistrer**
N'oublier pas **d'appliquer les modifications**

Configuration avancée

Pinger automatiquement l'hôte

192.168.10.254

Adresse IP



Voici le résultat pour le serveur Pfsense-Lyon

VPN / IPsec / Tunnels







Tunnels

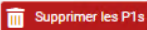
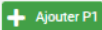
Clients mobiles

Clés pré-partagées

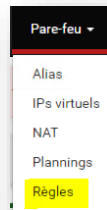
Paramètres avancés

Tunnels IPsec

	IKE	Passerelle distante	Mode	Protocole P1	Transformations P1	P1 DH-Group	Description P1	Actions	
<input type="checkbox"/>	Disable	V2	WAN						
		192.168.0.38		AES (128 bits)	SHA256	14 (2048 bit)	IPSEC vers PARIS	 	
			Mode	Sous-réseau local	Sous-réseau distant	Protocole P2	Transformations P2	Méthodes d'authentification P2	Actions P2
<input type="checkbox"/>	Disable	tunnel	LAN		192.168.10.0/24	ESP	AES192-GCM (128 bits)		 
									



Il faut aller dans le pare-feu pour créer des règles de filtrage pour le serveur Pfsense-Lyon.



Aller dans pare-feu puis règles

Il faut ajouter 2 règles, une pour l'ICMP et l'autre pour tout le Traffic.

Sélectionner **Interface IPsec** puis le protocole **ICMP**

Le sous type sera **tout**

Dans **Sources** choisir **Réseau** avec une IP réseau **192.168.10.0/24** (réseau LAN PARIS)

Dans **Destination** choisir **LAN-net**

Puis Enregistrer

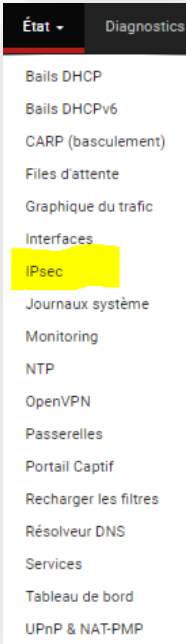
Sélectionner **Interface IPsec** puis le protocole **TCP/UDP**

Dans **Sources** choisir **Réseau** avec une IP réseau **192.168.10.0/24** (réseau LAN PARIS)

Dans **Destination** choisir **LAN-net** avec une page **tout**

Puis Enregistrer

Il suffit de vérifier depuis un serveur que la connexion est bien établie.
Pour cela aller dans **état** puis **ipsec**



Serveur : PFSENSE-PARIS

État IPsec							
ID IPsec	Description	Local	Distant	Rôle	Timers	Algo	État
con100000: #3		ID: pfsense-paris Host: 192.168.0.38:500 SPI: 85f3210b6e5900fc	ID: pfsense-lyon Host: 192.168.0.37:500 SPI: 6fa98367b0254072	IKEv2 initiator	Rekey: 24783s (06:53:03) Reauth: Désactivé	AES_CBC (128) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	ESTABLISHED Il y a 524 secondes (00:08:44)

Serveur : PFSENSE-LYON

État IPsec							
ID IPsec	Description	Local	Distant	Rôle	Timers	Algo	État
con100000: #2		ID: pfsense-lyon Host: 192.168.0.37:500 SPI: 6fa98367b0254072	ID: pfsense-paris Host: 192.168.0.38:500 SPI: 85f3210b6e5900fc	IKEv2 responder	Rekey: 23443s (06:30:43) Reauth: Désactivé	AES_CBC (128) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	ESTABLISHED Il y a 748 secondes (00:12:28)

Voici le résultat d'un ping entre 2 stations sur chaque Pfsense.

La station 192.168.10.100 ping bien le routeur du pfsense-Lyon ainsi que sa passerelle

```
Configuration IP de Windows

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . : formation.local
    Adresse IPv6 de liaison locale. . . . : fe80::a111:3d0c:4e06:1a82%6
    Adresse IPv4. . . . . : 192.168.10.100
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.10.254

Carte Ethernet Connexion réseau Bluetooth :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :

C:\Users\Luis>ping 192.168.20.254

Envoi d'une requête 'Ping' 192.168.20.254 avec 32 octets de données :
Réponse de 192.168.20.254 : octets=32 temps=21 ms TTL=63
Réponse de 192.168.20.254 : octets=32 temps=1 ms TTL=63
Réponse de 192.168.20.254 : octets=32 temps<1ms TTL=63
Réponse de 192.168.20.254 : octets=32 temps<1ms TTL=63

Statistiques Ping pour 192.168.20.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 21ms, Moyenne = 5ms

C:\Users\Luis>ping 192.168.20.101

Envoi d'une requête 'Ping' 192.168.20.101 avec 32 octets de données :
Réponse de 192.168.20.101 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.20.101 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.20.101 : octets=32 temps=1 ms TTL=126
Réponse de 192.168.20.101 : octets=32 temps=1 ms TTL=126

Statistiques Ping pour 192.168.20.101:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms

C:\Users\Luis>
```

Notes Personnel
