

PETIT Antoine

Date de début : 20/12/2024

Date de fin : 20/12/2024

# VPN Dynfi IPsec



## Sommaire

1	CONTEXTE	3
2	OBJECTIFS	3
3	MATÉRIEL ET LOGICIELS	3
4	PRÉREQUIS	3
5	RÉALISATION	4
	5.1 CONFIGURATION DU TUNNEL IPSEC	4
	5.2 CONFIGURATION DE RÈGLE IPSEC	6

# 1 CONTEXTE

---

- **Sites distants** : Deux sites géographiquement séparés, chacun disposant d'un pare-feu DynFi pour contrôler les connexions entrantes et sortantes.
- **Protocole VPN** : IPsec pour la création d'un tunnel sécurisé.

# 2 OBJECTIFS

---

- **Objectif principal** : Mettre en place un VPN site-à-site IPsec sécurisé entre deux sites.
- **Objectifs secondaires** :
  - Garantir la confidentialité, l'intégrité et l'authenticité des données échangées.
  - Utiliser DynFi comme pare-feu pour sécuriser et contrôler les flux de trafic réseau.
  - Assurer une haute disponibilité et une gestion centralisée de la sécurité réseau entre les sites.

# 3 MATÉRIEL ET LOGICIELS

---

- Pare-feu DynFi sur chaque site, configuré pour supporter les connexions VPN et les règles de sécurité.
- Routeurs ou dispositifs réseau capables de gérer le VPN IPsec.
- Logiciels ou dispositifs de gestion pour suivre la performance et la sécurité du réseau.

# 4 PRÉREQUIS

---

Avoir 2 DynFi prêt a l'emploi

## 5 RÉALISATION

### 5.1 CONFIGURATION DU TUNNEL IPSEC

Allez dans l'onglet « VPN > IPsec > Tunnel Settings [legacy] »

Cliquer « add phase 1 entry »

cette page va apparaître :

The screenshot shows the 'General information' section of the IPsec Tunnel Settings configuration page. The page is divided into several sections: General information, Phase 1 proposal (Authentication), Phase 1 proposal (Algorithms), and Advanced Options. Annotations with blue arrows point to specific fields:

- Remote gateway:** An annotation box says 'Adresse IP WAN du pare-feu destination'.
- Description:** An annotation box says 'Ex : VPN vert DynFi1'.
- Pre-Shared Key:** An annotation box says 'Écrire une clef de connexion ou coller une clef priver A écrire sur les deux Dynfi'.
- Encryption algorithm:** An annotation box says 'Choisir AES'.

The configuration details are as follows:

General information	
Disabled	<input type="checkbox"/> Disable this phase1 entry
Connection method	default
Key Exchange version	V2
Internet Protocol	IPv4
Interface	WAN
Remote gateway	
Dynamic gateway	<input type="checkbox"/> Allow any remote gateway to connect
Description	

  

Phase 1 proposal (Authentication)	
Authentication method	Mutual PSK
My identifier	My IP address
Peer identifier	Peer IP address
Pre-Shared Key	

  

Phase 1 proposal (Algorithms)	
Encryption algorithm	AES 128
Hash algorithm	SHA256
DH key group	14 (2048 bits)

  

Advanced Options	
Install policy	<input checked="" type="checkbox"/>
Disable Rekey	<input type="checkbox"/>
Disable Reauth	<input type="checkbox"/>
Tunnel Isolation	<input type="checkbox"/>
SHA256 96 Bit Truncation	<input type="checkbox"/>
NAT Traversal	Enable
Disable MOBIKE	<input type="checkbox"/>
Close Action	None
Unique	Replace

Une fois les étape prétendante fini cliquer sur «save» en bas de la page

Ensuite cliquer sur « add phase 2 entry »

cette page va apparaître :

General information		full help
Disabled	<input type="checkbox"/>	
Mode	Tunnel IPv4	
Description	<input type="text"/>	
Local Network		
Type	LAN subnet	
Address:	<input type="text"/>	32
Remote Network		
Type:	Network	
Address:	<input type="text"/>	32
Phase 2 proposal (SA/Key Exchange)		
Protocol	ESP	
Encryption algorithms	AES128	
Hash algorithms	SHA256	

Adresse IP LAN du pare-feu destination

Définir le masque qui correspond à IP LAN du pare-feu destination

## 5.2 CONFIGURATION DE RÈGLE IPSEC

Allez dans l'onglet « System > Gateways > Configuration »

Ensuite cliquer sur « add »

cette page va apparaître :

**Edit Gateway**

advanced mode aide complète

**Désactivé** ☐

**Nom**  Ex : VPN

**Description**

**Interface** WAN

**Famille d'Adresses** IPv4

**Adresse IP**  Adresse IP WAN du pare-feu destination

**Passerelle amont** ☐

**Passerelle Étendue** ☐

**Désactiver la surveillance de la passerelle** ☒

**Disable Host Route** ☐

**IP moniteur**

**Marquer cette passerelle comme hors-service** ☐

**Priorité** 255

Annuler Sauvegarde

Une fois les étapes précédentes finies cliquer sur «Sauvegarde»

Allez dans l'onglet « Firewall > Rules > IPsec »

Ensuite cliquer sur « add »

cette page va apparaître :

Edit Firewall rule

full help

Action	Pass
Disabled	<input type="checkbox"/> Disable this rule
Quick	<input checked="" type="checkbox"/> Apply the action immediately on match.
Interface	IPsec
Direction	in
TCP/IP Version	IPv4
Protocol	any
Source / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.
Source	any
Source	Advanced
Destination / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.
Destination	any
Destination port range	<div>any</div> <div>any</div>
Log	<input type="checkbox"/> Log packets that are handled by this rule
Category	
Description	PASS ALL
No XMLRPC Sync	<input type="checkbox"/>
Schedule	none
Gateway	default
Advanced features	Show/Hide
Rule Information	
Created	12/17/24 08:50:07 (root@192.168.2.20)
Updated	12/17/24 08:50:07 (root@192.168.2.20)
<div>SaveCancel</div>	

Une fois les étape prétendante fini cliquer sur «Save»