

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'emploie

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 :

General information

Disabled Disable this phase1 entry

Connection method: default

Key Exchange version: V2

Internet Protocol: IPv4

Interface: WAN

Remote gateway: Adresse IP WAN du pare-feu destination

Dynamic gateway: Allow any remote gateway to connect

Description: Ex : VPN vert DynFi1

Phase 1 proposal (Authentication)

Authentication method: Mutual PSK

My identifier: My IP address

Peer identifier: Peer IP address

Pre-Shared Key: Écrire une clef de connexion ou coller une clef privée A écrire sur les deux Dynfi

Phase 1 proposal (Algorithms)

Encryption algorithm: AES

Hash algorithm: SHA256

DH key group: 14 (2048 bits)

Choisir AES

Advanced Options

Install policy

Disable Rekey

Disable Reauth

Tunnel Isolation

SHA256 96 Bit Truncation

NAT Traversal: Enable

Disable MOBIKE

Close Action: None

Unique: Replace

Une fois les étapes prétendant fini cliquer sur «save» en bas de la page

Ensuite cliquer sur « add phase 2 entry »

cette page va apparaître :

General information

Disabled

Mode: Tunnel IPv4

Description:

Local Network

Type: LAN subnet

Address: 32

Adresse IP LAN du pare-feu destination

Remote Network

Type: Network

Address: 32

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

Phase 2 proposal (SA/Key Exchange)

Protocol: ESP

Encryption algorithms: AES128

Hash algorithms: SHA256

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

Famille d'Adresses

Adresse IP

Passerelle amont

Passerelle Étendue

Désactiver la surveillance de la passerelle

Disable Host Route

IP moniteur

Marquer cette passerelle comme hors-service

Priorité

Annuler **Sauvegarde**

Adresse IP WAN du pare-feu destination

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	any
Log	<input type="checkbox"/> Log packets that are handled by this rule
Category	<input type="text"/>
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)
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

Une fois les étapes précédentes finies cliquer sur « Save »