PETIT Antoine
Date de début : 20/12/2024
Date de fin : 20/12/2024

VPN Dynfi IPsec

Sommaire

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

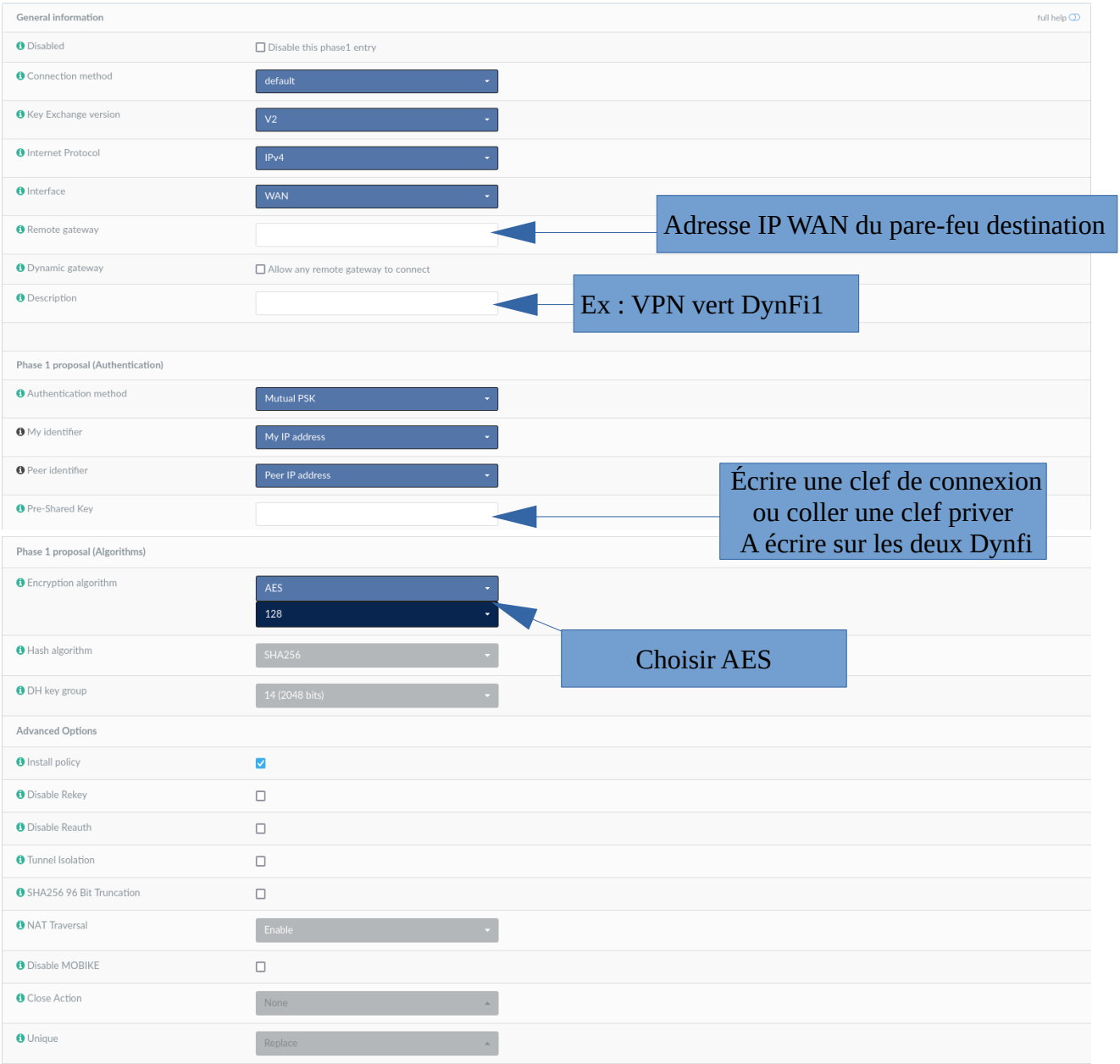
5 RÉALISATION

5.1 CONFIGURATION DU TUNNEL IPSEC

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

Cliquer « add phase 1 entry »

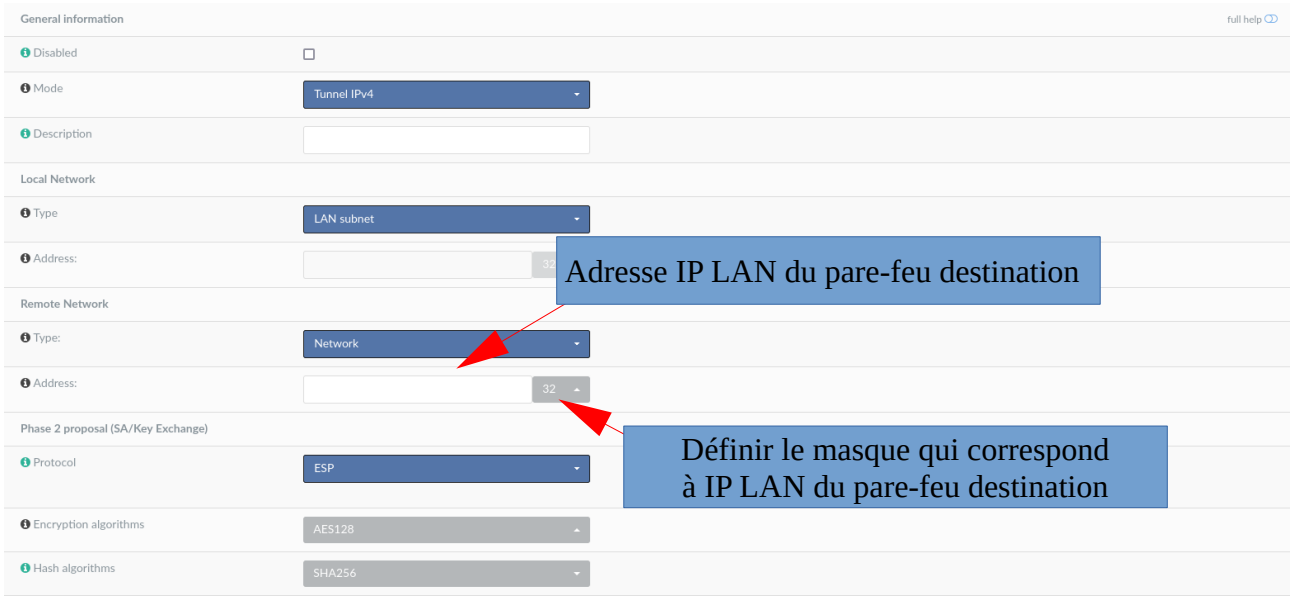
cette page va apparaître :



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 :

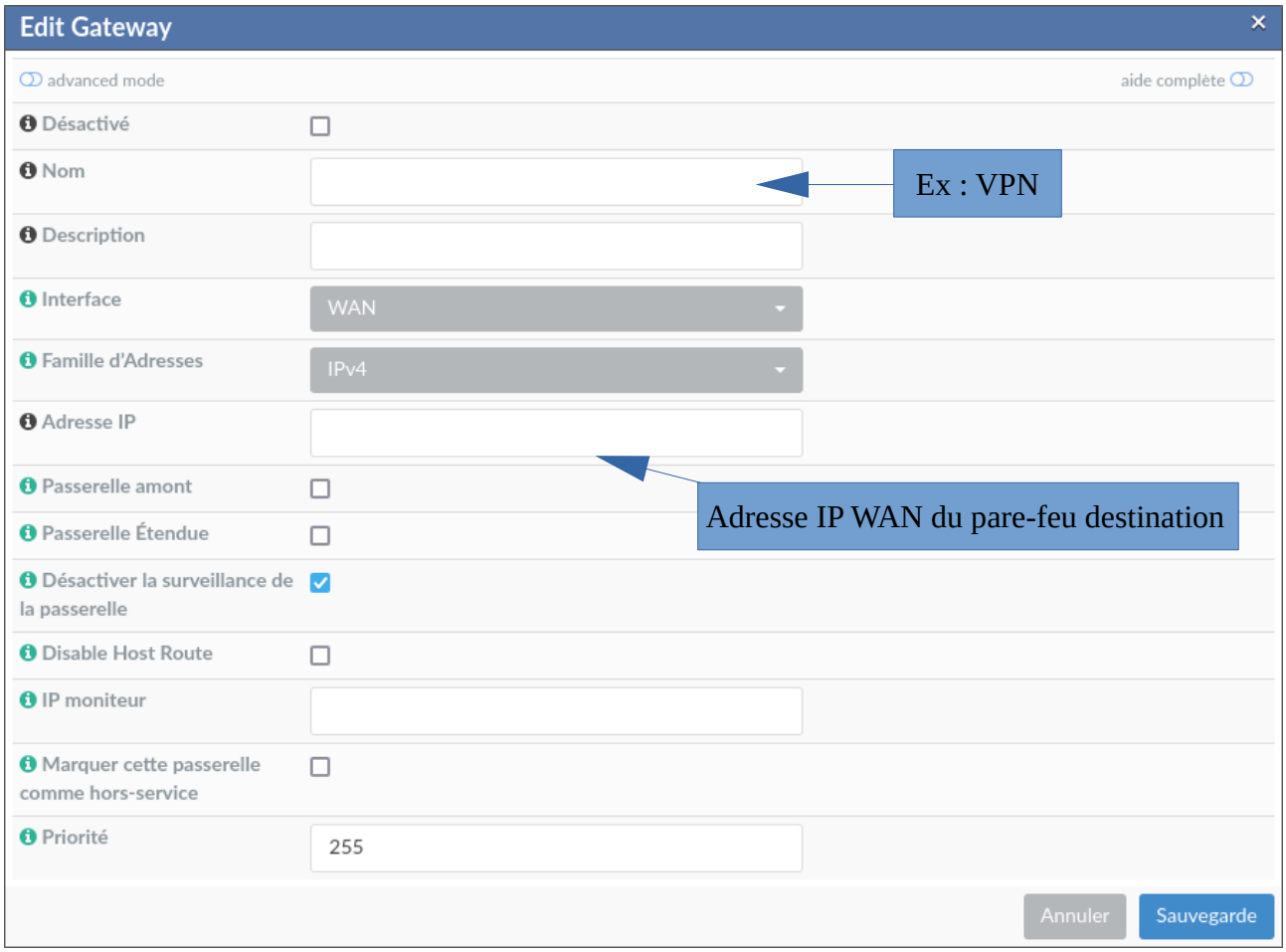


5.2 CONFIGURATION DE RÈGLE IPSEC

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

Ensuite cliquer sur « add »

cette page va apparaître :

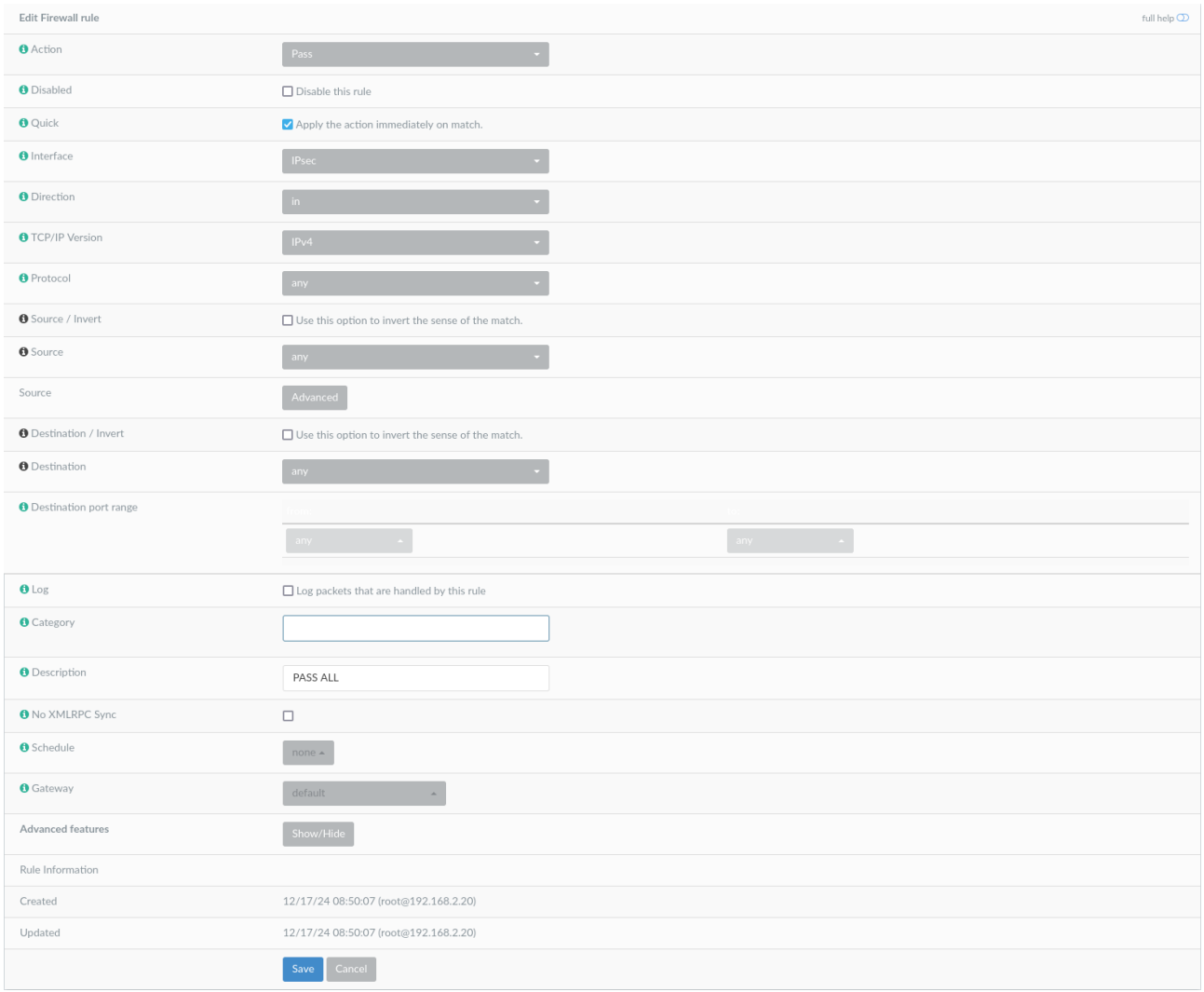


Une fois les étape prétendante fini cliquer sur «Sauvegarde»

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

Ensuite cliquer sur « add »

cette page va apparaître :



Une fois les étape prétendante fini cliquer sur «Save»