Mouhamed Messaoud HAMOUD **CAMPUS MEWO**

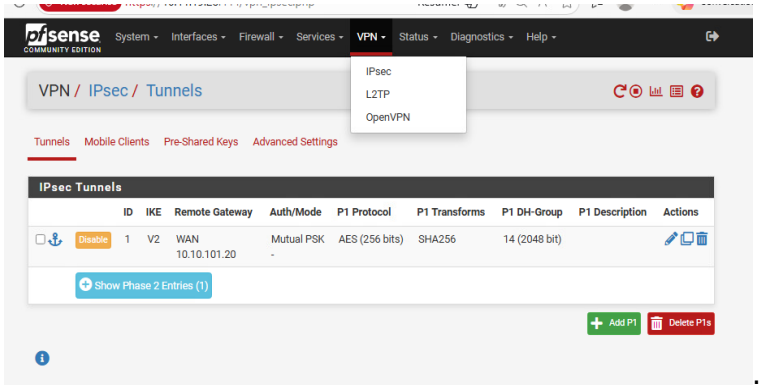
BTS SIO SISR 2024 / 2026

MISE EN PLACE D'UN VPN IPSec Site-to-Site

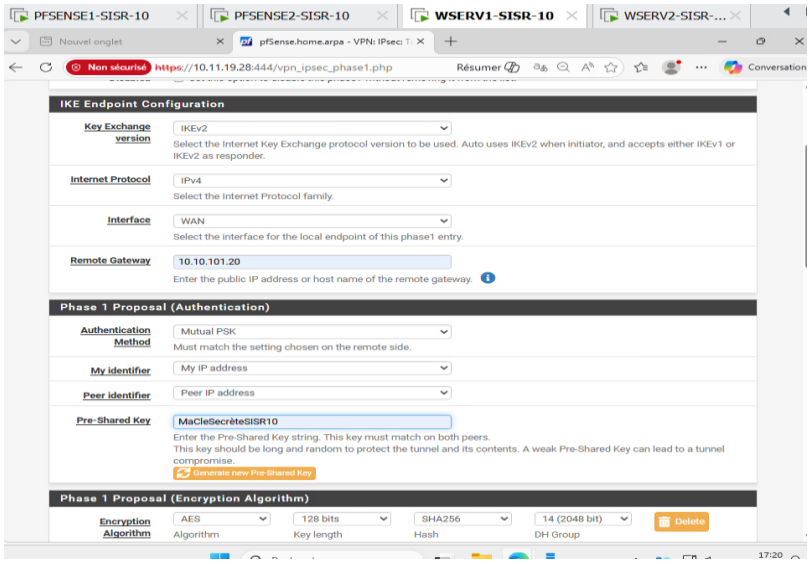
Contrairement à l'OpenVPN Client-to-Site que nous avons configuré précédemment pour un utilisateur nomade, l'**IPsec Site-to-Site** va créer un "pont" permanent entre nos deux bâtiments A et B. Les deux serveurs SRV1 et SRV2 pourront se pinguer comme s'ils étaient sur le même switch.

1- Configuration sur le pfSense 1 (10.11.19.28) du bâtiment A

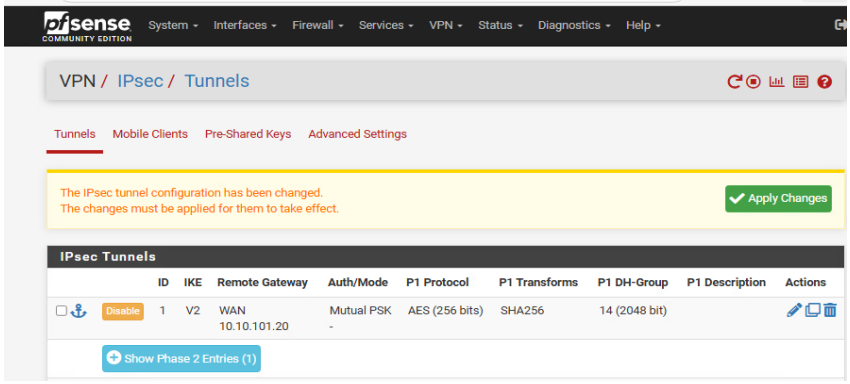
Je vais dans **VPN > IPsec > Tunnels** et je clique sur + Add P1



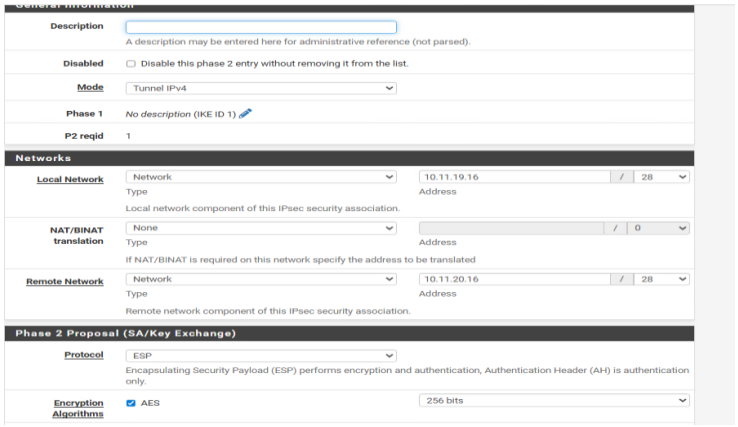
Je configure la phase 1, la poignée de main de ce tunnel.
Je mets l'**IP WAN 10.10.101.20** du pfSense 2 en **Remote Gateway** et une clé secrète que je noterai bien car elle doit être identique des deux côtés.



Une fois la P1 enregistrée, je clique sur +Add P2 juste en dessous de cette dernière.

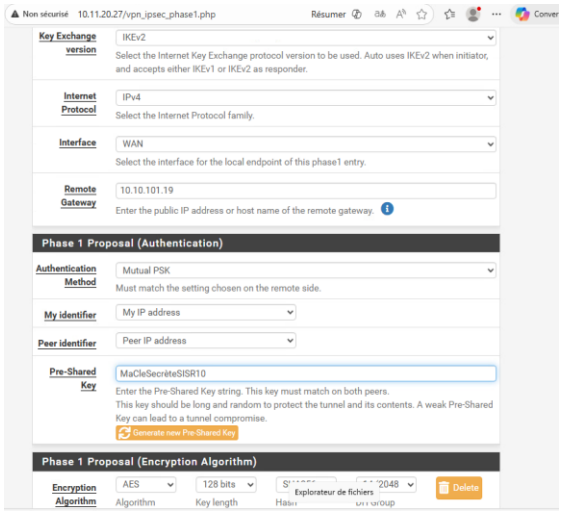


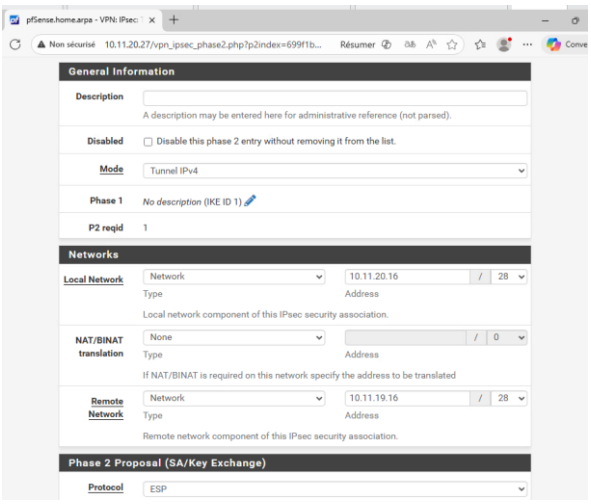
Pour la phase 2, le transport de données, je mets l'IP du réseau LAN du bâtiment A **10.11.19.16/28** en **Local Network** et celui du **LAN B 10.11.20.16/28** en **Remote Network**.



2- Configuration sur le pfSense 2 (10.11.20.27) du bâtiment B

C'est l'effet miroir, je fais exactement la même chose en inversant les IPs.



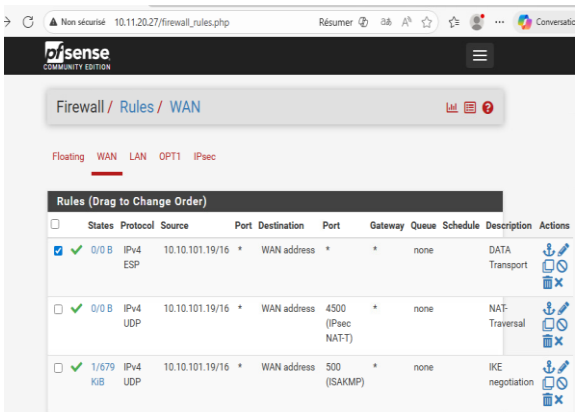


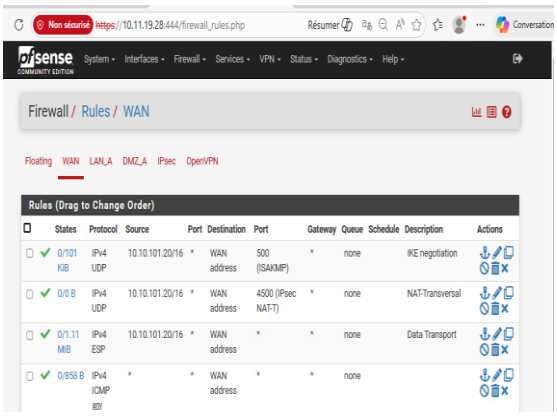
3- Les deux règles de Firewall obligatoires (Firewall > Rules)

Pour que le tunnel monte et que le ping passe, je dois ajouter des règles sur les deux pfSense.

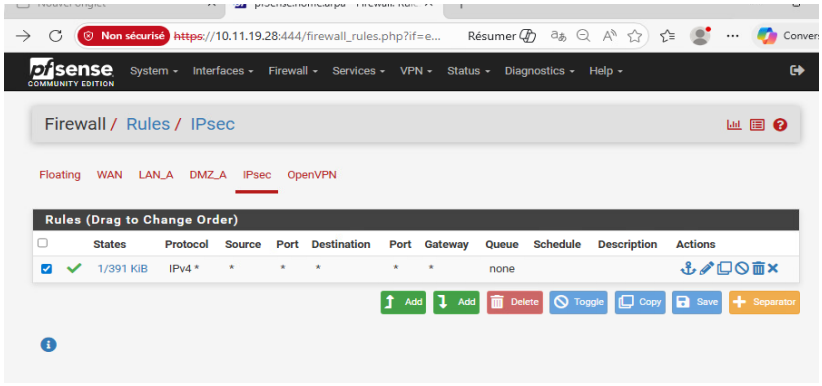
A- Sur l'interface WAN, j'autorise le protocole ESP et les ports UDP 500 et 4500 venant de l'autre pfSense.

-UDP 500 (IKE) : C'est le tunnel de contrôle. Les pfSense s'en servent pour vérifier la Pre-Shared Key (PSK) et se mettre d'accord sur les algorithmes (AES, SHA).
-UDP 4500 (NAT-T) : Utilisé pour la traversée de NAT, permettant aux paquets IPsec de passer par des dispositifs NAT sans modification.
-ESP (Encapsulating Security Payload) : C'est le "camion" qui transporte nos pings et nos fichiers. Sans lui, le tunnel est "établi" mais aucune donnée ne passe.



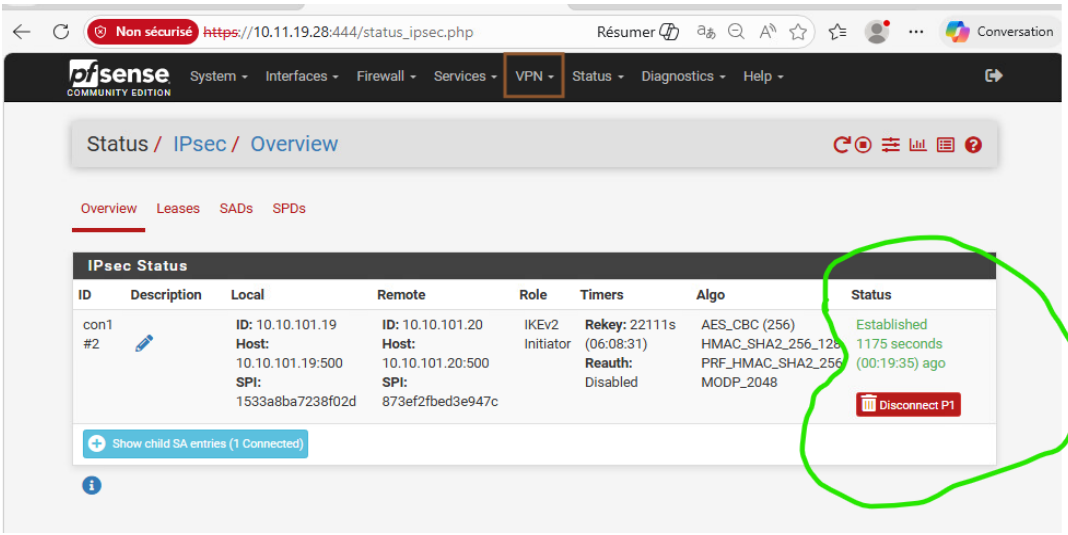


B- Sur l'onglet **IPsec**, je crée une règle **Any** ou **ICMP** pour le ping



4- Vérification du statut

Une fois terminé, je vais dans **Status > IPsec** et je dois voir un message **Established.**


Non sécurisé
https://10.11.19.28:444/status_ipsec.php
Résumer
Conversation
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Status / IPsec / Overview
Overview
Leases
SADs
SPDs
IPsec Status
ID
Description
Local
Remote
Role
Timers
Algo
Status
con1
#2
ID: 10.10.101.19
Host:
10.10.101.19:500
SPI:
1533a8ba7238f02d
ID: 10.10.101.20
Host:
10.10.101.20:500
SPI:
873ef2fbed3e947c
IKEv2
Initiator
Rekey: 22111s
(06:08:31)
Reauth:
Disabled
AES_CBC (256)
HMAC_SHA2_256_128
PRF_HMAC_SHA2_256
MODP_2048
Established
1175 seconds
(00:19:35) ago
Disconnect P1
Show child SA entries (1 Connected)