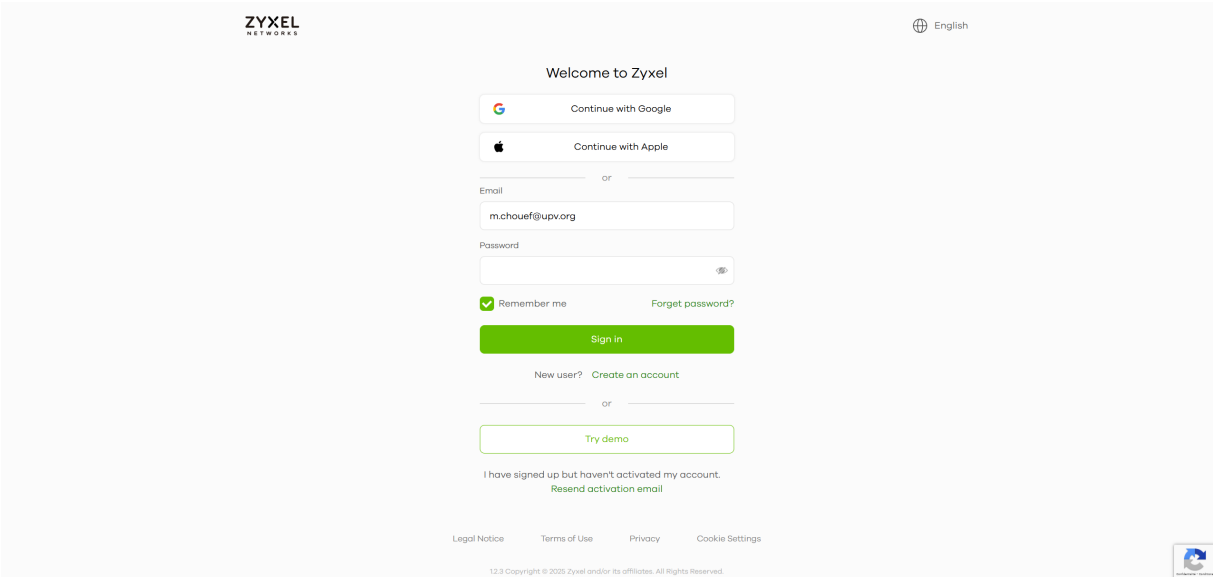
CONFIGURATION DE TUNNEL VPN

Dans le cadre du service informatique, j’ai dû configurer des tunnels VPN entre plusieurs sites équipés de pare-feux Zyxel. Chaque pare-feu est rattaché à un site différent dans la plateforme cloud Nebula. L'objectif est de sécuriser la communication entre ces sites via des tunnels VPN.

Les modèles utilisés sont un Zyxel ATP7000 pour un site et un Zyxel USG100H pour un autre site.

Étape 1 : Connexion à la plateforme Nebula

Je me suis connecté à la plateforme Nebula à l’adresse suivante : https://nebula.zyxel.com

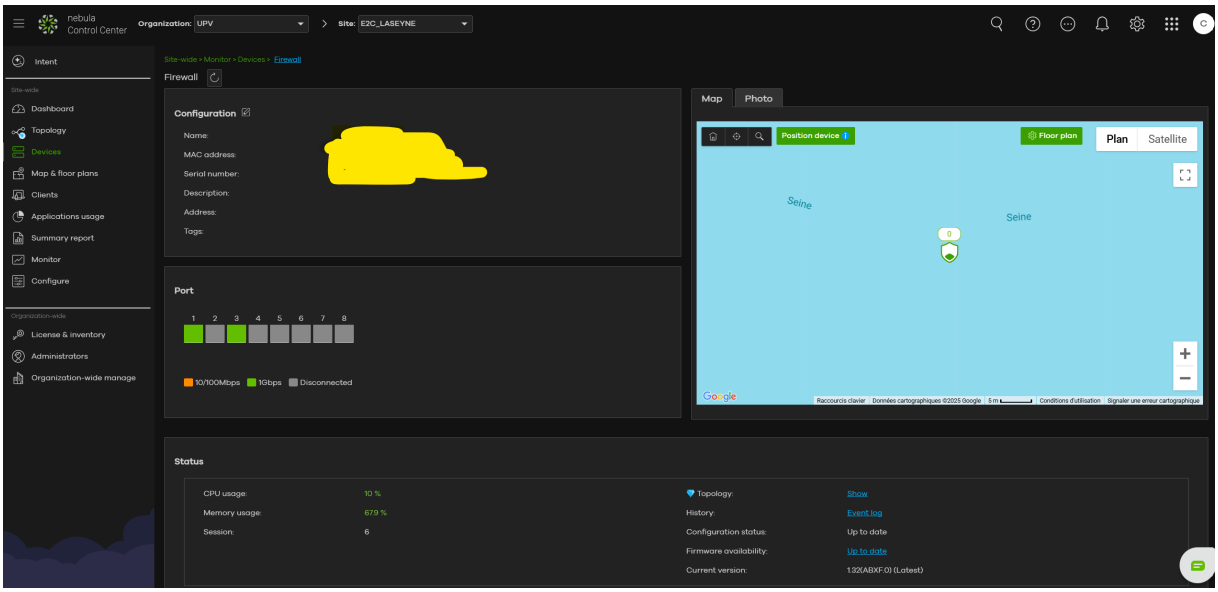


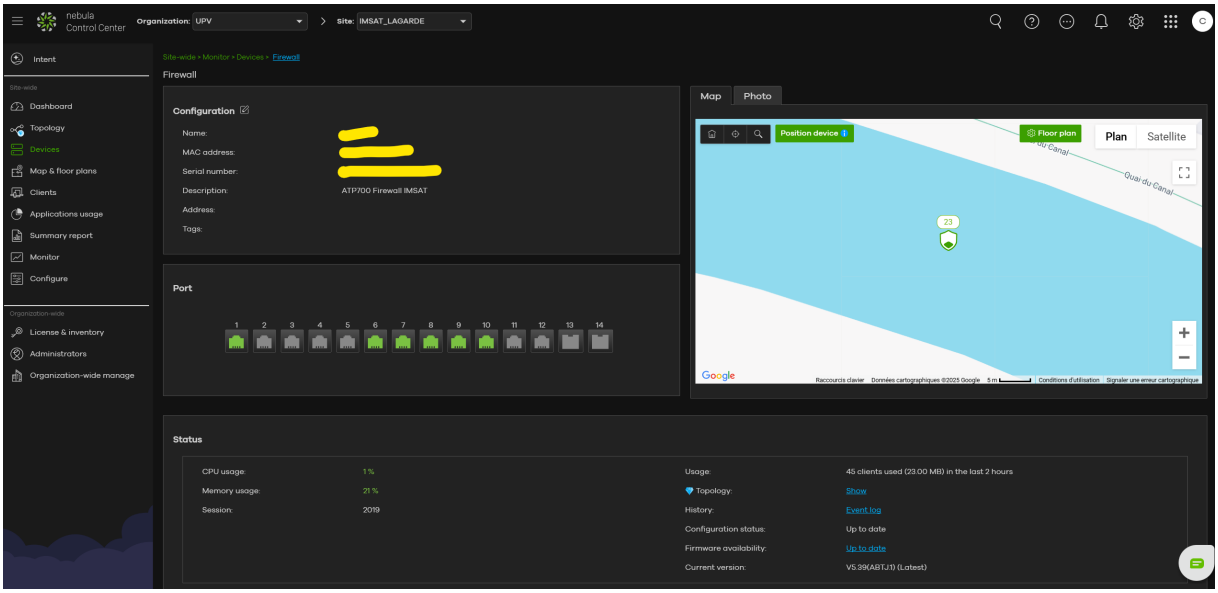
J’ai utilisé mon compte administrateur pour accéder à la gestion de chaque site, indépendamment, dans Nebula.

Étape 2 : Vérification des périphériques et des licences VPN

Depuis le menu « Site-wide > Device » pour chaque site, j’ai vérifié que :

- Les pare-feux ATP7000 et USG100H étaient bien enregistrés et en ligne.
- Les firmwares étaient à jour.

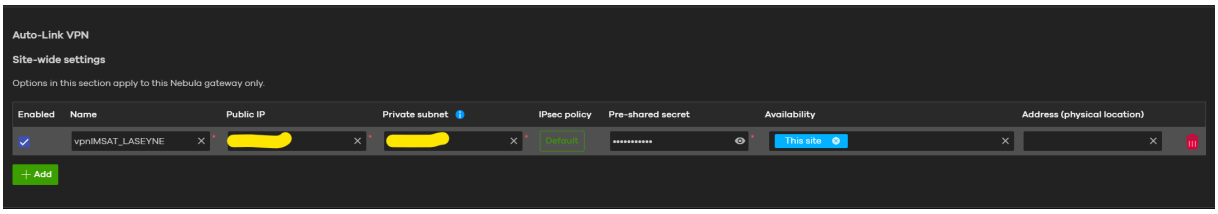




Étape 3 : Création du tunnel VPN IPSec

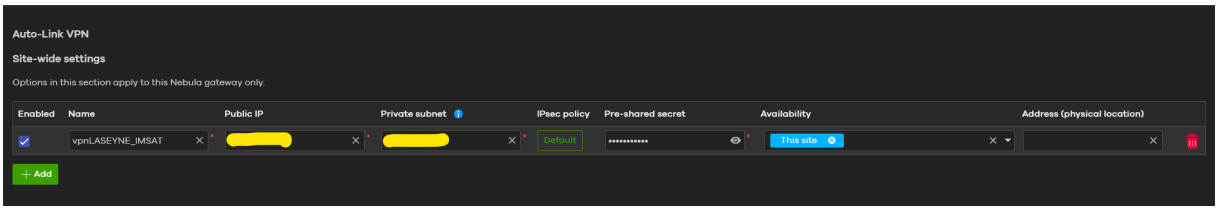
Sur le premier site (ATP7000) :

- J'ai cliqué sur Add VPN Connection.
- J'ai configuré :
  - Type : Site-to-Site VPN
  - VPN Gateway : Nouvelle Gateway
  - Peer IP Address : Adresse publique du pare-feu USG100H
  - Pre-shared key : Une clé secrète commune que j'ai définie.
  - Local Policy : Réseau local du site ATP7000
  - Remote Policy : Réseau distant du site USG100H



Sur le second site (USG100H) :

- J'ai créé une connexion identique mais en inversant les rôles :
  - Peer IP Address : Adresse publique du pare-feu ATP7000
  - Pre-shared key : La même que celle définie sur l'ATP7000
  - Local Policy : Réseau local du site USG100H
  - Remote Policy : Réseau distant du site ATP7000



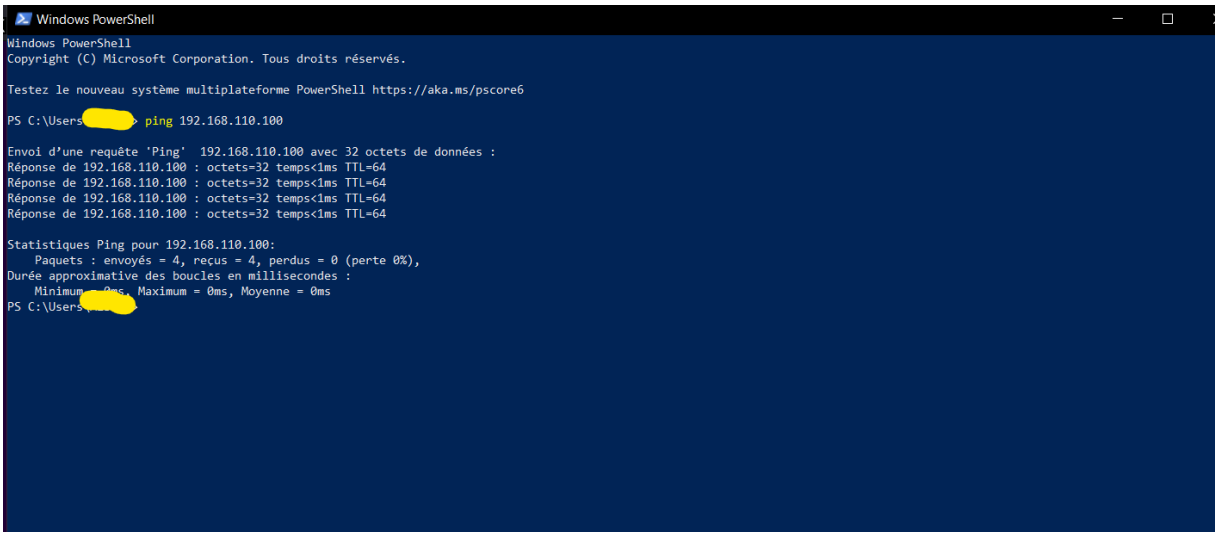
Paramètres communs utilisés :

- IKE Version : IKEv2
- Encryption : AES256
- Authentication : SHA256
- DH Group : Group 14
- PFS : Activé

Étape 4 : Application et vérification du tunnel VPN

Le tunnel est passé en Connected après l'établissement du premier échange de clés.

J'ai ensuite effectué un ping entre les réseaux des deux sites pour valider que les ressources étaient accessibles.



Conclusion

Cette activité m'a permis de configurer manuellement un tunnel VPN site-à-site entre deux sites distincts, en utilisant un ATP7000 et un USG100H sur. J'ai appris à paramétrer un tunnel IPSec classique, sécuriser les flux inter-sites et vérifier la connectivité réseau.

Compétences validées :

- Mettre à disposition des utilisateurs un service informatique
- Gérer le patrimoine informatique