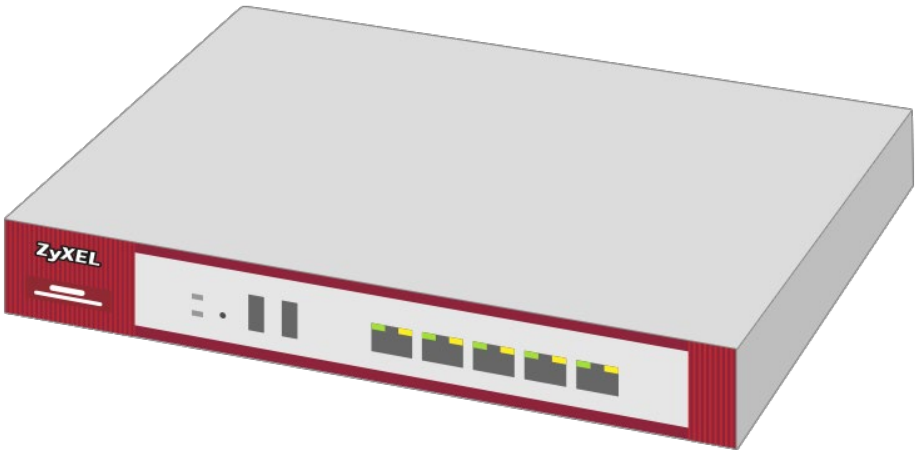
ZYXEL
Your Networking Ally



Bases pour la protection d'un pare-feu

Série pare-feu Zyxel
à partir de la version du firmware 5.35

Knowledge Base KB-3823
Janvier 2023

BASES POUR LA PROTECTION D'UN PARE-FEU

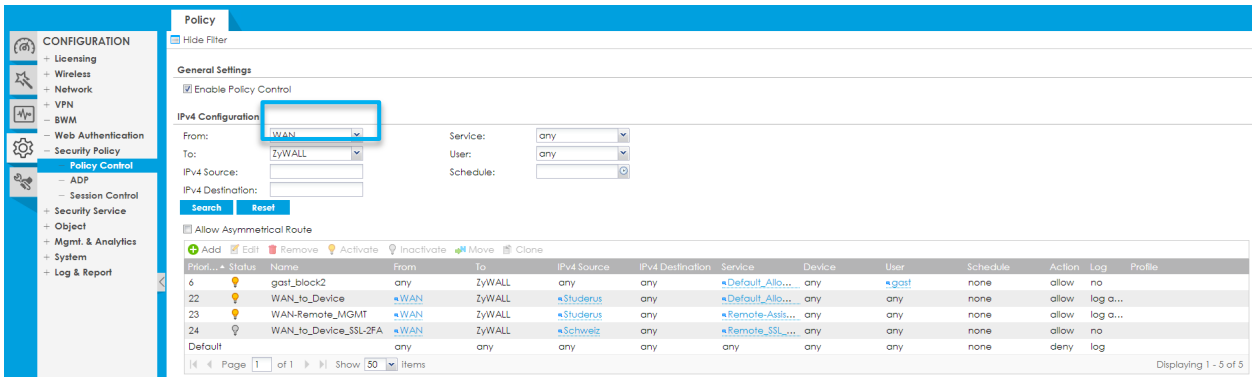
Le pare-feu est le premier obstacle pour des pirates sur Internet. Un pare-feu protège le réseau local des accès non autorisés. Il est ainsi partie intégrante de tout concept de sécurité. Mais que se passe-t-il si le pare-feu lui-même est la cible d'attaques de pirates et peut donc devenir une menace potentielle ? Le guide suivant a pour but de fournir des informations sur la manière de limiter les possibilités d'attaque.

POLICY CONTROL

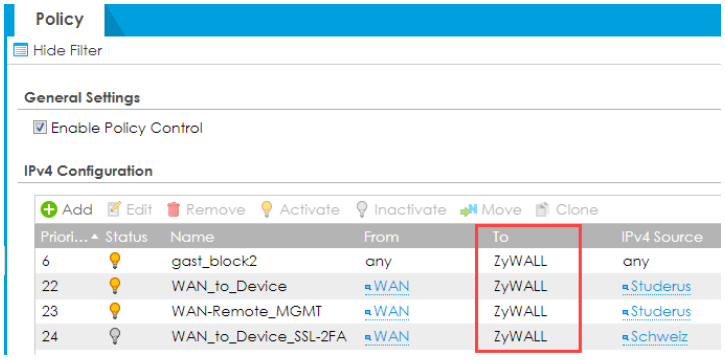
En principe, il faut limiter le nombre d'utilisateurs qui ont accès au pare-feu à aussi peu que possible. Pour garantir cela, il est conseillé de limiter autant que possible les droits d'accès.

Les règles de pare-feu sont créées dans le menu suivant :

Configuration > Security Policy > Policy Control



La zone ZyWALL joue un rôle particulier. En principe, il est seulement possible de créer des règles vers la zone ZyWALL. Elle contient toutes les adresses d'interface du pare-feu. Par exemple, l'adresse par défaut 192.168.1.1 n'appartient pas à la zone LAN1, mais à la zone ZyWALL.



Avec les paramètres par défaut, l'accès au pare-feu est largement ouvert. Il convient donc de les limiter davantage.

Restriction des règles « Policy Control »

Les règles de pare-feu peuvent être restreintes sur la base de plusieurs critères. Pour l'accès au pare-feu, 3 critères sont principalement utiles :

1. IPv4 Source (objets d'adresse),
2. service,
3. utilisateur.

Ces éléments sont créés en tant qu'objets.

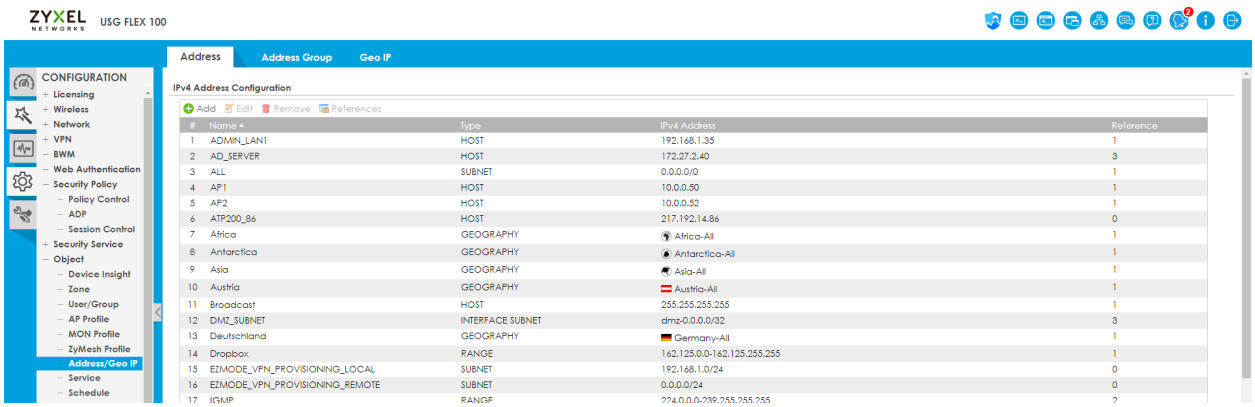
Objets d'adresse

Il existe en général 3 types d'objets adresse. De quels types s'agit-t-il ?

1. Adresses IP,
2. adresses FQDN,
3. adresses GeoIP.

Les objets adresses peuvent être rassemblés dans un groupe. Mais il n'est pas possible de mélanger différents types d'adresses.

Configuration > Object > Address > Address > Add :



1. Adresses IP

Lorsque c'est possible, il convient d'utiliser des adresses IP, car elles sont uniques. Il existe plusieurs types d'adresses IP :

1. Host > Décrit une adresse IP unique
2. Range > Il est possible de saisir n'importe quelle plage, définie par les adresses de début et de fin
3. Subnet > Celui-ci peut être créé en entrant un masque de sous-réseau ou un CIDR (par ex. /24)
4. Interface IP > prend en charge l'adresse IP d'une interface et s'adapte dynamiquement
5. Interface Subnet > prend en charge dynamiquement le Subnet d'une interface
6. Interface Gateway > prend en charge la passerelle d'une interface du type WAN ou général.

Host, Range, Subnet

Les types d'adresse Host, Range et Subnet servent spécialement en tant que IPv4 Source. Si un accès a lieu depuis le WAN, l'adresse IP publique du poste distant est indiquée.
À partir d'un réseau local, ces objets permettent de créer des groupes avec des autorisations différentes.

Interface IP

Cet objet peut être utilisé si l'accès ne doit être possible que sur une adresse IP donnée. Si, par exemple, il y a 2 interfaces WAN, mais qu'un service ne doit être disponible que sur une seule interface, l'IP de l'interface peut être saisie comme destination IPv4 dans la règle de contrôle des politiques.

Interface Subnet

Ce type d'adresse convient si des règles uniformes doivent être créées pour une interface locale (par ex. LAN1).

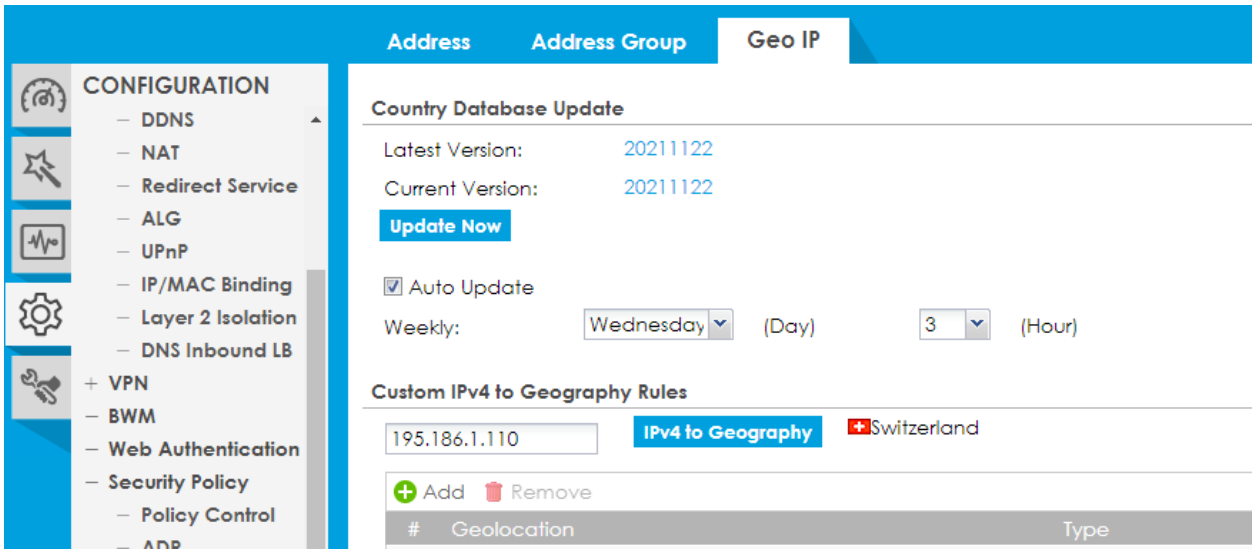
Passerelle interface

Ce type d'adresse n'est pas pertinent pour l'accès au pare-feu.

2. Objets FQDN

Pour les objets FQDN, il est possible de saisir un nom au lieu d'une adresse IP, par exemple www.mydomain.com. Ce type d'entrées convient surtout si un accès a lieu depuis le WAN et le poste distant n'a pas d'adresse IP publique statique. Dans ce cas, un nom DynDNS peut être utilisé à la place de l'adresse IP. Un serveur DNS rapide est nécessaire pour les objets FQDN. Il est également possible d'utiliser des entrées joker, comme *.mydomain.com. Ils ne peuvent toutefois pas être utilisés à cette fin.

Adresses Geo IP

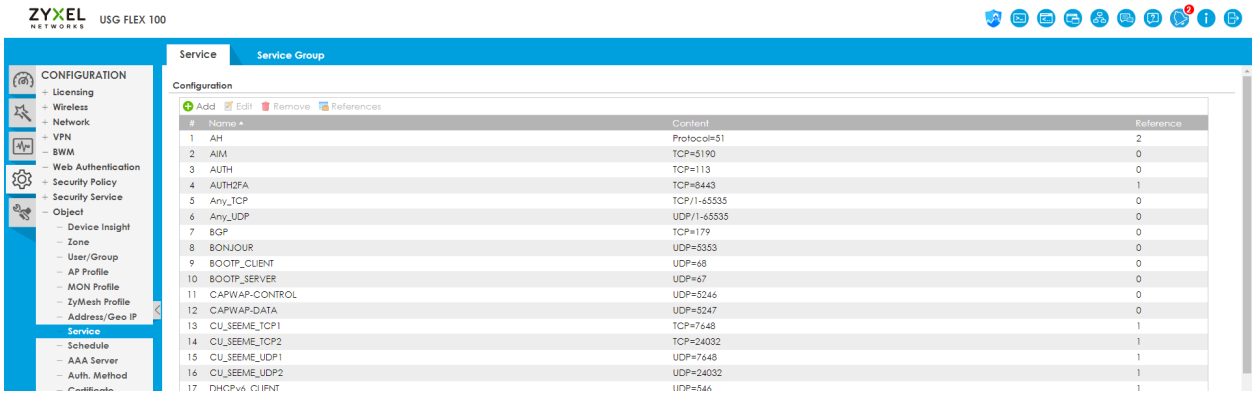


Avec GeoIP, il est possible de créer des objets basés sur des pays ou des régions. Le service fait appel à une base de données externe et devrait être régulièrement mis à jour. GeoIP n'offre pas de protection fiable, car il est très facile de manipuler l'adresse d'origine au moyen de services VPN librement disponibles.

Objets de service

Les objets de service permettent de définir les services auxquels l'accès est accordé ou refusé dans les paramètres de contrôle des politiques. Les services peuvent être regroupés. Les services peuvent également être utilisés ailleurs, par exemple dans les Policy Routes et les entrées NAT.
Outre les objets de service normaux, il existe quelques objets spéciaux tels que « Wiz_2FA, Wiz_HTTP, Wiz_HTTPS et Wiz_SSLVPN ». Le port de ces services s'adapte automatiquement lorsqu'il est redéfini dans le menu correspondant.

Configuration > Object > Service



User

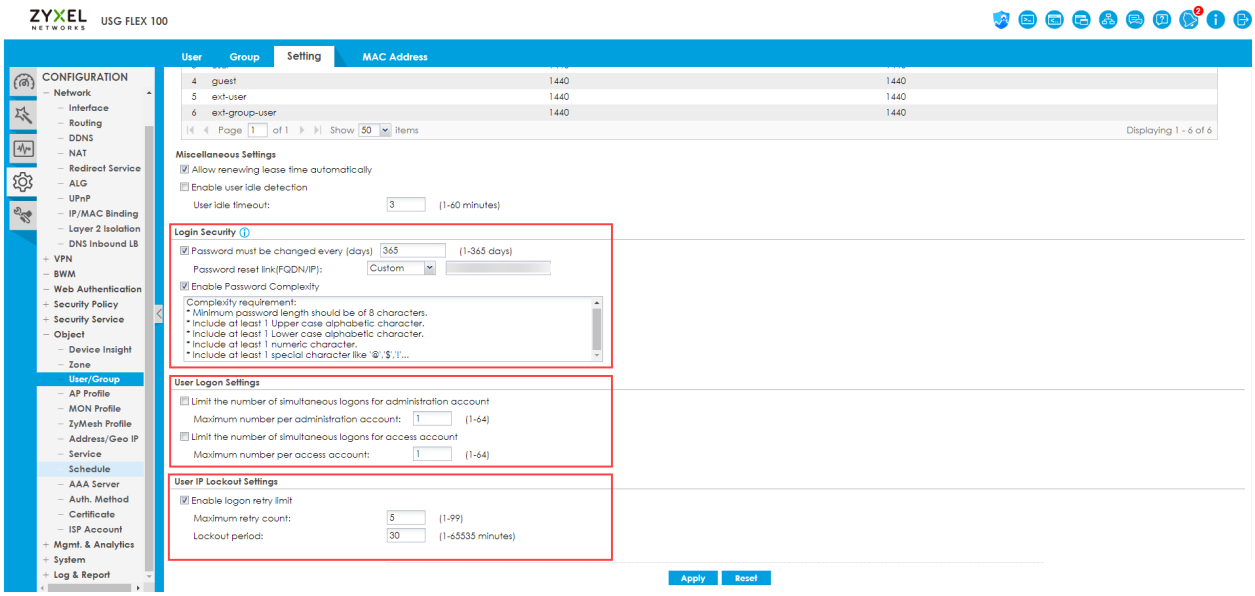
Configuration > Object > User

Il existe différents types d'utilisateurs (user) :
User : admin, peut apporter des modifications à la configuration,
User : limited-admin, peut accéder à la configuration mais ne peut pas la modifier,
User : user, peut s'authentifier par authentification à double facteur (2FA),
User : guest, peut se connecter au pare-feu,
User : ext-user/ext-group-user, s'authentifie sur un serveur externe,

Les « Built-in User » sont des utilisateurs prédéfinis qui ne peuvent pas être supprimés et qui sont destinés à des fins spécifiques.

Les utilisateurs doivent être définis de telle sorte qu'ils ne disposent que des autorisations nécessaires.
Les utilisateurs VPN ou 802.1x, par exemple, sont généralement définis en tant que type d'utilisateur « User ».

Configuration > Object > User/Group > Settings



Securité Login

Définit si les mots de passe doivent être modifiés et dans quel délai, et si une complexité des mots de passe est nécessaire.

Paramètres User Logon

Définit le nombre de fois qu'un utilisateur peut se connecter en même temps. Si la limite est fixée à 1, il peut arriver qu'un administrateur se bloque lui-même.

Paramètres User IP Lockout

Les entrées définissent le nombre de fois qu'une mauvaise saisie du mot de passe est autorisée jusqu'à ce que l'utilisateur soit bloqué pour une période donnée. Ce réglage protège surtout contre les attaques par force brute.

Règles « Policy Control » conseillés

From: WAN To: ZyWALL

Il est vivement recommandé de fermer tous les services qui ne sont pas expressément nécessaires.

Services fréquemment utilisés

VPN IPSec (IKEv1, IKEv2, L2TP) :
ESP, IKE, NATT, (L2TP-UDP)

VPN SSL :
Wiz_SSLVPN

L'authentification à double facteur pour VPN :
Wiz_2FA

Un accès à distance via HTTP/HTTPS :
Wiz_HTTP, Wiz_HTTPS

Pour éviter autant que possible les risques de sécurité, une gestion à distance s'effectue idéalement via IPSecVPN. Les adresses sources devraient, si possible, être limitées.
Le VPN SSL est déconseillé, car il offre un vecteur d'attaque possible via SSL.

Un accès à distance via HTTPS :
Si un accès à distance via HTTP/HTTPS est nécessaire, l'adresse source doit toujours être limitée à une adresse IP ou à un FQDN. L'utilisation de GeoIP comme adresse source n'est pas sûre et offre un potentiel d'attaque considérable. Pour la gestion HTTPS, il est recommandé d'utiliser un port alternatif.

From: Zone VPN To: ZyWALL (client vers site)

Par défaut, tous les ports sont ouverts. En principe, dans la plupart des cas, très peu de services sont nécessaires. Il s'agit par exemple du DNS et de L2TP-UDP. Pour d'autres services, l'accès doit être bloqué. Si une gestion à distance via VPN client à site est souhaitée, l'accès au pare-feu peut être limité à un utilisateur. Cela ne fonctionne toutefois que si l'utilisateur s'est déjà connecté au pare-feu lors de l'établissement du tunnel.

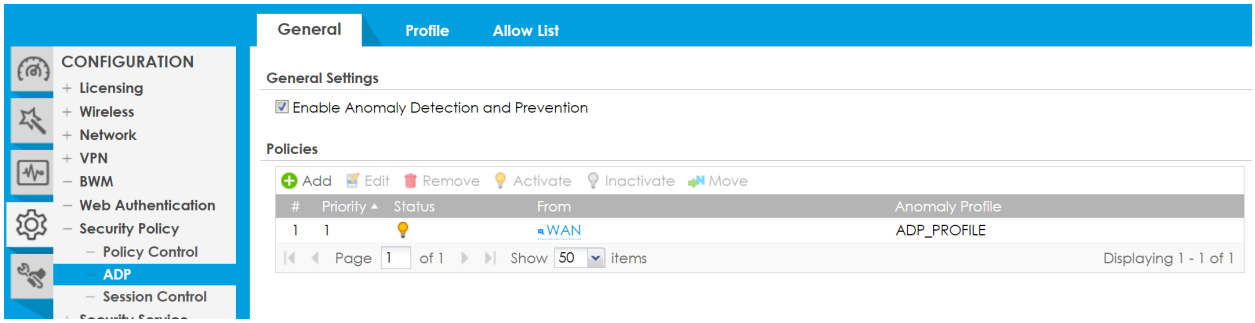
From: LAN To: ZyWALL

Ici aussi, les droits d'accès doivent être limités. L'accès complet au pare-feu ne devrait être accordé qu'à un LAN de gestion spécial ou à certaines adresses IP d'administrateurs. Pour que certains services fonctionnent correctement, l'accès au pare-feu doit être garanti. Cela concerne par exemple DNS, Multicast, Radius-Auth, NetBIOS, SNMT, SSO, etc. Les accès effectivement nécessaires dépendent fortement de la topologie du réseau et des technologies utilisées.

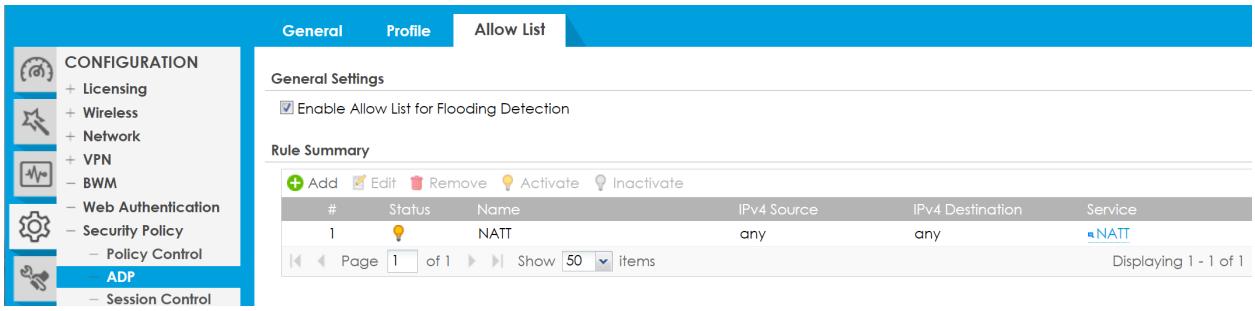
DÉTECTION ET PRÉVENTION D'ANOMALIE (ADP)

Configuration > Security Policy > ADP

L'ADP offre une protection contre les scans de ports et les comportements réseau inhabituels. Il est recommandé d'activer l'ADP avec le profil par défaut de la zone WAN. Des adaptations individuelles peuvent être apportées au profil en cas de problèmes.



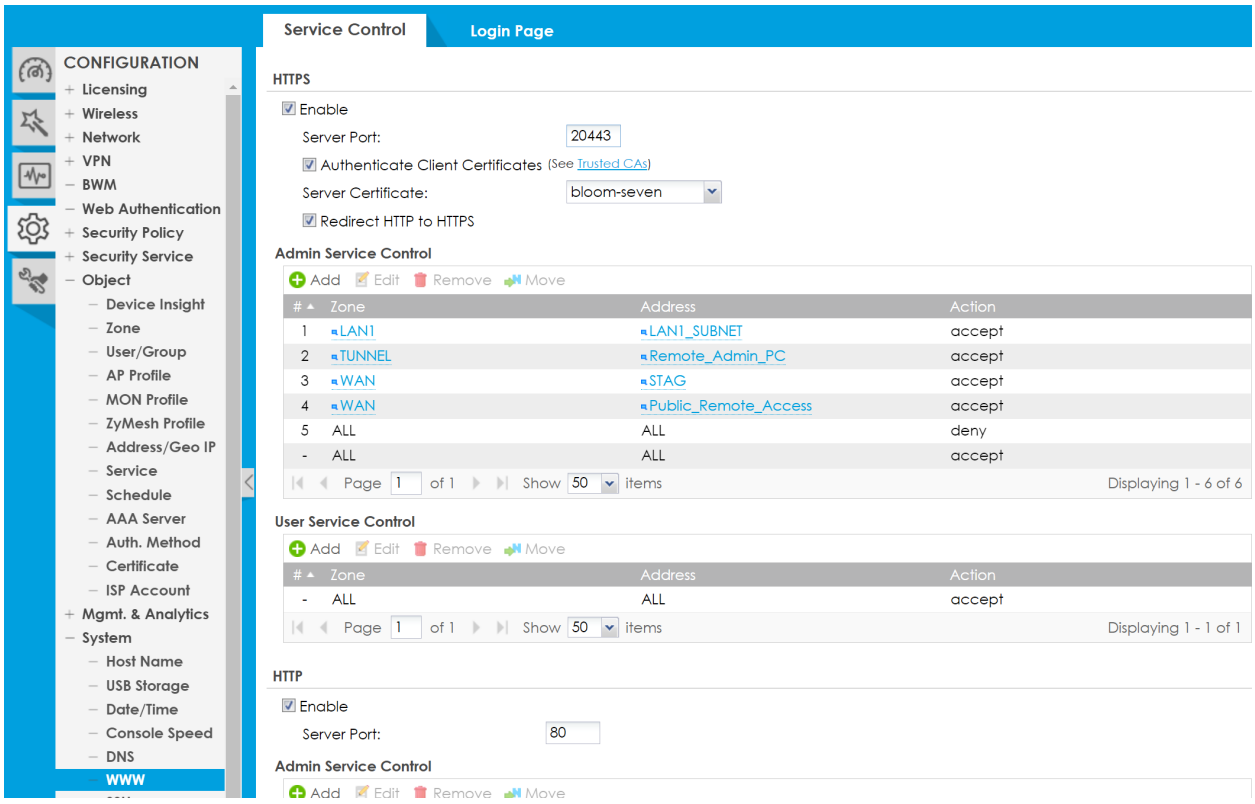
Dans certains cas, ADP peut affecter certains services. Cela concerne surtout la détection d'inondation. Pour cette raison, la protection contre l'inondation peut être désactivée pour certains services, par exemple NATT. Un tel réglage n'est utile qu'en cas de problèmes.



GESTION À DISTANCE VIA HTTPS

Certains réglages spécifiques dans les paramètres WWW ont une influence directe sur la sécurité du système.

Configuration > System > WWW



Port serveur

Pour la gestion à distance, il ne faut pas utiliser le port standard 443, car il est toujours scanné en cas d'attaques automatisées. Les ports alternatifs fréquemment utilisés (p. ex. 8443) ne sont pas non plus idéaux.

Rediriger HTTP vers HTTPS

Tous les appels HTTP de l'interface utilisateur graphique sont redirigés vers HTTPS. Attention ! Ce paramètre ne doit pas être activé si l'authentification web est utilisée. Dans tous les autres cas, cette option doit être activée.

Contrôle service admin

Il est possible de définir ici qui peut avoir un accès d'administrateur au pare-feu. Il est conseillé de limiter l'accès à certaines adresses IP. Seules les adresses IP sont autorisées comme objets d'adresse. La dernière règle (ici la règle 5) à créer est la règle ALL/ALL/deny. Lors de la création de la règle, il convient d'être prudent afin de ne pas s'exclure soi-même. C'est pourquoi il faut d'abord créer les règles Accept avant de créer la règle Deny en dernière position.

User Service Control (contrôle service utilisateur)

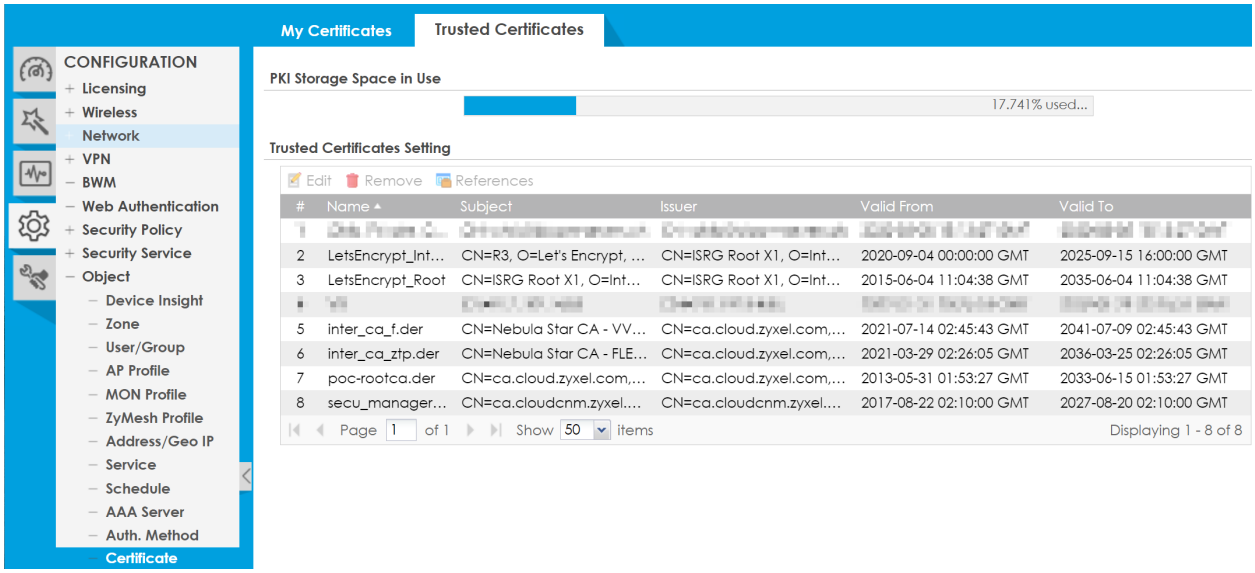
Dans le « User Service Control », on définit quels clients sont autorisés à s'authentifier sur le pare-feu.
La règle est pertinente pour le SSL-VPN, 2-FA, VPN Configuration Provisioning et WEB-Authentication.
Si cela n'est pas utilisé, une règle deny peut également être définie.

Authenticate Client Certificates

Si l'option « Authenticate Client Certificate » est activée, le client doit s'autoriser avec un certificat valide. Dans le cas contraire, la connexion est refusée. Cela concerne les accès via **HTTPS** et **VPN SSL**. VPN Configuration_Profisioning avec SecuExtender ne fonctionne pas si cette option est activée. Cependant, l'appel de la fenêtre 2FA reste possible sans certificat.

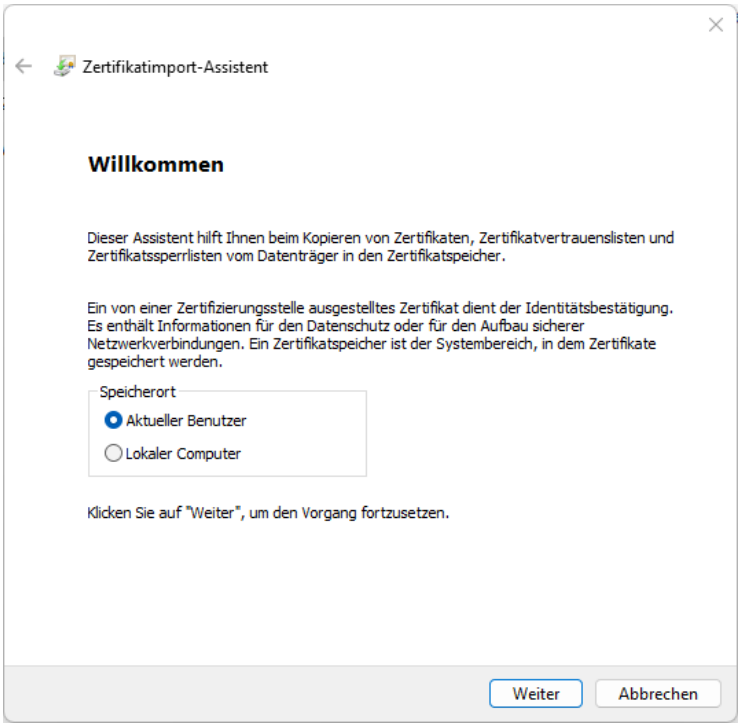
Pour qu'un certificat soit considéré comme fiable par le pare-feu, la chaîne de confiance de l'autorité de certification doit être installée. Celle-ci comprend généralement un certificat racine et un certificat intermédiaire. Le pare-feu fait confiance à chaque certificat avec une chaîne de certificats valable ainsi qu'à ses propres certificats auto-signés. Il convient de noter que certains navigateurs refusent systématiquement les certificats auto-signés (actuellement les navigateurs basés sur Firefox). Le certificat client ne doit pas être installé sur le pare-feu.

Configuration > Object > Certificate > Trusted Certificates

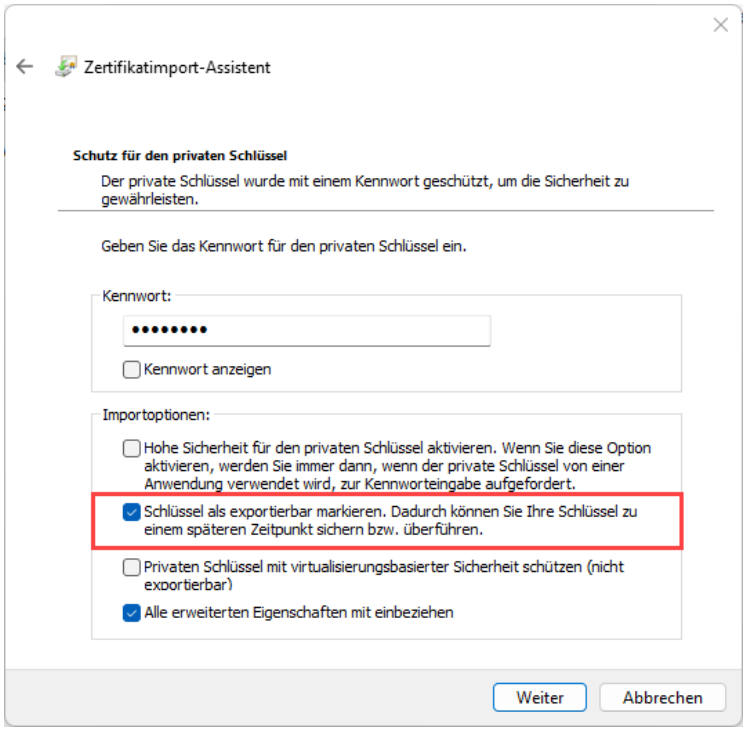


Le certificat client avec clé privée est installé sur le client. Voici une installation manuelle sous Windows :

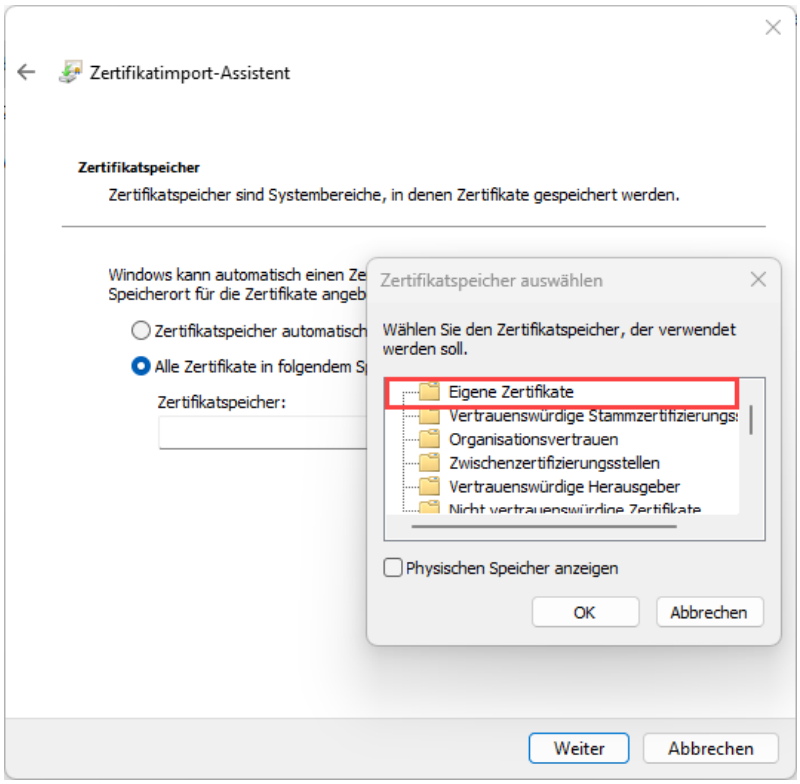
Ouvrir le certificat avec clé privée (PFX ou P12) par un double-clic et l'importer dans l'utilisateur actuel.



Lors de l'importation, veiller à ce que l'option « Marquer les clés comme exportables » soit activée.



L'importation se fait dans le magasin de certificats « Mes certificats ».



SERVICES GESTION À DISTANCE

Configuration > System

Sur le pare-feu, il existe plusieurs services qui ne sont que rarement ou pas du tout utilisés. Ces services peuvent être complètement désactivés.

SSH

Ce service peut être utilisé, par exemple, lorsque des modifications de configuration sont effectuées avec un script automatique. Si SSH n'est pas utilisé régulièrement pour l'administration, le service peut être désactivé. Pour les entrées CLI, la Web Console peut également être utilisée à la place de SSH.

TELNET

N'est pas nécessaire dans la plupart des cas et peut être désactivé.

FTP

Le FTP permet par exemple d'actualiser le firmware ou de télécharger des fichiers de configuration. Le FTP doit être activé si HA-Pro est utilisé. Si ce n'est pas le cas, FTP peut être désactivé. Si le service est utilisé de manière sporadique, il peut être activé temporairement en cas de besoin.

SNMP

Ce service est nécessaire pour la surveillance du réseau et est requis pour des solutions comme par ex : PRTG. Si aucune surveillance du réseau n'est effectuée, le service peut être désactivé.

ZON

Permet l'échange d'informations avec des appareils voisins (modèle, nom, firmware, adresse MAC, adresse IP) via LLDP ainsi qu'avec le logiciel ZON de Zyxel sur le même LAN. Le service n'est pas nécessaire pour le fonctionnement normal.

VPN

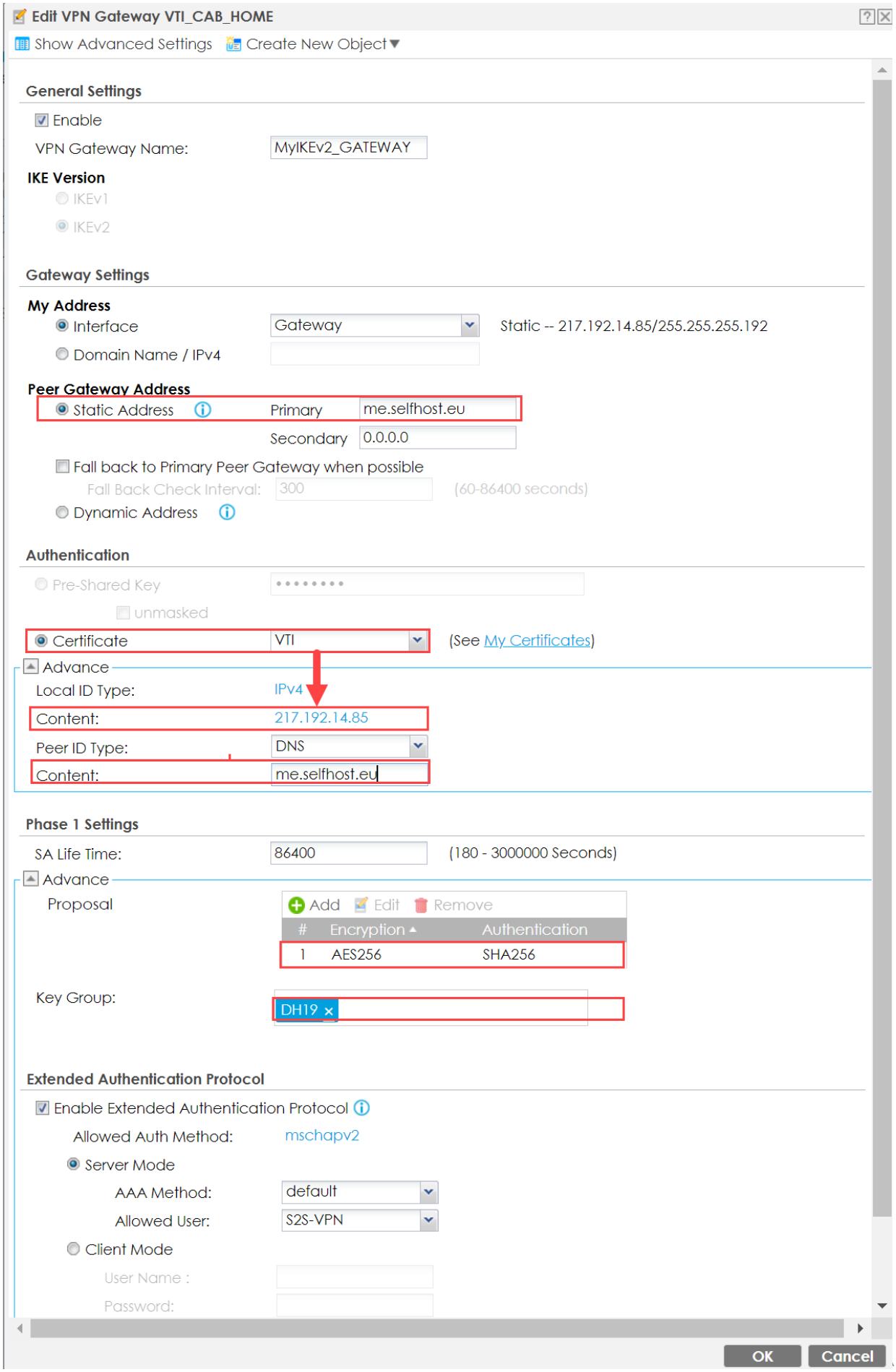
IPSec-VPN

Site à site

Lors de l'utilisation de tunnels site à site, une adresse de passerelle d'égal à égal doit être saisie dans la mesure du possible. Si l'autre partie a une adresse IP dynamique, il est également possible d'utiliser un nom DynDNS. Il est également possible d'utiliser un nom DynDNS si l'autre partie se trouve derrière un NAT/CG-NAT. Il est alors important que la connexion soit établie depuis le côté opposé et que le service DynDNS synchronise l'adresse IP publique.

Pour l'authentification, un certificat est préférable à un PSK. Il faut tenir compte des points suivants :

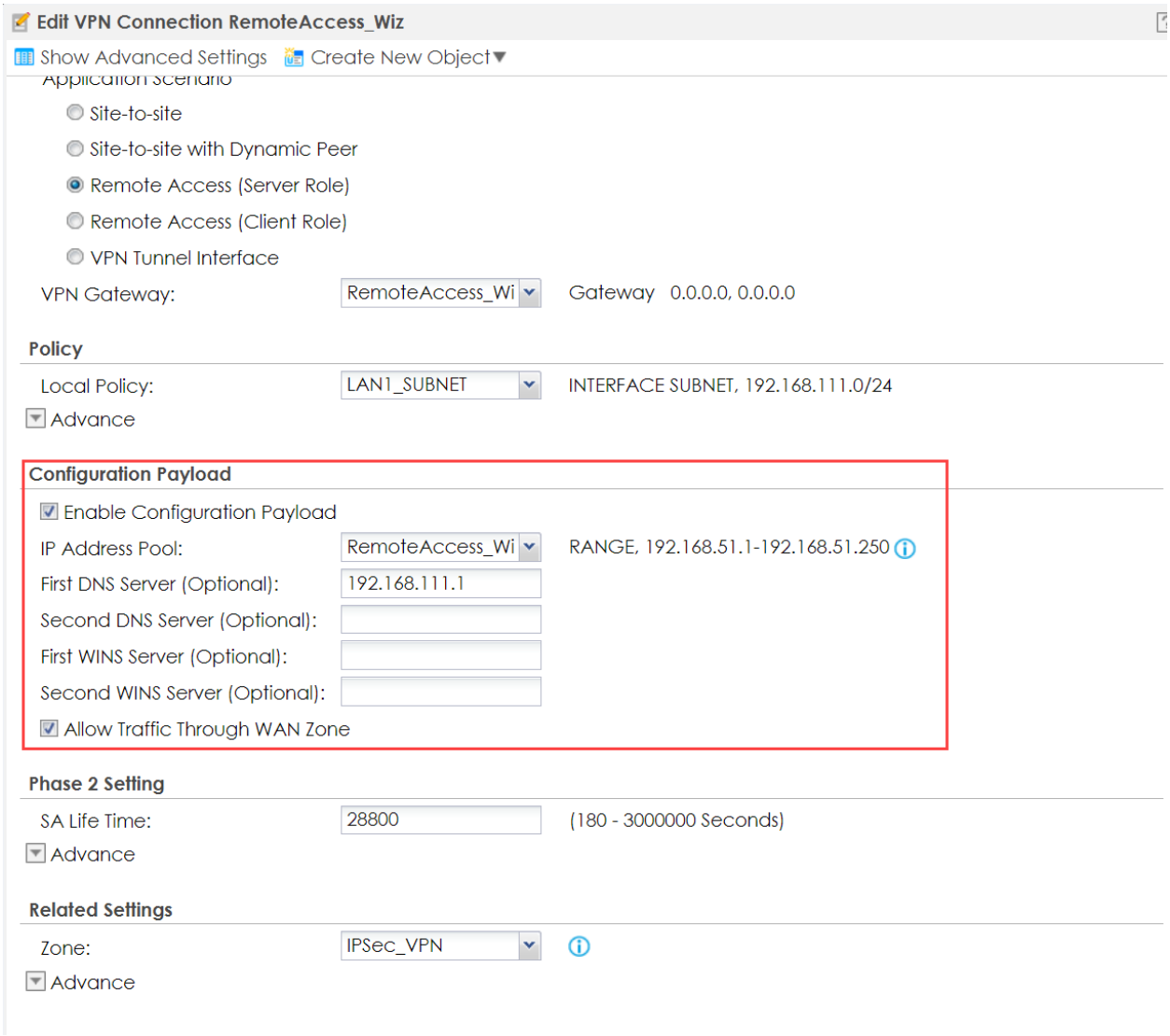
1. Le certificat utilisé peut être un « Self-Signed Certificate », mais doit être déposé sous « Trusted Certificates » du côté opposé.
2. Un certificat propre est créé des deux côtés.
3. Le type d'ID locale est extrait du certificat et doit être enregistré de manière identique en tant que Peer ID du côté opposé.
4. La recommandation pour la durée de vie SA maximale est de 86400 secondes dans la passerelle VPN et de 14400 secondes dans la connexion VPN.
5. Les paramètres suivants sont recommandés au minimum pour le cryptage VPN : AES256 / SHA256 / DH15. Ceci aussi bien dans la passerelle VPN que dans la connexion VPN.
6. Le protocole d'authentification étendu est également possible pour les tunnels site à site. Toutefois, l'utilisateur inscrit n'est pas connecté au pare-feu lors de l'établissement de la connexion.


Edit VPN Gateway VTI_CAB_HOME
Show Advanced Settings
Create New Object
General Settings
Enable
VPN Gateway Name:
MyIKEv2_GATEWAY
IKE Version
IKEv1
IKEv2
Gateway Settings
My Address
Interface
Gateway
Static -- 217.192.14.85/255.255.255.192
Domain Name / IPv4
Peer Gateway Address
Static Address
Primary
me.selfhost.eu
Secondary
0.0.0.0
Fall back to Primary Peer Gateway when possible
Fall Back Check Interval:
300
(60-86400 seconds)
Dynamic Address
Authentication
Pre-Shared Key
unmasked
Certificate
VTI
(See My Certificates)
Advance
Local ID Type:
IPv4
Content:
217.192.14.85
Peer ID Type:
DNS
Content:
me.selfhost.eu
Phase 1 Settings
SA Life Time:
86400
(180 - 3000000 Seconds)
Advance
Proposal
Add
Edit
Remove
Encryption Authentication
1 AES256 SHA256
Key Group:
DH19
Extended Authentication Protocol
Enable Extended Authentication Protocol
Allowed Auth Method:
mschapv2
Server Mode
AAA Method:
default
Allowed User:
S2S-VPN
Client Mode
User Name :
Password:
OK
Cancel

VPN client vers site

Pour les VPN client à site, IKEv2 avec certificat et Extended Authentication Protocol est recommandé.

Dans la connexion VPN, Configuration Payload est obligatoire.



Après l'établissement de la connexion, le client est connecté au pare-feu avec l'utilisateur.
Pour un éventuel accès admin au pare-feu, l'utilisateur admin correspondant peut donc être enregistré dans le Policy Control.

VPN L2TP

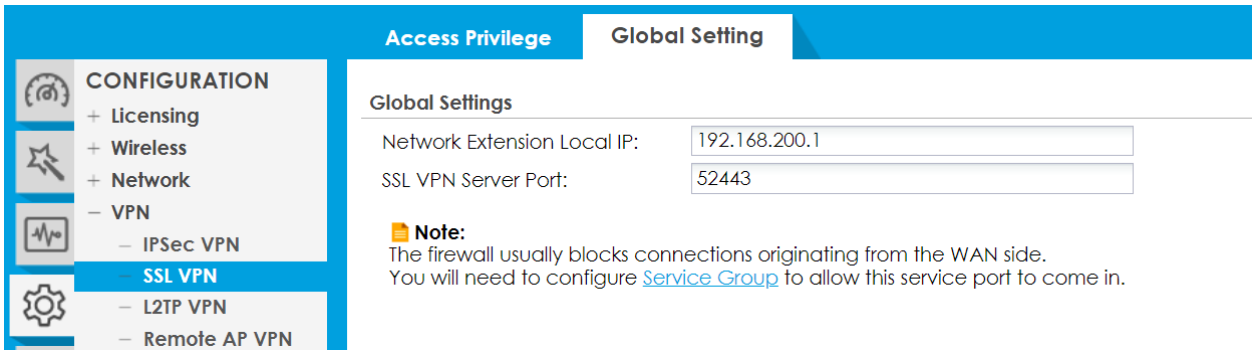
Il est déconseillé d'utiliser le VPN L2TP. IKEv2 peut être utilisé à la place.

VPN SSL

En raison des performances et des éventuels problèmes de sécurité, le VPN SSL n'est pas recommandé. Toutefois, comme il est souvent utilisé en raison de sa facilité de configuration, il convient de tenir compte des points suivants :

Configuration > VPN > SSL VPN > Global Setting

L'utilisation d'un port séparé pour SSL VPN est obligatoire. Le port 443 ne doit en aucun cas être utilisé.



La sécurité est considérablement renforcée par l'utilisation d'un certificat pour l'authentification. La configuration est décrite sous « Gestion à distance via HTTPS > Authenticate Client Certificate ».

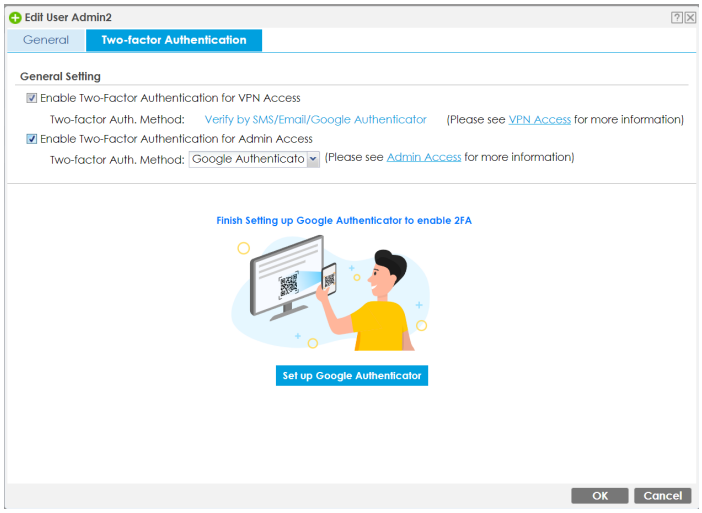
Dans le Policy Control, il est conseillé de limiter l'IP source pour l'accès du WAN au ZyWALL pour le service Wiz_SSLVPN. Au moins sur une GeoIP, mieux sur un FQDN ou une adresse IP.

Il est également possible de limiter l'accès de l'administrateur au pare-feu depuis la zone SSL-VPN à l'utilisateur admin. Cela est possible car l'utilisateur se connecte déjà au pare-feu lors de l'établissement du tunnel.

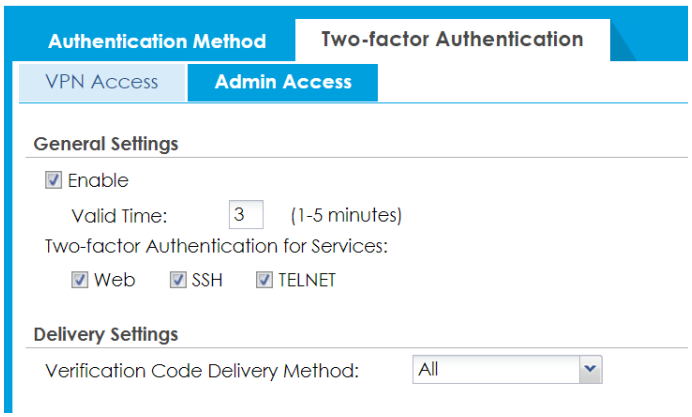
Les utilisateurs normaux n'ont pas besoin d'accéder au pare-feu depuis la zone SSL-VPN. Il suffit d'autoriser ici les services typiques tels que DNS.

AUTHENTIFICATION À DOUBLE FACTEUR

Une authentification à double facteur (2FA) est recommandée pour Admin Access, de préférence avec Google Authenticator.
La configuration pour 2FA doit être effectuée séparément pour chaque utilisateur. La méthode Google Authenticator est recommandée. Il convient de noter que les utilisateurs pour lesquels 2FA n'est pas configuré peuvent continuer à se connecter sans authentification supplémentaire. C'est pourquoi 2FA n'offre qu'une protection limitée.

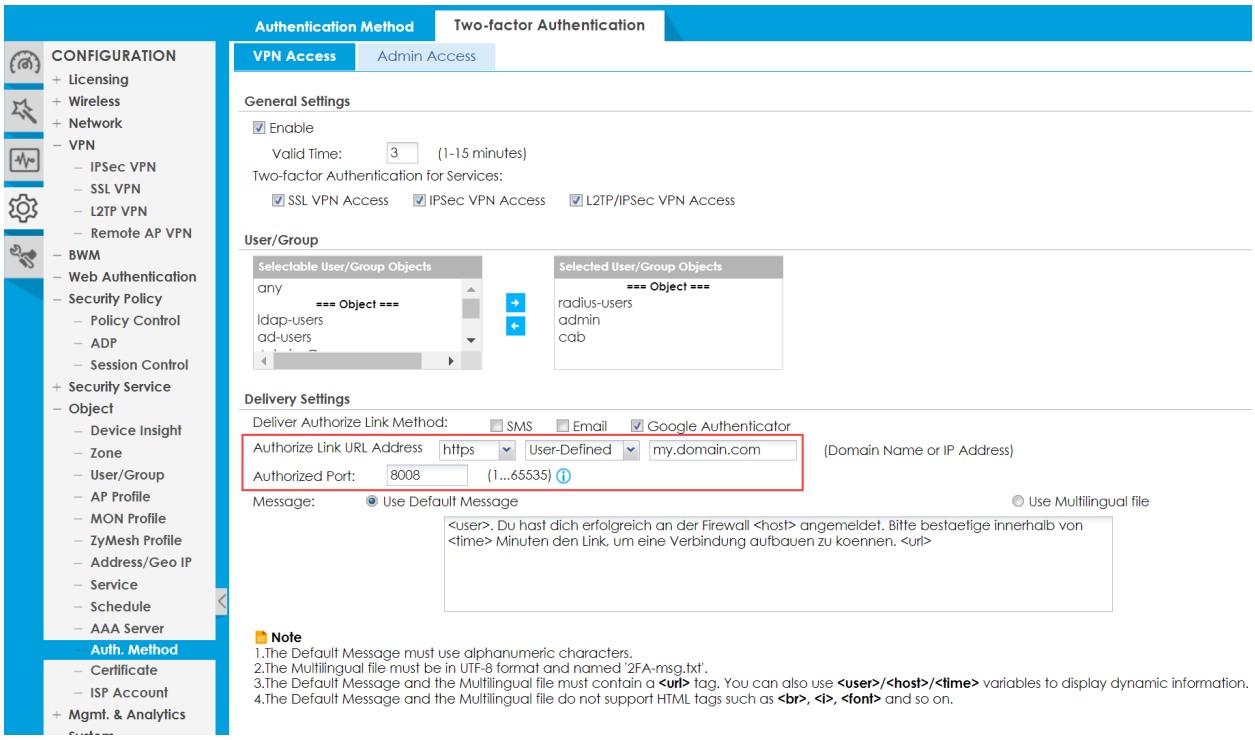


Configuration > Object > Auth. Method > Two-factor Authentication > Admin Access



Configuration > Object > Auth. Method > Two-factor Authentication > VPN Access

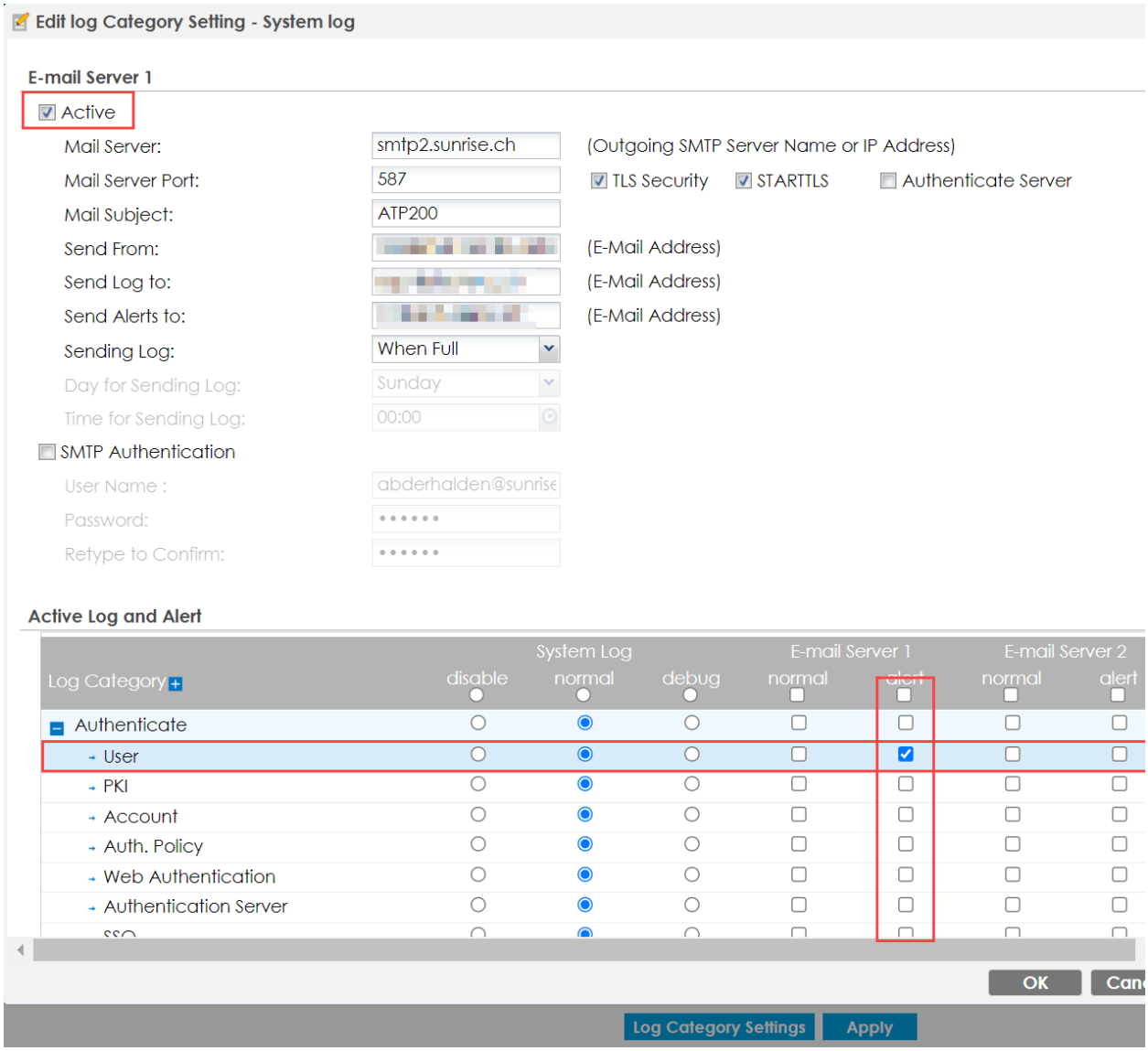
2FA peut également être activé pour l'accès VPN.
Un port spécifique est toujours utilisé pour l'authentification (objet Wiz_2FA).
Il existe également différentes méthodes pour envoyer un lien. En fin de compte, toutes les méthodes appellent un lien vers l'interface utilisateur web.
Comme l'interface web doit être accessible depuis le WAN pour 2FA, il existe ici aussi un risque d'attaque potentiel. C'est pourquoi cette fonction doit être utilisée avec prudence



ALERT LOGS

Pour certaines options, il peut avoir du sens de paramétrer un Alert Log qui déclenche tout de suite une alerte e-mail lors d'un évènement choisi. Cette fonction s'avère utile par exemple si un administrateur se connecte, notamment pour des pare-feux surveillés à intervalles irréguliers.

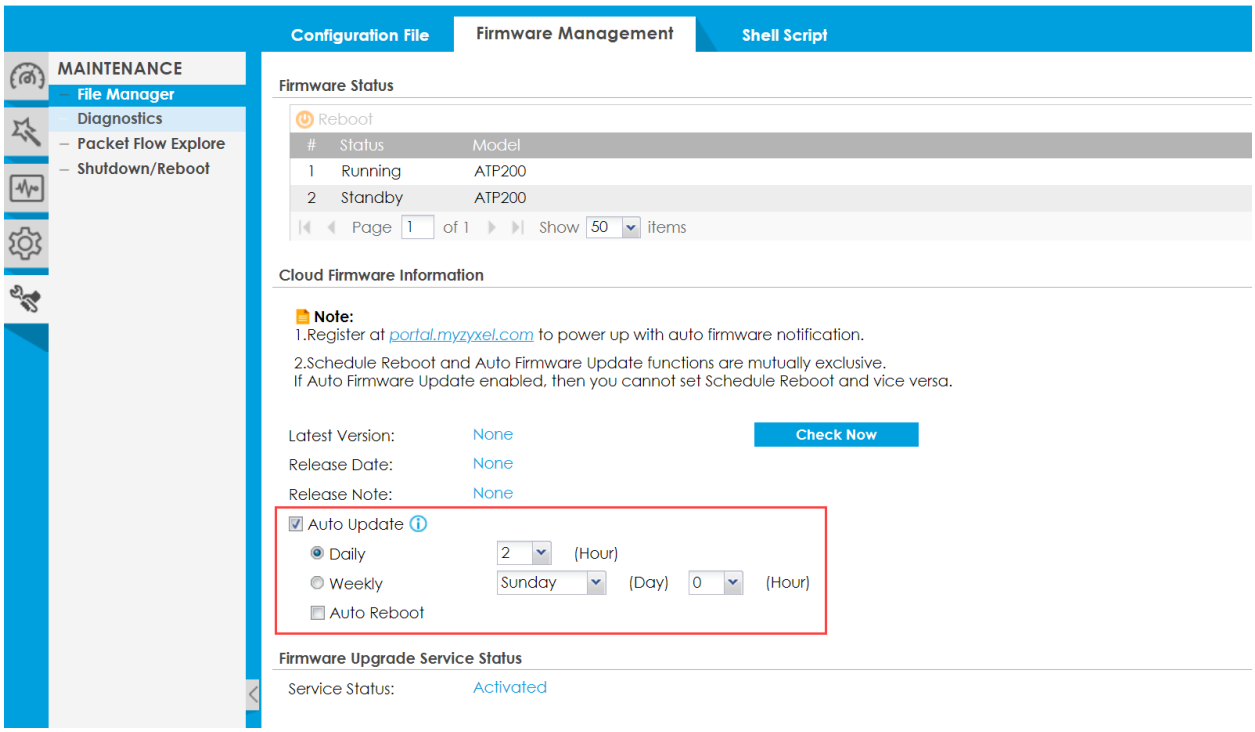
Configuration > Log & Report > Log Settings



MISES À JOUR DE FIRMWARE AUTOMATIQUES

Il faut toujours veiller à ce que le firmware du pare-feu soit à jour. Les mises à jour peuvent être effectuées manuellement sur les systèmes qui sont gérés activement. Cependant, dans la réalité, il arrive souvent que cela soit négligé et que les pare-feux présentant des failles de sécurité connues ne soient pas mis à jour pendant une longue période.
En particulier dans les environnements de ce type, il est recommandé d'activer les mises à jour automatiques.

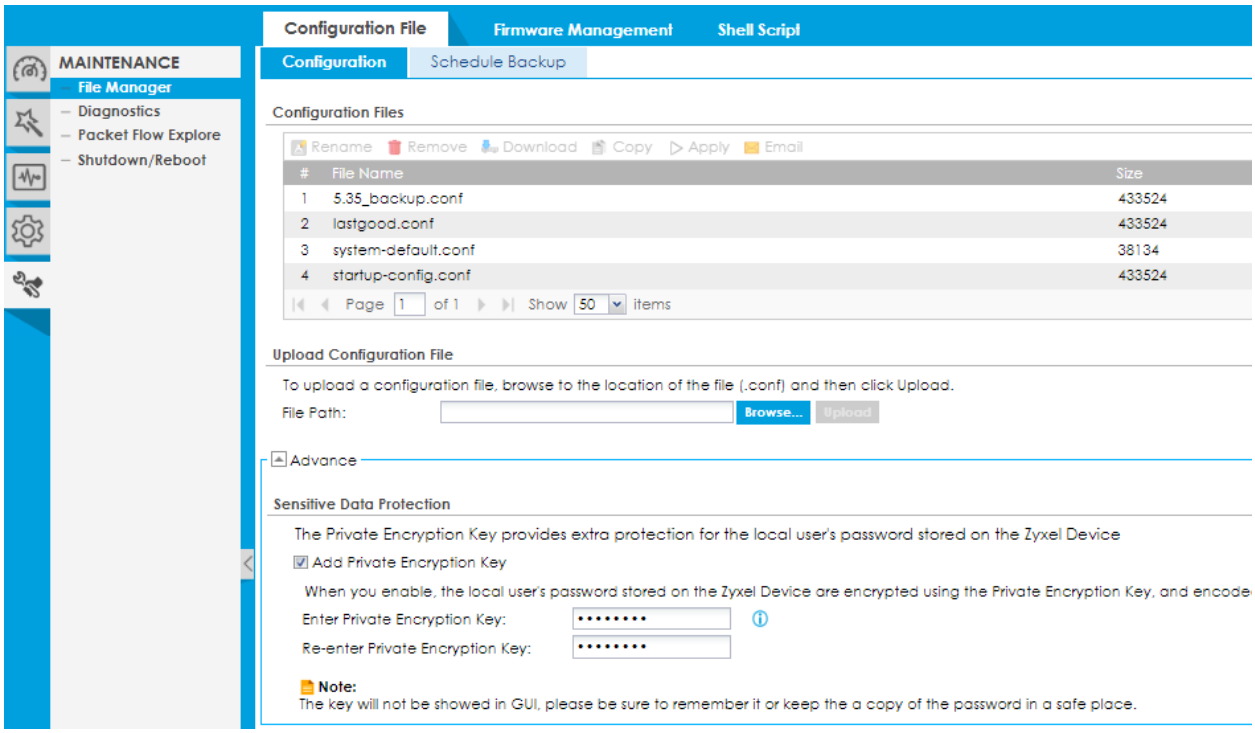
Maintenance > File Manager > Firmware Management



PROTECTION DES DONNÉES SENSIBLES

À partir de la version 5.35 du firmware, les mots de passe peuvent être cryptés avec une clé propre au lieu de l'algorithme par défaut.
Cette fonction protège également contre la lecture des mots de passe des utilisateurs dans les fichiers de configuration à l'aide d'outils de piratage.
Les autres mots de passe continuent d'utiliser la méthode par défaut.

Maintenance > File Manager > Configuration File > Configuration > Sensitive Data Protection



Si le fichier est réimporté sur un pare-feu. Cela n'est possible qu'avec la clé correspondante.