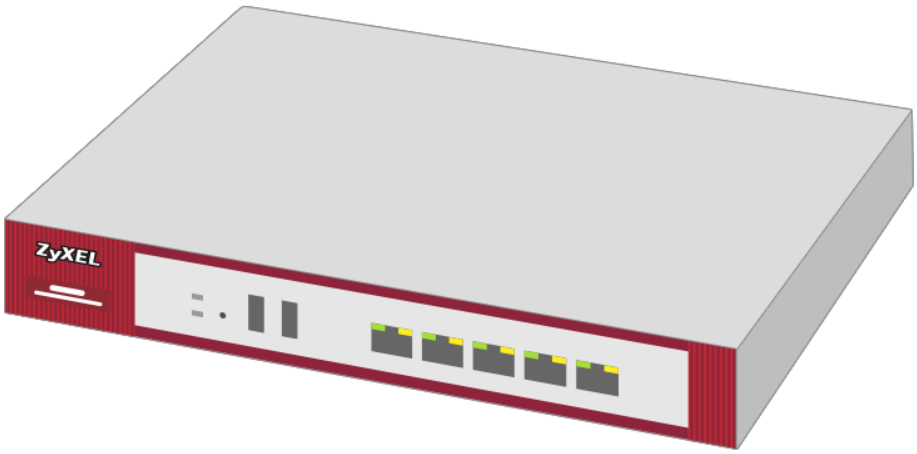
ZYXEL
Your Networking Ally



Grundlagen zur Absicherung einer Firewall

Zyxel Firewall-Serie
ab Firmware Version 5.35

Knowledge Base KB-3823
Januar 2023

GRUNDLAGEN ZUR ABSICHERUNG EINER FIREWALL

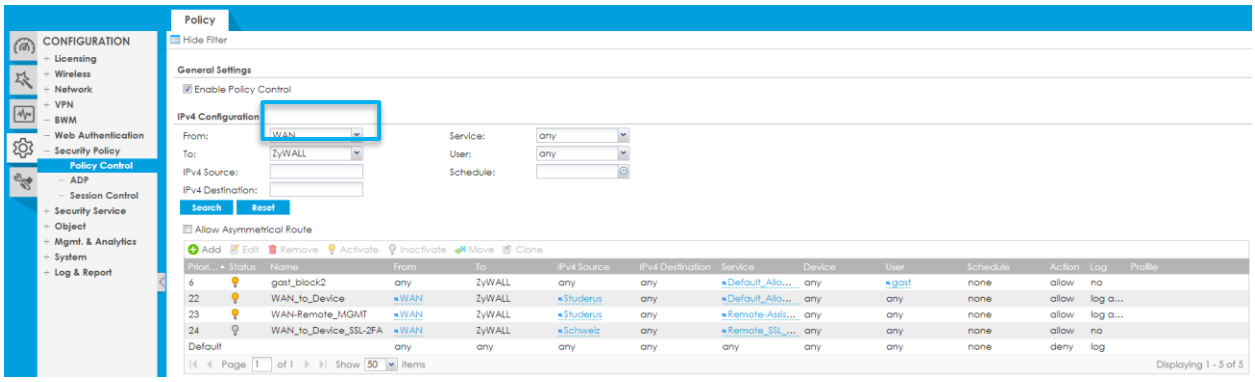
Die Firewall ist die erste Hürde für Angreifer aus dem Internet. Sie schützt das Lokale Netzwerk vor unberechtigten Zugriffen und stellt somit einen wesentlichen Bestandteil eines Sicherheitskonzeptes dar. Was aber, wenn die Firewall selbst Ziel von Hackerattacken wird und dadurch zu einer potenziellen Bedrohung werden kann? Der nachfolgende Leitfaden soll Aufschluss darüber geben, wie Angriffsmöglichkeiten eigeschränkt werden können.

POLICY CONTROL

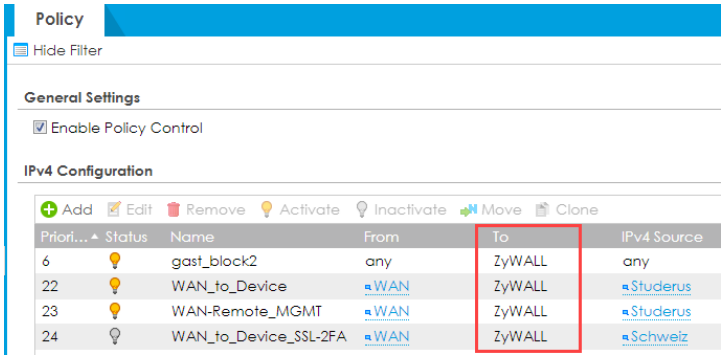
Grundsätzlich sollten so wenige User wie nötig Zugriff auf die Firewall haben. Um dies zu gewährleisten, ist es ratsam, die Zugriffsrechte weitmöglichst einzuschränken.

Firewall-Regeln werden im nachfolgenden Menu erstellt:

Configuration > Security Policy > Policy Control



Die Zone ZyWALL nimmt eine spezielle Rolle ein. Grundsätzlich können nur Regeln zu dieser hin erstellt werden. Sie beinhaltet alle Interface-Adressen der Firewall. So gehört z.B. die Default Adresse 192.168.1.1 nicht zu der Zone LAN1, sondern zur Zone ZyWALL.



Mit den Default-Einstellungen ist der Zugriff auf die Firewall weitgehend offen. Daher sollten diese weiter eingeschränkt werden.

Einschränken von Policy-Control-Regeln

Firewall-Regeln können aufgrund mehrerer Kriterien eingeschränkt werden. Für den Zugriff auf die Firewall sind vorwiegend 3 Kriterien sinnvoll:

1. IPv4 Source (Adress-Objekte)
2. Service
3. User

Diese Elemente werden als Objekte angelegt.

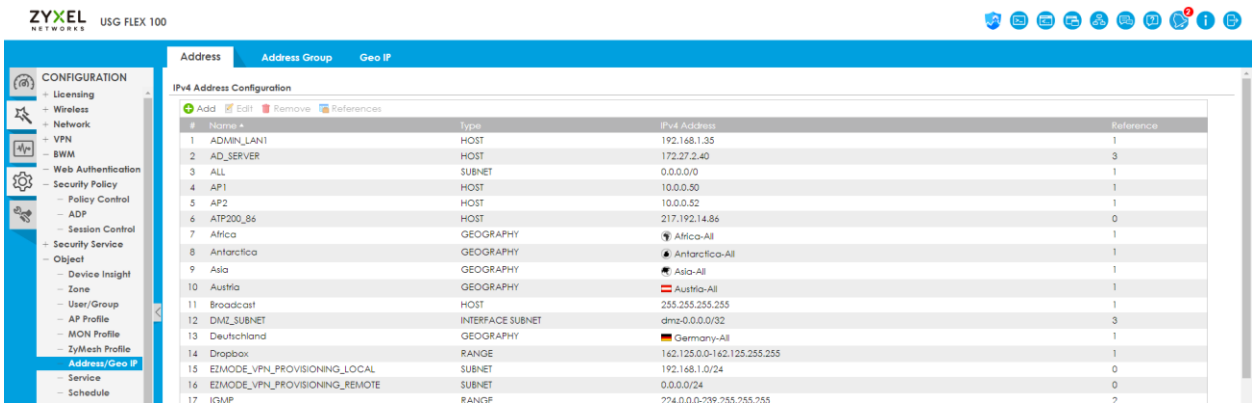
Adress-Objekte

Es gibt grundsätzlich 3 Arten von Adress-Objekten. Dabei handelt es sich um:

1. IP-Adressen
2. FQDN-Adressen
3. GeoIP Adressen

Adress-Objekte können in einer Gruppe zusammengefasst werden. Jedoch ist es nicht möglich, unterschiedliche Adress-Typen zu mischen.

Configuration > Object > Address/Geo IP > Address



1. IP-Adressen

Wenn immer möglich, sollten IP-Adressen verwendet werden, da diese eindeutig sind. Es gibt mehrere Typen von IP-Adressen:

1. Host > Dieser beschreibt eine einzelne IP-Adresse
2. Range > Es kann ein beliebiger Range eingegeben werden, definiert durch die Start- und End-Adresse
3. Subnet > Dieses kann durch die Eingabe einer Subnet Maske oder CIDR (z.B. /24) angelegt werden
4. Interface IP > übernimmt die IP-Adresse eines Interfaces und passt sich dynamisch an
5. Interface Subnet > übernimmt dynamisch das Subnet eines Interfaces
6. Interface Gateway > übernimmt das Gateway eines Interfaces des Typs WAN oder general.

Host, Range, Subnet

Die Adresstypen Host, Range und Subnet, eignen sich besonders als IPv4 Source. Erfolgt ein Zugriff aus dem WAN, wird die öffentliche IP-Adresse der Gegenstelle angegeben.
Aus einem LAN lassen sich mit diesen Objekten-Gruppen mit unterschiedlichen Berechtigungen erstellen.

Interface IP

Dieses Objekt kann verwendet werden, wenn der Zugriff nur auf einer bestimmten IP-Adresse möglich sein soll. Wenn z.B. 2 WAN-Interfaces vorhanden sind, ein Service aber nur auf einem Interface zur Verfügung stehen soll, kann die Interface IP in der Policy Control Regel als IPv4 Destination eingetragen werden.

Interface Subnet

Dieser Adresstyp eignet sich, wenn für ein lokales Interface (z.B. LAN1) einheitliche Regeln erstellt werden sollen.

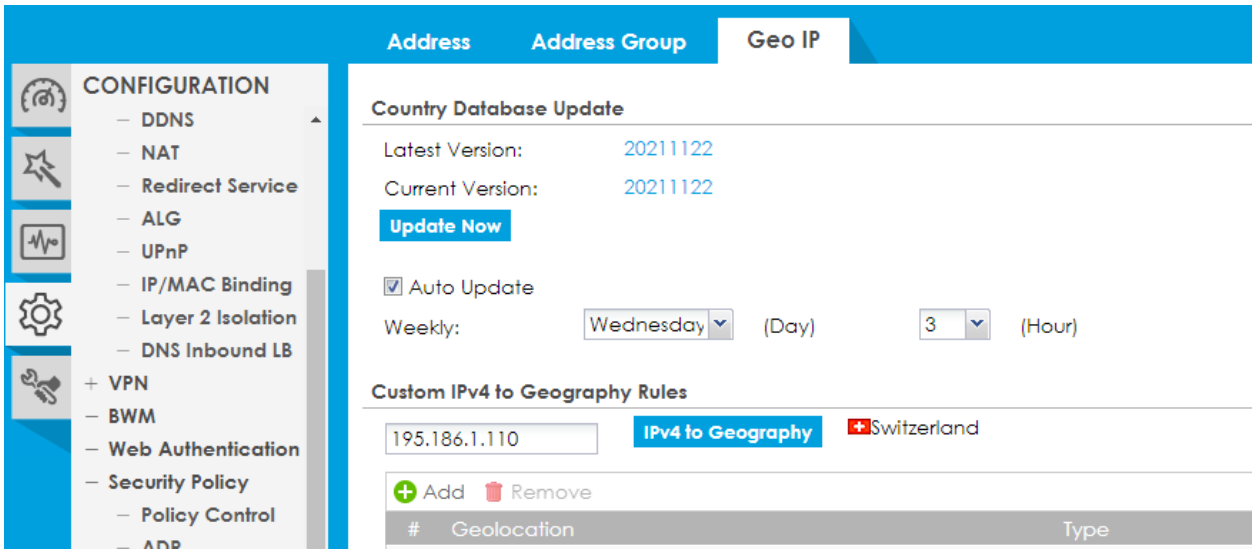
Interface Gateway

Dieser Adresstyp ist für den Zugriff auf die Firewall nicht relevant.

2. FQDN-Objekte

Bei FQDN Objekten kann anstelle einer IP-Adresse ein Name eingegeben werden, z.B. www,mydomain.com. Diese Art von Einträgen eignet sich vor allem dann, wenn ein Zugriff aus dem WAN erfolgt und die Gegenstelle keine statische Public IP-Adresse hat. In diesem Fall kann ein DynDNS Name anstelle der IP-Adresse verwendet werden. Für FQDN-Objekte wird ein schneller DNS-Server benötigt. Möglich sind auch Wildcard Einträge wie z.B. *.mydomain.com. Diese können jedoch nicht für diesen Zweck verwendet werden.

Geo-IP-Adressen

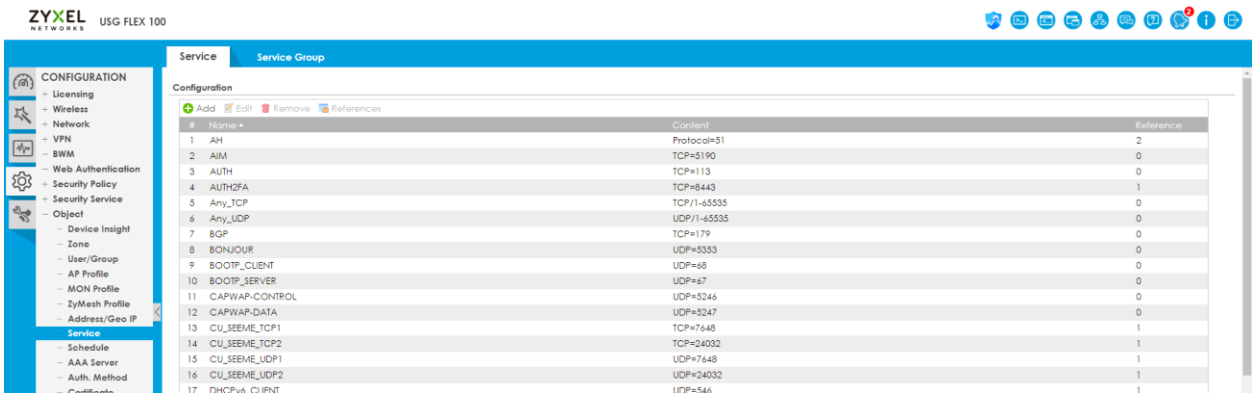


Mit GeoIP lassen sich Länder bzw. Regionen basierte Objekte erstellen. Der Service greift auf eine externe Datenbank zurück und sollte regelmässig aktualisiert werden. GeoIP bietet keinen zuverlässigen Schutz, da mittels frei verfügbaren VPN-Diensten die Ursprungsadresse sehr einfach manipuliert werden kann.

Service-Objekte

Mit den Service-Objekten wird definiert, welchen Diensten in den Policy-Control-Einstellungen Zugriff gewährt oder verweigert wird. Die Services können zu Gruppen zusammengefügt werden. Die Services können auch an anderer Stelle verwendet werden, z.B. in Policy Routen und NAT-Einträgen.
Neben den normalen Service Objekten gibt es einige spezielle Objekte. Es handelt sich dabei um die Objekte «Wiz_2FA, Wiz_HTTP, Wiz_HTTPS und Wiz_SSLVPN». Der Port dieser Services passt sich automatisch an, wenn dieser im entsprechenden Menu neu definiert wird.

Configuration > Object > Service



User

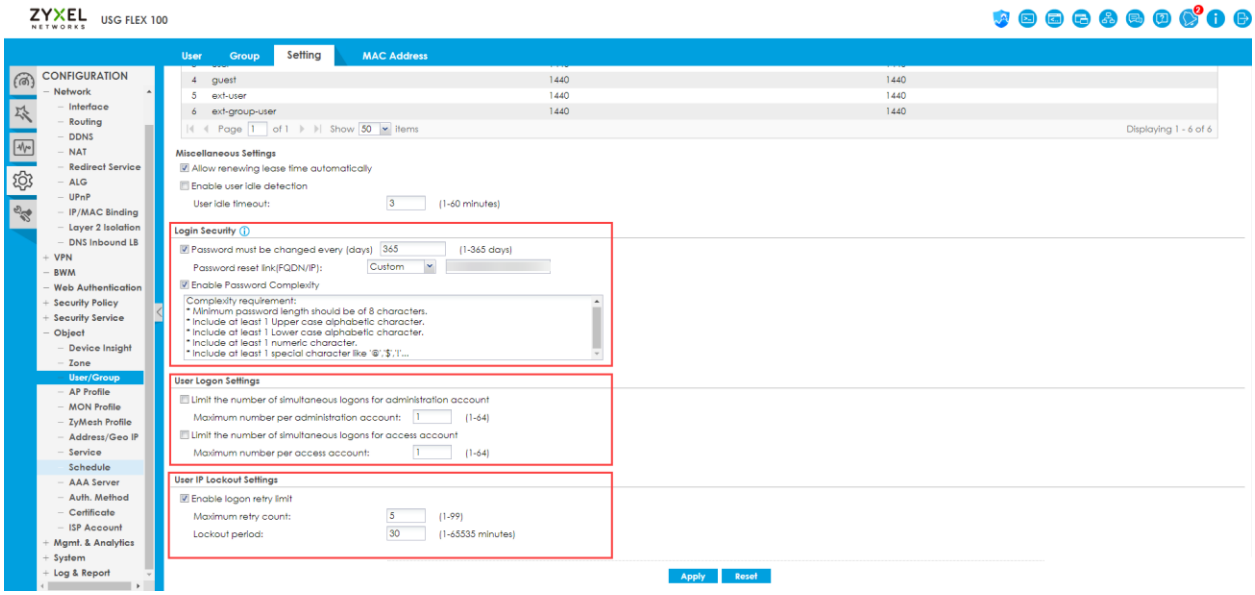
Configuration > Object > User

Es gibt unterschiedliche Arten von Usern.
User-type: admin, kann Änderungen an der Konfiguration vornehmen
User-type: limited-admin, kann auf die Konfiguration zugreifen, jedoch keine Änderungen vornehmen
User-type: user, kann sich mittel 2FA authentifizieren
User-type: guest, kann sich an der Firewall anmelden
User-type: ext-user/ext-group-user, authentifizieren sich an einem externen Server.

Built-in User sind vordefiniert User, welche nicht gelöscht werden können und für bestimmte Zwecke vorgesehen sind.

User sollen so definiert werden, dass Sie nur über die notwendigen Berechtigungen verfügen. Typischerweise sind z.B. VPN oder 802.1x User als User-type user definiert.

Configuration > Object > User/Group > Settings



Login Security

Definiert, ob und in welchem Zeitraum Passwörter geändert werden müssen und ob eine Passwort-Komplexität erforderlich ist.

User Logon Settings

Definiert, wie oft sich ein User gleichzeitig anmelden kann. Wenn das Limit auf „1“ gesetzt wird, kann es vorkommen, dass sich ein Administrator selbst aussperrt.

User IP Lockout Settings

Die Einträge definieren, wie oft eine falsche Passworteingabe erlaubt ist, bis der User für einen bestimmten Zeitraum blockiert wird. Diese Einstellung schütz vor allem vor Brute-Force-Attacken.

Empfohlene Policy Control Regeln

From: WAN To: ZyWALL

Es wird dringend empfohlen, alle Services zu schliessen, welche nicht ausdrücklich benötigt werden.

Häufig benötigte Services:

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

SSL-VPN:
Wiz_SSLVPN

2-Faktor-Authentifizierung für VPN:
Wiz_2FA

Remote-Zugriff über HTTP/HTTPS:
Wiz_HTTP, Wiz_HTTPS

Um Sicherheitsrisiken weitmöglichst zu vermeiden, erfolgt ein Remote Management idealerweise über IPSecVPN. Die Source-Adressen sollten, wenn möglich eingeschränkt werden.
Von SSL-VPN wird abgeraten, da dies einen möglichen Angriffsvektor über SSL bietet.

Remote-Zugriff über HTTPS:
Falls ein Remote-Zugriff über HTTP/HTTPS erforderlich ist, sollte die Source-Adresse immer auf eine IP-Adresse oder FQDN eingeschränkt werden. GeoIP als Source-Adresse ist nicht sicher und bietet ein erhebliches Angriffspotential. Für HTTPS-Management wird empfohlen, einen Alternativ-Port zu verwenden.

From: VPN-Zone To: ZyWALL (Client-to-Site)

Per Default sind alle Ports offen. Grundsätzlich sind in den meisten Fällen nur sehr wenige Services erforderlich. Dies sind z.B. DNS und L2TP-UDP. Für andere Services sollte der Zugriff blockiert werden. Ist ein Remote Management über Client-to-Site VPN gewünscht, kann der Zugriff auf die Firewall auf einen User eingegrenzt werden. Dies funktioniert jedoch nur, wenn sich der User bereits beim Tunnel-Aufbau an der Firewall angemeldet hat.

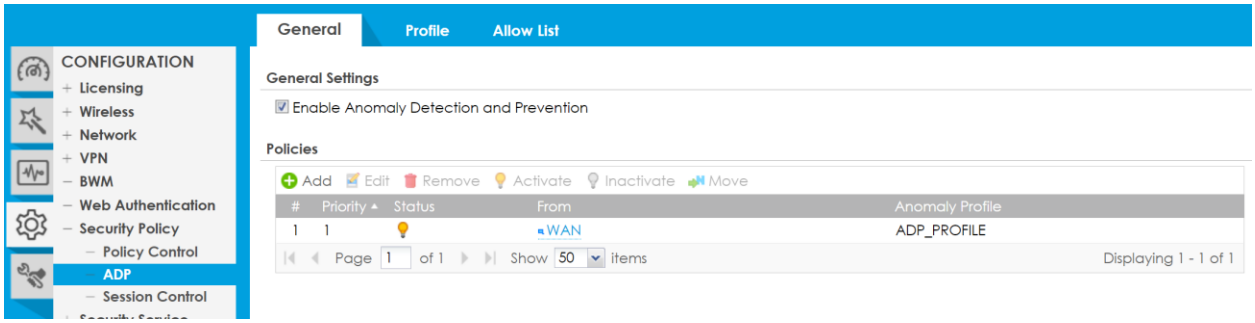
From: LAN To: ZyWALL

Auch hier sollten die Zugriffsrechte eingeschränkt werden. Voll-Zugriff auf die Firewall sollten nur einem speziellen Management-LAN oder einzelnen Administrator-IP-Adressen gewährt werden. Damit einige Services korrekt funktionieren, muss Zugriff auf die Firewall gewährleistet sein. Dies betrifft z.B. DNS, Multicast, Radius-Auth, NetBIOS, SNMT, SSO usw. Welche Zugriffe effektiv erforderlich sind, hängt stark von der Netzwerktopologie und eingesetzten Technologien ab.

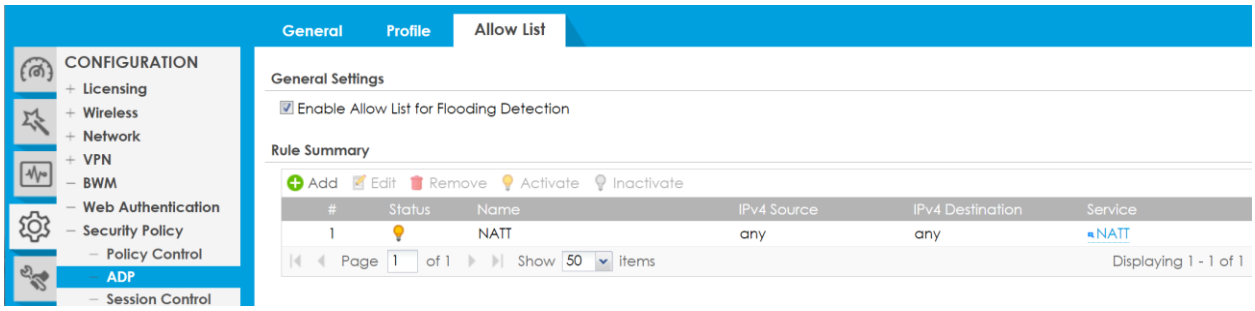
ANOMALY DETECTION AND PREVENTION (ADP)

Configuration > Security Policy > ADP

ADP bietet Schutz vor Portscans und ungewöhnlichem Netzwerkverhalten. Empfohlen wird, ADP mit dem Default-Profil aus der Zone WAN zu aktivieren. Individuelle Anpassungen können Profil vorgenommen werden, wenn Probleme auftreten sollten.



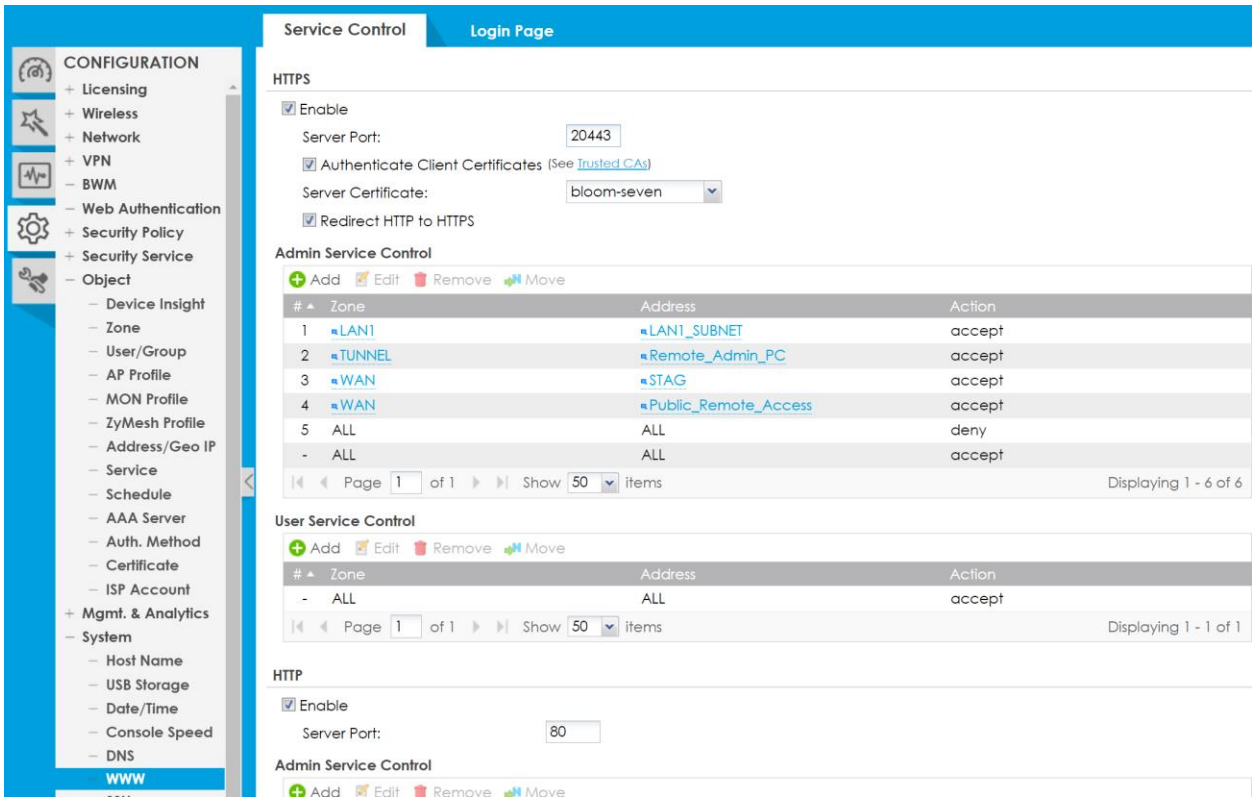
In Einzelfällen kann ADP bestimmte Services beeinträchtigen. Dies betrifft vor Allem Flooding Detection. Aus diesem Grund kann für einzelnen Services die Flooding Protection deaktiviert werden, z.B. NATT. Eine solche Einstellung ist nur dann sinnvoll, wenn Probleme auftreten sollten.



REMOTE MANAGEMENT ÜBER HTTPS

Einige spezifische Einstellungen in den WWW-Settings haben einen direkten Einfluss auf die Systemsicherheit.

Configuration > System > WWW



Server Port

Für das Remote Management sollte nicht der Standard-Port 443 verwendet werden, da dieser bei automatisierten Attacken immer gescannt wird. Häufig verwendete Alternativ-Ports (z.B. 8443) sind ebenfalls nicht ideal.

Redirect HTTP to HTTPS

Alle HTTP-Aufrufe des GUI werden auf HTTPS umgeleitet. Achtung! Diese Einstellung darf nicht aktiviert sein, wenn Web Authentication zum Einsatz kommt. In allen anderen Fällen sollte diese Option aktiviert werden.

Admin Service Control

Hier kann eingestellt werden, wer Administrator-Zugriff auf die Firewall haben darf. Es ist ratsam, den Zugriff auf einzelne IP-Adressen einzuschränken. Als Adress-Objekte sind nur IP-Adressen zugelassen. Als letzte Regel (hier Regel 5) sollte eine Regel ALL/ALL/deny erstellt werden. Beim Anlegen der Regel ist Vorsicht geboten, um sich nicht selbst auszusperren. Daher müssen zuerst die Accept-Regeln erstellt werden, bevor die Deny-Regel an letzter Stelle angelegt wird.

User Service Control

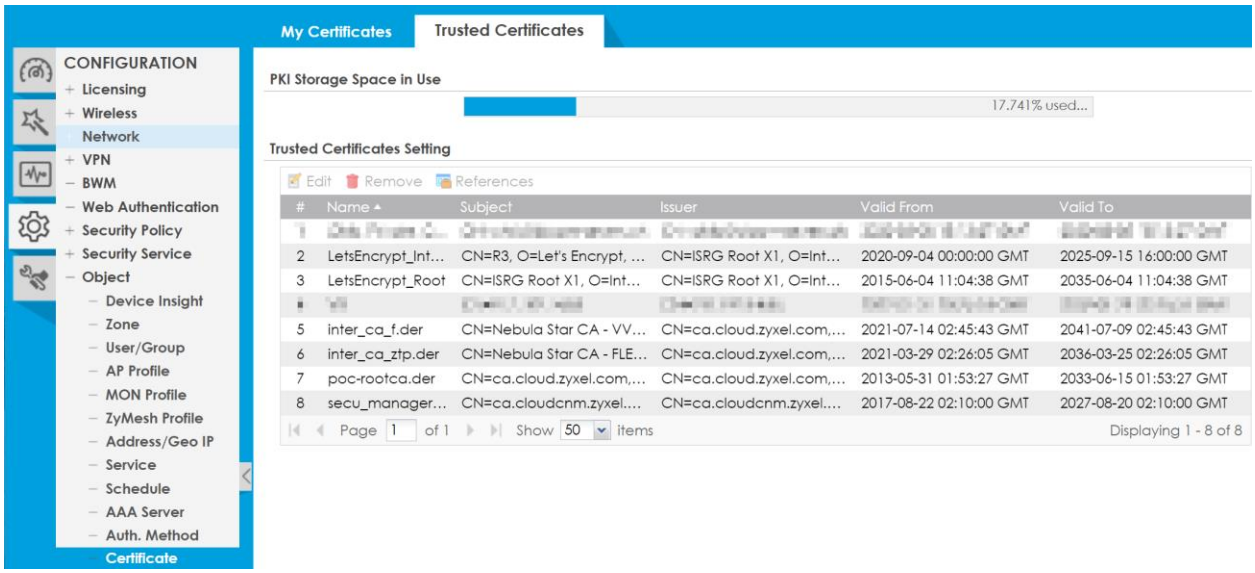
Im User Service Control wird definiert, welche Clients sich an der Firewall authentifizieren dürfen. Die Regel ist relevant für SSL-VPN, 2-FA, VPN Configuration Provisioning und WEB-Authentication. Falls dies nicht verwendet wird, kann ebenfalls eine deny Regel gesetzt werden.

Authenticate Client Certificates

Wenn die Option Authenticate Client Certificate aktiviert ist, muss sich der Client mit einem gültigen Zertifikat autorisieren. Andernfalls wird eine Verbindung abgelehnt. Dies betrifft Zugriffe über **HTTPS** und **SSL-VPN**. VPN Configuration_Profisioning mit SecuExtender funktioniert nicht, wenn diese Option aktiviert ist. Jedoch ist der Aufruf des 2FA-Fensters weiterhin ohne Zertifikat möglich.

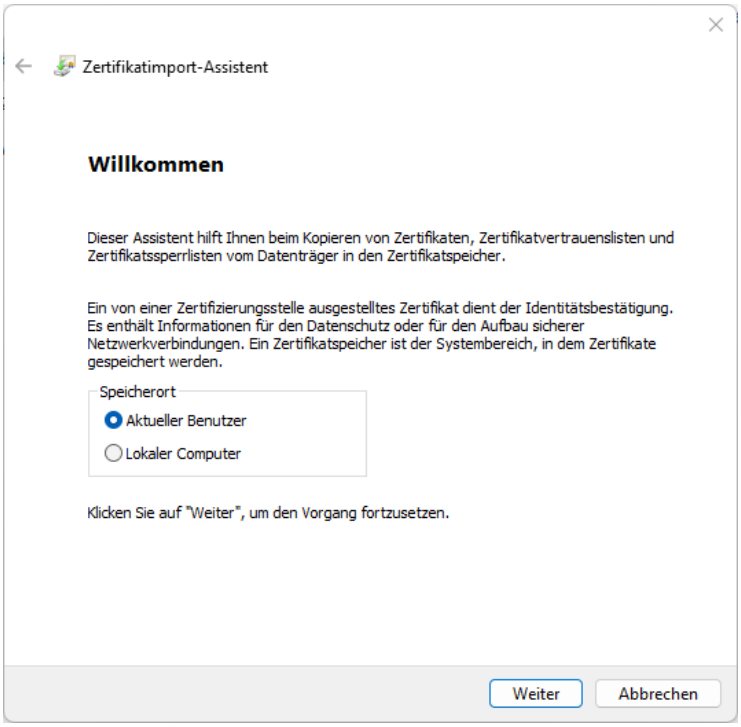
Damit ein Zertifikat für die Firewall als vertrauenswürdig betrachtet wird, muss die Vertrauenskette der Zertifizierungsstelle installiert werden. Diese umfasst in der Regel ein Root und Intermediate Zertifikat. Die Firewall vertraut jedem Zertifikat mit gültiger Zertifikatskette sowie eigenen selbstsignierten Zertifikaten. Es ist zu beachten, dass einige Browser selbstsignierte Zertifikate grundsätzlich ablehnen (aktuell Firefox basierte Browser). Das Client-Zertifikat muss nicht auf der Firewall installiert sein.

Configuration > Object > Certificate > Trusted Certificates

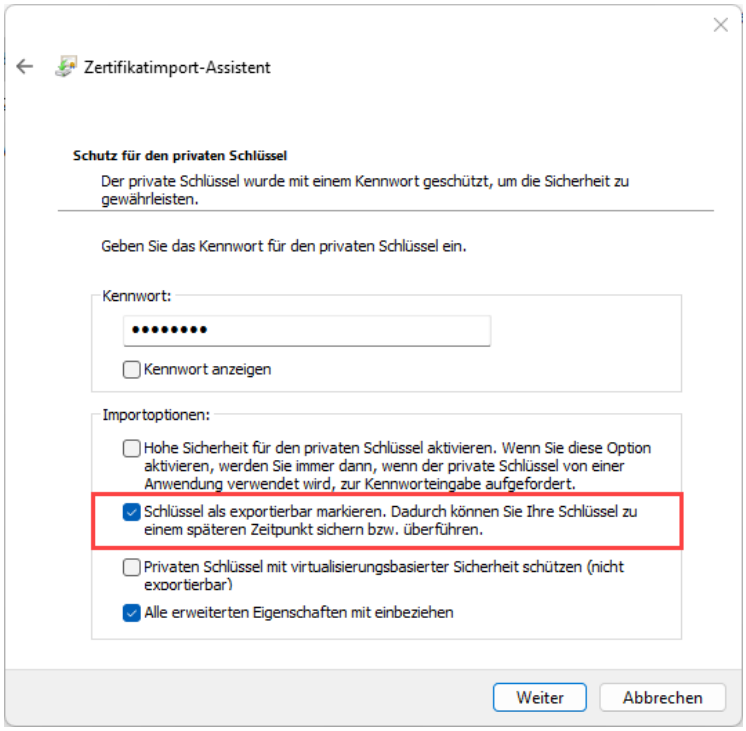


Das Client-Zertifikat mit Private Key wird auf dem Client installiert. Hier eine manuelle Installation unter Windows:

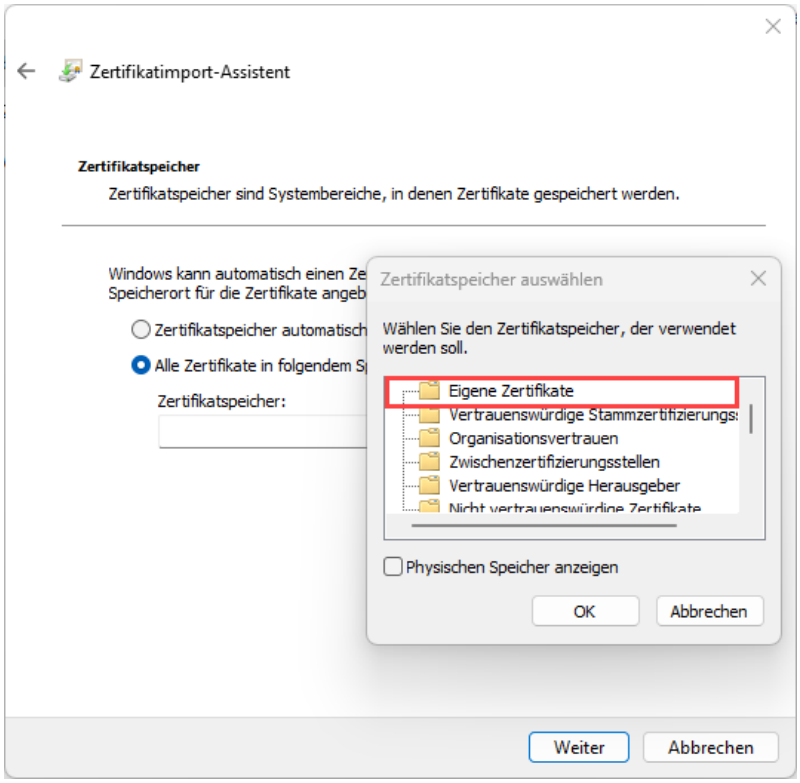
Zertifikat mit Private Key (PFX oder P12) mit Doppelklick öffnen und im Aktuellen Benutzer importieren.



Beim Import darauf achten, dass die Option «Schlüssel als exportierbar markieren» aktiviert ist.



Der Import erfolgt in den Zertifikatspeicher «Eigene Zertifikate».



REMOTE MANAGEMENT DIENSTE

Configuration > System

Auf der Firewall gibt es mehrere Dienste, die nur selten oder gar nicht benötigt werden. Diese Dienste können komplett deaktiviert werden.

SSH

Dieser Dienst kann z.B. verwendet werden, wenn Konfigurationsänderungen mit einem automatischen Script ausgeführt werden. Wenn SSH nicht regelmässig zur Administration verwendet wird, kann der Dienst abgeschaltet werden. Für CLI-Eingaben kann anstelle von SSH auch die Web Console verwendet werden.

TELNET

Wird in den meisten Fällen nicht benötigt und kann deaktiviert werden.

FTP

Über FTP kann z.B. die Firmware aktualisiert werden oder Konfigurationsfiles können heruntergeladen werden. FTP muss aktiviert sein, wenn HA-Pro im Einsatz ist. Falls das nicht der Fall ist, kann FTP deaktiviert werden. Falls der Service sporadisch benötigt wird, kann dieser im Bedarfsfall temporär aktiviert werden.

SNMP

Der Service wird zur Netzwerküberwachung benötigt und ist erforderlich für Lösungen wie z.B.: PRTG. Erfolgt keine Überwachung des Netzwerkes kann der Service deaktiviert werden.

ZON

Ermöglicht den Informationsaustausch mit benachbarten Geräten (Model, Name, Firmware, MAC-Adresse, IP-Adresse) über LLDP sowie mit der Zyxel eigenen Software ZON im gleichen LAN. Für den normalen Betrieb ist der Service nicht erforderlich.

VPN

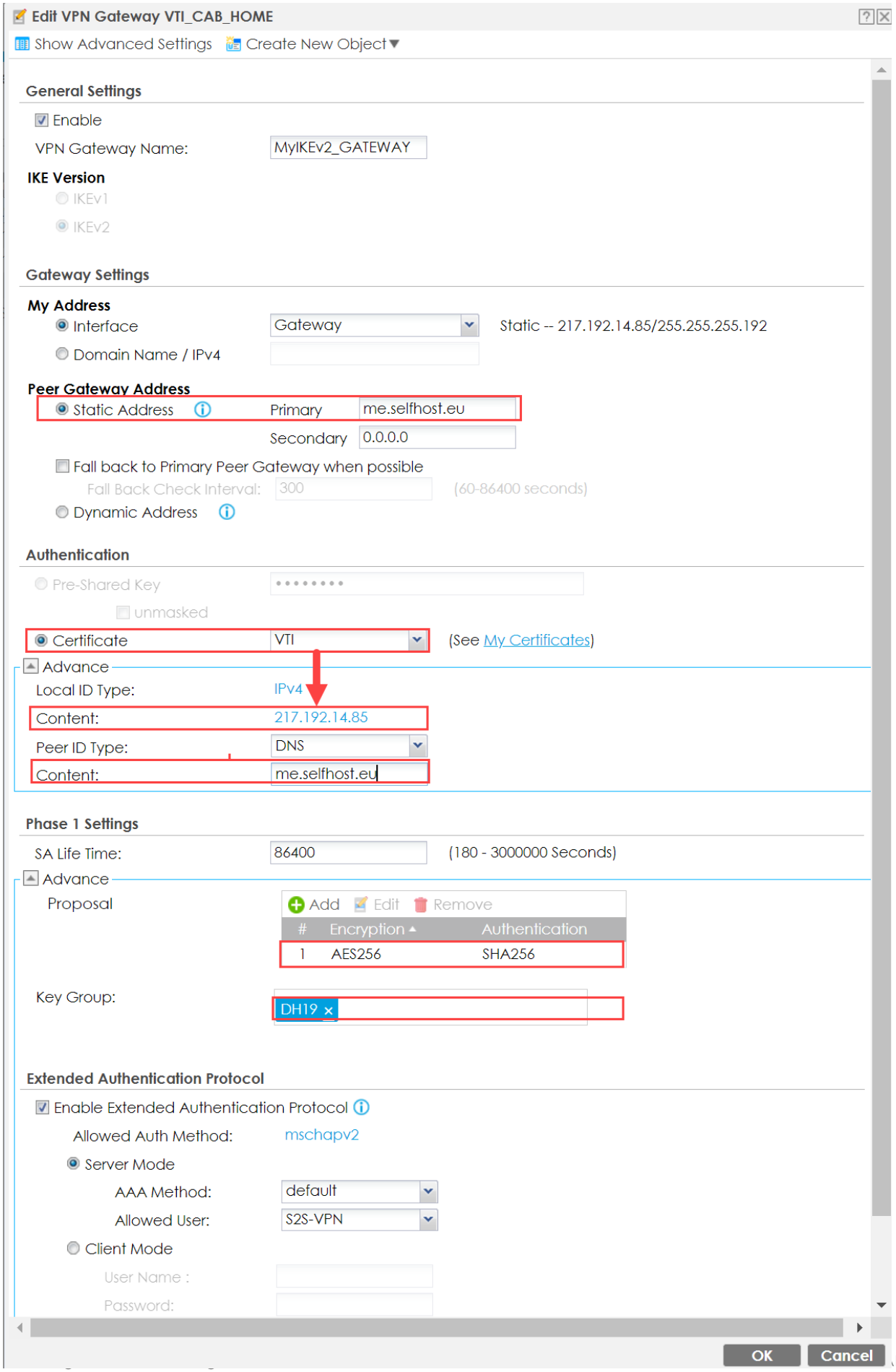
IPSec-VPN

Site-to-Site

Bei der Verwendung von Site-to-Site Tunnel sollte, wenn immer möglich eine Peer Gateway Adresse eingetragen werden. Wenn die Gegenseite eine dynamische IP-Adresse hat, kann auch ein DynDNS Name verwendet werden. Es kann auch ein DynDNS Name verwendet werden, wenn sich die Gegenseite hinter einem NAT/CG-NAT befindet. Wichtig ist dann, dass der Verbindungsaufbau von der Gegenseite aus erfolgt und der DynDNS Dienst die Public IP-Adresse synchronisiert.

Für die Authentifizierung ist ein Zertifikat besser als ein PSK. Folgendes ist zu beachten:

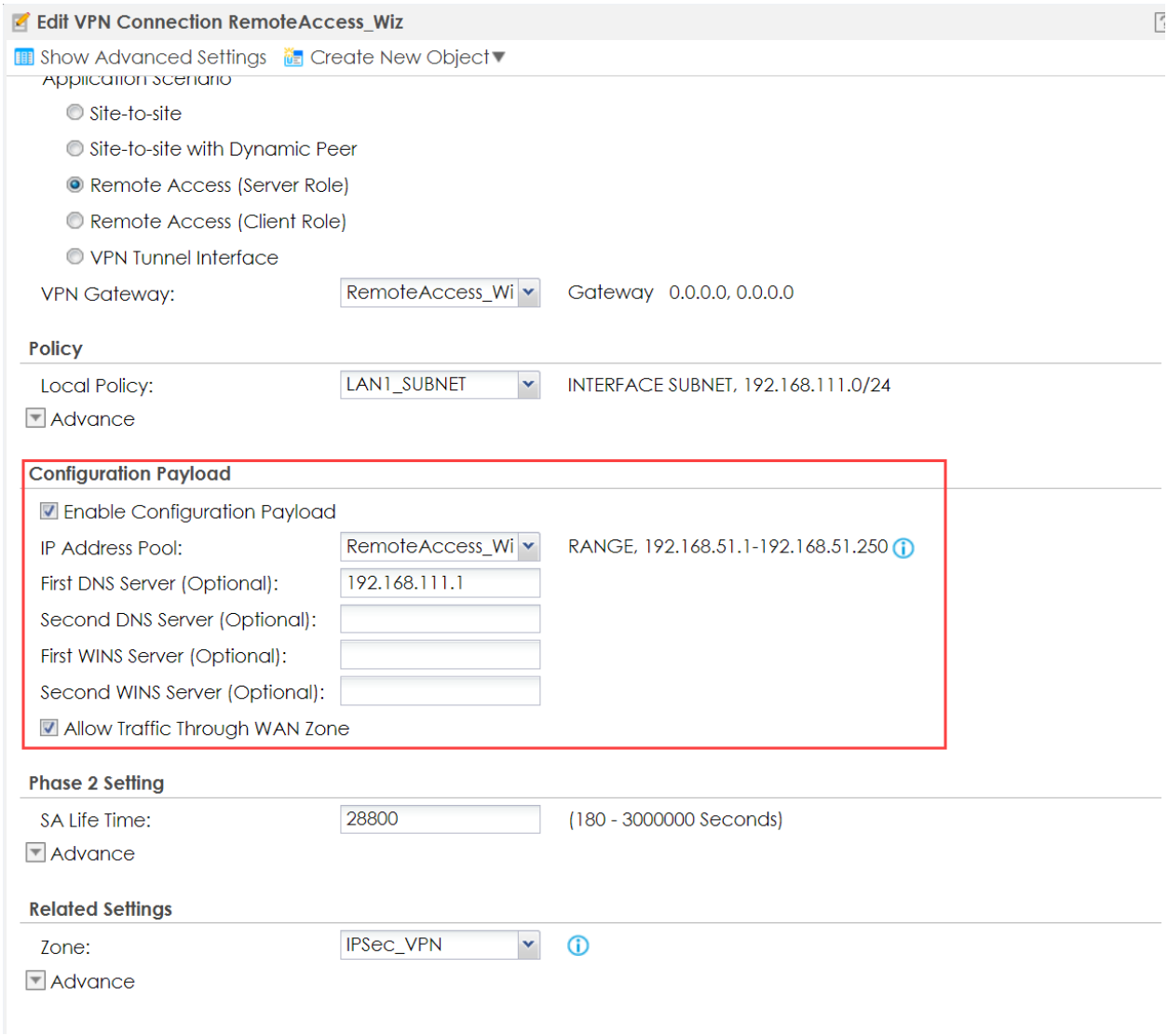
1. Das verwendetet Zertifikat kann ein Self-Signed Certificate sein, muss aber auf der Gegenseite unter «Trusted Certificates» hinterlegt werden.
2. Auf beiden Seiten wird ein eigenes Zertifikat angelegt
3. Der Local ID Type wird aus dem Zertifikat entnommen und muss auf der Gegenseite identisch als Peer ID eingetragen werden.
4. Die Empfehlung für die maximale SA-Life Time ist im VPN Gateway 86400 Sekunden und in der VPN Connection 14400 Sekunden
5. Als VPN-Verschlüsselung werden folgende Einstellungen als Minimum empfohlen: AES256 / SHA256 / DH15. Dies sowohl im VPN-Gateway als auch in der VPN-Connection.
6. Extended Authentication Protocol ist auch bei Site-to-Site Tunnels möglich. Jedoch wird der eingetragene User beim Verbindungsaufbau nicht an der Firewall angemeldet.


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

Client-to-Site VPN

Bei Client-to-Site VPN wird IKEv2 mit Zertifikat und Extended Authentication Protocol empfohlen.

In der VPN-Connection ist Configuration Payload zwingend erforderlich.



Nach dem Verbindungsaufbau ist der Client an der Firewall mit dem Benutzer angemeldet. Für einen allfälligen Admin-Zugriff auf die Firewall kann somit der entsprechende Admin User im Policy Control hinterlegt werden.

L2TP-VPN

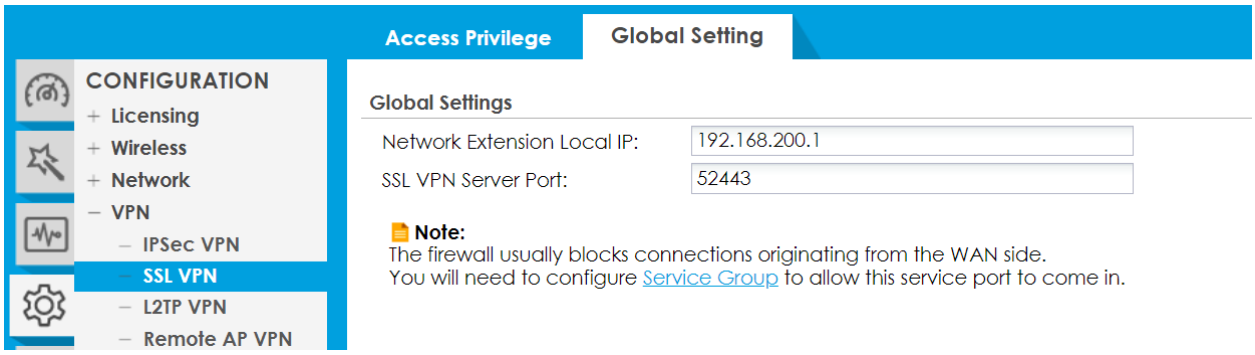
Von der Verwendung von L2TP-VPN wird abgeraten. Stattdessen kann IKEv2 eingesetzt werden.

SSL-VPN

Aufgrund der Performance und allfälligen Sicherheitsproblemen wird SSL-VPN nicht empfohlen. Da dies jedoch aufgrund der Einfach-Konfiguration gerne eingesetzt wird, sollte folgendes beachtet werden:

Configuration > VPN > SSL VPN > Global Setting

Die Verwendung eines separaten Ports für SSL VPN ist Pflicht. Unter keinen Umständen sollte der Port 443 verwendet werden.



Die Sicherheit wird durch die Verwendung eines Zertifikates zur Authentifizierung erheblich erhöht. Die Konfiguration ist unter «Remote Management über HTTPS > Authenticate Client Certificate» beschrieben.

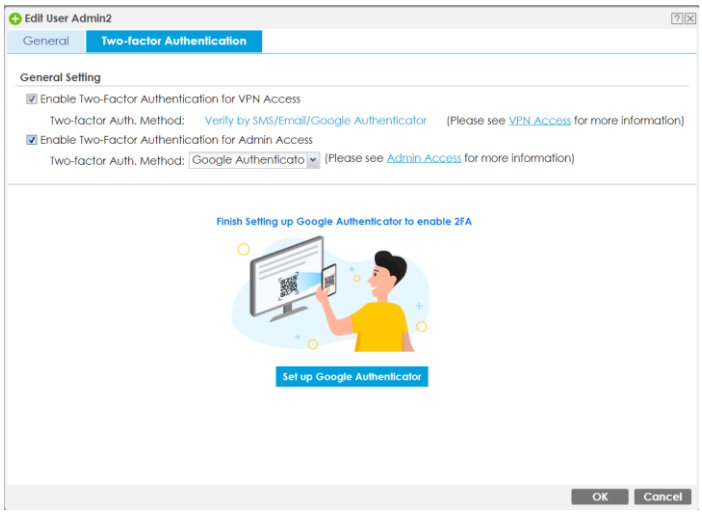
Im Policy Control ist es ratsam die Source IP für den Zugriff von WAN zu ZyWALL für den Service Wiz_SSLVPN einzuschränken. Mindestens auf eine GeoIP, besser auf einen FQDN oder eine IP-Adresse.

Ebenfalls kann der Administrator-Zugriff auf die Firewall aus der SSL-VPN Zone auf den Admin User eingegrenzt werden. Dies ist möglich, da sich der User bereits beim Tunnel Aufbau an der Firewall anmeldet.

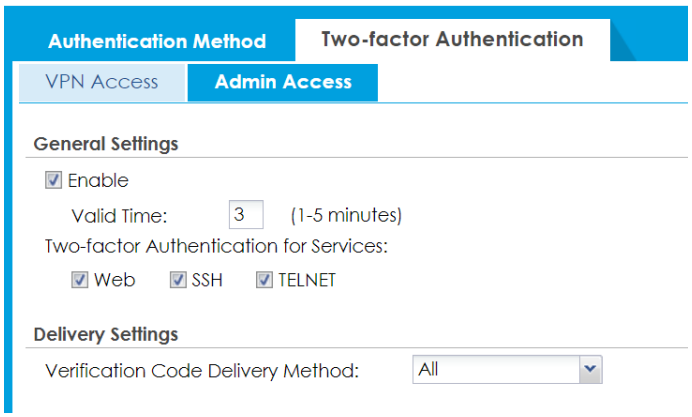
Normale User benötigen keinen Zugriff aus der SSL-VPN Zone auf die Firewall. Es reicht aus, wenn hier die typischen Services wie DNS erlaubt werden.

TWO-FACTOR-AUTHENTICATION

Eine 2-Faktor-Authentifizierung wird für Admin Access empfohlen, vorzugsweise mit Google Authenticator.
Das Einrichten für 2FA muss für jeden User separat durchgeführt werden. Empfohlen wird die Google-Authenticator-Methode. Zu beachten ist, dass sich User, bei den 2FA nicht eingerichtet ist, weiterhin ohne zusätzliche Authentifizierung anmelden können. Aus diesem Grund bietet 2FA nur bedingt Schutz.

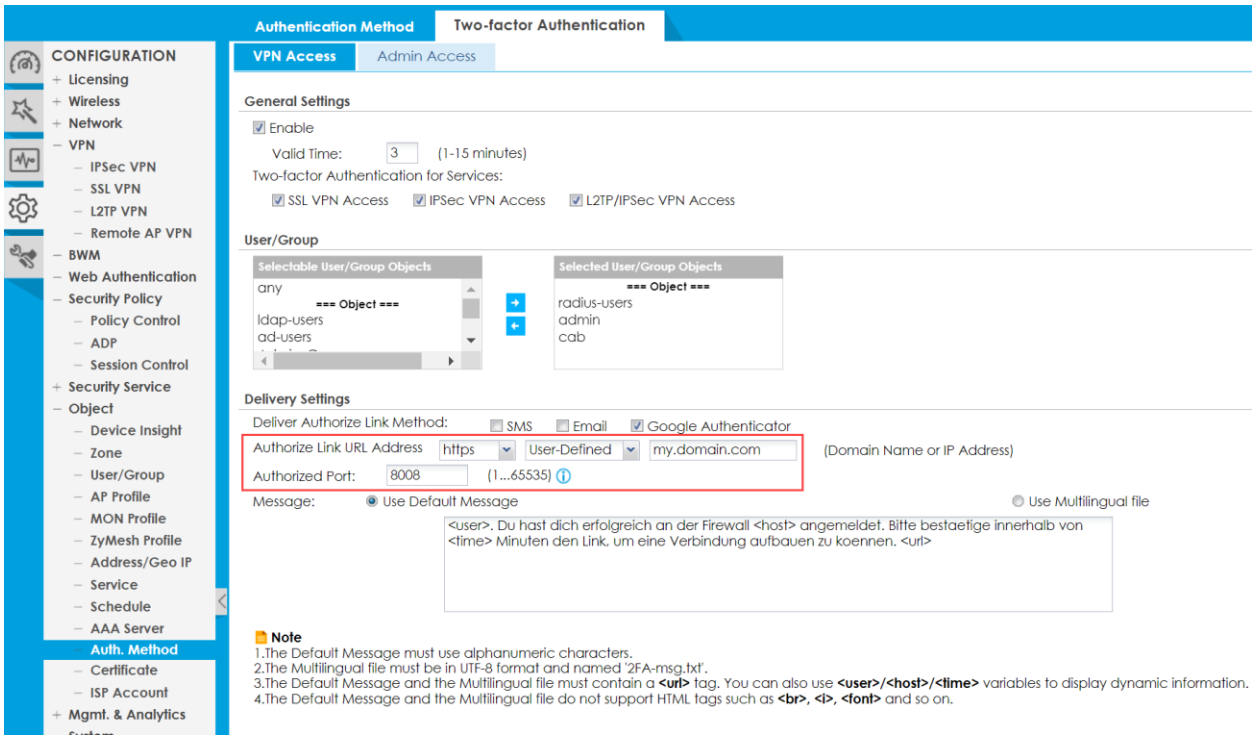


Configuration > Object > Auth. Method > Two-factor Authentication > Admin Access



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

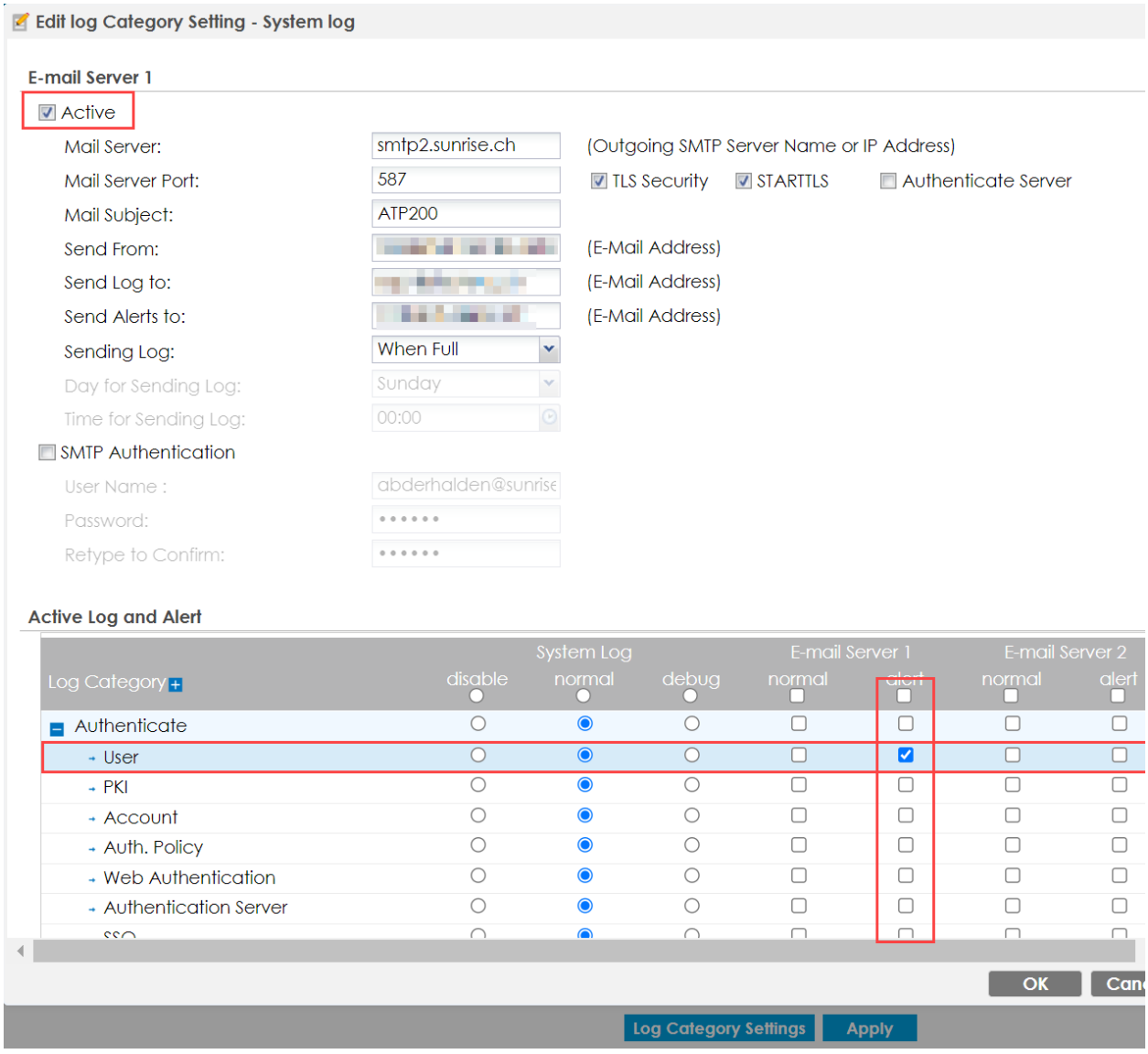
2FA kann auch für VPN-Access aktiviert werden.
Zur Authentifizierung wird immer ein eigener Port verwendet (Objekt Wiz_2FA).
Es stehen auch verschieden Methoden zur Verfügung, wie ein Link gesendet werden soll. Schlussendlich wird jedoch bei allen Methoden ein Link auf das WEB-GUI aufgerufen.
Da das WEB-GUI für 2FA aus dem WAN erreichbar sein muss, besteht hier auch ein potenzielles Angriffsrisiko. Aus diesem Grund ist diese Funktion mit Vorsicht zu geniessen.



ALERT LOGS

Für einige Optionen kann es sinnvoll sein, ein Alert Log einzurichten. Dabei kann beim Eintreffen eines Events sofort eine E-Mail-Benachrichtigung ausgelöst werden. Sinnvoll ist dies zum Beispiel, wenn sich ein Administrator einloggt. Besonders bei Firewalls, die nur in unregelmässigen Abständen überwacht werden.

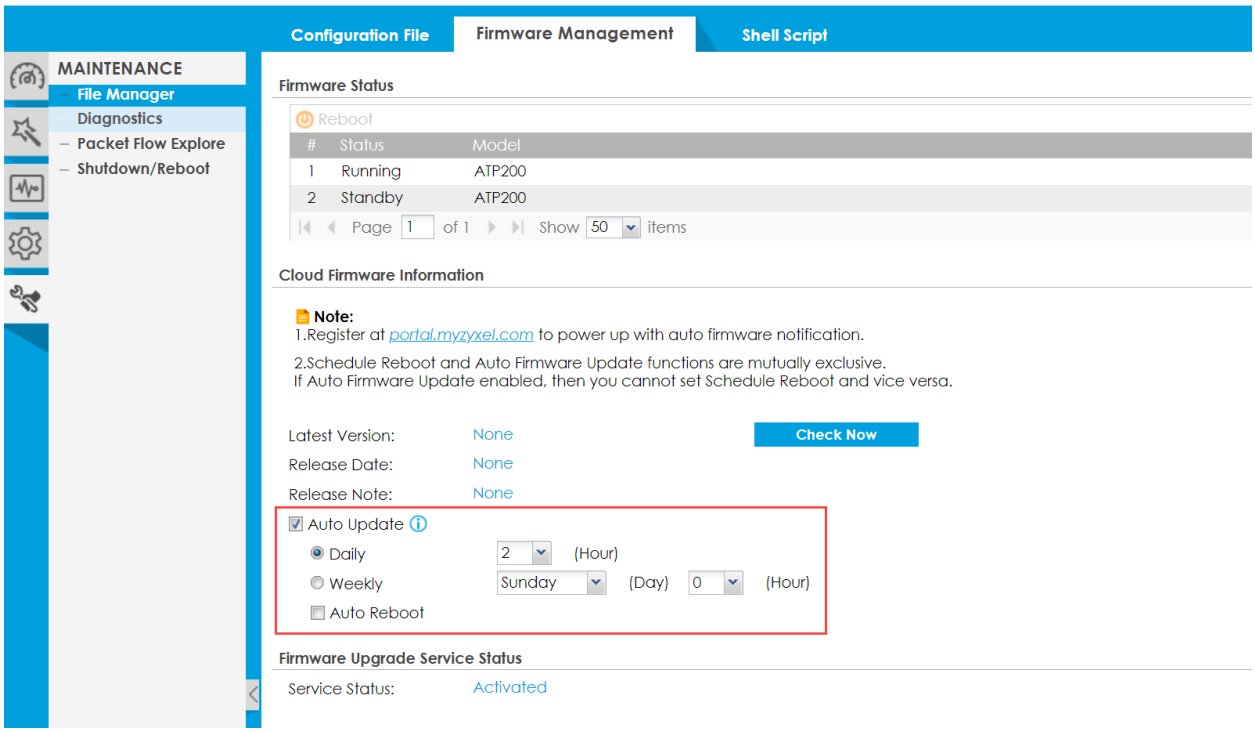
Configuration > Log & Report > Log Settings



AUTOMATISCHE FIRMWARE UPDATES

Es sollte immer darauf geachtet werden, dass die Firmware der Firewall auf dem aktuellen Stand ist. Bei Systemen die aktiv betreut werden können Aktualisierungen manuell erfolgen. Jedoch ist es in der Realität häufig der Fall, dass dies vernachlässigt wird und Firewalls mit bekannten Sicherheitslücken über einen langen Zeitraum nicht aktualisiert werden.
Besonders in Umgebungen dieser Art empfiehlt es sich aus Sicherheitsgründen, Automatische Updates zu aktivieren.

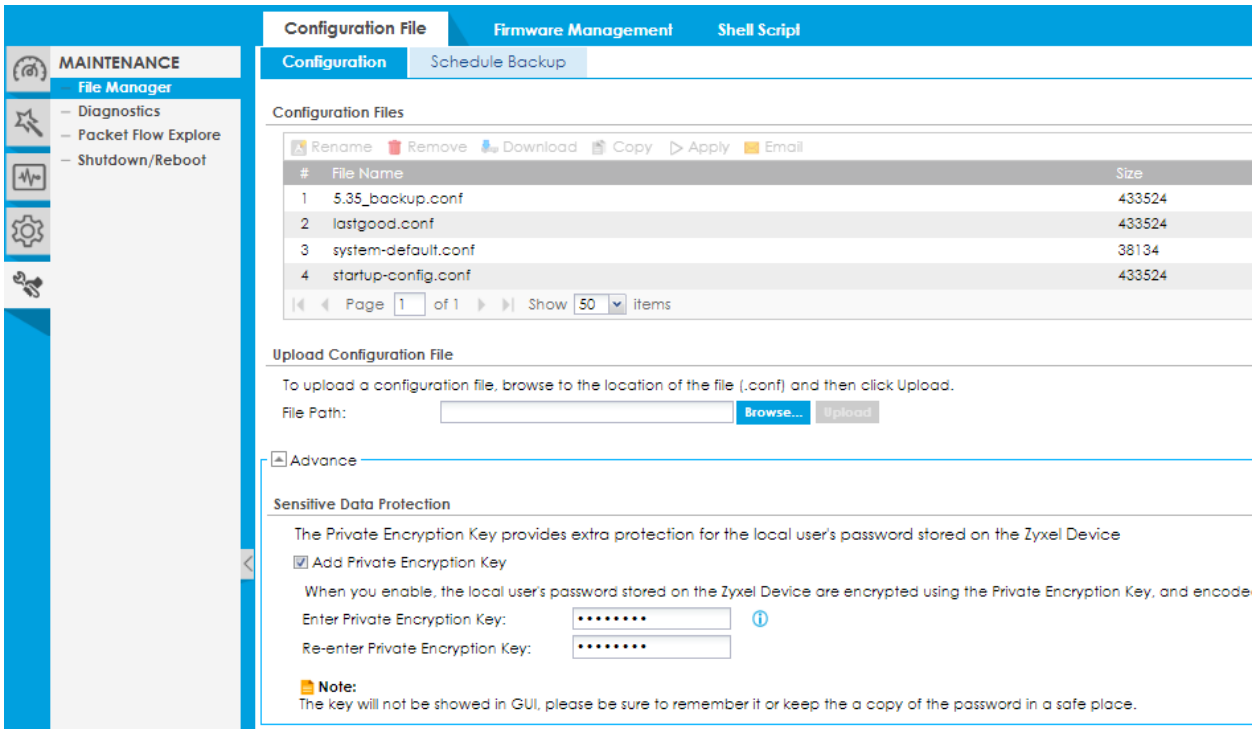
Maintenance > File Manager > Firmware Management



SENSITIVE DATA PROTECTION

Ab Firmware Version 5.35 lassen sich Passwörter mit einem eigenen Schlüssel anstelle des Default-Algorithmus verschlüsseln.
Die Funktion Schütz auch vor dem Auslesen von Benutzer-Passwörtern aus Konfigurationsfiles mit Hilfe von Hacking-Tools.
Andere Passwörter verwenden weiterhin die Default-Methode.

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



Wird die Datei wieder auf eine Firewall eingespielt. Ist dies nur mit dem entsprechenden Schlüssel möglich.