Workshop

Hands-on Workshop H-Firewall-Serie

Dashmir Kasa Leiter Technischer Support & Kursleiter
Studerus AG

Agenda

1. Einführung & Übersicht der Firewall H-Serie
2. Gerätemanagement
3. Geräteregistration (Nebula)
4. Security Policy
5. Security Services
6. VPN & 2FA
7. WLAN-Controller (Nebula)
8. CLI
9. Coole Features

1. Einführung

- Assistenten während des Workshops
  - Armand Blechner
  - Christian Abderhalden

- Neue Firewall-Serie
  - Überblick über Flex H Series (uOS)
  - uOS FW Release Plan

Überblick über Flex H Series (uOS)

USG FLEX **H SERIES**

USG FLEX 100H / 100HP

3 Gbps

Size:	SOHO / SB
SPI firewall throughput:	3,000 Mbps
UTM throughput:	750Mbps
VPN throughput:	750Mbps
Ports:	8 x 1GbE
Fanless:	YES
PoE:	1 Port (100HP)

USG FLEX **H SERIES**

USG FLEX 200H / 200HP

5 Gbps

Size:	SB
SPI firewall throughput:	5,000 Mbps
UTM throughput:	1,500 Mbps
VPN throughput:	1,200 Mbps
Ports:	6 x 1GbE, 2 x 2.5GbE
Fanless:	YES
PoE:	1 Port (200HP)

USG FLEX **H SERIES**

USG FLEX 500H

10 Gbps

Size:	SMB
SPI firewall throughput:	10,000 Mbps
UTM throughput:	2,500 Mbps
VPN throughput:	2,000 Mbps
Ports:	8 x1GbE 4 x 2.5GbE
Fanless:	-
PoE:	2 Ports

USG FLEX **H SERIES**

USG FLEX 700H

15 Gbps

Size:	Medium Business
SPI firewall throughput:	15,000 Mbps
UTM throughput:	4,000 Mbps
VPN throughput:	3,000 Mbps
Ports:	2 x Multi-GbE (up to 10G) 2 x SFP+, 8 x 1GbE, 2 x 2.5GbE
Fanless:	-
PoE:	2 Ports

STUDERUS network technologies

H Series uOS Release Plan

	Oct'24/uOS1.30/Nebula 18.20	Jan'25/uOS1.31/Nebula 18.30	April'25/uOS1.32/Nebula 19.00	July'25/uOS1.35/Nebula 19.10
On-prem	• New USG FLEX 50H(P) • FQDN Object • BWM (Support ppp, bridge and VTI interfaces) • Source IP spoofing prevention • Web Console • Entry Defense Pack • Schedule Reboot	• Email Alerts • SIP ALG • Device HA • Packet Flow Explore	• Tailscale-like VPN (Wireguard) • Secure WiFi (AP Controller) • Captive portal • 802.1x Authentication • Layer 2 Isolation • BWM for per user/per source-IP • IGMP • Routing Trace • **DoH/DoT** • **LAG** • **700H upgrade license**	• IPv6 dual stack • Speed Test on GUI • SNMP OID MIBs enhancements • **CDR**
NCC Portal	**Multi-Site Management** • Topology • Device Status (CPU/memory/session) • Event Log • Security Profile Synchronizations • Support Nebula pro pack transfer • Priority Support	**Nebula Configurations phase I** • Dashboard • **Auto VPN** • Port, Interface, Object • NAT, Routing • Firewall • Security Policy • Security Service (site-wide) • Summary Reports • Application/Client Usage	**Nebula Configurations phase II** • LAG • Non-Nebula VPN • Remote VPN (IPSec/SSL) • Authentication (Cloud Auth) • **Device HA Status & Topology** • License migration from FLEX/ATP • **700H upgrade license**	• **CDR** • **DoH/DoT** • Firewall schedule Reboot • Smart virtual server (auto-generate security policy)

Tools, Converter & License Migration

OP Tool (E/Aug, 2024)

Country/RMA Device License Transfer

Device Owner Transfer

Device Unregister/Trial Reset

License Check

License Lock/Unlock

Configuration Converter (Dec, 2024)

FLEX/ATP on-prem to H Series

License Migration (April, 2025)

FLEX/ATP license transfer to H Series on Nebula

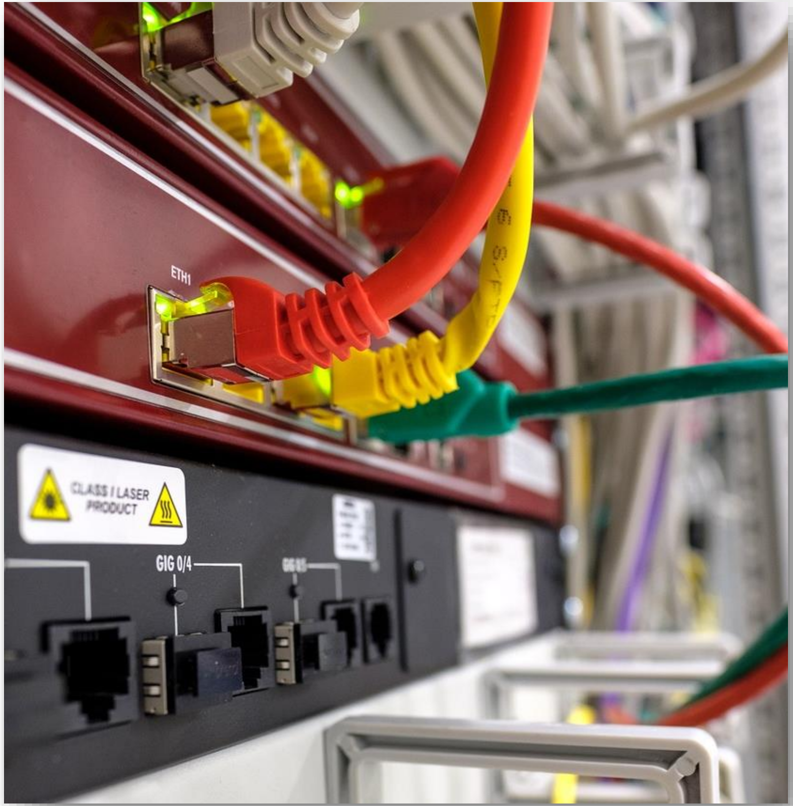
Configuration Convert Tool (H2, 2025)

(FLEX/ATP on-cloud to H Series)

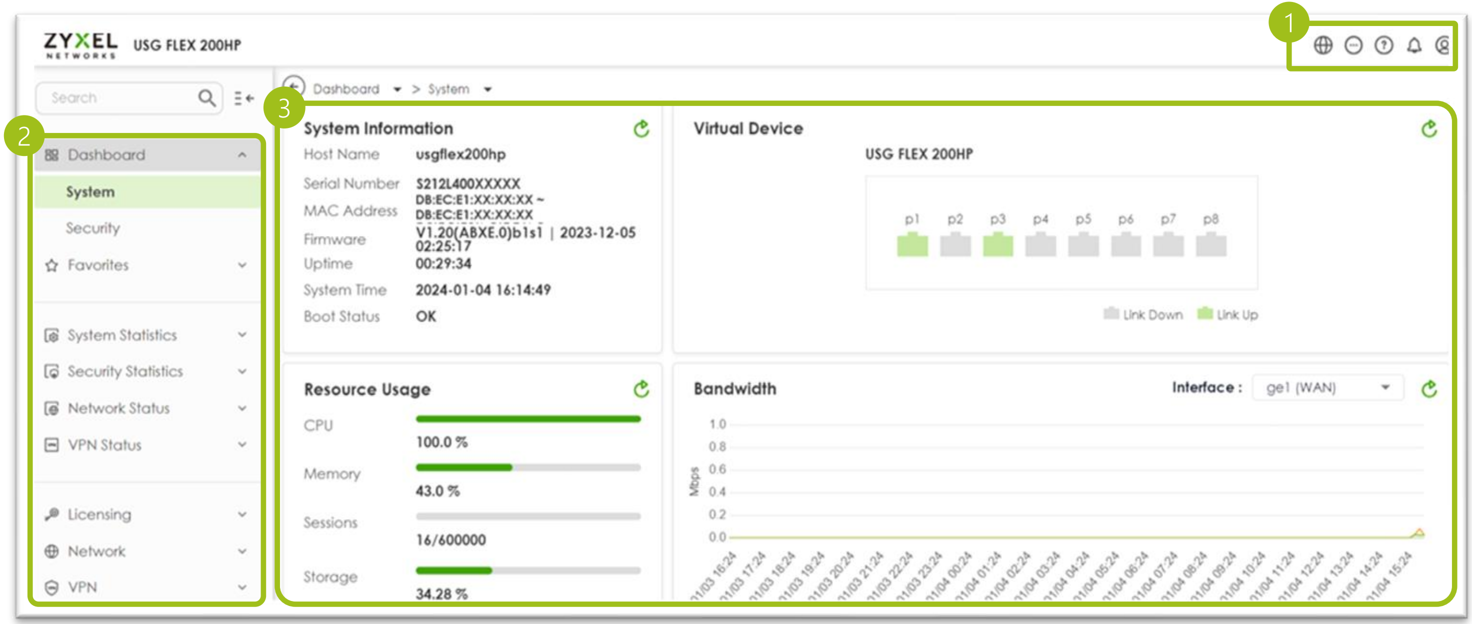
2. Gerätemanagement

- Theorie:
  - Zugriffsmöglichkeiten
  - Vereinfachtes Management

- Praxis:
  - Verbindung zur Firewall herstellen
  - Oberfläche erkunden



GUI-Übersicht



1 Title bar

2 Navigation panel

3 Main Window

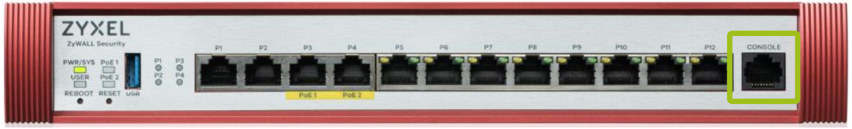
Management Tools

- Zugriffsmöglichkeiten
  - Konsole
  - SSH
  - Web GUI
  - Web Console (ab 1.30)

Management Tools

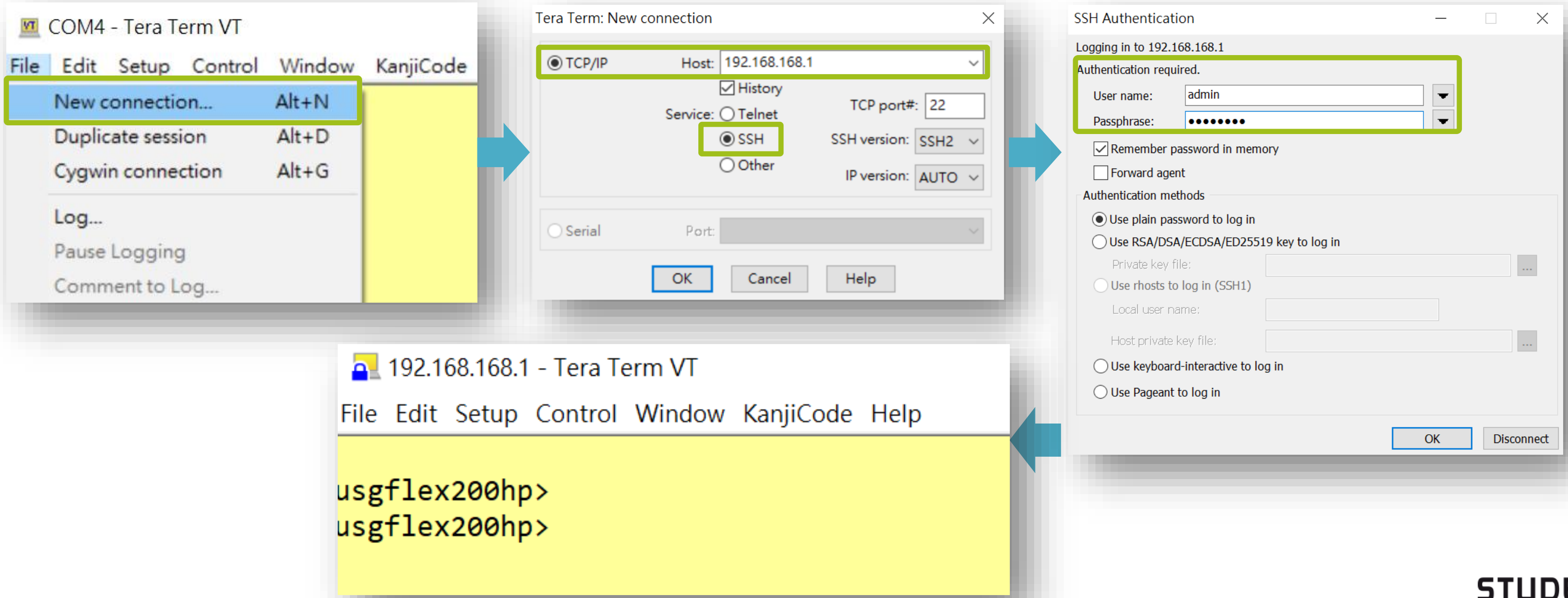
- Konsolenport
  - RJ-45 auf DB-9 Rollover-Kabel

RJ-45 zu DB-9 Konsolenkabel



Management Tools

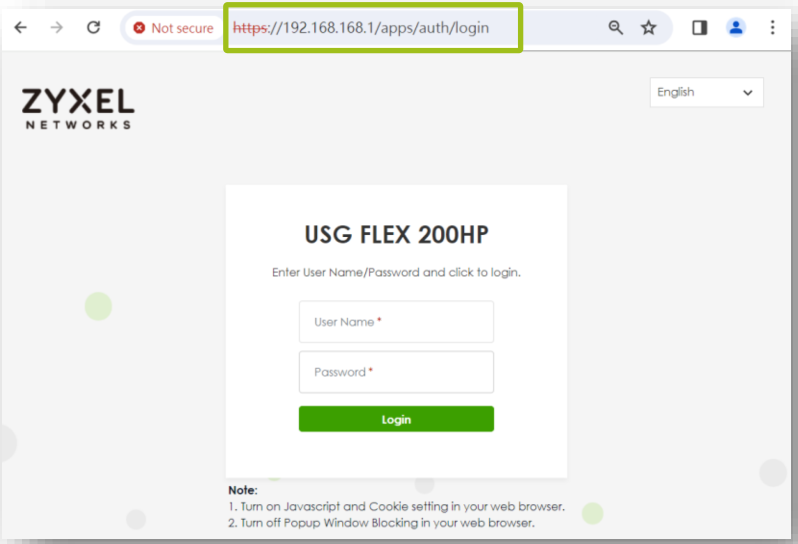
- SSH Zugang
  - Mit Putty oder TeraTerm eine Verbindung aufbauen



STUDERUS network technologies

Management Tools

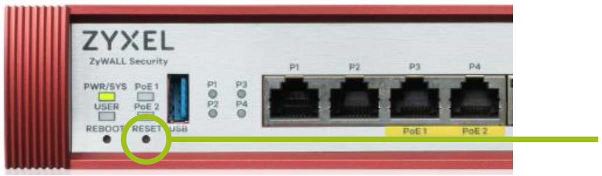
- Web-Gui
  - Beliebigen Browser die IP des Gateways eingeben “**192.168.168.1**”



Reset Firewall – System Default

- Reset zu System Default
  - Nur die Zertifikate und Signaturen werden aufbewahrt.

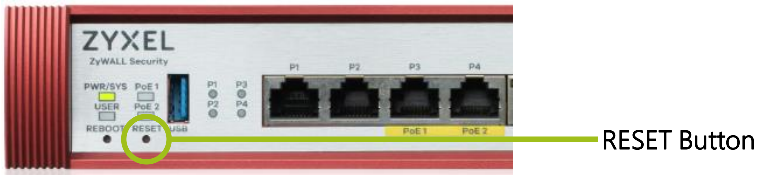
- Wie wird das gemacht?
  - Drücken Sie die „RESET"-Taste länger als 7 Sekunden, bis die LED grün blinkt, und lassen Sie sie dann los.
  - GUI: wählen Sie das Konfigurationsfile "**system-default.conf**" aus.
  - CLI: **hostname > cmd config-apply system-default.conf**



Reset Firewall – Factory Default

- Reset zu <u>Factory Default</u>
  - Die Konfigurationsdateien, Zertifikate und Signaturen werden <u>nicht</u> aufbewahrt.

- Wie wird das gemacht?
  - Drücken Sie die Taste „**RESET**“ länger als <u>**30 Sekunden**</u>. Die LED-Anzeige blinkt zunächst grün, drücken Sie dann weiter, bis die LED-Anzeige rot blinkt, und lassen Sie sie dann los.
  - CLI: **hostname > cmd system _recovery factory-default**

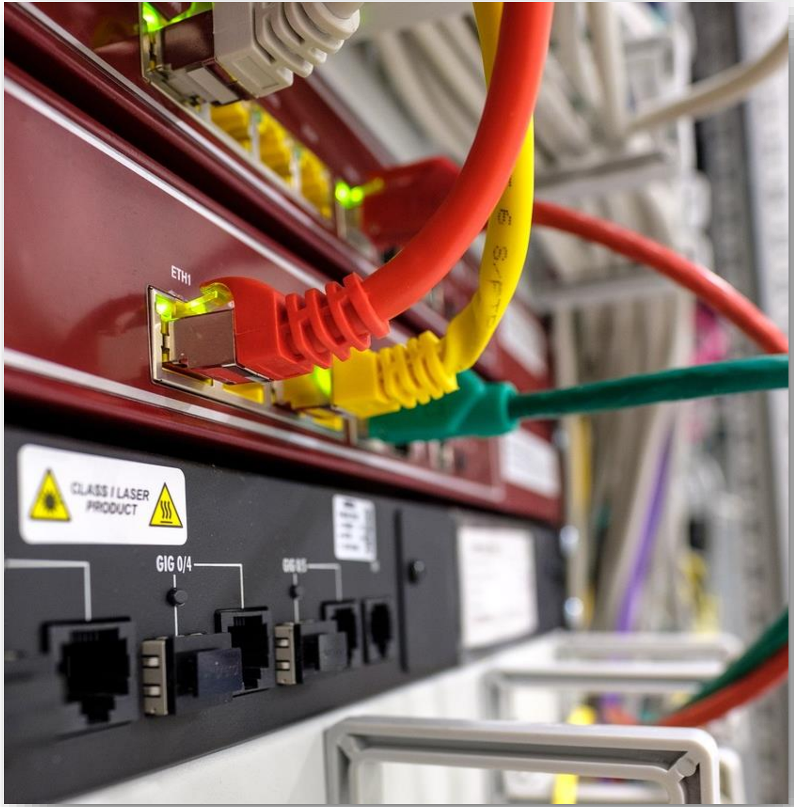


STUDERUS network technologies

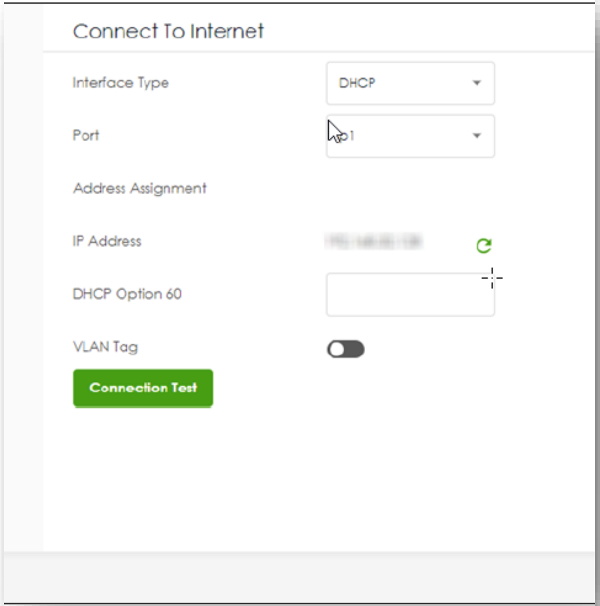
Gerätemanagement

- Theorie:
  - Zugriffsmöglichkeiten
  - Vereinfachtes Management

- Praxis:
  - Verbindung zur Firewall herstellen
  - Oberfläche erkunden
  - **Lokales Subnetz ändern**



3. Geräteregistration (Nebula)



STUDERUS
network technologies

4. Security Policy

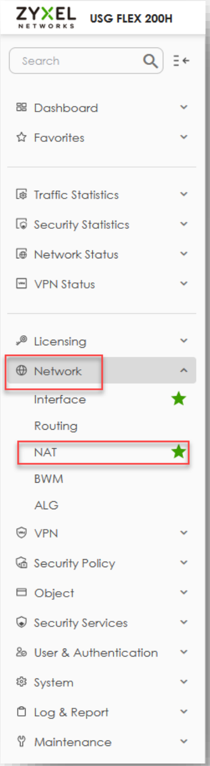
- Wo finde ich die Security Policy
- Hat sich etwas geändert?
- Was hat die Hits Spalte auf sich?

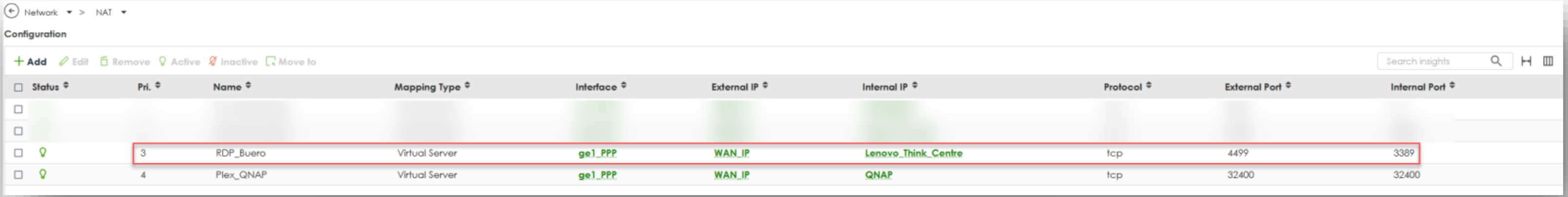
Aufgabe

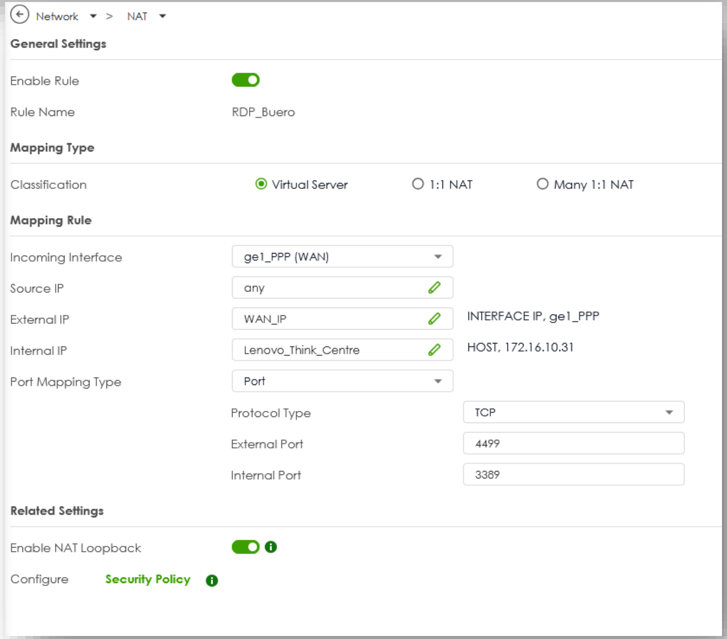
- Wie erstelle ich eine NAT-Regel auf der H-Serie?
- Wie erstelle ich die Objekte?
- Wird für die NAT-Regel noch etwas benötigt?
- Wo sehe ich, warum die NAT-Regel nicht greift?

4.1 NAT-Regel erstellen

https://your-IP/apps/network/nat/add

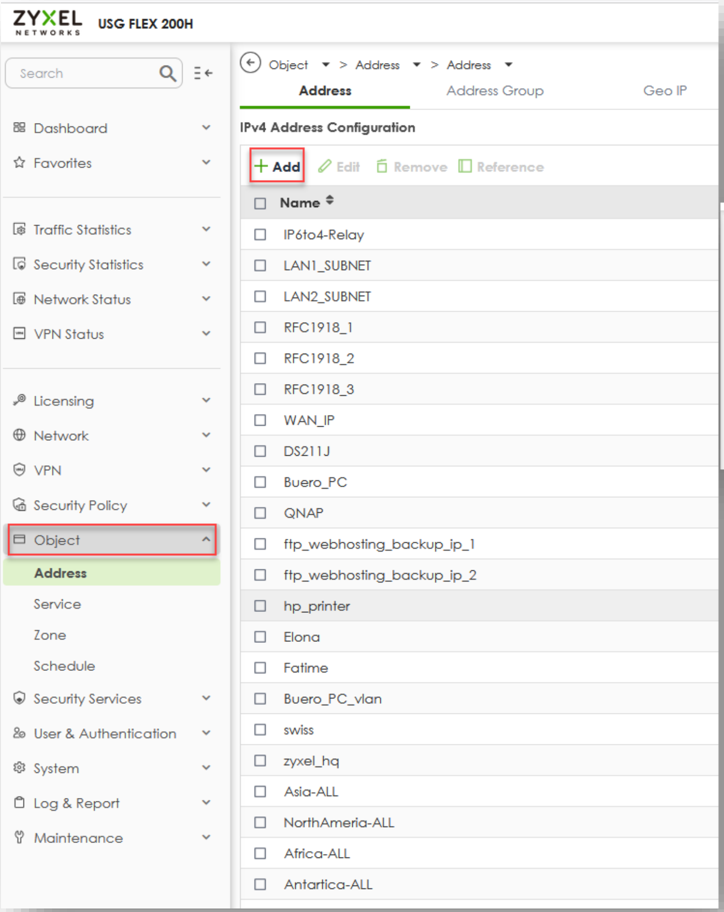


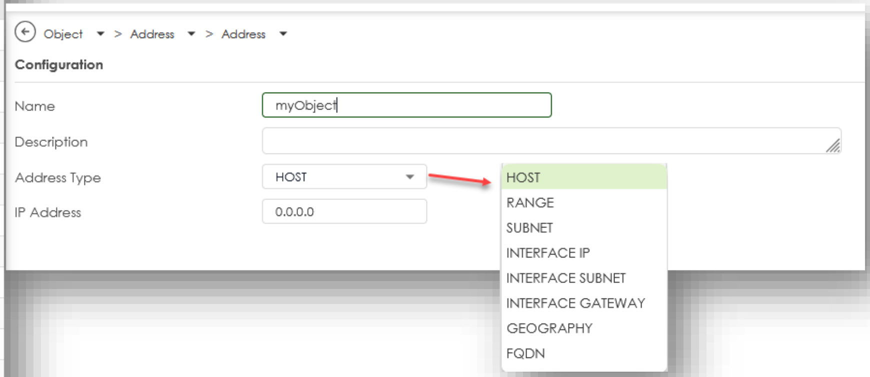




STUDERUS
network technologies

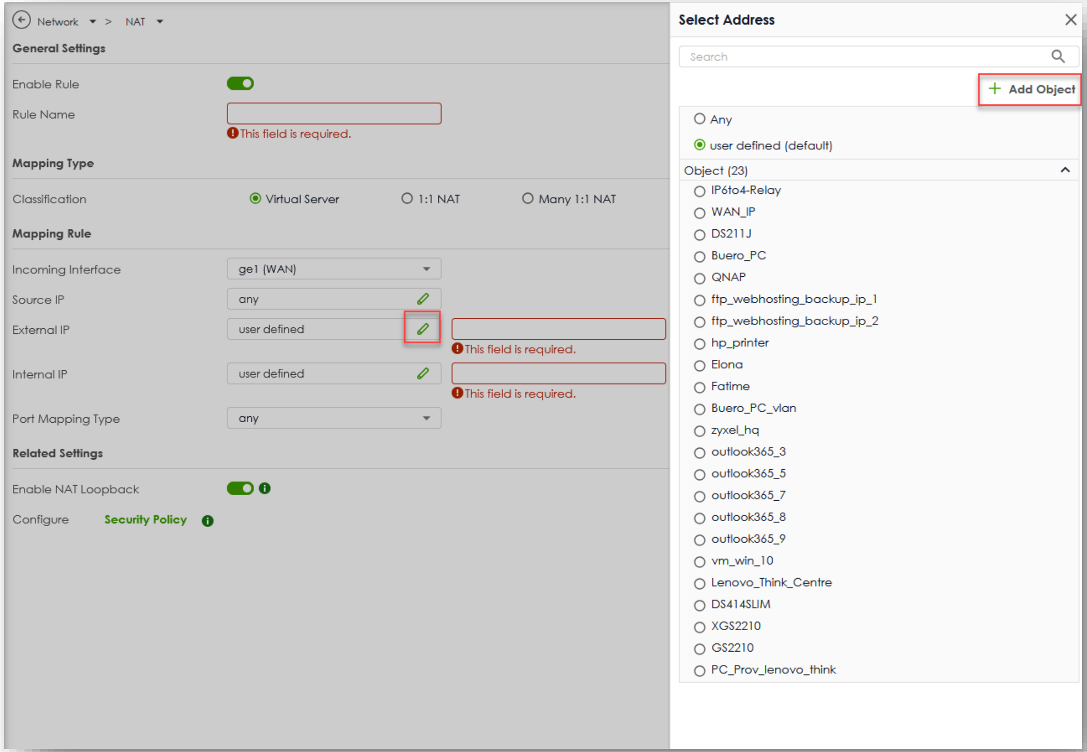
4.2 Objekte erstellen (Methode 1)

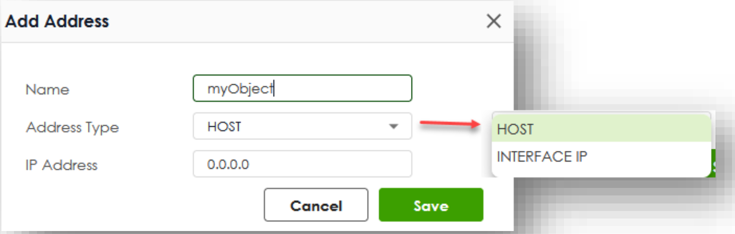


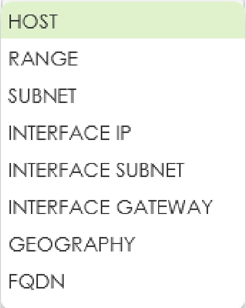


STUDERUS network technologies

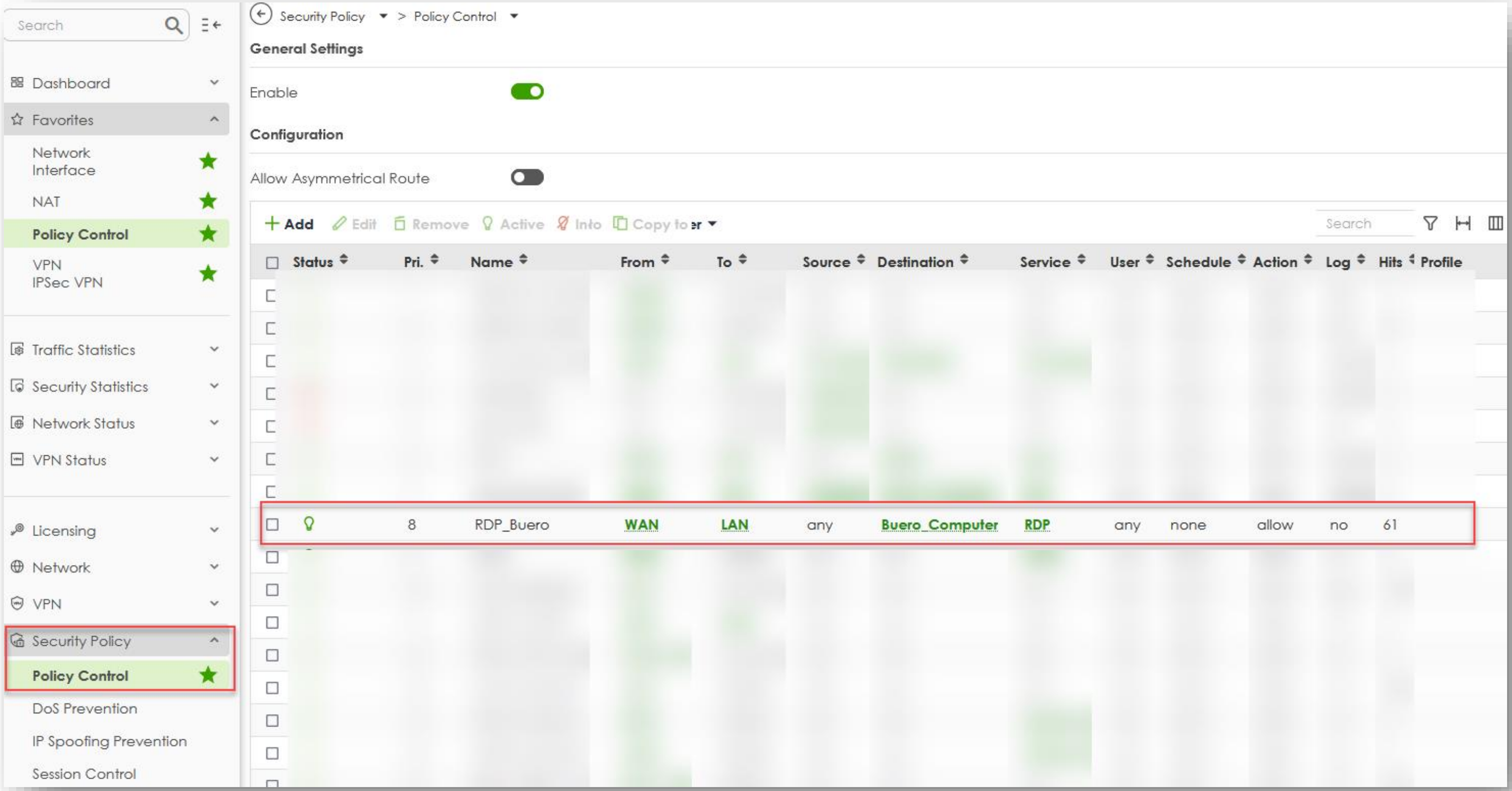
4.2 Objekte erstellen (Methode 2)





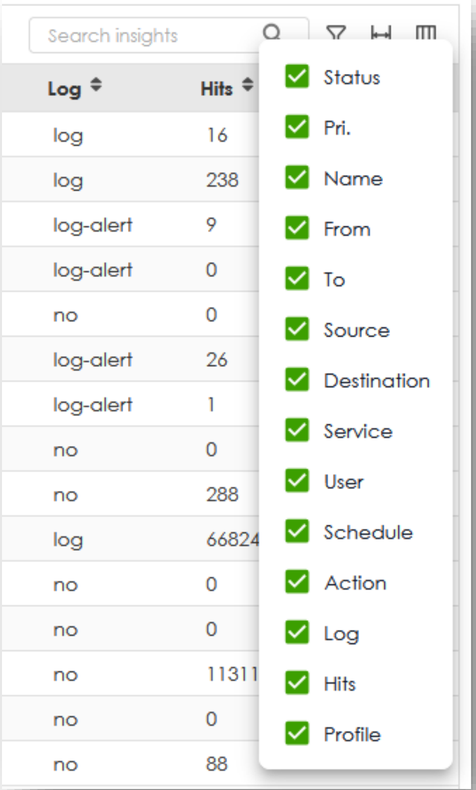


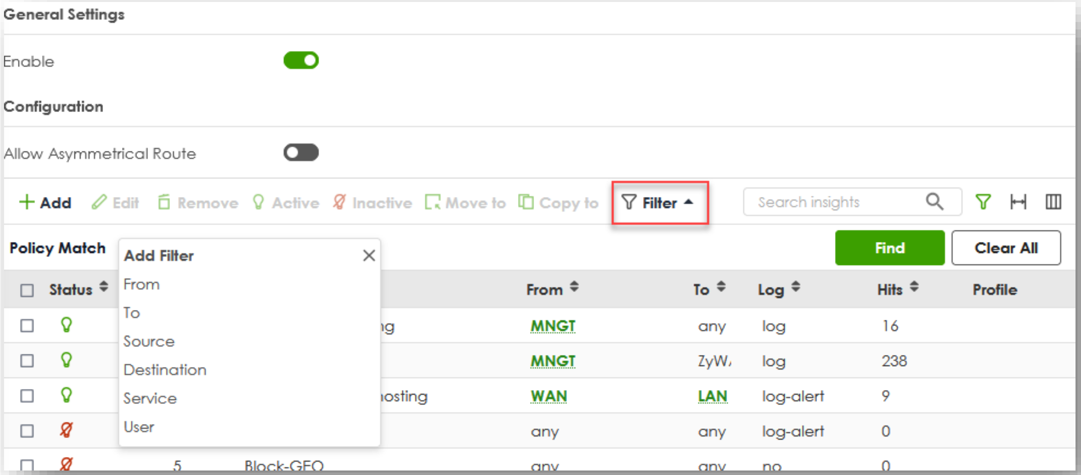
4.3 Policy Control (Firewall Regel)



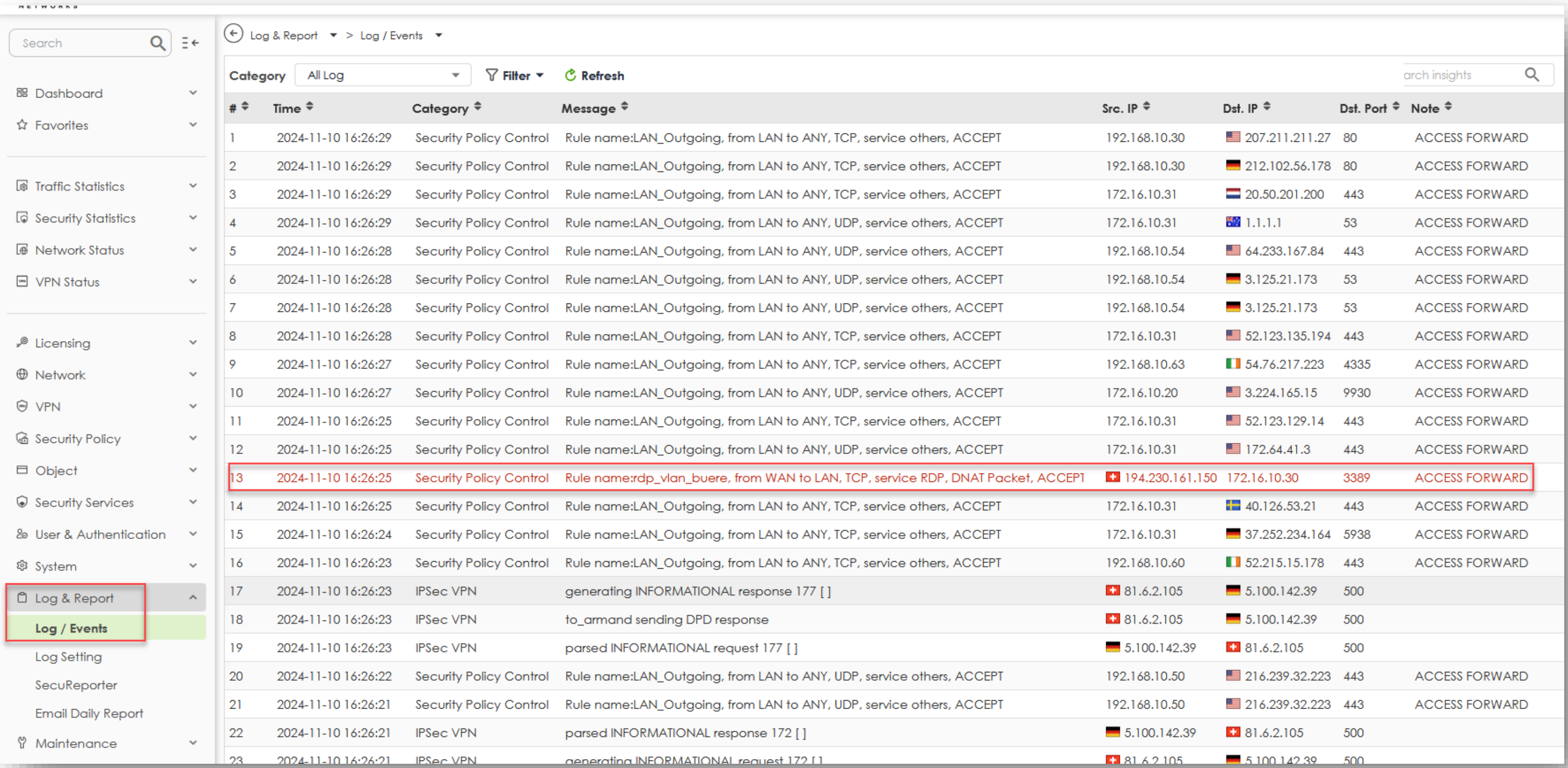
STUDERUS network technologies

4.3 Policy Control - Filter





4.4 Loggen

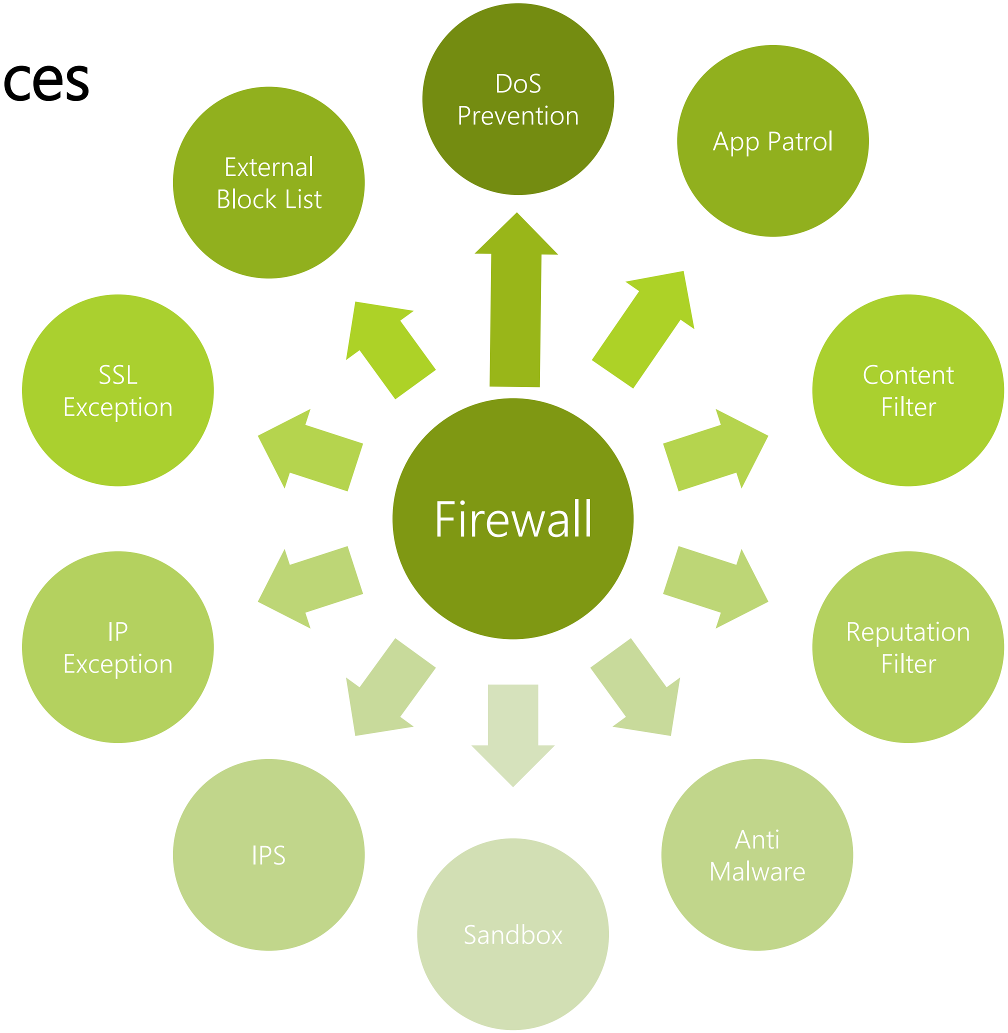


#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
1	2024-11-10 16:26:29	Security Policy Control	Rule name:LAN_Outgoing, from LAN to ANY, TCP, service others, ACCEPT	192.168.10.30	207.211.211.27	80	ACCESS FORWARD
2	2024-11-10 16:26:29	Security Policy Control	Rule name:LAN_Outgoing, from LAN to ANY, TCP, service others, ACCEPT	192.168.10.30	212.102.56.178	80	ACCESS FORWARD
3	2024-11-10 16:26:29	Security Policy Control	Rule name:LAN_Outgoing, from LAN to ANY, TCP, service others, ACCEPT	172.16.10.31	20.50.201.200	443	ACCESS FORWARD
4	2024-11-10 16:26:29	Security Policy Control	Rule name:LAN_Outgoing, from LAN to ANY, UDP, service others, ACCEPT	172.16.10.31	1.1.1.1	53	ACCESS FORWARD
5	2024-11-10 16:26:28	Security Policy Control	Rule name:LAN_Outgoing, from LAN to ANY, UDP, service others, ACCEPT	192.168.10.54	64.233.167.84	443	ACCESS FORWARD
6	2024-11-10 16:26:28	Security Policy Control	Rule name:LAN_Outgoing, from LAN to ANY, UDP, service others, ACCEPT	192.168.10.54	3.125.21.173	53	ACCESS FORWARD
7	2024-11-10 16:26:28	Security Policy Control	Rule name:LAN_Outgoing, from LAN to ANY, UDP, service others, ACCEPT	192.168.10.54	3.125.21.173	53	ACCESS FORWARD
8	2024-11-10 16:26:28	Security Policy Control	Rule name:LAN_Outgoing, from LAN to ANY, TCP, service others, ACCEPT	172.16.10.31	52.123.135.194	443	ACCESS FORWARD
9	2024-11-10 16:26:27	Security Policy Control	Rule name:LAN_Outgoing, from LAN to ANY, TCP, service others, ACCEPT	192.168.10.63	54.76.217.223	4335	ACCESS FORWARD
10	2024-11-10 16:26:27	Security Policy Control	Rule name:LAN_Outgoing, from LAN to ANY, UDP, service others, ACCEPT	172.16.10.20	3.224.165.15	9930	ACCESS FORWARD
11	2024-11-10 16:26:25	Security Policy Control	Rule name:LAN_Outgoing, from LAN to ANY, TCP, service others, ACCEPT	172.16.10.31	52.123.129.14	443	ACCESS FORWARD
12	2024-11-10 16:26:25	Security Policy Control	Rule name:LAN_Outgoing, from LAN to ANY, UDP, service others, ACCEPT	172.16.10.31	172.64.41.3	443	ACCESS FORWARD
13	2024-11-10 16:26:25	Security Policy Control	Rule name:rdp_vlan_buere, from WAN to LAN, TCP, service RDP, DNAT Packet, ACCEPT	194.230.161.150	172.16.10.30	3389	ACCESS FORWARD
14	2024-11-10 16:26:25	Security Policy Control	Rule name:LAN_Outgoing, from LAN to ANY, TCP, service others, ACCEPT	172.16.10.31	40.126.53.21	443	ACCESS FORWARD
15	2024-11-10 16:26:24	Security Policy Control	Rule name:LAN_Outgoing, from LAN to ANY, TCP, service others, ACCEPT	172.16.10.31	37.252.234.164	5938	ACCESS FORWARD
16	2024-11-10 16:26:23	Security Policy Control	Rule name:LAN_Outgoing, from LAN to ANY, TCP, service others, ACCEPT	192.168.10.60	52.215.15.178	443	ACCESS FORWARD
17	2024-11-10 16:26:23	IPSec VPN	generating INFORMATIONAL response 177 [ ]	81.6.2.105	5.100.142.39	500	
18	2024-11-10 16:26:23	IPSec VPN	to_armand sending DPD response	81.6.2.105	5.100.142.39	500	
19	2024-11-10 16:26:23	IPSec VPN	parsed INFORMATIONAL request 177 [ ]	5.100.142.39	81.6.2.105	500	
20	2024-11-10 16:26:22	Security Policy Control	Rule name:LAN_Outgoing, from LAN to ANY, UDP, service others, ACCEPT	192.168.10.50	216.239.32.223	443	ACCESS FORWARD
21	2024-11-10 16:26:21	Security Policy Control	Rule name:LAN_Outgoing, from LAN to ANY, UDP, service others, ACCEPT	192.168.10.50	216.239.32.223	443	ACCESS FORWARD
22	2024-11-10 16:26:21	IPSec VPN	parsed INFORMATIONAL response 172 [ ]	5.100.142.39	81.6.2.105	500	
23	2024-11-10 16:26:21	IPSec VPN	generating INFORMATIONAL request 172 [ ]	81.6.2.105	5.100.142.39	500	

Praktische Aufgabe

- Erstellt eine NAT-Regel für einen Web-Server
- Objekt für eine WAN-IP
- Objekt für einen Web-Server
- Firewall Regel erstellen

5. Securitiy Services



5.1 Entry Defense Pack

- Seit 21. Oktober auf nicht gebündelte Geräte der H-Serie
- Gold Security Pack hat immer höhere Priorität

1. Sicherheit für Ihr Netzwerk - ohne zusätzliche Kosten
   - DNS Threat Filter
   - URL Threat Filter
   - IP Reputation
2. Cybersecurity Monitoring & Log Aufbewarung
   - Zentralisierte Sichtbarkeit im SecuReporter
3. Priority Support
   - Eröffnen von Support Tickets direkt im Nebula möglich.
   - Live chat mit Zyxel HQ Technikern

Weitere Infos: https://www.zyxel.com/de/de/entry-defense-pack

5.2 External Blocklist

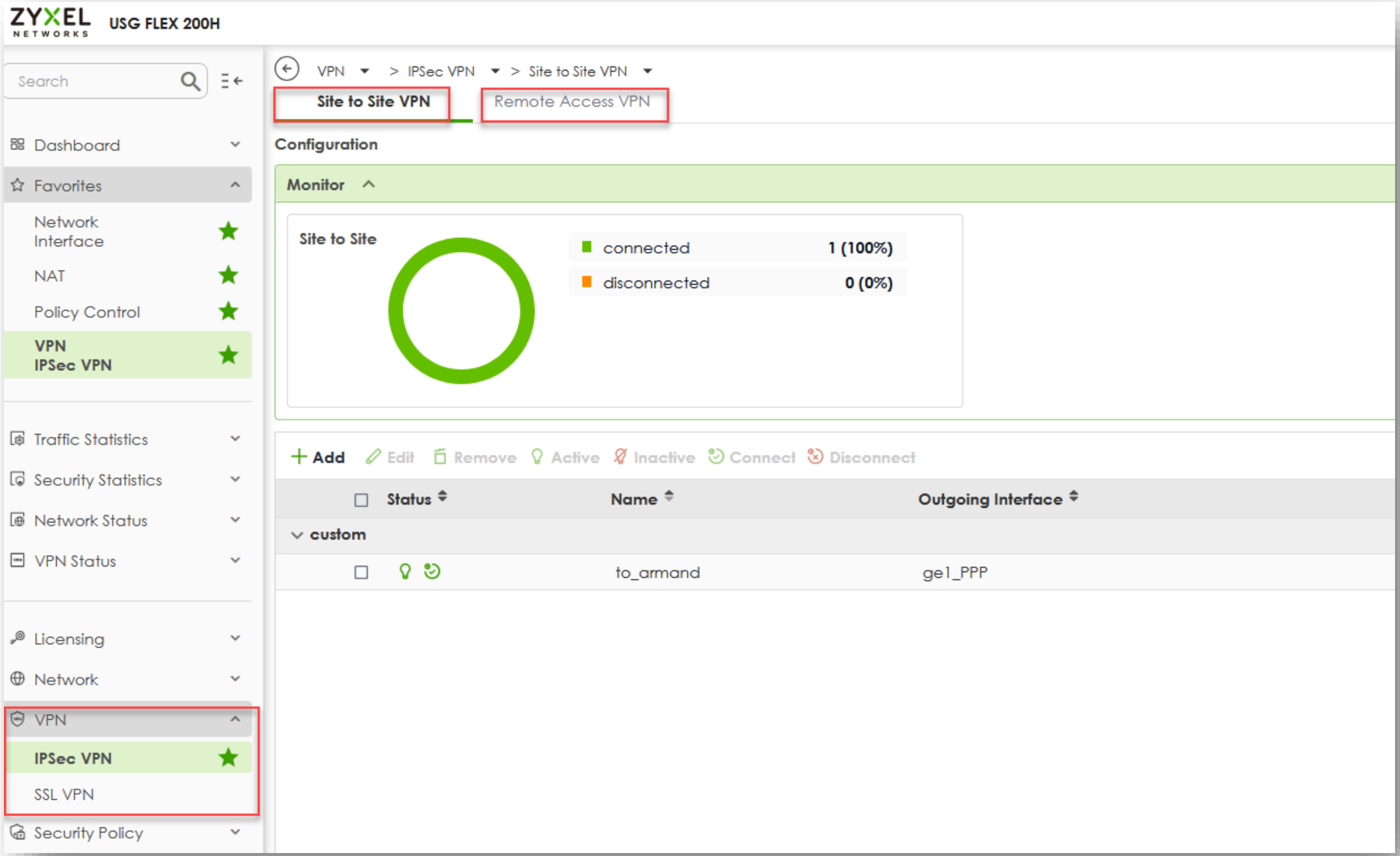
Microsoft	https://threatfeed.blob.core.windows.net/threatfeed/iplist/webattackip.txt
Ipsum	https://raw.githubusercontent.com/stamparm/ipsum/master/levels/4.txt

Nützliche KB-Artikel für DDoS Attacken
Die Empfehlungen von Zyxel zur sanften Abschwächung von DDoS-Angriffen auf Firewall-Geräte (https://support.zyxel.eu)
How to mitigate DDoS Attacks (https://community.zyxel.com/en/discussion/25382/how-to-mitigate-ddos-attacks)

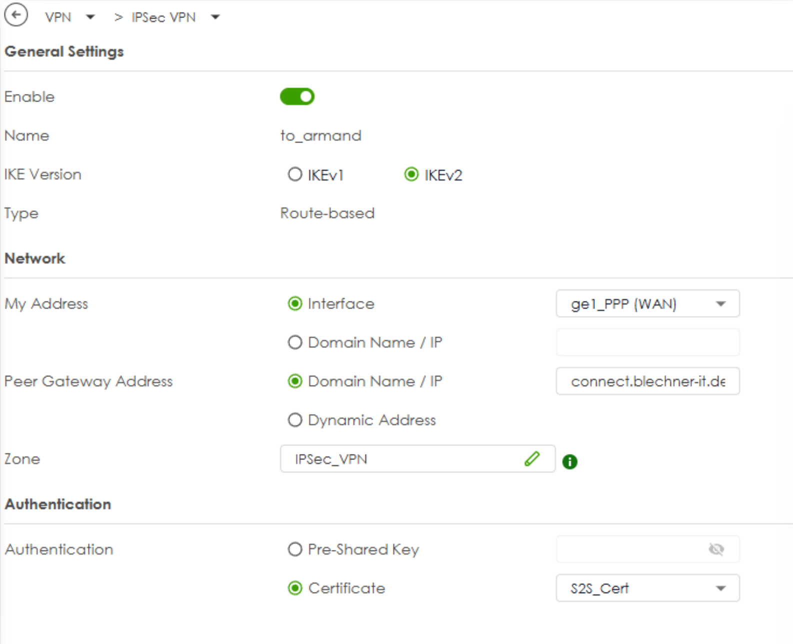
Praktische Aufgabe

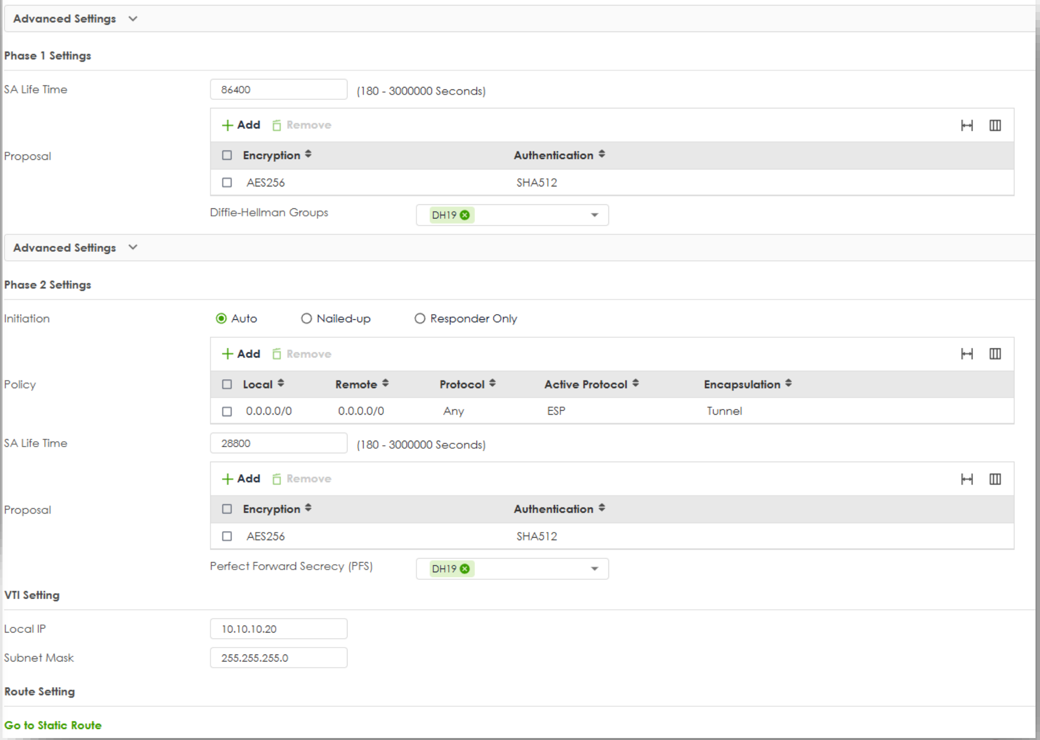
- Security Services auf der Firewall erkunden

5. VPN - Site To Site / Remote Access / SSL

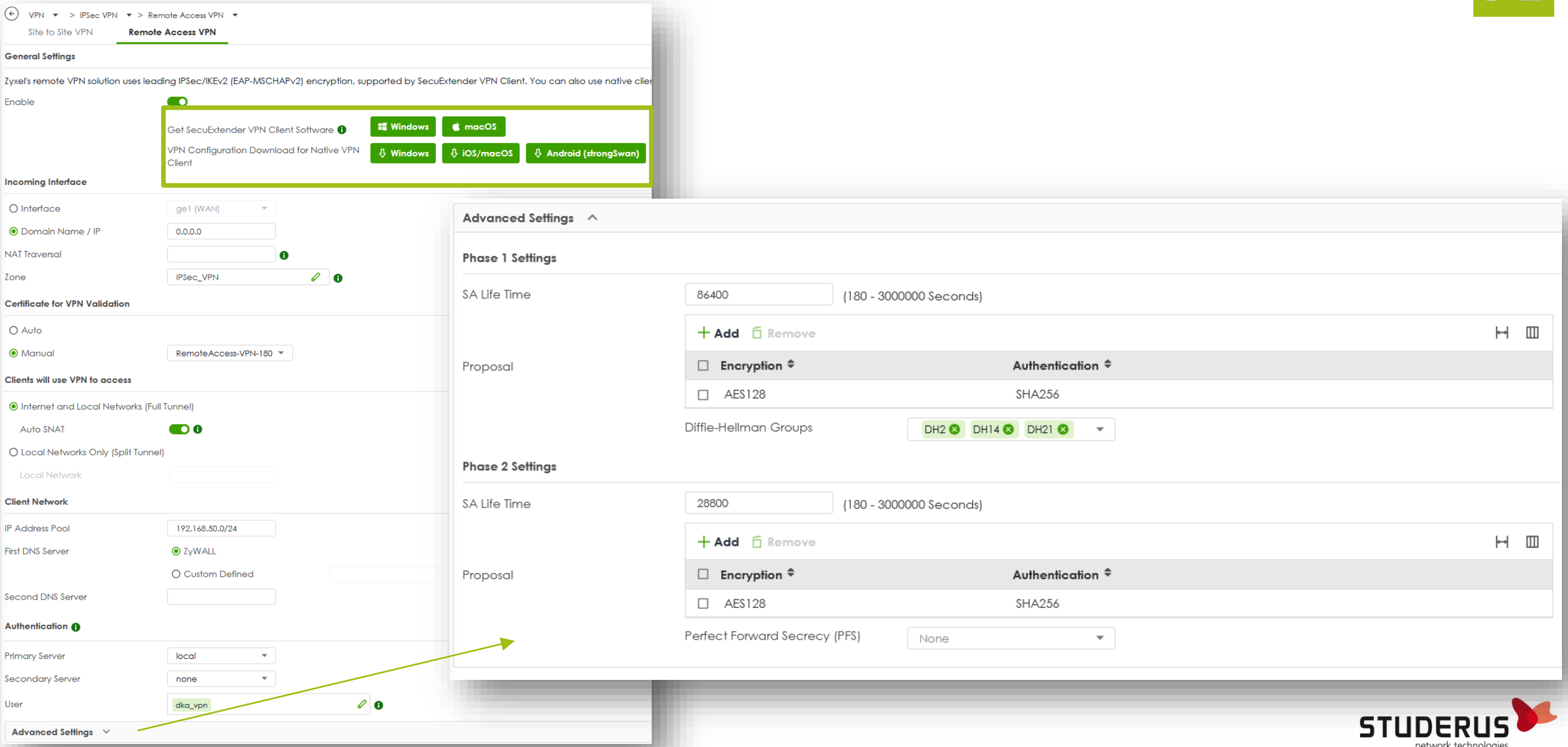


VPN - Site To Site



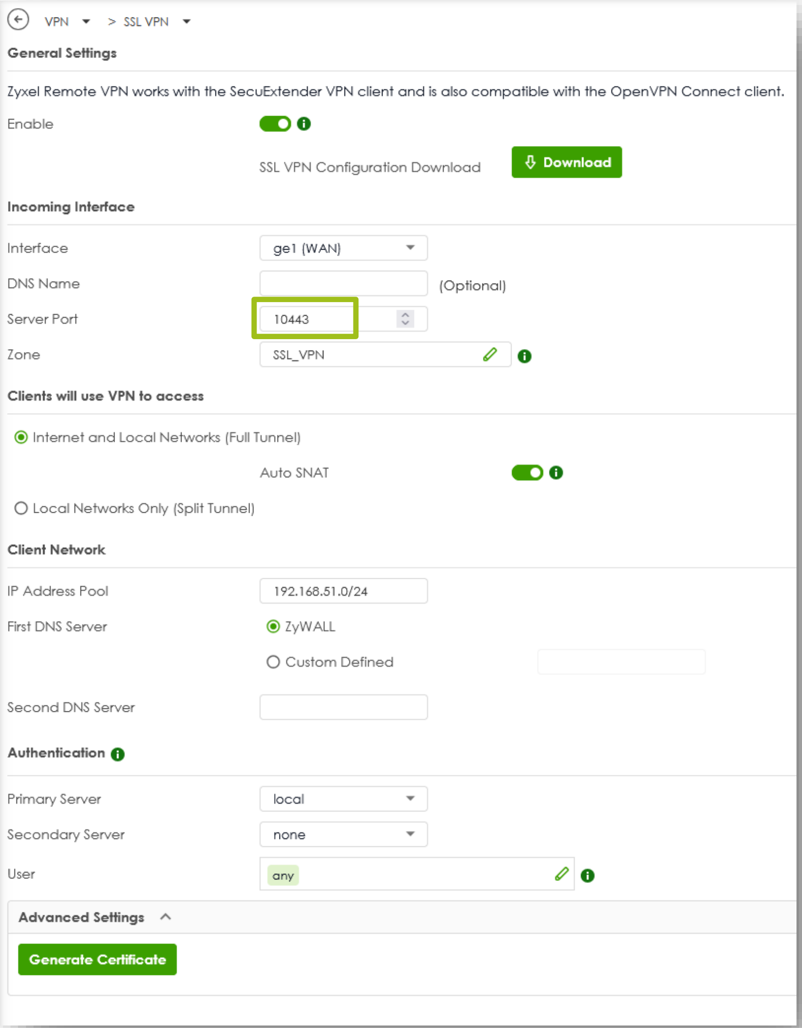


VPN – Remote Access VPN



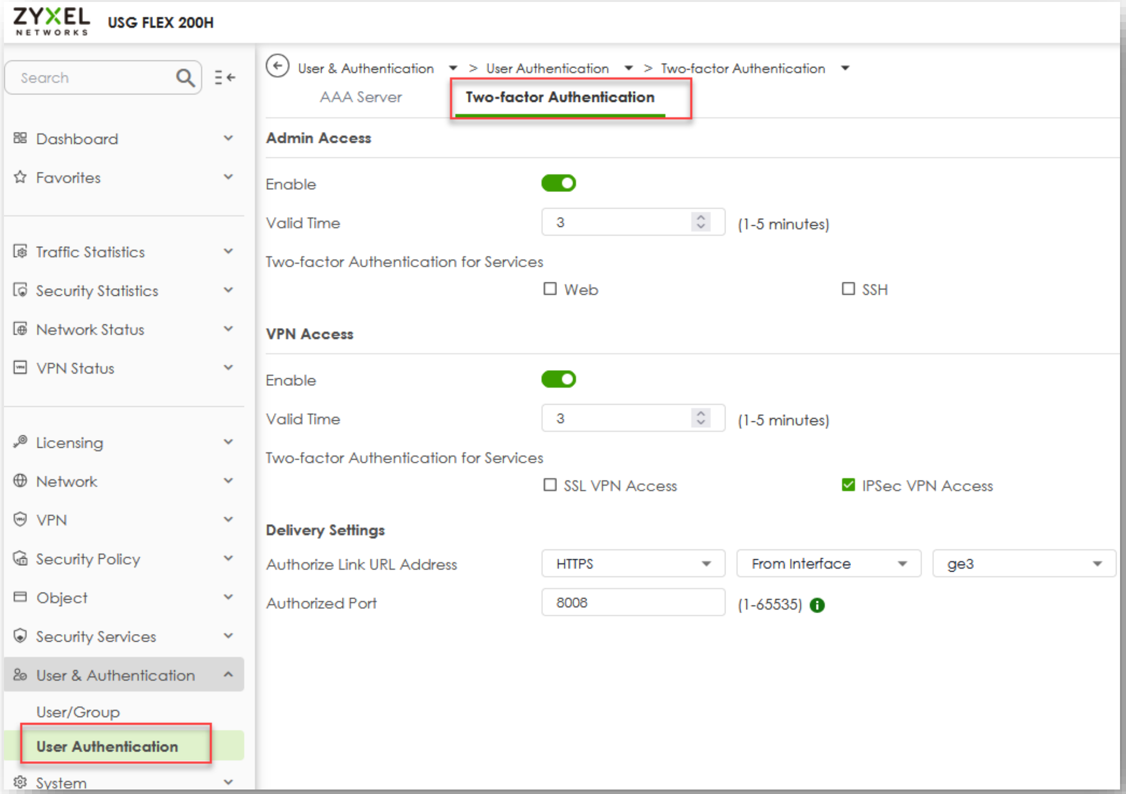
STUDERUS network technologies

VPN – SSL VPN

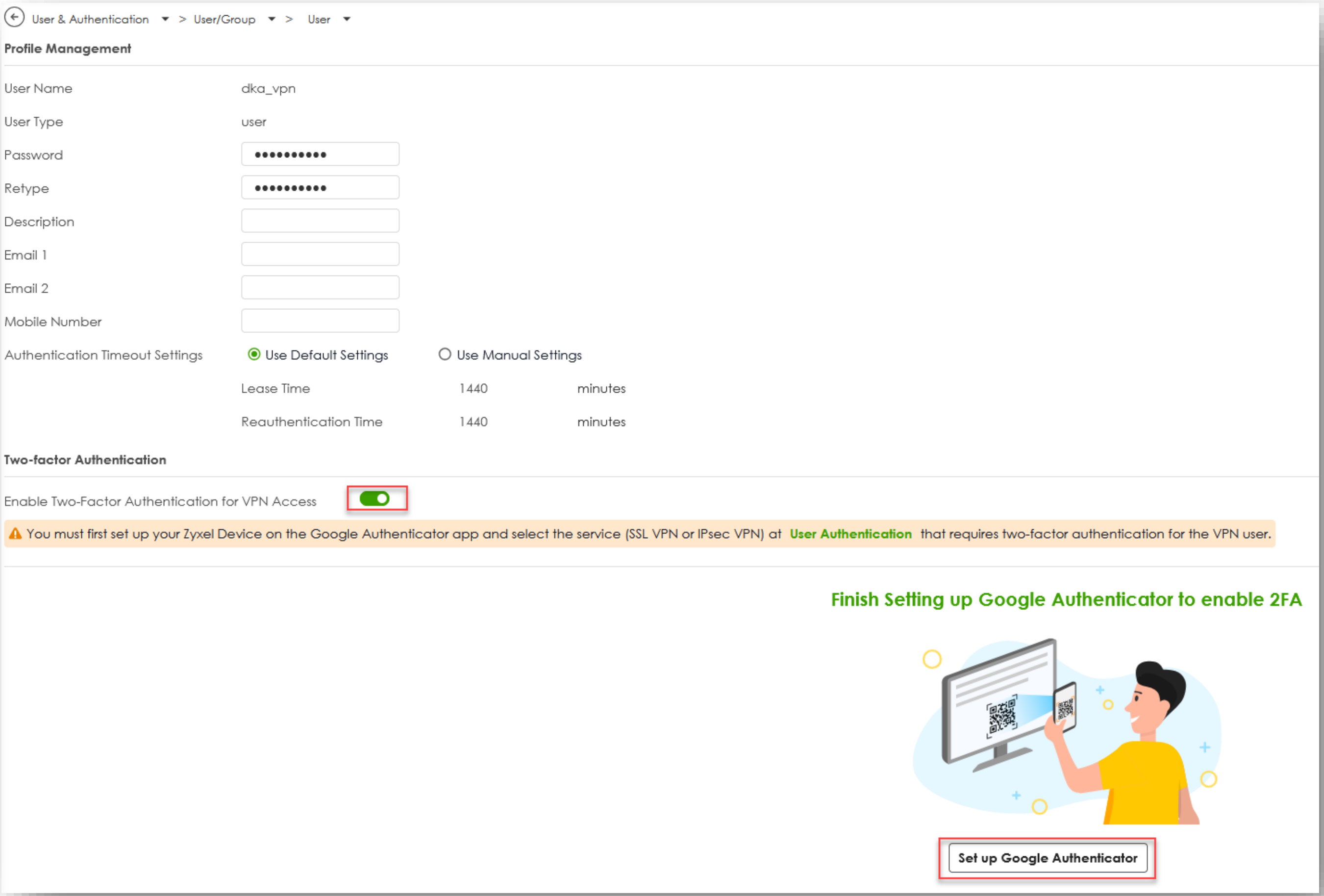


VPN > SSL VPN
General Settings
Zyxel Remote VPN works with the SecuExtender VPN client and is also compatible with the OpenVPN Connect client.
Enable
SSL VPN Configuration Download
Download
Incoming Interface
Interface
ge1 (WAN)
DNS Name
(Optional)
Server Port
10443
Zone
SSL_VPN
Clients will use VPN to access
Internet and Local Networks (Full Tunnel)
Auto SNAT
Local Networks Only (Split Tunnel)
Client Network
IP Address Pool
192.168.51.0/24
First DNS Server
ZyWALL
Custom Defined
Second DNS Server
Authentication
Primary Server
local
Secondary Server
none
User
any
Advanced Settings
Generate Certificate

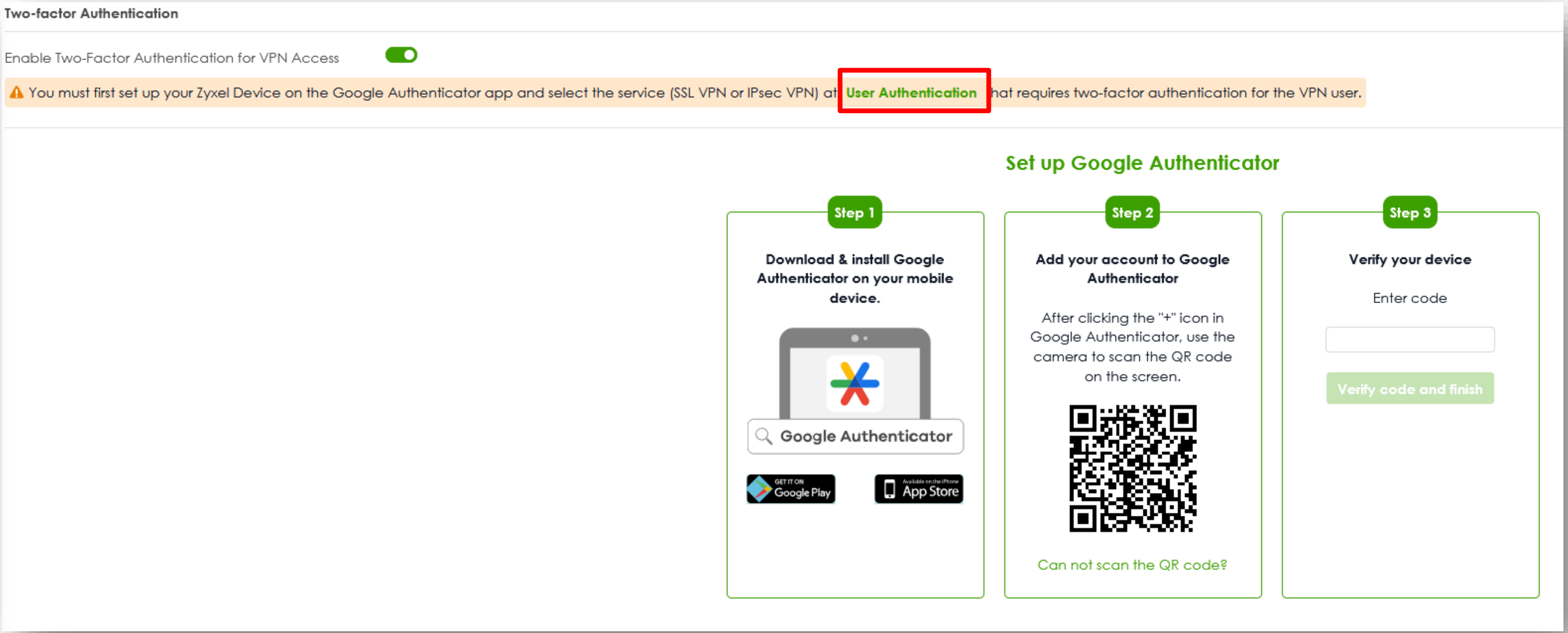
2FA – User Authentication



2FA


User & Authentication > User/Group > User
Profile Management
User Name dka_vpn
User Type user
Password
Retype
Description
Email 1
Email 2
Mobile Number
Authentication Timeout Settings
Use Default Settings
Use Manual Settings
Lease Time 1440 minutes
Reauthentication Time 1440 minutes
Two-factor Authentication
Enable Two-Factor Authentication for VPN Access
You must first set up your Zyxel Device on the Google Authenticator app and select the service (SSL VPN or IPsec VPN) at User Authentication that requires two-factor authentication for the VPN user.
Finish Setting up Google Authenticator to enable 2FA
Set up Google Authenticator

2FA – Aktivierung beim User



Praktische Aufgabe

- Site to Site VPN erstellen
- Remote Access VPN erstellen
- Benutzer erstellen
- 2FA für Admin Access
    - Admin User erstellen und 2FA aktivieren

7. WLAN-Controller

H Series uOS Release Plan

	Oct'24/uOS1.30/Nebula 18.20	Jan'25/uOS1.31/Nebula 18.30	April'25/uOS1.32/Nebula 19.00	July'25/uOS1.35/Nebula 19.10
On-prem	• New USG FLEX 50H(P) • FQDN Object • BWM (Support ppp, bridge and VTI interfaces) • Source IP spoofing prevention • Web Console • Entry Defense Pack • Schedule Reboot	• Email Alerts • SIP ALG • Device HA • Packet Flow Explore	• Tailscale-like VPN (Wireguard) • Secure WiFi (AP Controller) • Captive portal • 802.1x Authentication • Layer 2 Isolation • BWM for per user/per source-IP • IGMP • Routing Trace • **DoH/DoT** • **LAG** • **700H upgrade license**	• IPv6 dual stack • Speed Test on GUI • SNMP OID MIBs enhancements • **CDR**
NCC Portal	**Multi-Site Management** • Topology • Device Status (CPU/memory/session) • Event Log • Security Profile Synchronizations • Support Nebula pro pack transfer • Priority Support	**Nebula Configurations phase I** • Dashboard • **Auto VPN** • Port, Interface, Object • NAT, Routing • Firewall • Security Policy • Security Service (site-wide) • Summary Reports • Application/Client Usage	**Nebula Configurations phase II** • LAG • Non-Nebula VPN • Remote VPN (IPSec/SSL) • Authentication (Cloud Auth) • **Device HA Status & Topology** • License migration from FLEX/ATP • **700H upgrade license**	• **CDR** • **DoH/DoT** • Firewall schedule Reboot • Smart virtual server (auto-generate security policy)

STUDERUS network technologies

Praktische Aufgabe

- Nebula einloggen und WEB GUI zeigen
- WLAN-Einrichtung zeigen

Login für Teilnehmer:
Link: nebula.zyxel.com
User: student01@studerus.ch
PW: NebulaKurse2024!

8. CLI

- Welche Tools benötigen wir?

Nebula Anbindung neu initialisieren

```
usgflex200h> cmd service-inspect all official
OK.
usgflex200h> edit running
usgflex200h running config# nebula enabled false
usgflex200h running config# commit
Configuration committed.
usgflex200h running config# nebula enabled true
usgflex200h running config# commit
Configuration committed.
usgflex200h running config#
```

USG FLEX H als NTP-Server verwenden:

```
usgflex500h> edit running
usgflex500h running config# vrf main
usgflex500h running vrf main# ntp enabled true
usgflex500h running vrf main# commit
Configuration committed.
usgflex500h running vrf main# copy running
startup
Overwrite startup configuration? [y/N] y
```

8. CLI

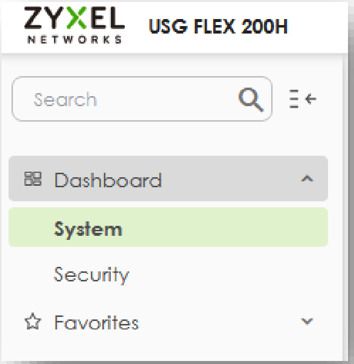
Auslesen von 2FA Informationen

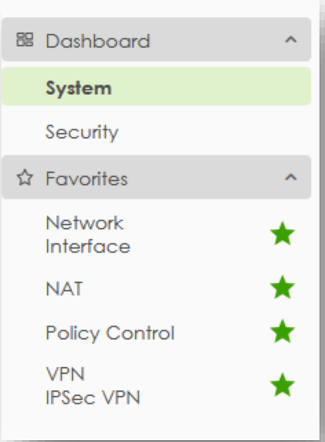
```
usgflex200h> cmd two-factor-auth google-auth user admin
two-factor-auth-google-auth
    ok
        verified false
        qrcode-url
otpauth://totp/admin?secret=4QF5GD6MRMMQHLSBVD6JS6F5IU&issuer=usgflex200h
        backup-code 7*******1
        backup-code 8*******8
        backup-code 9*******7
        backup-code 3*******1
        backup-code 5*******2
        ..
    ..
usgflex200h>
```

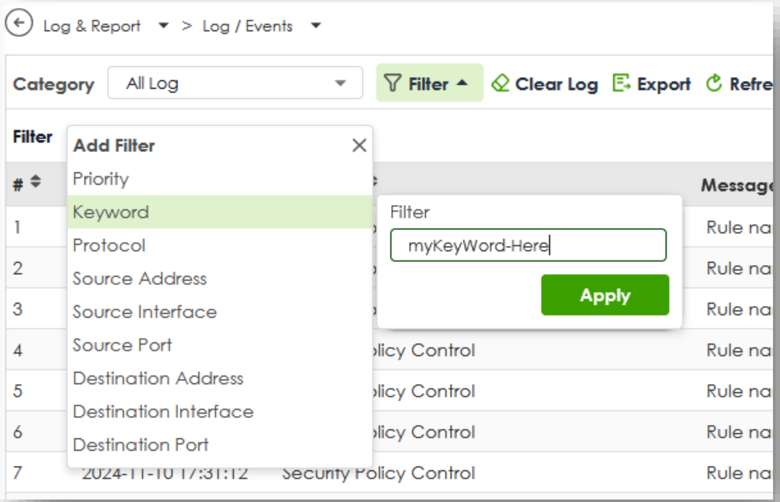
Anzeige der aktiven Routen

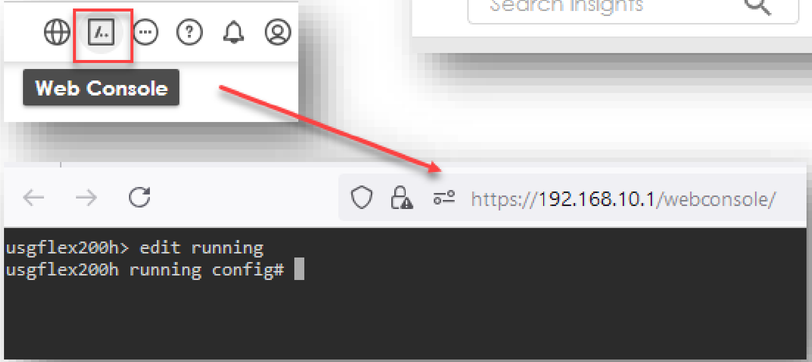
```
usgflex200h> show ipv4-routes
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, A - Babel, F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

K>* 0.0.0.0/0 [0/0] via 146.228.17.101, ge1_PPP, 00:00:05
C>* 10.10.10.0/24 is directly connected, vti_custom_341, 3d08h12m
C>* 146.228.17.101/32 is directly connected, ge1_PPP, 3d08h12m
C>* 172.16.10.0/24 is directly connected, Produktiv, 3d08h12m
C>* 172.16.50.0/24 is directly connected, Management, 3d08h12m
C>* 172.16.60.0/24 is directly connected, DataStore, 3d08h12m
C>* 172.16.70.0/24 is directly connected, Server-LAN, 3d08h12m
C>* 172.16.80.0/24 is directly connected, Client-LAN, 3d08h12m
C>* 172.16.100.0/24 is directly connected, VMs_Subnet, 3d08h12m
C>* 192.168.10.0/24 is directly connected, ge3, 3d08h12m
C>* 192.168.51.0/24 is directly connected, tun0, 3d08h12m
K>* 192.168.100.0/24 [0/0] is directly connected, vti_custom_341,
3d08h08m
C>* 192.168.169.0/24 is directly connected, ge4, 3d08h12m
usgflex200h>
```

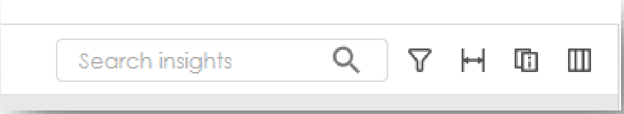
9. Coole Features

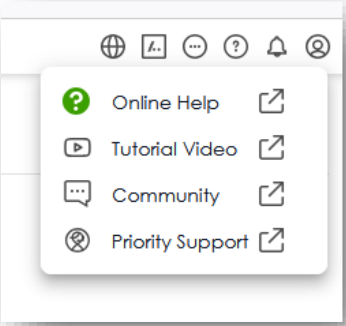












Fragen

TE
FO

2024