SparkView Integration

mit

Securepoint UTM V12.1.1

oder aktueller

Diese Anleitung beschreibt die Beispielkonfiguration für eine Securepoint UTM im Zusammenspiel mit SparkView.

Ziel ist es, dass sich der Benutzer, bevor er die SparkView Anwendung von außerhalb des Firmennetzes erreichen kann, an der Securepoint UTM authentifiziert und er nach erfolgreicher Authentifizierung weitergeleitet wird.

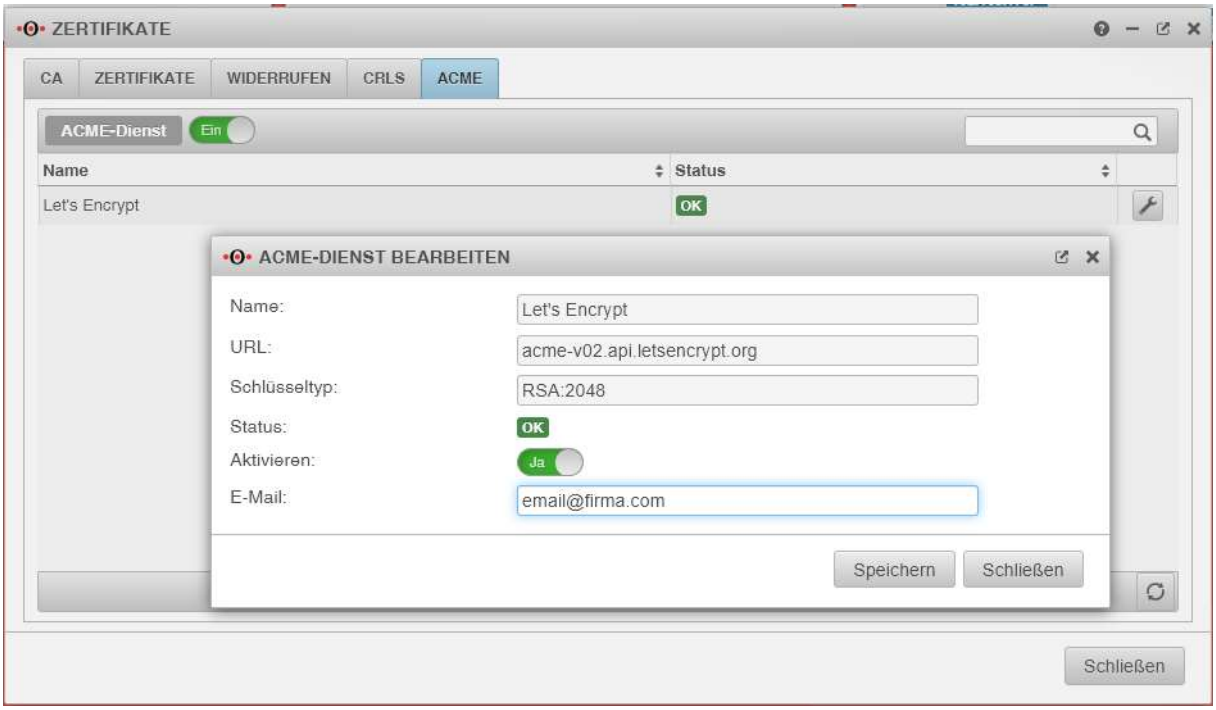
Die Bezeichnung „Securepoint UTM“ ist Eigentum der Firma Securepoint GmbH

Zertifikat einrichten

Aktivieren „Let’s Encrypt Zertifikat“

Authentifizierung > Zertifikate > ACME > EIN (Dienst aktivieren) und die Ansicht aktualisieren

Auf das Schlüsselzeichen vom Let’s Encrpyt gehen und folgendes Ausfüllen (Aktivieren und E-Mail) Danach die Nutzungsbedingungen akzeptieren und die Ansicht aktualisieren.

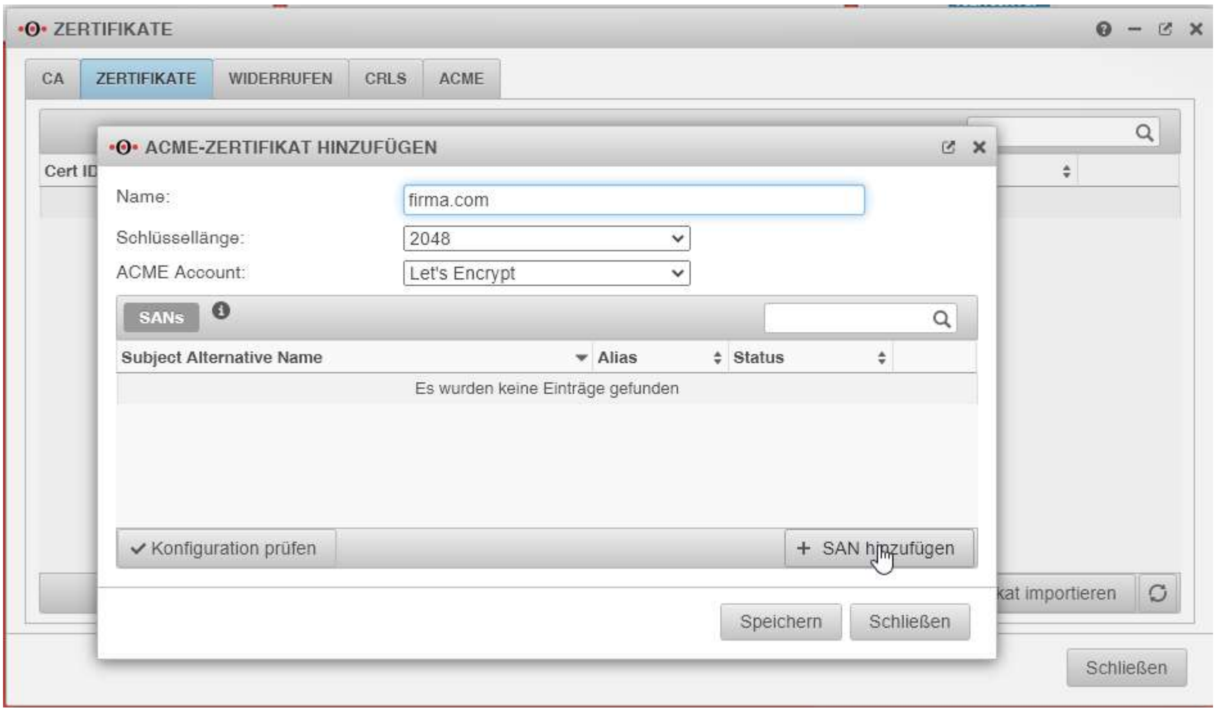


Im Browser das spDYN öffnen und im Menü Token den „ACME CHALLENGE TOKEN“ auswählen. https://spdyn.de

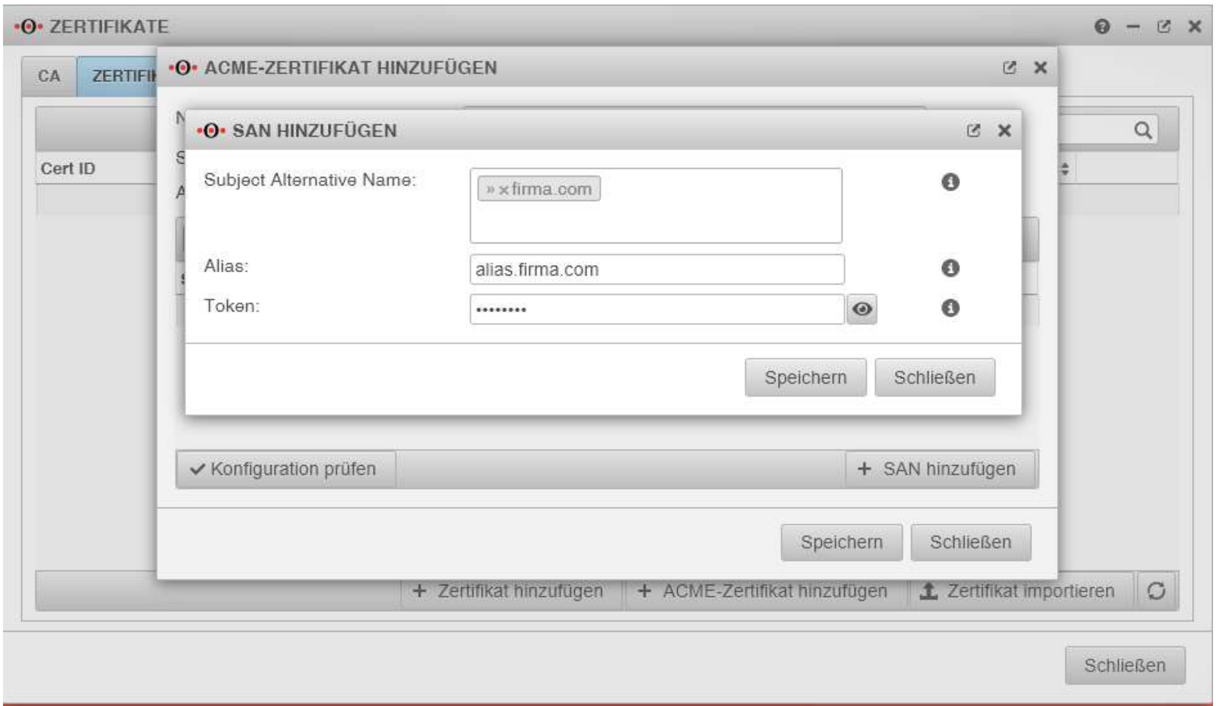
Host erstellen oder auswählen. Der Token sollte notiert werden, da es nicht mehr aufrufbar ist!

Dann unter Authentifizierung> Zertifikate > Zertifikate > + ACME-Zertifikat hinzufügen

Da müssen wir den Namen für das Zertifikat vergeben. (Best practice – Domainname) und auf SAN hinzufügen klicken

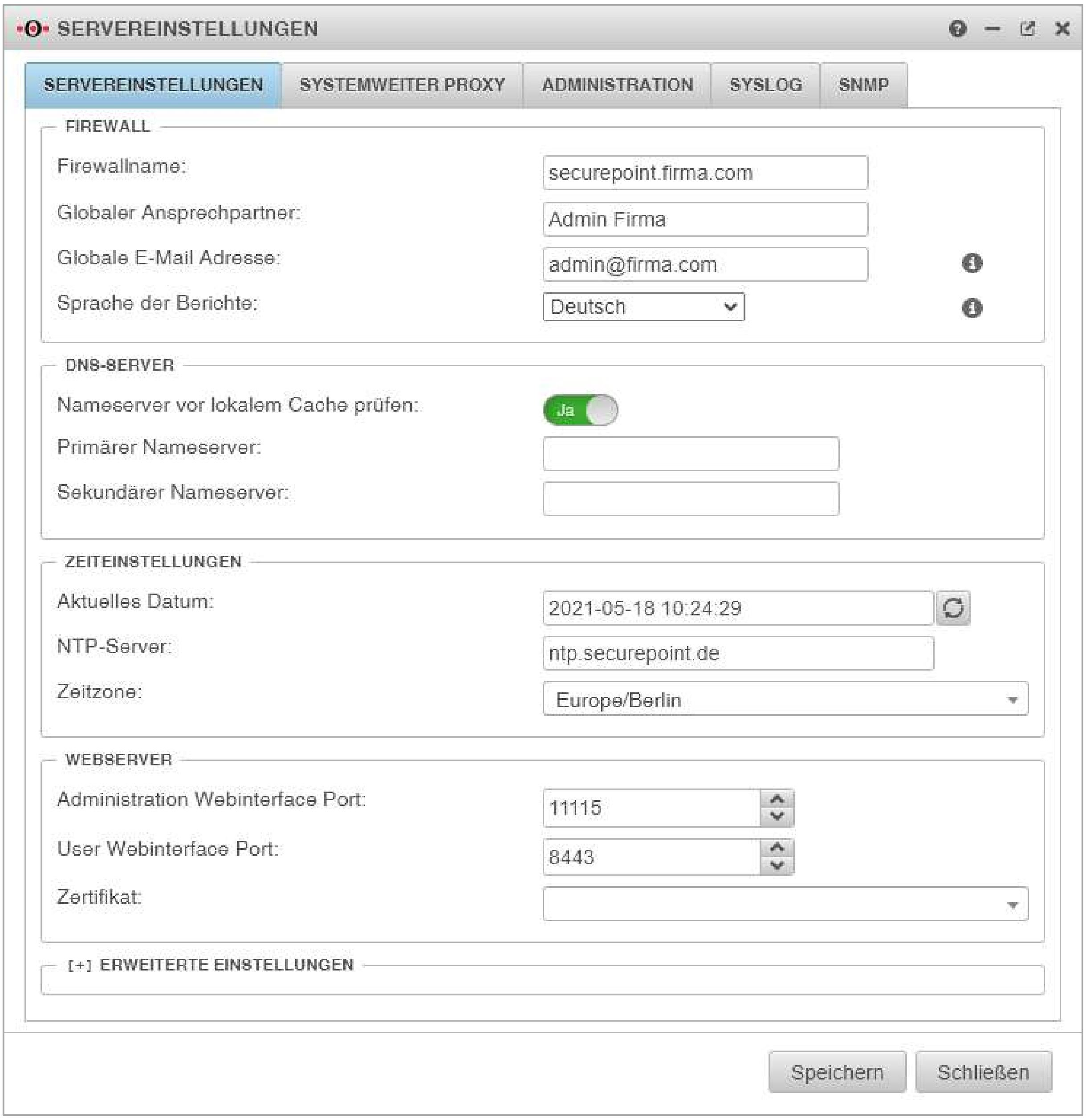


Als SAN müssen wir die URL angeben. (als Alias fügen wir den neu erstellen SPDYN host hinzu) und das Token kopieren wir von der SPDYN Seite in das freie Feld.



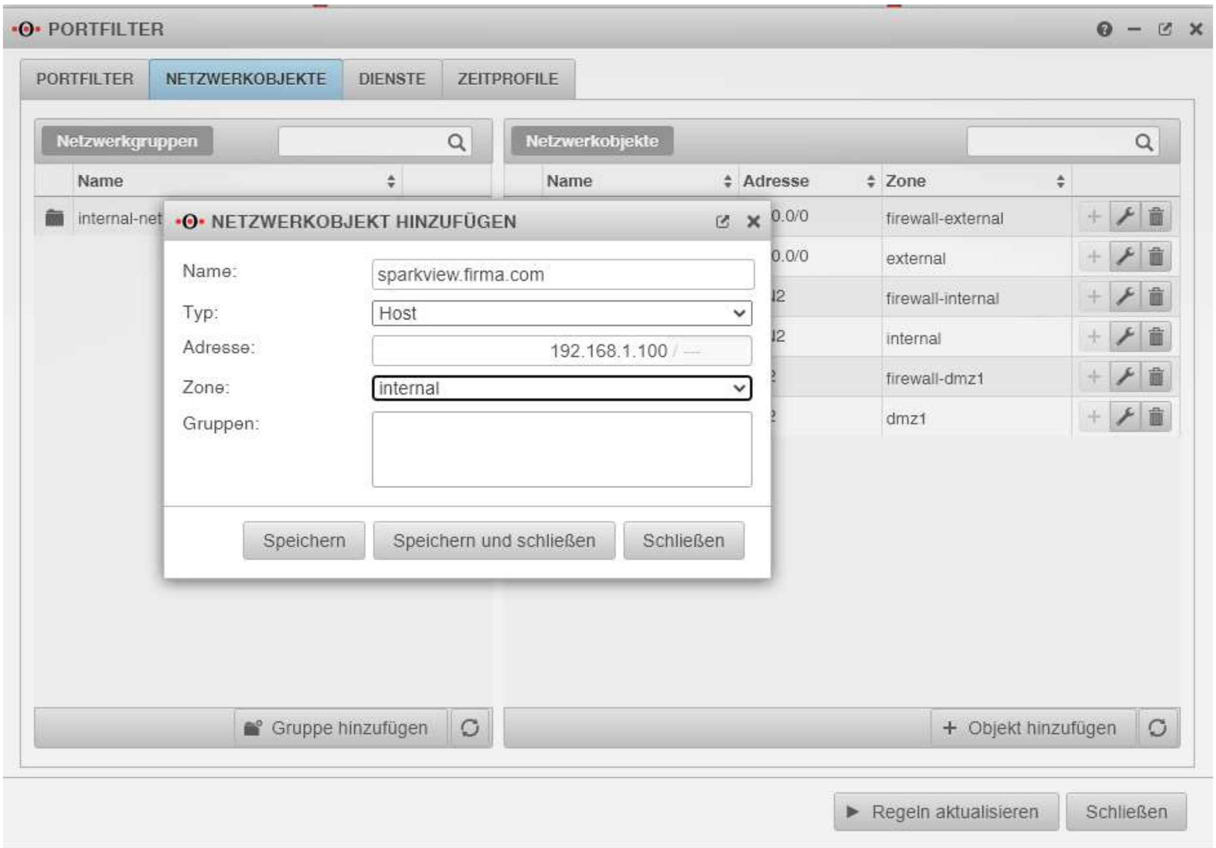
Reverse Proxy

Unter Netzwerk > Servereinstellungen wird der User Webinterface Port auf 443 geändert.

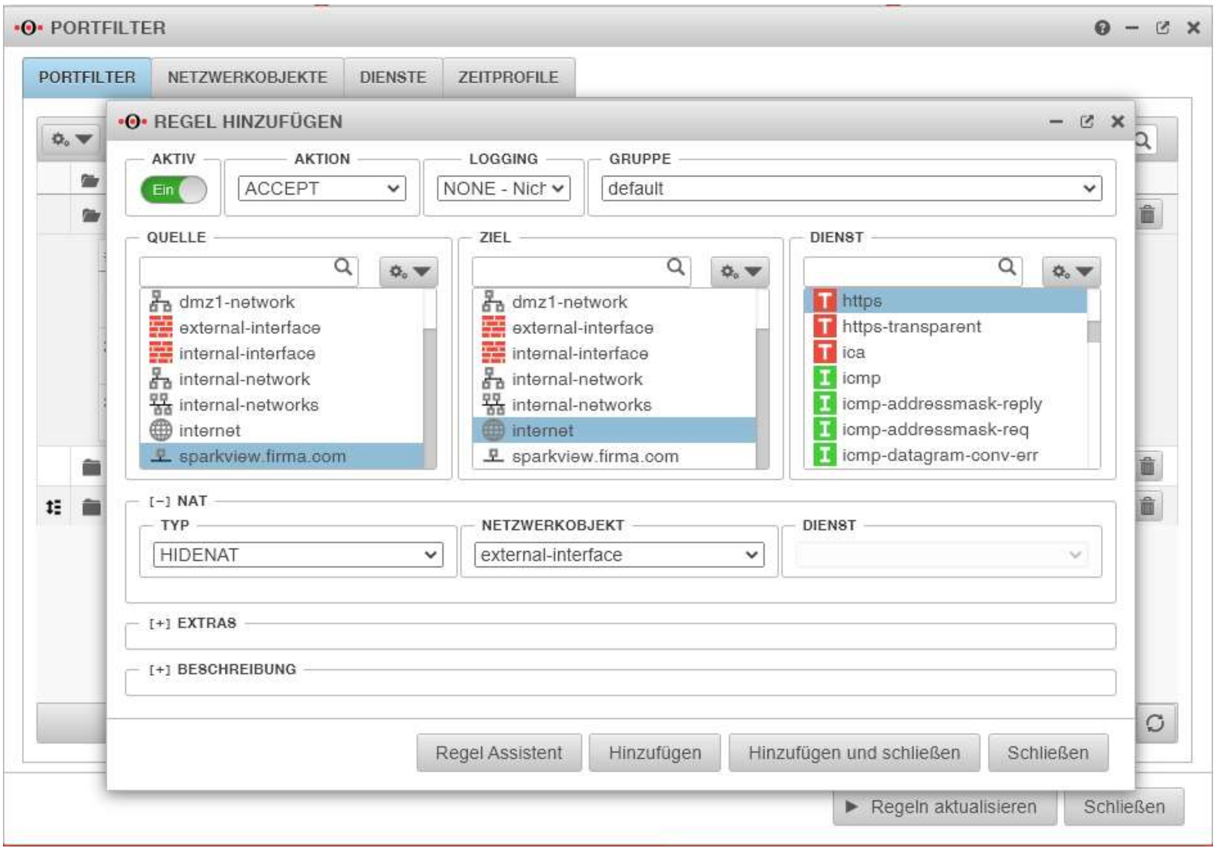


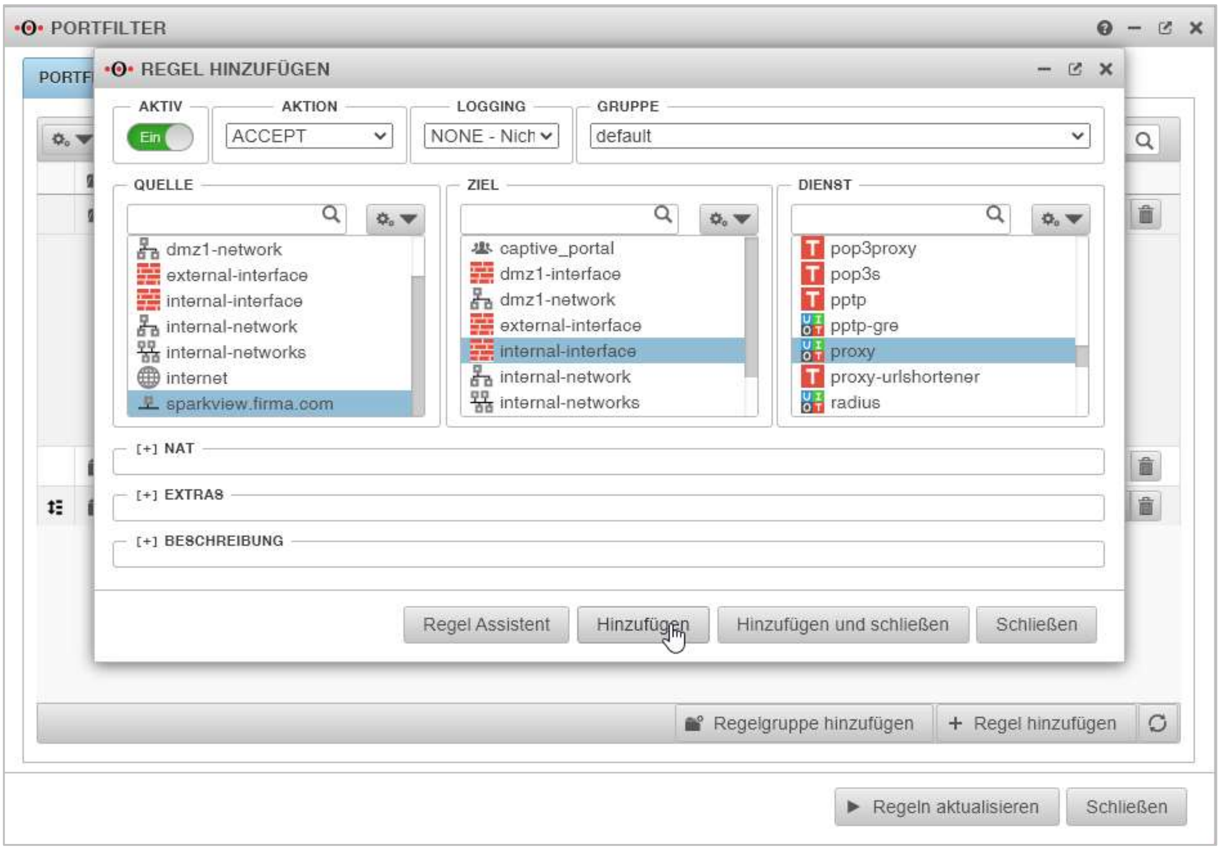
Der User Webinterface Port kann bis auf Port 443, dieser wird seitens der Securepoint besetzt, frei gewählt werden.

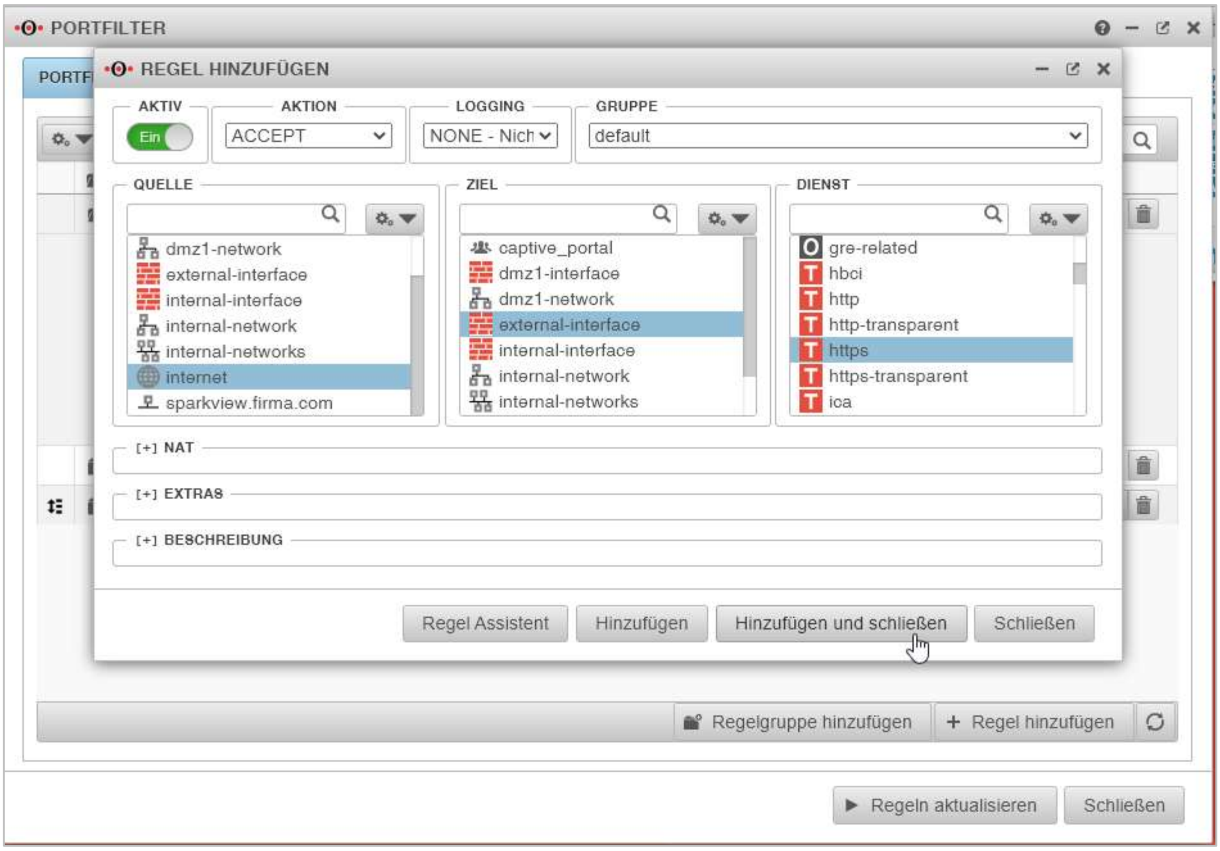
Im Menü Firewall > Portfilter, dann im Reiter Netzwerkobjekte unten rechts auf „+ Objekt hinzufügen“ klicken und die nötigen Daten eingeben. Dann „Speichern und schließen“.

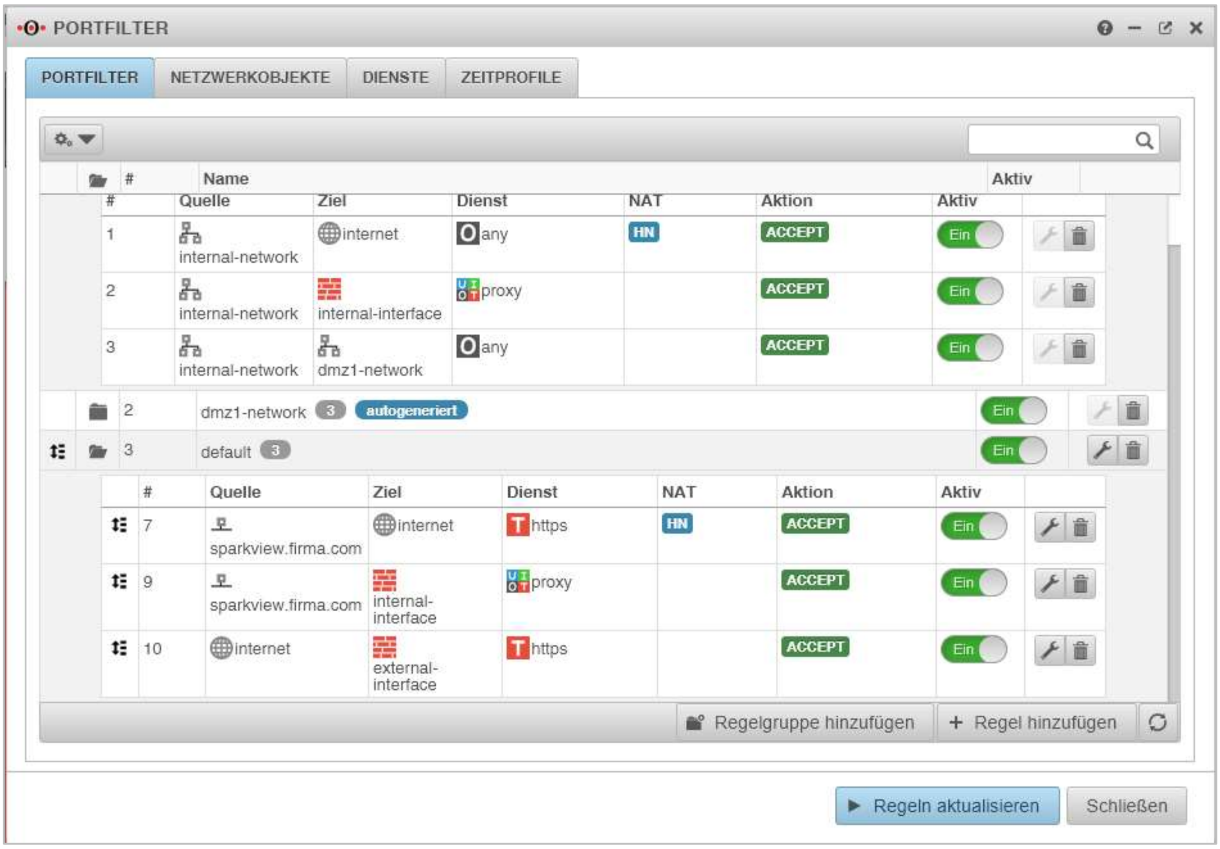


Im Reiter Portfilter auf „+ Regel hinzufügen“ klicken und folgende drei Regeln erstellen. Die ersten beiden Regeln mit „Hinzufügen“ und die dritte mit „Hinzufügen und schließen“ bestätigen.




PORTFILTER
REGEL HINZUFÜGEN
AKTIV
Ein
AKTION
ACCEPT
LOGGING
NONE - Nich
GRUPPE
default
QUELLE
dmz1-network
external-interface
internal-interface
internal-network
internal-networks
internet
sparkview.firma.com
ZIEL
captive_portal
dmz1-interface
dmz1-network
external-interface
internal-interface
internal-network
internal-networks
DIENST
pop3proxy
pop3s
pptp
pptp-gre
proxy
proxy-urlshortener
radius
[+] NAT
[+] EXTRAS
[+] BESCHREIBUNG
Regel Assistent
Hinzufügen
Hinzufügen und schließen
Schließen
Regelgruppe hinzufügen
+ Regel hinzufügen
Regeln aktualisieren
Schließen

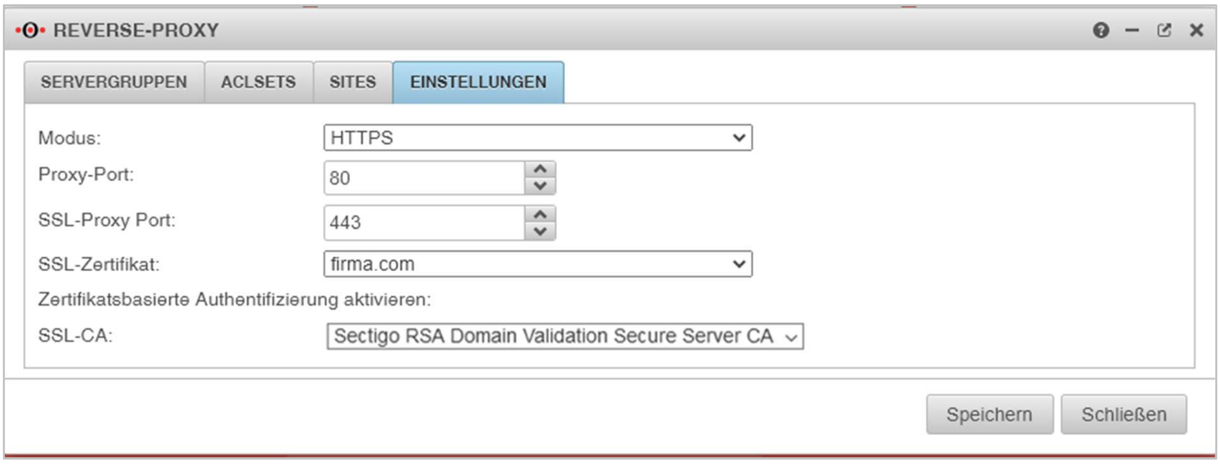

PORTFILTER
REGEL HINZUFÜGEN
AKTIV
Ein
AKTION
ACCEPT
LOGGING
NONE - Nich
GRUPPE
default
QUELLE
dmz1-network
external-interface
internal-interface
internal-network
internal-networks
internet
sparkview.firma.com
ZIEL
captive_portal
dmz1-interface
dmz1-network
external-interface
internal-interface
internal-network
internal-networks
DIENST
gre-related
hbci
http
http-transparent
https
https-transparent
ica
[+] NAT
[+] EXTRAS
[+] BESCHREIBUNG
Regel Assistent
Hinzufügen
Hinzufügen und schließen
Schließen
Regelgruppe hinzufügen
+ Regel hinzufügen
Regeln aktualisieren
Schließen



Im Menü unter Anwendungen > Reverse-Proxy im Reiter Servergruppen unten links auf „+ Reverse-Proxy-Assistent“ klicken und bei Schritt 1 folgendes einstellen


REVERSE-PROXY
SERVERGRUPPEN
ACLSETS
SITES
EINSTELLUNGEN
Name
Netzwerkobjekt
REVERSE-PROXY ASSISTENT
Schritt 1
Intern
Schritt 2
Extern
Schritt 3
Authentifizierung
Externer Domainname:
sparkview.firma.com
Modus:
HTTPS
SSL-Proxy Port:
443
SSL-Zertifikat:
firma.com
Zurück
Weiter
Abbrechen
Reverse-Proxy Assistent
Servergruppe hinzufügen
Speichern
Schließen


REVERSE-PROXY
SERVERGRUPPEN
ACLSETS
SITES
EINSTELLUNGEN
Name
Netzwerkobjekt
REVERSE-PROXY ASSISTENT
Schritt 1
Intern
Schritt 2
Extern
Schritt 3
Authentifizierung
Authentifizierung weiterleiten:
Zugangsdaten festlegen
Anmeldename:
Passwort:
Authentifizierung:
an
Zurück
Fertig
Abbrechen
Reverse-Proxy Assistent
Servergruppe hinzufügen
Speichern
Schließen


REVERSE-PROXY
SERVERGRUPPEN
ACLSETS
SITES
EINSTELLUNGEN
Modus:
HTTPS
Proxy-Port:
80
SSL-Proxy Port:
443
SSL-Zertifikat:
firma.com
Zertifikatsbasierte Authentifizierung aktivieren:
SSL-CA:
Sectigo RSA Domain Validation Secure Server CA
Speichern
Schließen