

Securepoint Security Systems

Version 2007nx Release 3



•• **SECUREPOINT**

Inhalt

1	Einstellung der Server Appliance vornehmen	4
1.1	Zertifikate anlegen.....	4
1.2	Zertifikate exportieren.....	6
1.3	Private Key aus der exportierten Datei löschen	8
1.4	Route hinzufügen	10
1.5	OpenVPN Konfigurationsdatei bearbeiten	11
1.6	Externe Netzgruppe hinzufügen	13
1.7	Regeln hinzufügen	14
1.8	Konfiguration speichern und Regelupdate durchführen	15
2	Einstellungen der Client Appliance vornehmen	16
2.1	Importieren der Zertifikate	16
2.2	OpenVPN Konfigurationsdatei ändern.....	17
2.3	Netzwerkobjekt anlegen	17
2.4	Regel anlegen	18
2.5	Speichern, Regelupdate und Dienst starten	19
3	Hinweis für den Betrieb im Multipath Routing	19

Site-to-Site Verbindung mit OpenVPN

Ein VPN verbindet einen oder mehrere Rechner oder Netzwerke miteinander, indem es ein anderes Netzwerk, z. B. das Internet, als Transportweg nutzt. Das kann z. B. der Rechner eines Mitarbeiters zu Hause oder einer Filiale sein, der mit dem Netzwerk der Zentrale über das Internet verbunden ist.

Für den Benutzer sieht das VPN wie eine normale Netzwerkverbindung zum Zielrechner aus. Den tatsächlichen Übertragungsweg sieht er nicht. Das VPN stellt dem Benutzer eine virtuelle IP-Verbindung zur Verfügung, die durch eine tatsächliche getunnelt wird. Die über diese Verbindung übertragenen Datenpakete werden am Client verschlüsselt und vom Securepoint Server wieder entschlüsselt und umgekehrt.

Es öffnet sich der Dialog Zertifikate.

- Wählen Sie die Option **Stammzertifikat**.
- Füllen Sie die Felder mit den entsprechenden Daten.
- Bestätigen Sie ihre Eingabe mit **OK**.
- Erstellen Sie anschließend **OpenVPN Zertifikate**.
- Wählen Sie hierfür die Option **OpenVPN Serverzertifikat** und danach die Option **OpenVPN Clientzertifikat**.

Nach Betätigen des **OK** Buttons bleibt der Dialog mit den eingetragenen Daten bestehen, um die Erstellung weiterer Zertifikate zu vereinfachen. Wenn Sie alle Zertifikate erstellt haben, schließen Sie den Dialog mit der Schaltfläche **Abbrechen**.

Zertifikate

Zertifikat anlegen für firewall.foo.local

Benutzer / Serverzertifikat
 Stammzertifikat
 OpenVPN Serverzertifikat
 OpenVPN Clientzertifikat

Schlüssellänge: 1024
Frühestes Gültigkeitsdatum: 01.01.2000 00:00:00
Spätestes Gültigkeitsdatum: 28.11.2018 23:59:59
Bezeichnung: openVPN_CA
Land: GERMANY
Bundesland: Niedersachsen
Ort: Lueneburg
Organisation: Securepoint
Organisationseinheit: Support
Email: support@securepoint.de
CA:

OK Abbrechen

Abb. 2 Ein Stammzertifikat (CA) erstellen

Zertifikate

Zertifikat anlegen für firewall.foo.local

Benutzer / Serverzertifikat
 Stammzertifikat
 OpenVPN Serverzertifikat
 OpenVPN Clientzertifikat

Schlüssellänge: 1024
Frühestes Gültigkeitsdatum: 01.01.2000 00:00:00
Spätestes Gültigkeitsdatum: 29.11.2011 23:59:59
Bezeichnung: ovServer_site1
Land: GERMANY
Bundesland: Niedersachsen
Ort: Lueneburg
Organisation: Securepoint
Organisationseinheit: Support
Email: support@securepoint.de
CA: openVPN_CA

Alternativer X509v3 Name

IP
 Host-Name
 Email

OK Abbrechen

Abb. 3 Ein OpenVPN Serverzertifikat erstellen

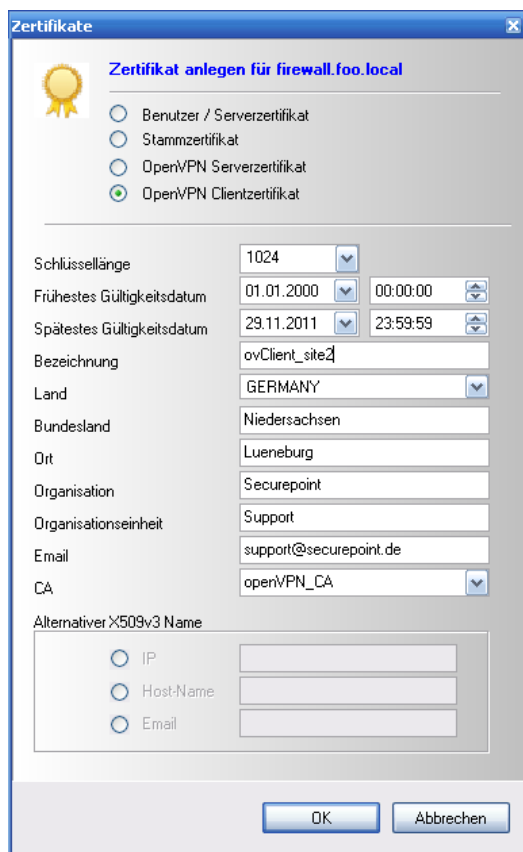


Abb. 4 Ein OpenVPN Clientzertifikat erstellen

1.2 Zertifikate exportieren

- Exportieren Sie das **Stammzertifikat (CA)** und das **ovClient_site2** Zertifikat und geben Sie es an die entfernte Appliance weiter.
- Gewöhnlich wird das Standard Format (PEM-Datei) gewählt. Wenn Sie das pkcs#12 Format wählen, brauchen Sie nur das **ovClient_site2** Zertifikat zu exportieren, weil in diesem Format das Stammzertifikat mit enthalten ist. Außerdem ist der Private Key des Stammzertifikats in diesem Format verschlüsselt und muss nicht vor der Weitergabe entfernt werden (siehe 1.3).
- Wählen Sie im linken Teilfenster der Registerkarte den Eintrag **Certs** aus. Markieren Sie in der rechten Liste das Clientzertifikat **ovClient_site2** und klicken Sie auf das Icon **Export**. Wählen Sie im erscheinenden Dialog das gewünschte Format. Wenn Sie das Format pkcs#12 wählen, dann müssen Sie noch ein Kennwort angeben.
- Im nächsten Dialog müssen Sie noch einen Speicherort angeben.

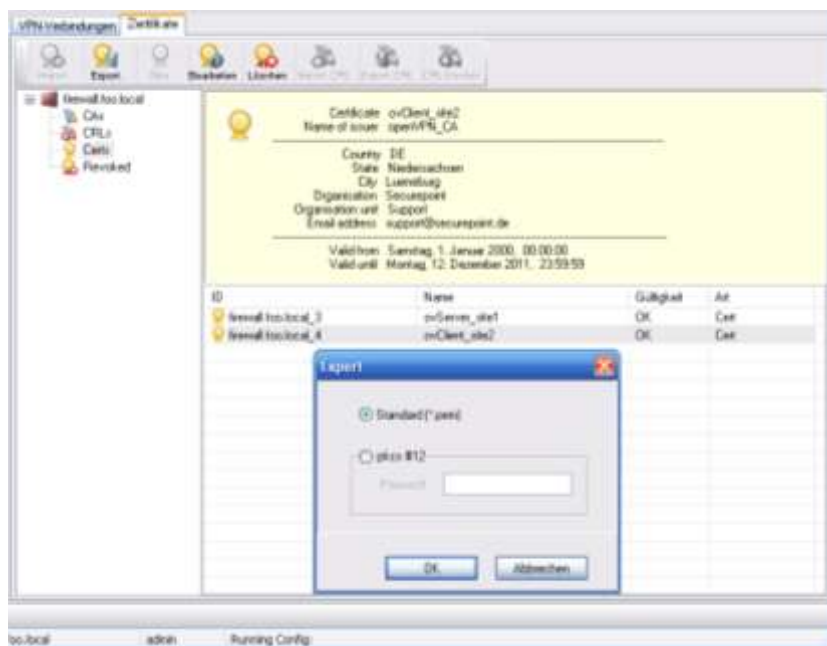


Abb. 5 Clientzertifikat exportieren

- Wählen Sie im linken Teilfenster der Registerkarte den Eintrag **CAs** aus. Markieren Sie in der rechten Liste das Stammzertifikat **openVPN_CA** und klicken Sie auf das Icon **Export**. Wenn Sie das Clientzertifikat im pkcs#12 Format exportiert haben, entfällt dieser Schritt.

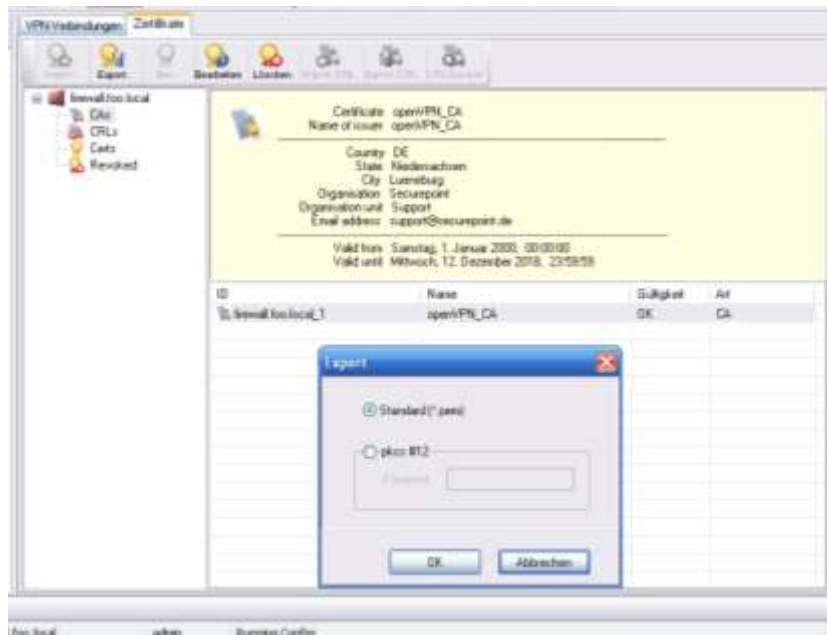


Abb. 6 Stammzertifikat exportieren

Beachten Sie: Wenn Sie das Stammzertifikat im Standardformat exportieren, wird auch der Private Key des Stammzertifikats mit in der PEM-Datei gespeichert. Den Private Key der CA sollten Sie nie an Clients weitergeben, um Missbrauch vorzubeugen. Löschen Sie daher den Private Key aus der zu exportierenden Datei.

1.3 Private Key aus der exportierten Datei löschen

Wenn Sie den Private Key nicht aus der PEM-Datei löschen und so an den Client weitergeben, kann der Client neue Zertifikate erstellen und diese mit der CA signieren. Sie könnten die so erstellten Zertifikate nicht von originalen von Ihnen erstellten Zertifikaten unterscheiden.

- Suchen Sie die exportierte Datei heraus und klicken Sie mit der rechten Maustaste auf die Datei. Es öffnet sich ein Kontextmenü.



Abb. 7 exportiertes Zertifikat öffnen

- Klicken Sie auf **Öffnen**.
- Geben Sie im nächsten Dialog an **Programm aus der Liste wählen** und bestätigen mit **OK**.
- Wählen Sie aus der Liste einen Editor z.B. den Microsoft Editor.
- Entfernen Sie ggf. den Haken bei **Dateityp immer mit dem ausgewählten Programm öffnen**.
- Bestätigen Sie mit **OK**.

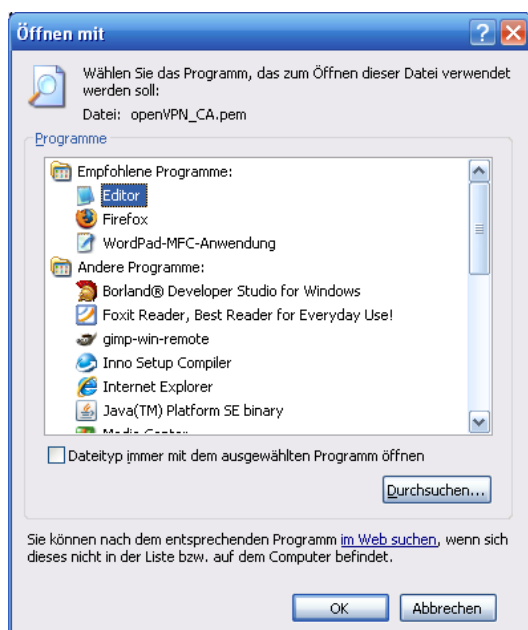


Abb. 8 Programm zum Öffnen wählen

1.4 Route hinzufügen

- Gehen Sie über die Menüleiste auf den Punkt **Netzwerk** und wählen Sie den Eintrag **Routing** oder klicken Sie auf das Icon **Netzwerk** und wechseln Sie auf die Registerkarte **Routing**.
- Klicken Sie auf das Icon **Neu**.
- Legen Sie die Route wie gezeigt an.
Das **Ziel-Netzwerk** ist das Netzwerk hinter dem Client.
- Klicken Sie anschließend auf das Icon **Aktualisieren**.

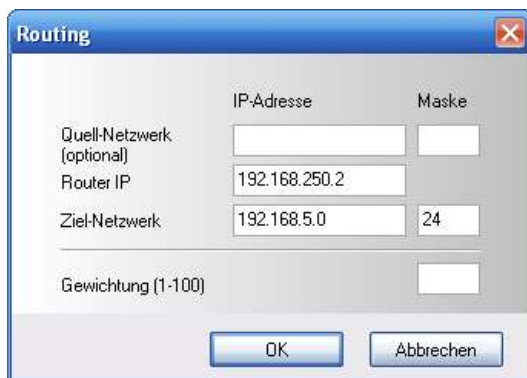


Abb. 11 Route zum Client Netzwerk

1.5 OpenVPN Konfigurationsdatei bearbeiten

Melden Sie sich per SSH auf der Konsole des Servers an. Benutzen Sie einen geeigneten SSH Client (z. B. PuTTY).

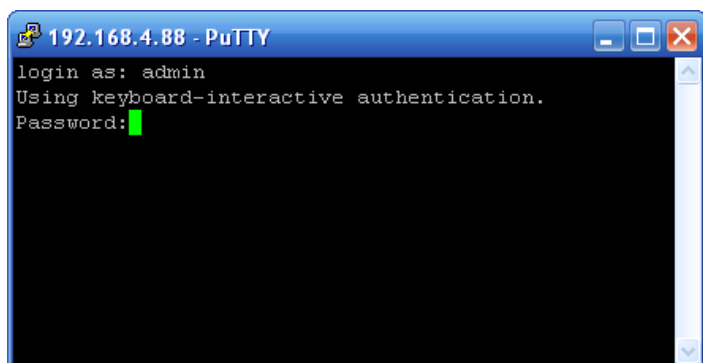


Abb. 12 per SSH am Server anmelden

- Geben Sie dann folgende Befehle ein. Betätigen Sie nach jeder Zeile die **Eingabe** Taste.

```
change extc_value openvpn CLIENT_MODE 0
change extc_value openvpn CERT_CN ovServer_site1
change extc_value openvpn PASSWORD_AUTH 0
```

- Jetzt erstellen Sie ein Template für die verbindungspezifische OpenVPN-Config

```
add extc_template openvpn /tmp/clients/ovClient_site2
ifconfig-push IP_des_Clients_im_Tunnel IP_des_Servers_im_Tunnel
iroute IP_Netz_hinter_dem_Client 255.255.255.0
**
```

Die Angaben **IP_des_Clients_im_Tunnel** wäre in diesem Beispiel 192.168.250.2 und die **IP_des_Servers_im_Tunnel** 192.168.250.1.

Auch in der allgemeinen OpenVPN Konfigurationsdatei müssen Änderungen vorgenommen werden.

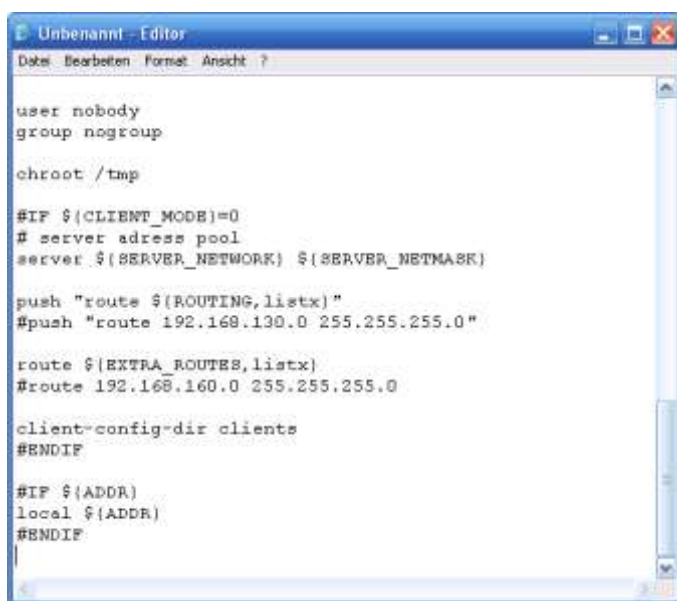
- Geben sie Folgenden Befehl ein:

```
show extc_template /etc/openvpn.conf
```

In der Ausgabe erscheint die Konfigurationsdatei. Kopieren Sie diese und fügen Sie die Daten in einen Editor ein. Gehen Sie hierfür wie folgt vor.

- Markieren Sie alle Zeilen der Konfigurationsdatei bis auf die zwei Sterne (*) der letzten Zeile und kopieren Sie diese in die Zwischenablage. Wenn Sie PuTTY verwenden, dann sind die Zeilen durch das Markieren schon in die Zwischenablage kopiert. Gehen Sie sonst nach den jeweiligen Einstellungen Ihres Programms vor.

- Fügen Sie den Inhalt der Zwischenablage in einen Editor (z.B. MS Editor) ein.



```
Unbenannt - Editor
Datei Bearbeiten Format Ansicht ?

user nobody
group nogroup

chroot /tmp

#IF ${CLIENT_MODE}=0
# server address pool
server ${SERVER_NETWORK} ${SERVER_NETMASK}

push "route ${ROUTING,listx}"
#push "route 192.168.130.0 255.255.255.0"

route ${EXTRA_ROUTES,listx}
#route 192.168.160.0 255.255.255.0

client-config-dir clients
#ENDIF

#IF ${ADDR}
local ${ADDR}
#ENDIF
```

Abb. 13 eingefügtes Template im Editor

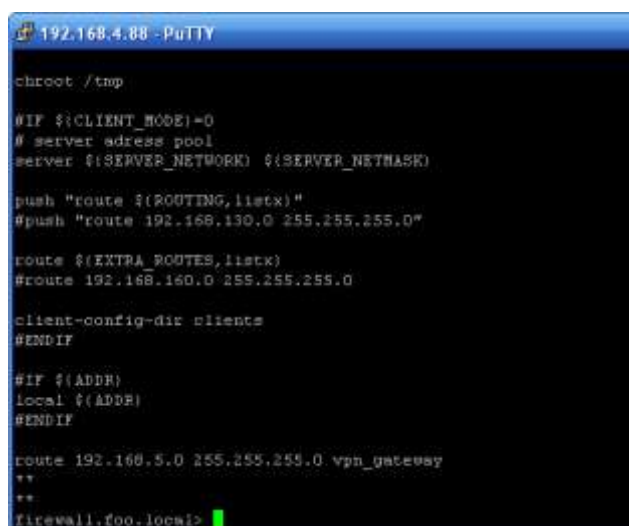
- Fügen Sie am Ende der Datei folgende Zeile hinzu:

```
route IP_Netz_hinter_dem_Client 255.255.255.0 vpn_gateway
```

- Kopieren Sie nun das geänderte Template in die Zwischenablage.
- Geben Sie folgenden Befehl im SSH Client ein:

```
change extc_template /etc/openvpn.conf
```

- Fügen Sie den Inhalt der Zwischenablage in den SSH-Client ein.
- Kennzeichnen Sie das Ende der Datei, indem Sie eine Zeile mit zwei Sternen anfügen und drücken Sie anschließend die Eingabe Taste.



```
192.168.4.88 - PuTTY

chroot /tmp

#IF ${CLIENT_MODE}=0
# server address pool
server ${SERVER_NETWORK} ${SERVER_NETMASK}

push "route ${ROUTING,listx}"
#push "route 192.168.130.0 255.255.255.0"

route ${EXTRA_ROUTES,listx}
#route 192.168.160.0 255.255.255.0

client-config-dir clients
#ENDIF

#IF ${ADDR}
local ${ADDR}
#ENDIF

route 192.168.5.0 255.255.255.0 vpn_gateway
**
**
firewall.foo.local>
```

Abb. 14 Abschluss des Templates mit **

- Speichern Sie die Änderungen mit dem Befehl:

```
config save Name_der_Konfiguration
```

- Sie können hierfür natürlich auch den Security Manager benutzen.

1.6 Externe Netzgruppe hinzufügen

- Gehen Sie über die Menüleiste auf den Punkt **Firewall** und wählen Sie den Eintrag **Netzwerkobjekte** oder klicken Sie auf das Icon **Firewall** und wechseln Sie auf die Registerkarte **Netzwerkobjekte**.
- Klicken Sie auf den Pfeil neben dem Icon **Rechner** und wählen Sie aus dem Dropdown Menü den Eintrag **Netz**.
- Legen Sie ein Objekt für das Netzwerk hinter dem Client an. Die Zone hierfür ist **vpn-openvpn**.
- Klicken Sie anschließend auf **OK**.



Abb. 15 Objekt für Filialen Netz anlegen

1.7 Regeln hinzufügen

- Für den Zugriff müssen Sie noch folgende Regeln zufügen:

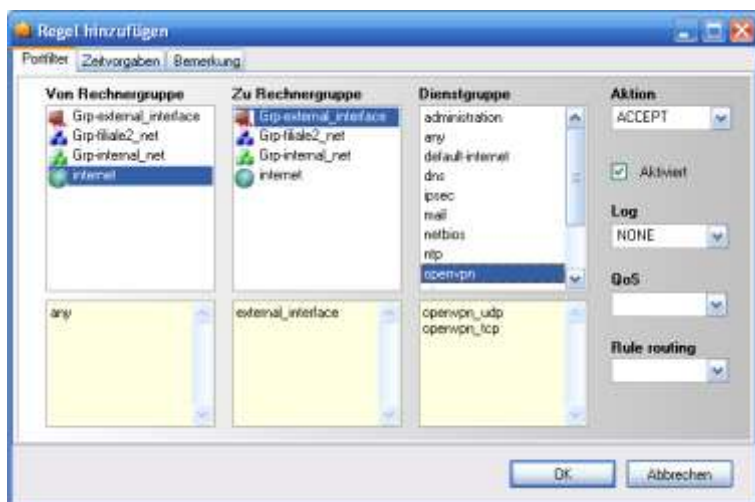


Abb. 16 Internet → Grp-external_interface → openvpn

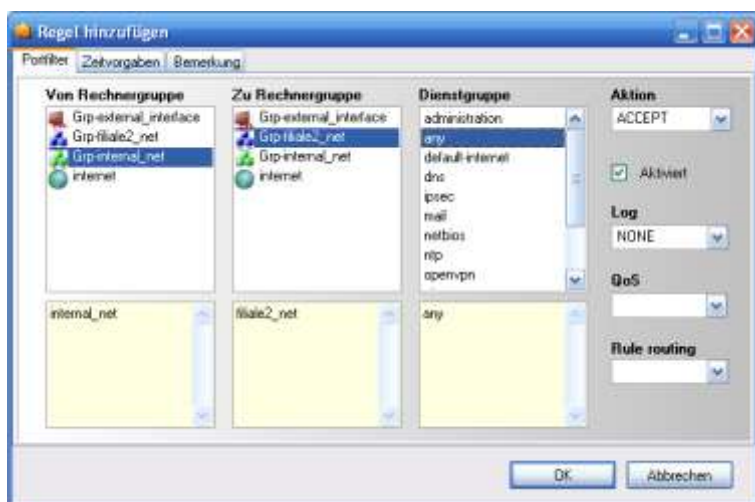


Abb. 17 Grp-internal_net → Grp-filiale2_net → any

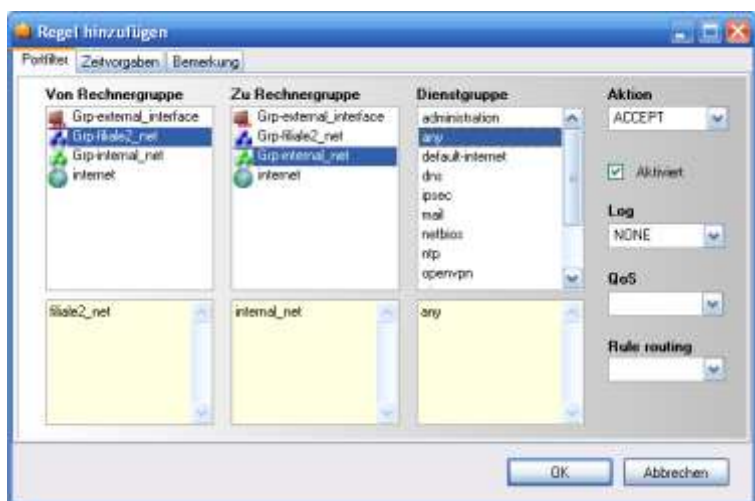


Abb. 18 Grp-filiale2_net → Grp-internal_net → any

1.8 Konfiguration speichern und Regelupdate durchführen

Speichern Sie anschließend Ihre Konfiguration und führen Sie ein Regelupdate durch, um die Änderungen zu aktivieren.



Abb. 19 Speichern und Regelupdate Buttons

- Gehen Sie über die Menüleiste auf den Punkt **Applikationen** und wählen Sie den Eintrag **Dienste Status** oder klicken Sie auf das Icon **Applikationen** und wechseln Sie auf die Registerkarte **Dienste Status**.
- Suchen Sie die Zeile **SERVICE_OPENVPN**. Wenn ein **X** im roten Kreis eingetragen ist, dann ist der Dienst nicht aktiviert.
- Um den Dienst zu aktivieren, klicken Sie doppelt auf das Icon oder drücken Sie die rechte Maustaste und wählen aus dem Kontextmenü **Dienst starten**.
- Klicken Sie anschließend auf **Einstellungen übernehmen**.



Dienstname	Status	Cluster
SERVICE_OPENSSH	✓	✗
SERVICE_SENDMAIL	✓	✗
SERVICE_DNS	✓	✗
SERVICE_POP3_PROXY	✓	✗
SERVICE_HTTP_PROXY	✓	✗
SERVICE_VOIP_PROXY	✗	✗
SERVICE_VNC_PROXY	✗	✗
SERVICE_DYNDNS	✗	✗
SERVICE_NTP	✓	✗
SERVICE_IDS	✓	✗
SERVICE_L2TP	✗	✗
SERVICE_PPTP	✗	✗
SERVICE_SPINA	✓	✗
SERVICE_WEBSERVER	✓	✗
SERVICE_DHCPD	✗	✗
SERVICE_IPSEC	✗	✗
SERVICE_OPENVPN	✓	✗

Abb. 20 Dienste Status überprüfen

2 Einstellungen der Client Appliance vornehmen

2.1 Importieren der Zertifikate

Importieren Sie das Stamm- und das Clientzertifikat.

- Gehen Sie über die Menüleiste auf den Punkt **VPN** und wählen Sie den Eintrag **Zertifikate** oder klicken Sie auf das Icon **VPN** und wechseln Sie auf die Registerkarte **Zertifikate**.
- Markieren Sie im linken Teilfenster der Registerkarte die Firewall und klicken Sie auf das Icon **Import**.
- Importieren Sie so nacheinander das Stammzertifikat und das Clientzertifikat. Wenn die Zertifikate im pkcs#12 Format vorliegen, dann müssen Sie nur ein Zertifikat importieren.

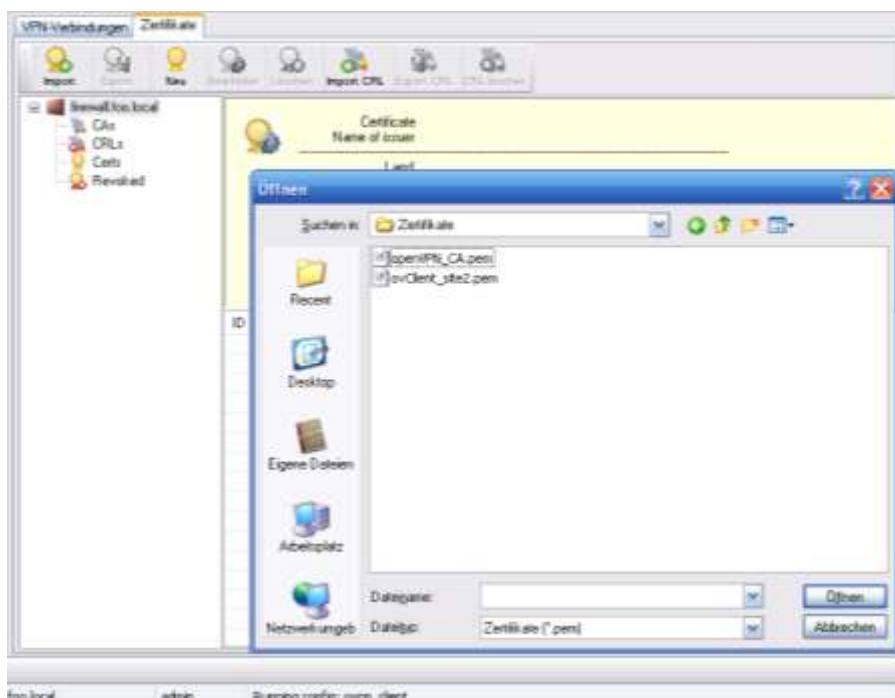


Abb. 21 Zertifikate importieren

2.2 OpenVPN Konfigurationsdatei ändern

Melden Sie sich per SSH auf der Konsole des Clients an. Benutzen Sie einen geeigneten SSH Client (z. B. PuTTY).

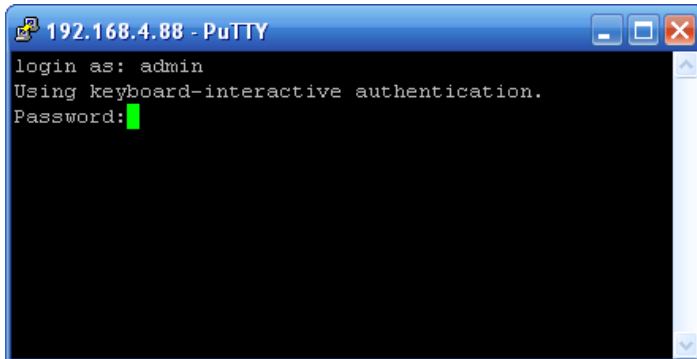


Abb. 22 per SSH am Client anmelden

- Geben Sie dann folgende Befehle ein. Betätigen Sie nach jeder Zeile die **Eingabe** Taste.

```
change extc_value openvpn CLIENT_MODE 1
change extc_value openvpn CERT_CN ovClient_site2
change extc_value openvpn openvpn REMOTE externe_IP_des_Servers
```

2.3 Netzwerkobjekt anlegen

- Gehen Sie über die Menüleiste auf den Punkt **Firewall** und wählen Sie den Eintrag **Netzwerkobjekte** oder klicken Sie auf das Icon **Firewall** und wechseln Sie auf die Registerkarte **Netzwerkobjekte**.
- Klicken Sie auf den Pfeil neben dem Icon **Rechner** und wählen Sie aus dem Dropdown Menü den Eintrag **Netz**.
- Legen Sie ein Objekt für das Netzwerk hinter dem Server an. Die Zone hierfür ist **vpn-openvpn**.
- Klicken Sie anschließend auf **OK**.



Abb. 23 Objekt für das entfernte Netz anlegen

2.4 Regel anlegen

- Für den Zugriff müssen Sie noch folgende Regeln zufügen:

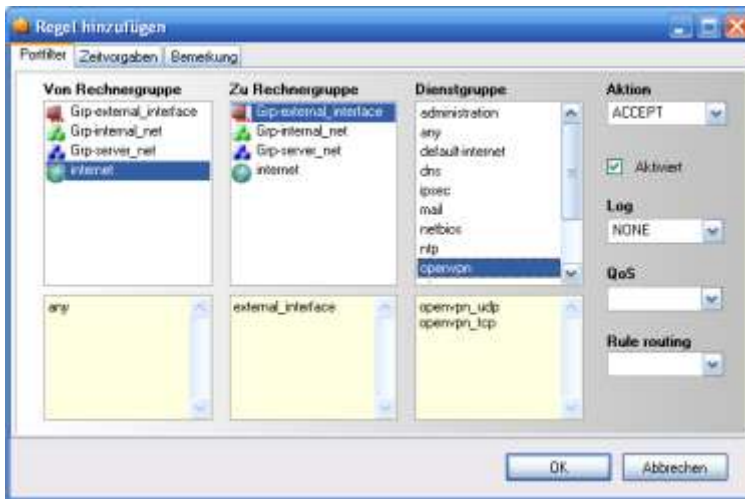


Abb. 24 internet → Grp-external_net → openvpn

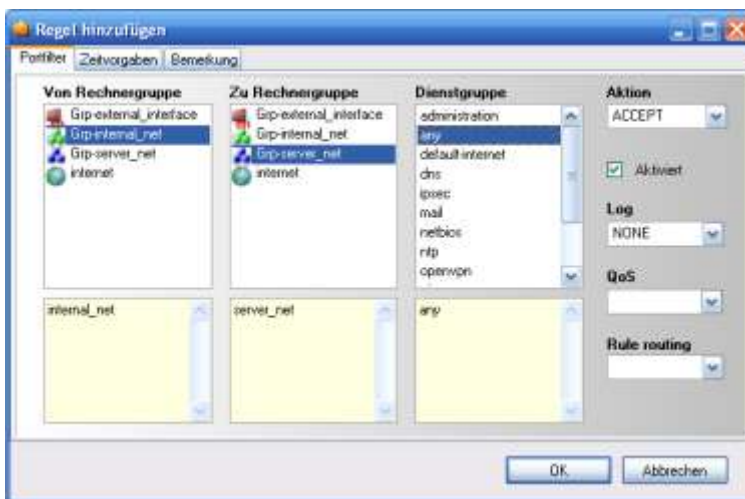


Abb. 25 Grp-internal_net → Grp-server_net → any

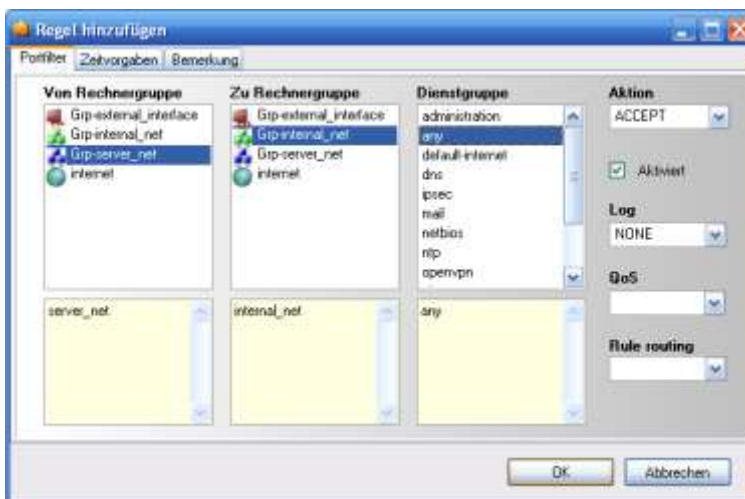


Abb. 26 Grp-server_net → Grp-internal_net → any

2.5 Speichern, Regelupdate und Dienst starten

- Speichern Sie auch auf dieser Appliance die Konfiguration.
- Führen Sie dann ein Regelupdate durch.
- Dann müssen Sie noch den Dienst starten.

Gehen Sie dafür vor, wie in Kapitel 1.8 beschrieben.

3 Hinweis für den Betrieb im Multipath Routing

Wenn Sie OpenVPN im Multipath Routing Betrieb betreiben, dann müssen Sie den Dienst an ein Interface binden.

- Gehen Sie über die Menüleiste auf den Punkt **VPN** und wählen Sie den Eintrag **VPN OpenVPN**.
- Wählen Sie als **Serverzertifikat** das entsprechende Zertifikat. Wenn die Appliance im ClientMode läuft, dann ist hier das Clientzertifikat zu wählen.
- Binden sie den Dienst an ein Interface. Nicht das Interface tun0 sondern ein ausgehendes Interface.

Wenn beide Appliances im Multipathbetrieb laufen, ist diese Einstellung natürlich für beide Systeme vorzunehmen.



Abb. 27 Dienst an ein Interface binden