Einrichtung einer VPN-SSL-Verbindung mit dem OpenVPN Clien

Beschreibung:

In diesem Dokument ist beschrieben, wie eine VPN-SSL-Verbindung mit dem OpenVPN Client zu einer LANCOM R&S® Unified Firewall (im Folgenden Unified Firewall genannt) eingerichtet werden kann.

> Aufgrund einer **Umstellung in den Verschlüsselungs-Algorithmen in OpenVPN ab Version 2.6.0** können **VPN-SSL-Verbindungen zur Unified Firewall erst ab LCOS FX 10.13 Rel aufgebaut** werden. In **älteren LCOS FX Versionen** muss **OpenVPN mit einer Version kleiner 2.6.0** eingesetzt werden (z.B. Version **2.5.8**).

Voraussetzungen:

- **Bestandsinstallation** einer LANCOM R&S®Unified Firewall
- OpenVPN Client
- Microsoft Windows ab Version 7
- Bereits eingerichtete und funktionsfähige Internet-Verbindung auf der Unified Firewall
- Web-Browser für den Zugriff auf das Webinterface der Unified Firewall

  Es werden folgende Browser unterstützt:

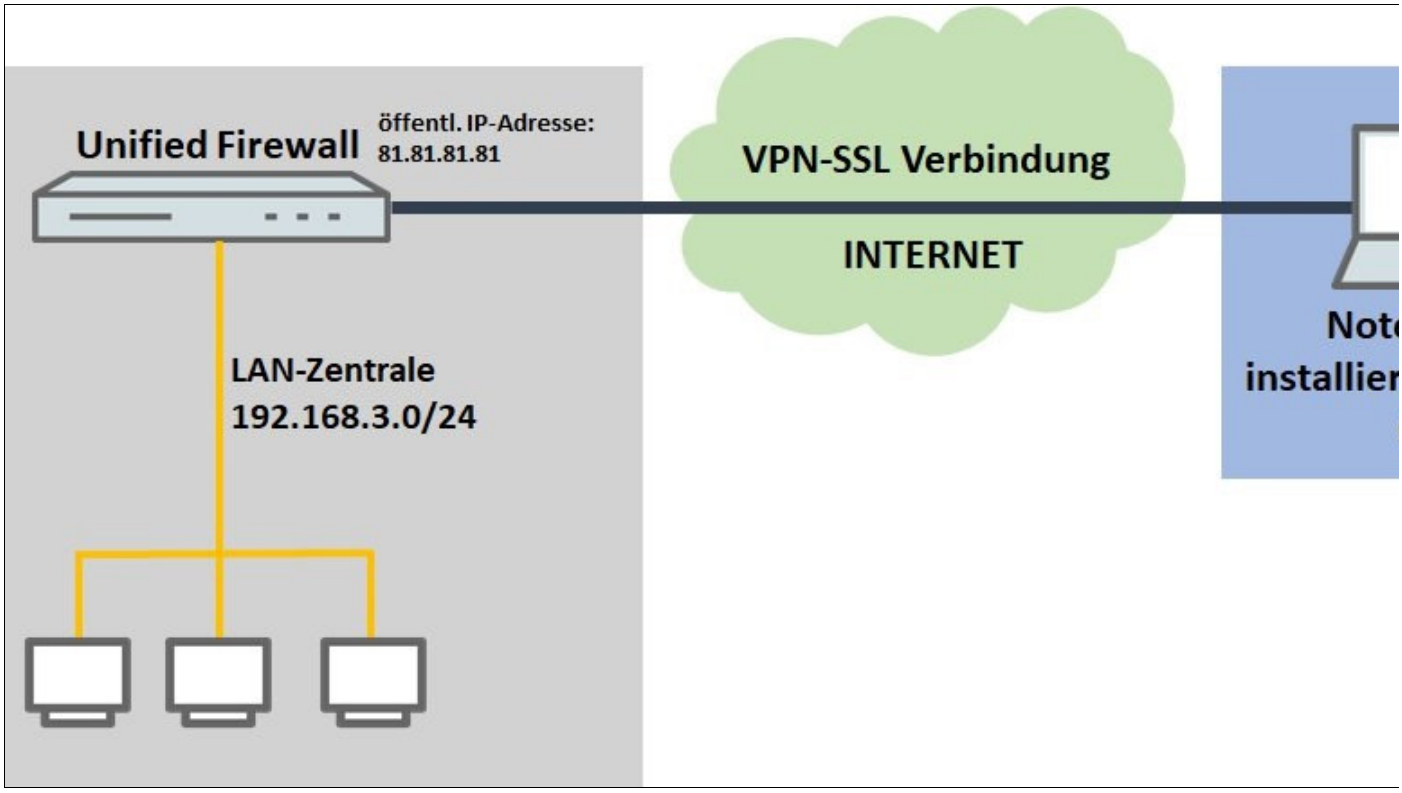
  - Google Chrome
  - Chromium
  - Mozilla Firefox

> Wir empfehlen **für VPN Client-Verbindungen die Verwendung des LANCOM Advanced VPN Client.** Passende Artikel zur Konfiguration finden Sie in diesem Sammel-Dokument.

Szenario:

1. Die Unified Firewall ist direkt mit dem Internet verbunden und verfügt über eine öffentliche IPv4-Adresse:

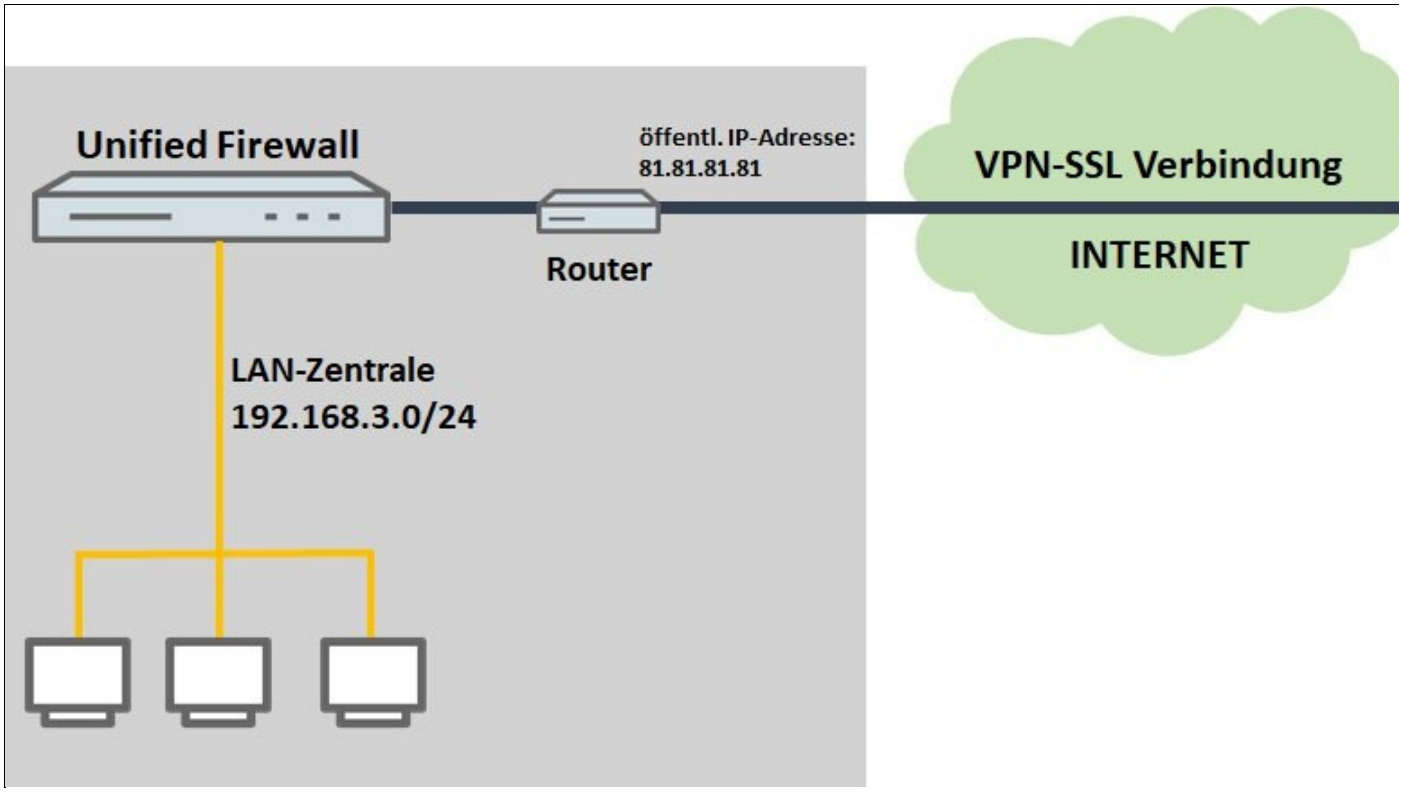
- Ein Unternehmen möchte seinen Außendienst-Mitarbeitern den Zugriff auf das Firmennetzwerk per **VPN-SSL Client-to-Site Verbindung** ermöglichen.
- Dazu ist auf den Notebooks der Außendienst-Mitarbeiter der **OpenVPN Client installiert**.
- Die Firmenzentrale verfügt über eine Unified Firewall als Gateway und eine **Internetverbindung mit der festen öffentlichen IP-Adresse 81.81.81.81**.
- Das **lokale Netzwerk der Zentrale** hat den IP-Adressbereich **192.168.3.0/24**.



2. Die Unified Firewall geht über einen vorgeschalteten Router ins Internet:

- Ein Unternehmen möchte seinen Außendienst-Mitarbeitern den Zugriff auf das Firmennetzwerk per **VPN-SSL Client-To-Site Verbindung** ermöglichen.
- Dazu ist auf den Notebooks der Außendienst-Mitarbeiter der **OpenVPN Client installiert**.
- Die Firmenzentrale verfügt über eine Unified Firewall als Gateway und einen vorgeschalteten Router, welcher die Internet-Verbindung herstellt. Der Router hat die **feste öffentliche IP-Adresse 81.81.81.81**.
- Das **lokale Netzwerk der Zentrale** hat den IP-Adressbereich **192.168.3.0/24**.

ⓘ Dieses Szenario beinhaltet auch die "Parallel"-Lösung wie in diesem Artikel beschrieben.

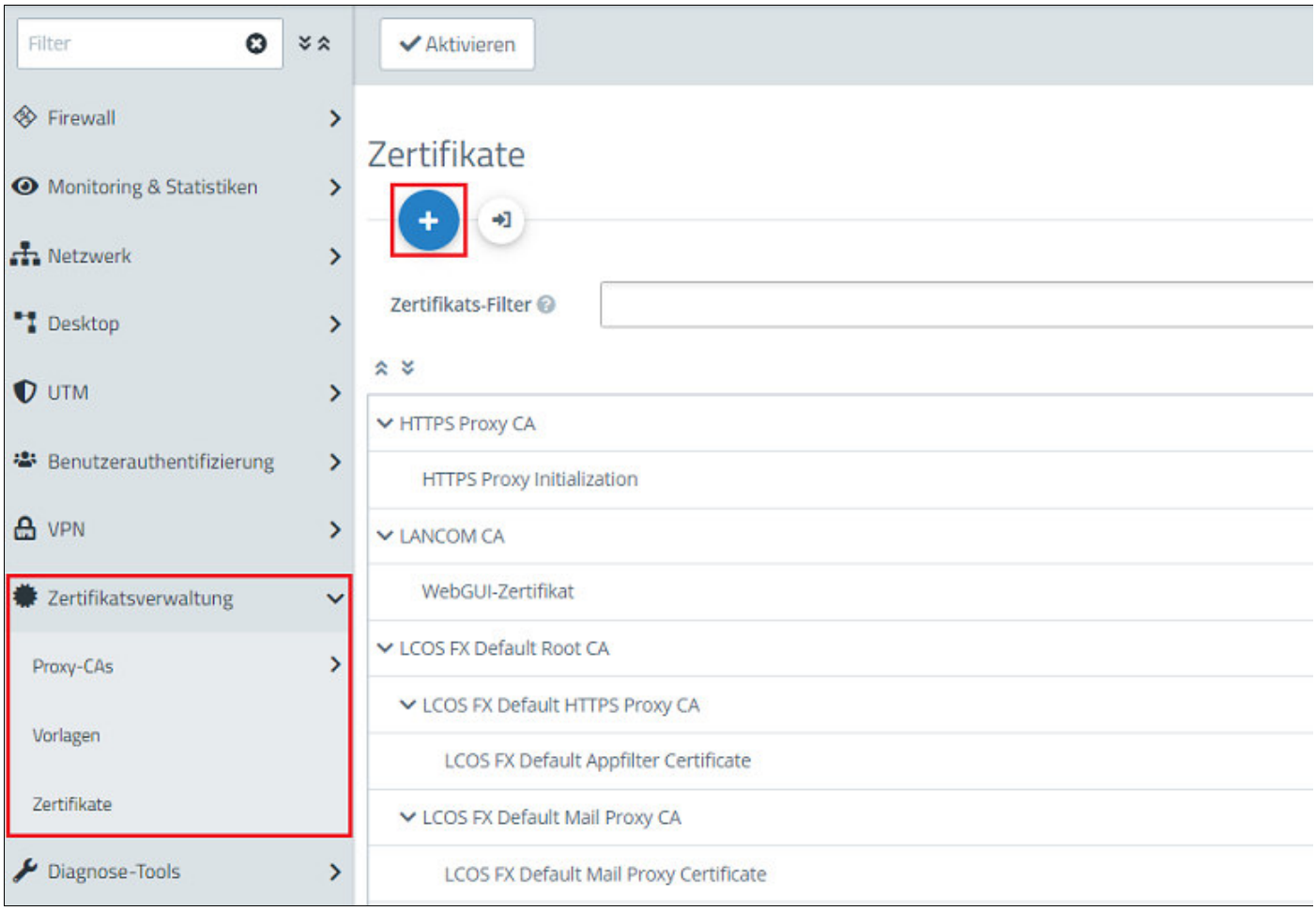


Vorgehensweise:

Die Einrichtung ist bei **Szenario 1** und **2** grundsätzlich gleich. Bei **Szenario 2** muss zusätzlich ein **Portforwarding** auf dem vorgeschalteten Router eingerichtet werden (siehe **Abschnitt 3**).

1. Konfigurationsschritte auf der Unified Firewall:

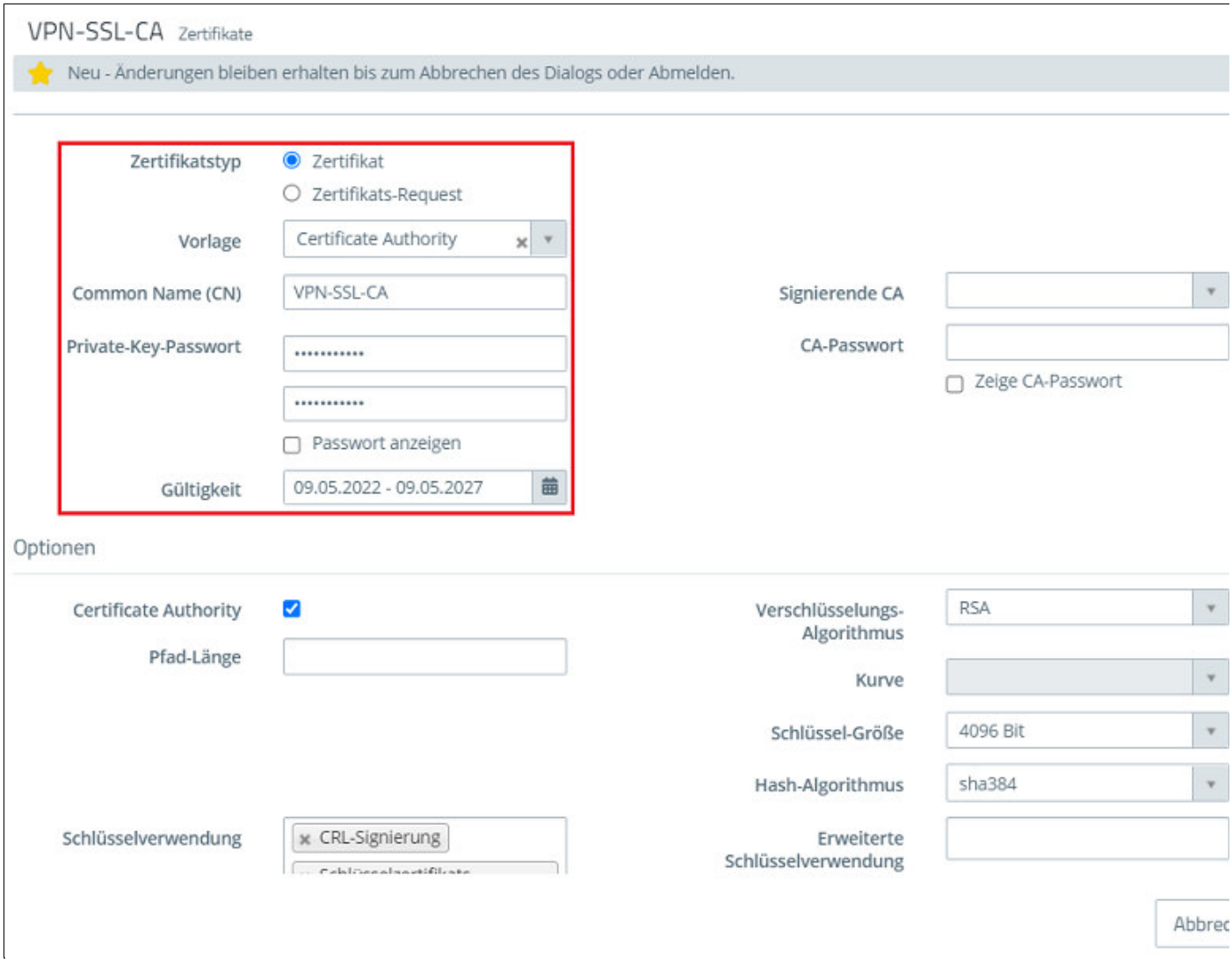
1.1 Verbinden Sie sich mit der Unified Firewall, wechseln in das Menü **Zertifikatsverwaltung** → **Zertifikate** und klicken auf das "Plus-Zeichen", um eine neue **CA** zu erstellen.



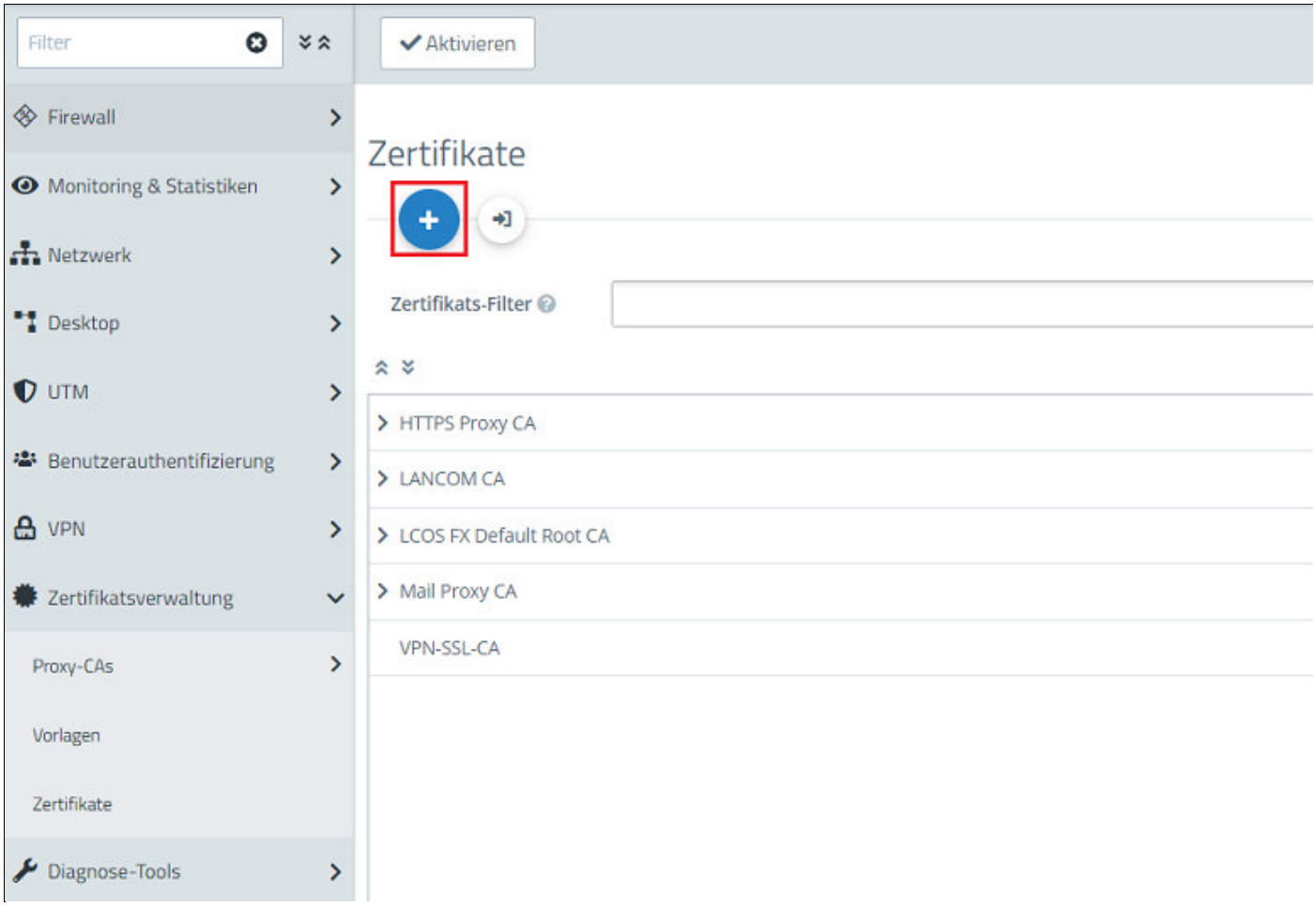
1.2 Passen Sie die folgenden Parameter an und klicken auf **Erstellen**:

- **Zertifikatstyp**: Belassen Sie die Einstellung auf der Option **Zertifikat**.
- **Vorlage**: Wählen Sie im Dropdownmenü die Option **Certificate Authority** aus.
- **Common-Name (CN)**: Vergeben Sie einen aussagekräftigen **Common Name** (in diesem Beispiel **VPN-SSL-CA**).
- **Private-Key-Passwort**: Hinterlegen Sie ein **Passwort**. Dieses dient dazu den Private Key zu verschlüsseln.
- **Gültigkeit**: Legen Sie fest wie lange das Zertifikat gültig sein soll. Bei einer **CA** wird die **Gültigkeitsdauer** üblicherweise sehr hoch gewählt. In der **Standard-Einstellung** ist eine **Gültigkeit von 5 Jahren** voreingestellt.

> ⓘ Die restlichen Einstellungen (etwa die Verschlüsselung) können auf den Standard-Einstellungen belassen werden.



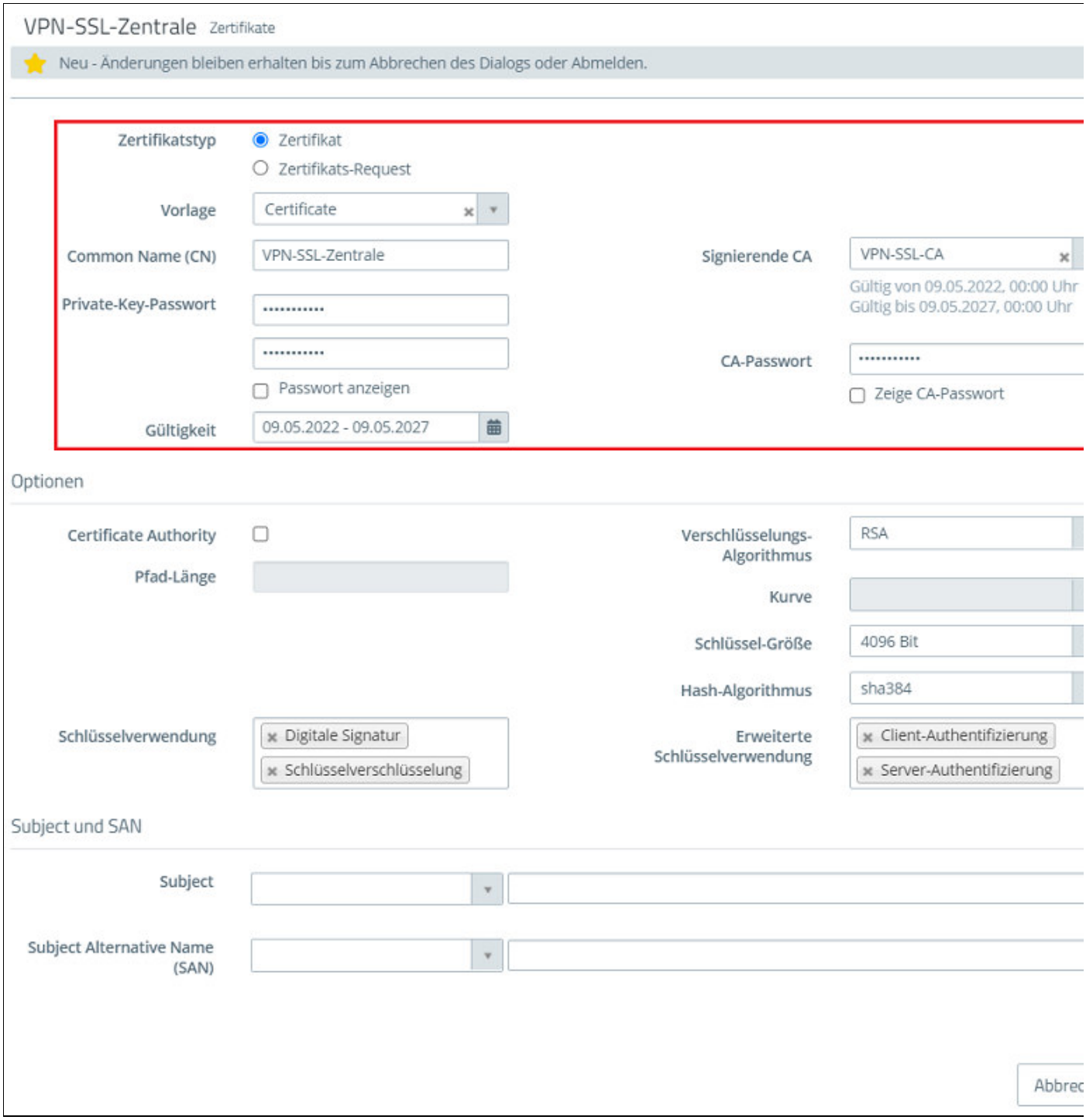
1.3 Erstellen Sie mit einem Klick auf das "Plus-Zeichen" ein weiteres Zertifikat. Dieses dient zur Authentifizierung von VPN-SSL Verbindungen auf der Unified Firewall.



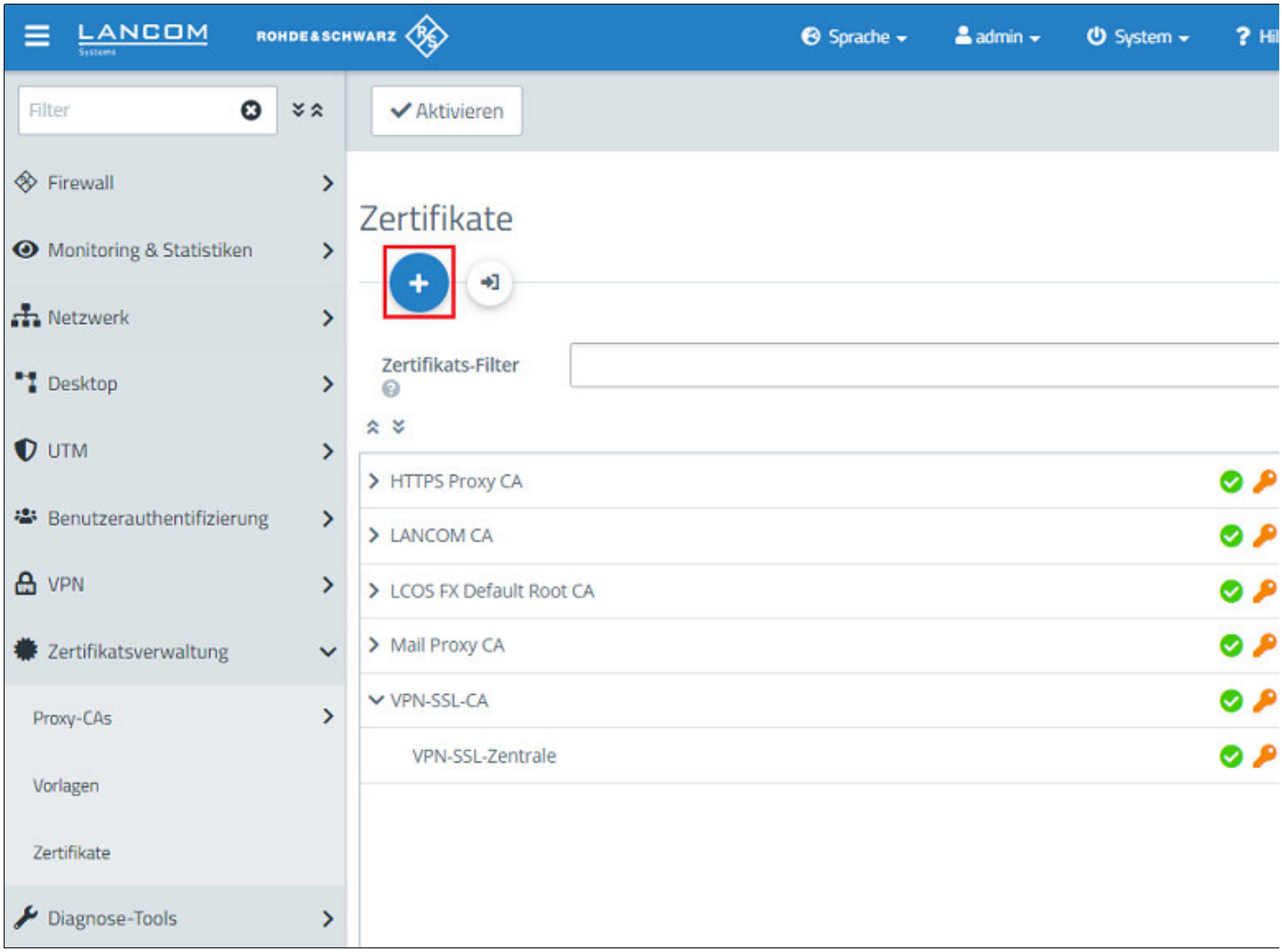
1.4 Passen Sie die folgenden Parameter an und klicken auf **Erstellen**:

- **Zertifikatstyp**: Belassen Sie die Einstellung auf der Option **Zertifikat**.
- **Vorlage**: Wählen Sie im Dropdownmenü die Option **Certificate** aus.
- **Common-Name (CN)**: Vergeben Sie einen aussagekräftigen **Common Name** (in diesem Beispiel **VPN-SSL-Zentrale**).
- **Private-Key-Passwort**: Hinterlegen Sie ein **Passwort**. Dieses dient dazu den Private Key zu verschlüsseln.
- **Gültigkeit**: Legen Sie fest wie lange das Zertifikat gültig sein soll. Bei einem **VPN-Zertifikat** zur Annahme von VPN-Clients wird die **Gültigkeitsdauer** üblicherweise sehr hoch gewählt (in diesem Beispiel **5 Jahre**).
- **Signierende CA**: Wählen Sie im Dropdownmenü die in **Schritt 1.2** erstellte **CA** aus.
- **CA-Passwort**: Hinterlegen Sie das in **Schritt 1.2** vergebene **Private-Key-Passwort.**

Die restlichen Einstellungen (etwa die Verschlüsselung) können auf den Standard-Einstellungen belassen werden.



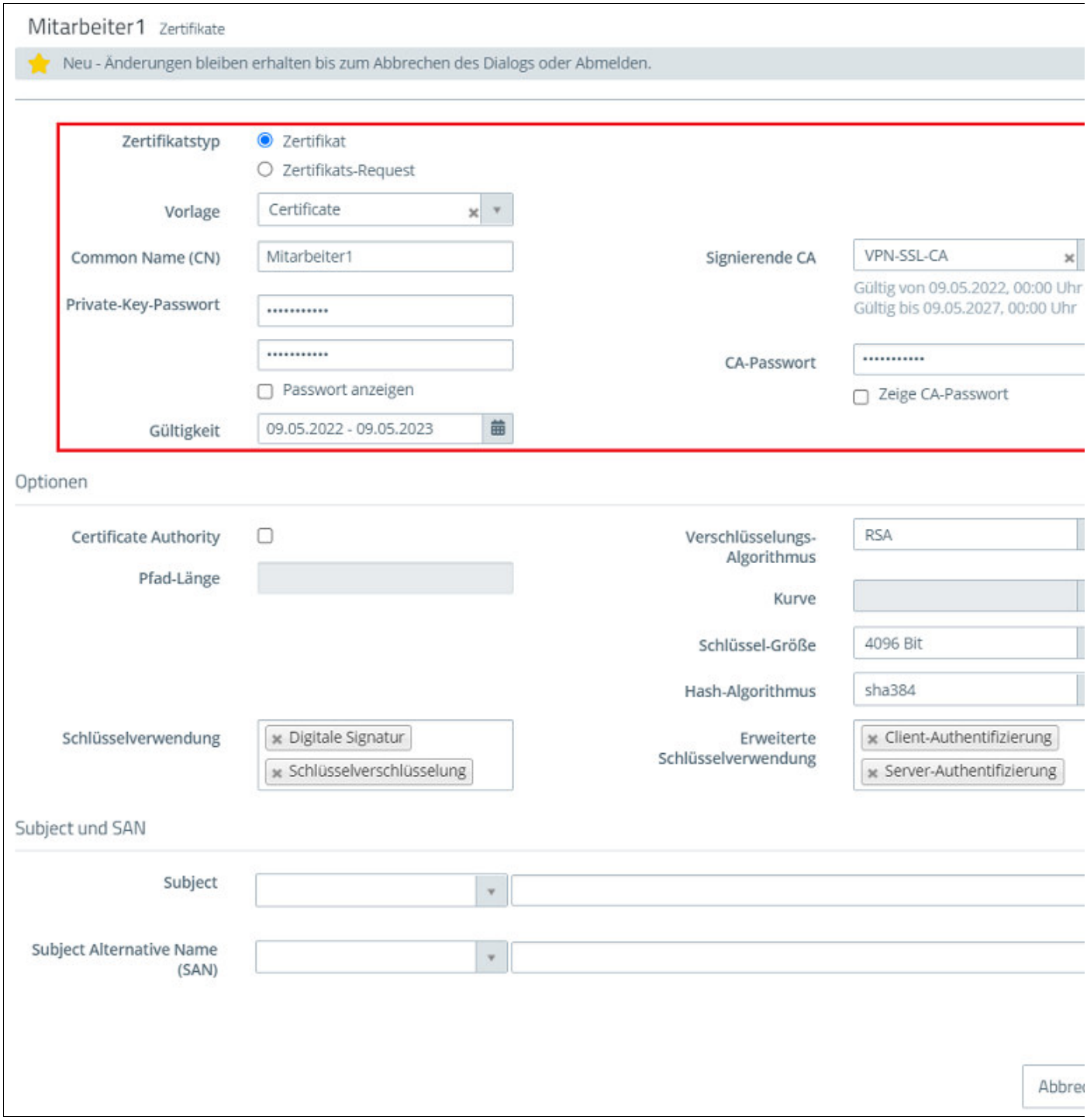
1.5 Erstellen Sie mit einem Klick auf das "Plus-Zeichen" ein weiteres Zertifikat. Dieses dient zur Einwahl eines bestimmten Mitarbeiters bzw. VPN-Clients.



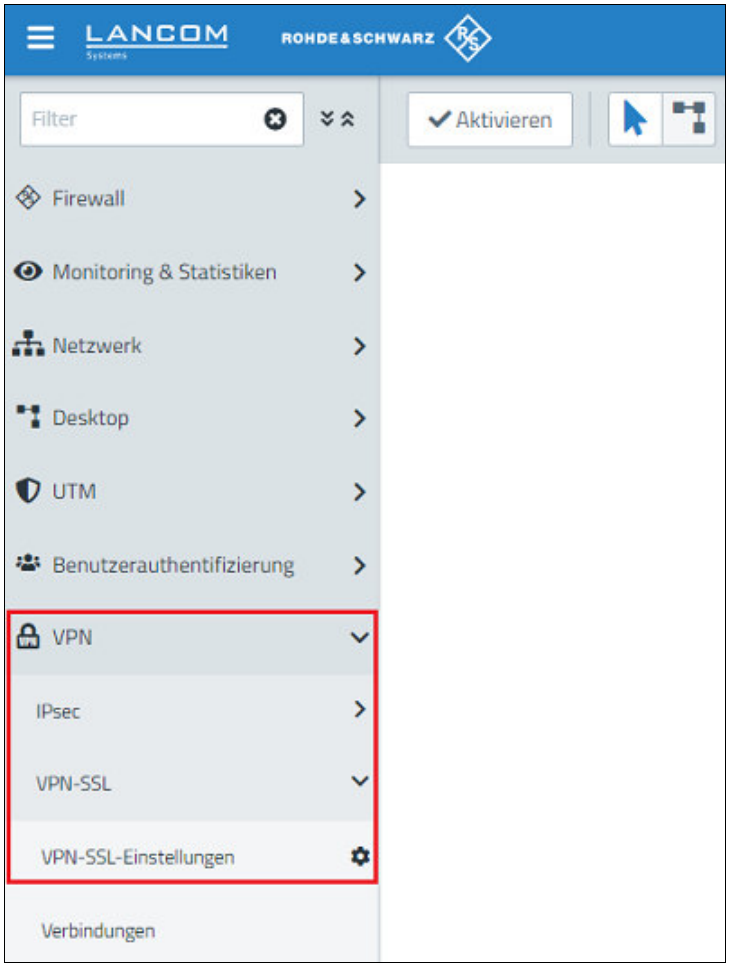
1.6 Passen Sie die folgenden Parameter an und klicken auf **Erstellen**:

- **Zertifikatstyp**: Belassen Sie die Einstellung auf der Option **Zertifikat**.
- **Vorlage**: Wählen Sie im Dropdownmenü die Option **Certificate** aus.
- **Common-Name(CN)**: Vergeben Sie einen aussagekräftigen **Common Name**, der den Mitarbeiter bezeichnet.
- **Private-Key-Passwort**: Hinterlegen Sie ein **Passwort**. Dieses dient dazu den Private Key zu verschlüsseln.
- **Gültigkeit**: Legen Sie fest wie lange das Zertifikat gültig sein soll. Bei einem **VPN-Zertifikat** für einen einzelnen Benutzer wird die **Gültigkeitsdauer** üblicherweise eher gering gewählt (in diesem Beispiel 1 Jahr).
- **Signierende CA**: Wählen Sie im Dropdownmenü die in **Schritt 1.2** erstellte **CA** aus.
- **CA-Passwort**: Hinterlegen Sie das in **Schritt 1.2** vergebene **Private-Key-Passwort.**

In dem Feld **Subject Alternative Name** können zur einfacheren Zuordnung eines Mitarbeiters weitere Merkmale wie z.B. die E-Mail-Adresse hinterlegt werden. Die restlichen Einstellungen (etwa die Verschlüsselung) können auf den Standard-Einstellungen belassen werden.



1.7 Wechseln Sie in das Menü **VPN** → **VPN-SSL** → **VPN-SSL-Einstellungen**.



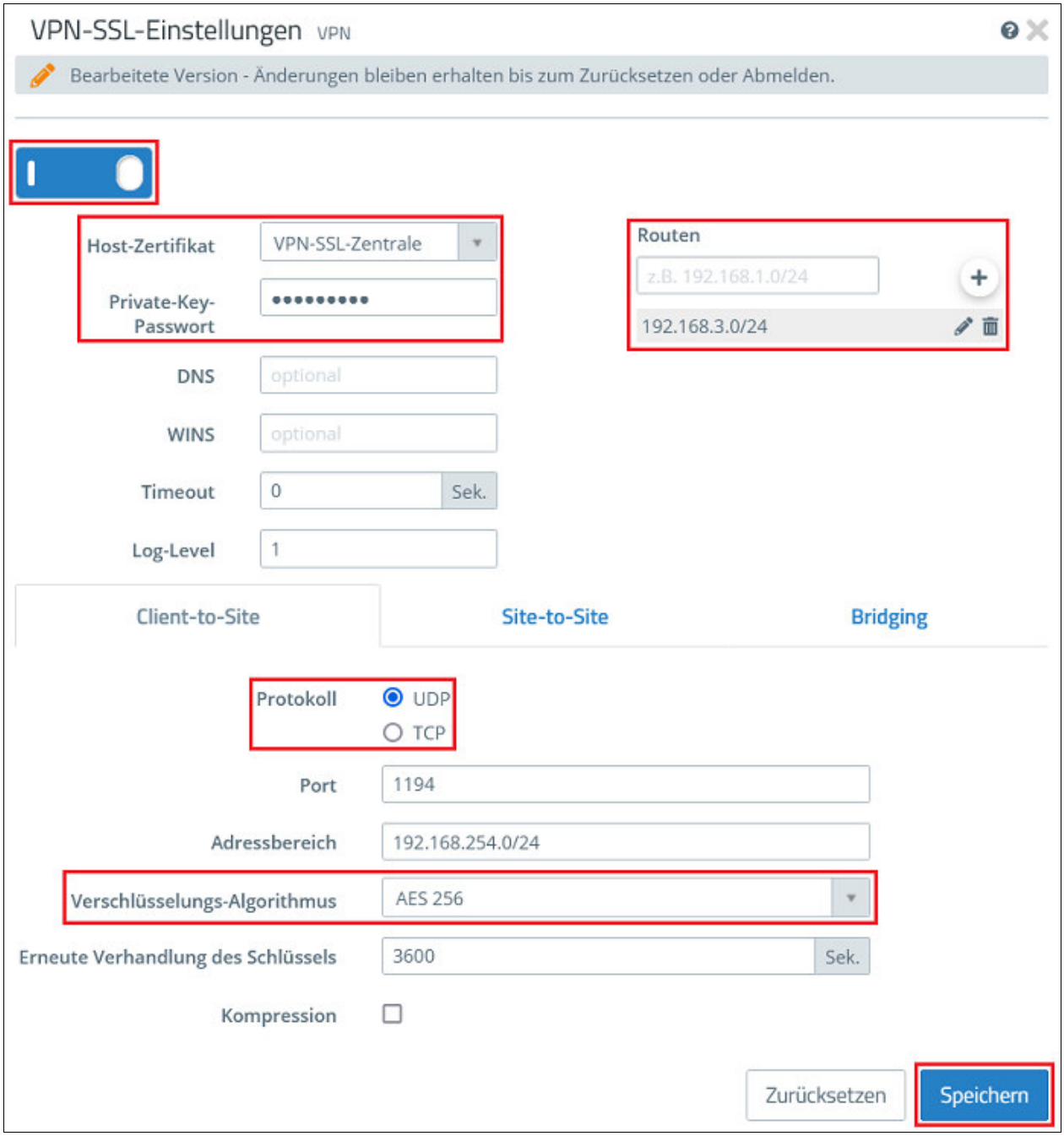
1.8 **Aktivieren Sie den VPN-SSL-Dienst** über den Schieberegler, passen die folgenden Parameter an und klicken auf **Speichern**:

- **Host-Zertifikat**: Wählen Sie im Dropdownmenü das in **Schritt 1.4** erstellte **VPN-Zertifikat** aus.
- **Private-Key-Passwort**: Tragen Sie das in **Schritt 1.4** vergebene **Private-Key-Passwort** ein.
- **Routen**: Hinterlegen Sie die **Netzwerke** in **CIDR** Schreibweise (**C**lassless **I**nter**D**omain **R**outing), in die der VPN-Client Zugriff haben soll. Diese werden an alle VPN-SSL-Clients ausgeteilt.
- **Protokoll**: Stellen Sie sicher, dass die Option **UDP** ausgewählt ist. Wird für den VPN-SSL-Tunnel **TCP** verwendet und innerhalb des Tunnels Daten per **TCP** übertragen, kann dies ansonsten zu einem "TCP-Meltdown" führen.
- **Verschlüsselungs-Algorithmus**: Wählen Sie im Dropdownmenü **AES 256** aus.

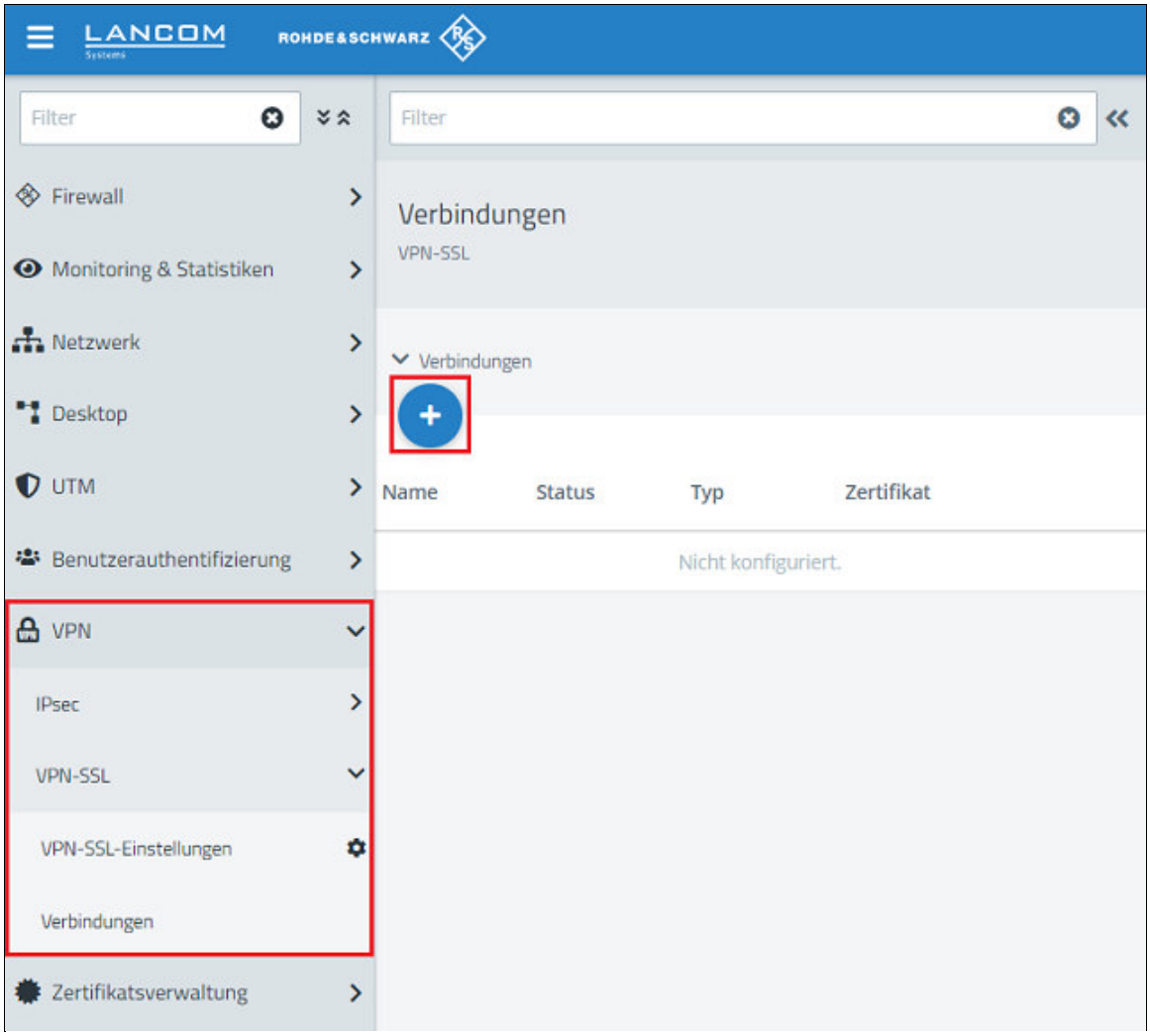
Optional können Sie einen **DNS**- oder **WINS**-Server hinterlegen, die allen VPN-SSL-Clients zugewiesen werden.

Bei Bedarf können Sie den **Port** abändern.

Bei dem **Adressbereich** handelt es sich um den Einwahl-Adressbereich, aus dem ein VPN-SSL-Client eine IP-Adresse zugewiesen bekommt. Dieser Adressbereich darf nicht bereits als internes Netzwerk in der Unified Firewall verwendet werden.



1.9 Wechseln Sie in das Menü **VPN** → **VPN-SSL** → **Verbindungen** und klicken auf das "Plus-Zeichen", um eine neue VPN-SSL-Verbindung zu erstellen.



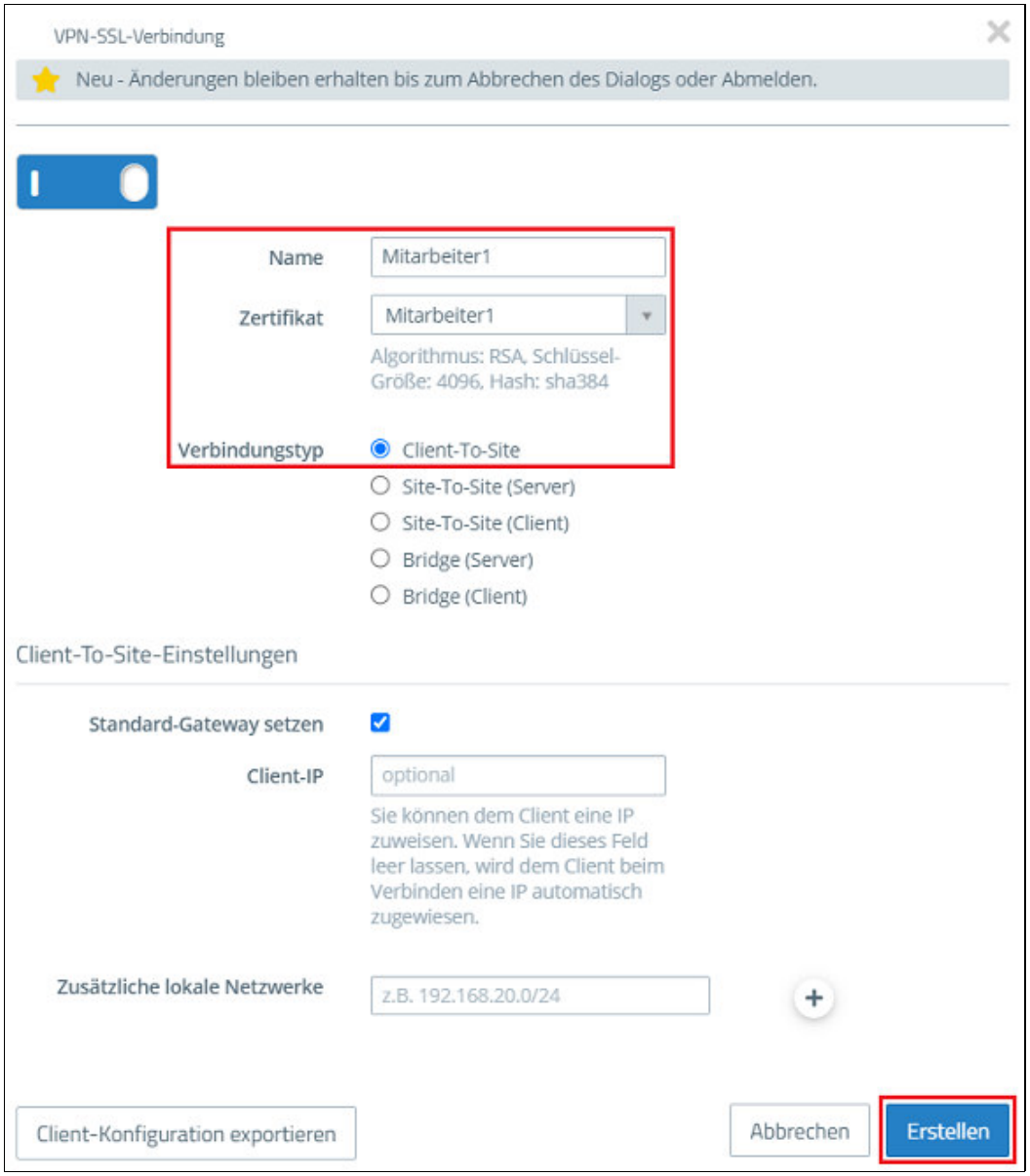
1.10 Passen Sie die folgenden Parameter an und klicken auf **Erstellen**:

- **Name**: Vergeben Sie einen **aussagekräftigen Namen** (in diesem Beispiel **Mitarbeiter1**).
- **Zertifikat**: Wählen Sie im Dropdownmenü das in **Schritt 1.6** erstellte **VPN-Zertifikat für den Mitarbeiter** aus.
- **Verbindungstyp**: Wählen Sie **Client-To-Site** aus.

Wird die Funktion **Standard-Gateway setzen** aktiviert, kann der VPN-Client über die Internet-Verbindung der Unified Firewall mit dem Internet kommunizieren.

Bei **Client IP** besteht die Möglichkeit dem VPN-Client eine feste IP-Adresse zuzuweisen. Bleibt dieser Eintrag leer, wird dem VPN-Client eine IP-Adresse aus dem **Adressbereich** zugewiesen (siehe **Schritt 1.8**).

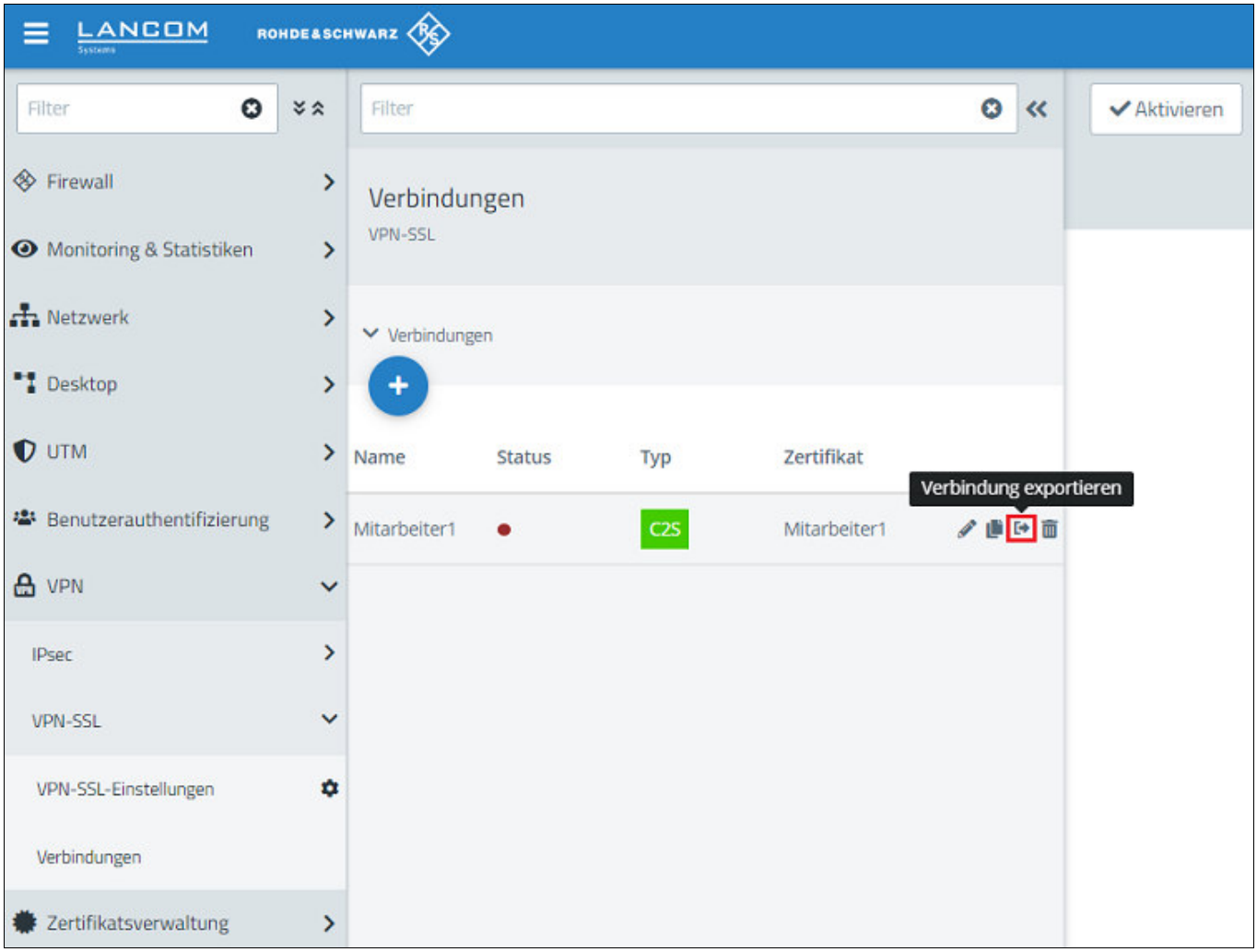
Bei **Zusätzliche Server-Netzwerke** besteht die Möglichkeit dem VPN-Client den Zugriff auf weitere lokale Netzwerke zu erlauben. So kann einzelnen Mitarbeitern der Zugriff auf unterschiedliche lokale Netzwerke ermöglicht werden.



1.11 Klicken Sie bei der VPN-SSL Verbindung auf die Schaltfläche **Verbindung exportieren**, um das VPN-Profil mitsamt dem Zertifikat zu exportieren.

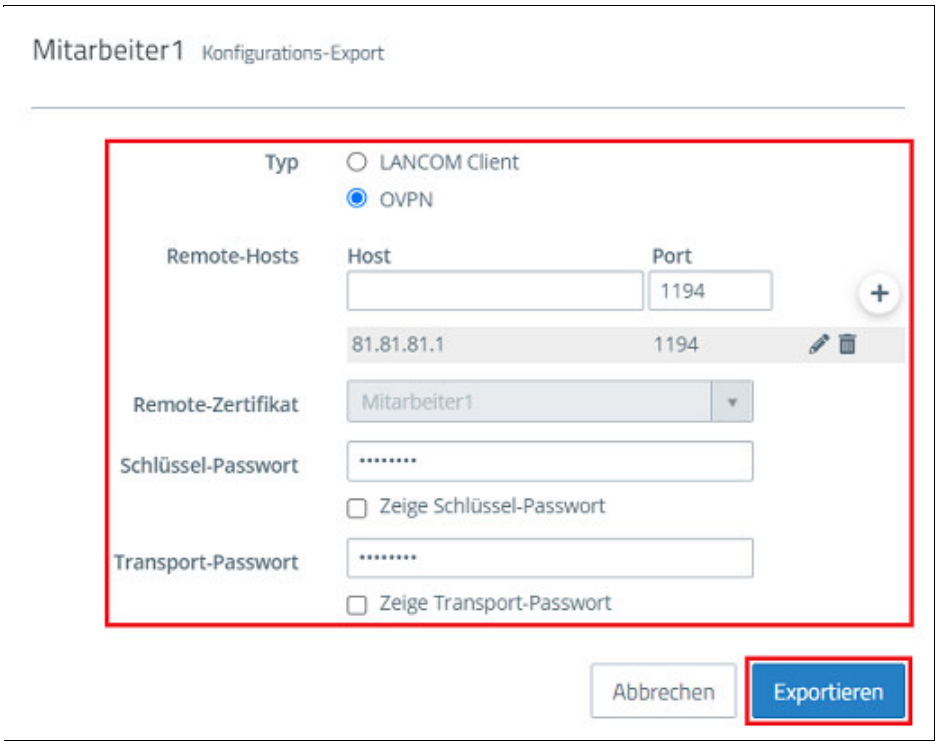
Gegebenenfalls müssen Sie im Vorfeld auf das Doppelpfeil-Symbol klicken (neben dem Feld **Filter**), um das Menü zu expandieren, damit das Symbol für den Export sichtbar ist.

Alternativ können Sie die Verbindung auch über das "Stift-Symbol" editieren und dort auf **Client-Konfiguration exportieren** klicken, um das VPN-Profil mitsamt dem Zertifikat zu exportieren.

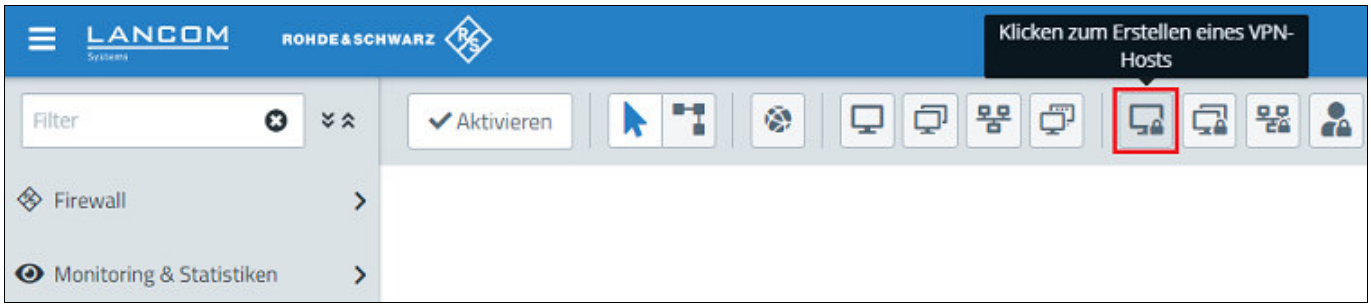


1.12 Passen Sie die folgenden Parameter an und klicken auf **Exportieren**:

- **Type**: Wählen Sie **OVPN**, damit ein Profil für den OpenVPN Client generiert wird.
- **Remote-Hosts**: Geben Sie die **öffentliche IPv4-Adresse bzw. den DynDNS-Namen der Unified-Firewall** sowie den **Port für VPN-SSL** (siehe **Schritt 1.8**) an. Fügen Sie die Parameter über das "Plus-Zeichen" dem Profil hinzu.
- **Schlüssel-Passwort**: Hinterlegen Sie das in **Schritt 1.6** vergebene **Private-Key-Passwort**.
- **Transport Password**: Vergeben Sie ein **Passwort**. Dieses muss bei dem Aufbau der VPN-Verbindung im OpenVPN Client angegeben werden.

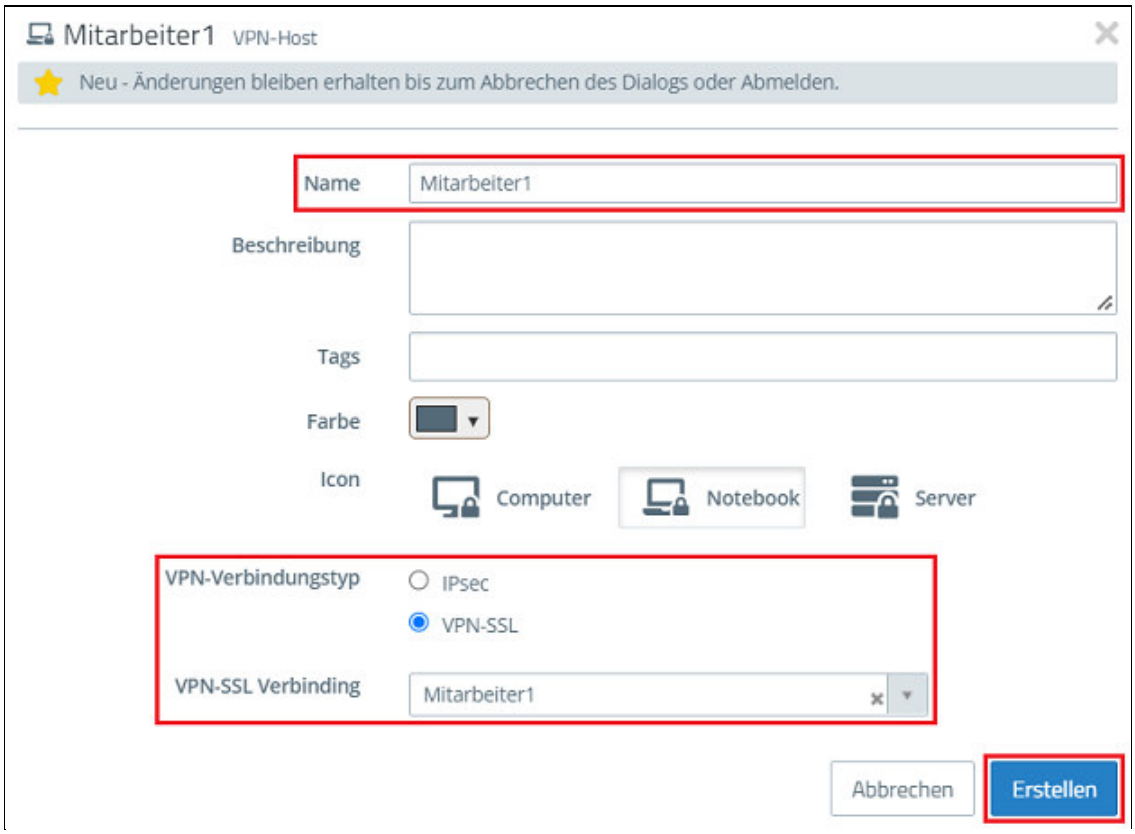


1.13 Klicken Sie auf die Schaltfläche zum Erstellen eines neuen **VPN-Hosts**.

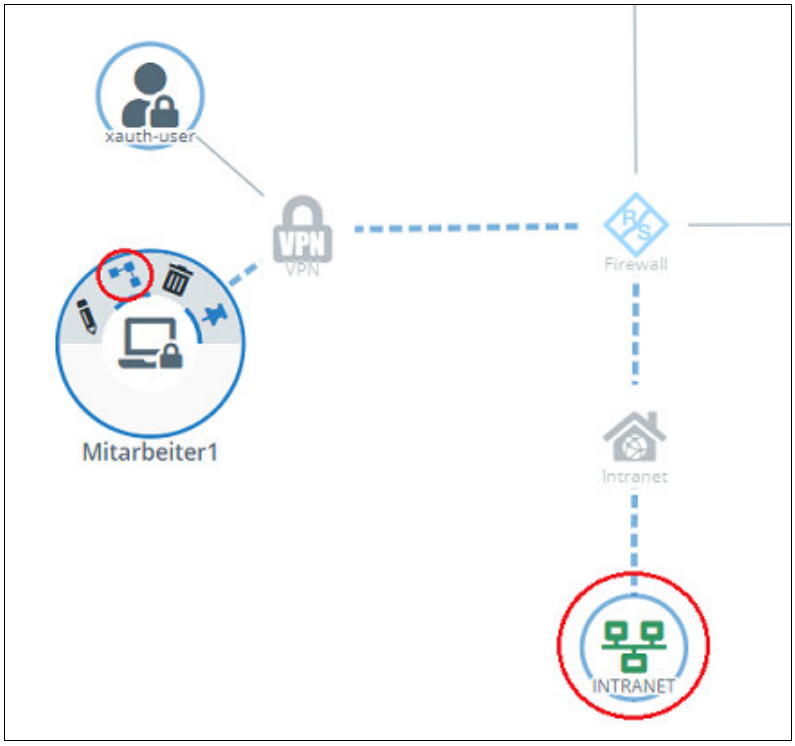


1.14 Passen Sie die folgenden Parameter an und klicken auf **Erstellen**:

- **Name**: Vergeben Sie einen **aussagekräftigen Namen** (in diesem Beispiel **Mitarbeiter1**).
- **VPN-Verbindungstyp**: Wählen Sie die Option **VPN-SSL** aus.
- **VPN-SSL-Verbindung**: Wählen Sie im Dropdownmenü die in **Schritt 1.10** erstellte **VPN-SSL** Verbindung aus.

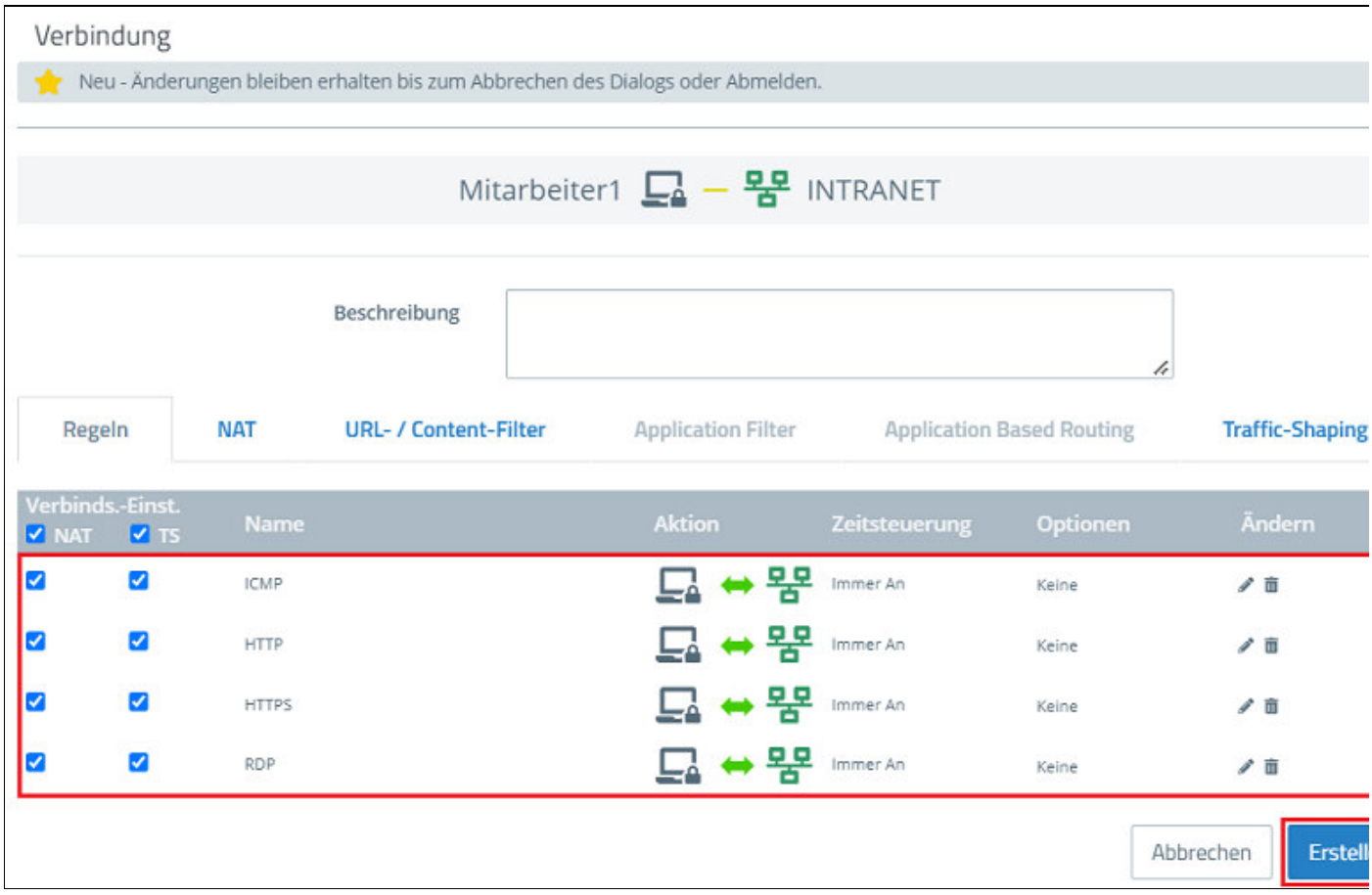


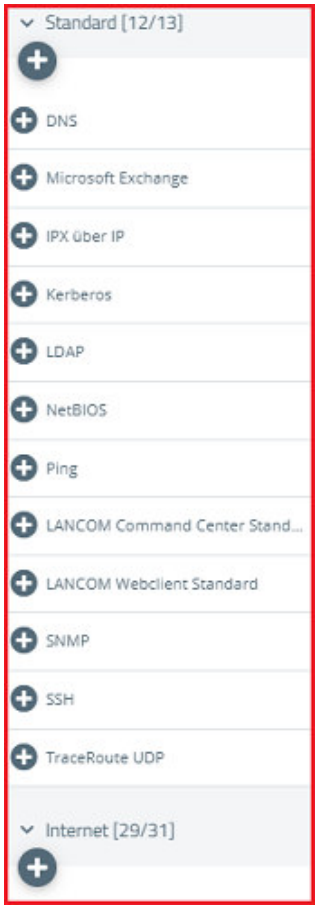
1.15 Klicken Sie in dem **VPN-Host** auf das "Verbindungswerkzeug" und klicken anschließend auf das Netzwerk-Objekt, auf welches der **OpenVPN Client** zugreifen können soll, damit die Firewall-Objekte geöffnet werden. Wiederholen Sie diesen Schritt für jedes weitere Netzwerk, in welches der **OpenVPN Client** Zugriff haben soll.



1.16 Weisen Sie über die "Plus-Zeichen" dem **VPN-Host** die erforderlichen Protokolle zu.

Eine Unified Firewall verwendet eine Deny-All Strategie. Die Kommunikation muss also explizit erlaubt werden.





1.17 Klicken Sie zuletzt in der Unified Firewall auf **Aktivieren**, damit die Konfigurations-Änderungen umgesetzt werden.

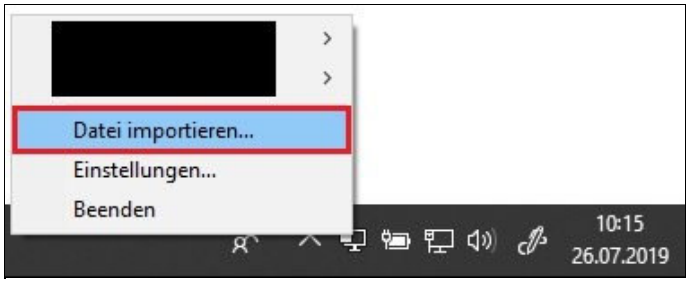
1.18 Die Konfigurationsschritte auf der Unified Firewall sind damit abgeschlossen.

> Führen Sie bei Bedarf die **Schritte 1.5 - 1.6** sowie **1.9 - 1.17** erneut durch, um einen weiteren VPN-Zugang zu erstellen.

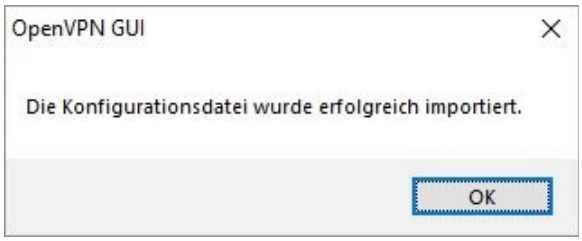
2. Konfigurationsschritte im OpenVPN Client:

2.1 Führen Sie auf das OpenVPN Symbol in der Taskleiste einen Rechtsklick aus.

2.2 Klicken Sie auf **Datei importieren**, um das VPN-Profil zu importieren.



2.3 Der erfolgreiche Profil-Import wird mit einer entsprechenden Meldung quittiert.



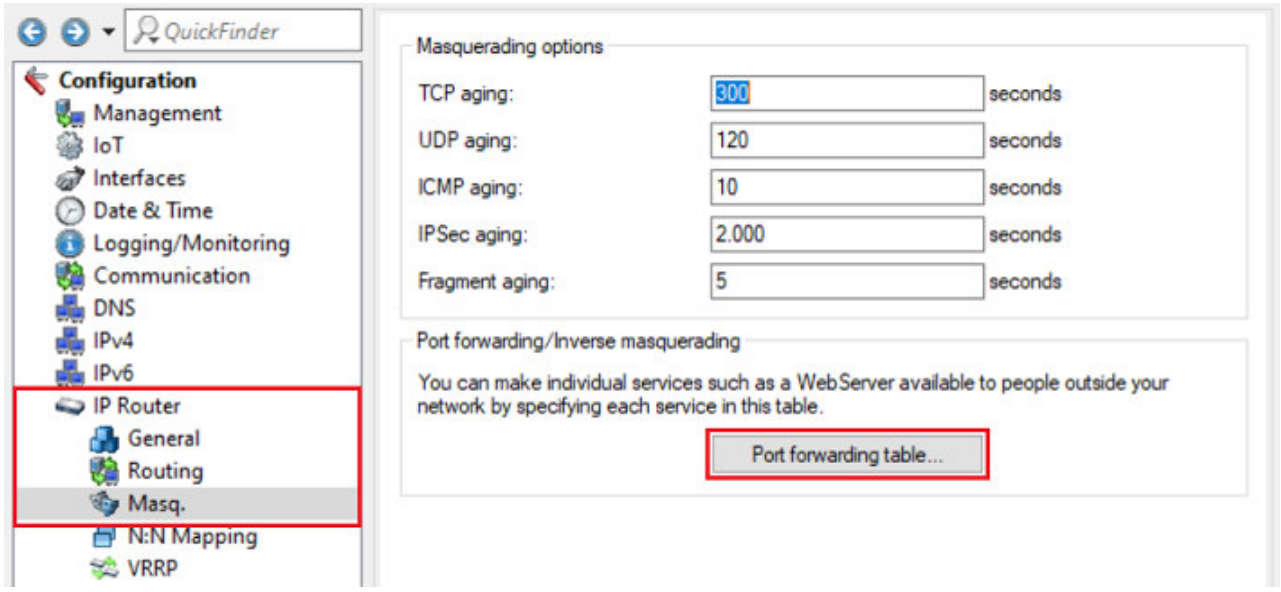
2.4 Die Konfigurationsschritte im OpenVPN Client sind damit abgeschlossen.

3. Einrichtung eines Port-Forwarding auf einem LANCOM Router (nur Szenario 2):

Für **VPN-SSL** wird im Standard der **UDP-Port 1194** verwendet. Dieser muss auf die Unified Firewall weitergeleitet werden.

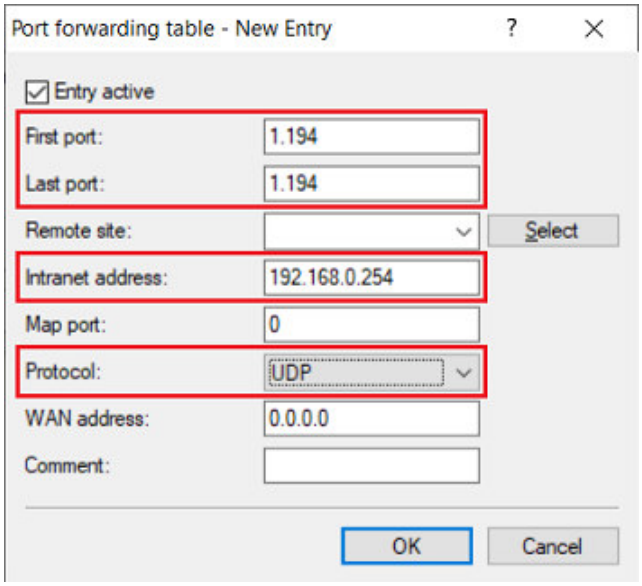
> ⓘ Der Port für SSL-VPN lässt sich in der Unified Firewall ändern (siehe **Schritt 1.8**). Sollte ein Router eines anderen Herstellers verwendet werden, erfragen Sie die Vorgehensweise bei dem jeweiligen Hersteller.

3.1 Öffnen Sie die Konfiguration des Routers in LANconfig und wechseln in das Menü **IP-Router → Maskierung → Port-Forwarding-Tabelle**.



3.2 Hinterlegen Sie folgende Parameter:

- **Anfangs-Port**: Hinterlegen Sie den **Port 1194**.
- **End-Port**: Hinterlegen Sie den **Port 1194**.
- **Intranet-Adresse**: Hinterlegen Sie die **IP-Adresse der Unified-Firewall im Transfernetz** zwischen Unified Firewall und LANCOM Router.
- **Protokoll**: Wählen Sie im Dropdown-Menü **UDP** aus.



3.3 Schreiben Sie die Konfiguration in den Router zurück.