

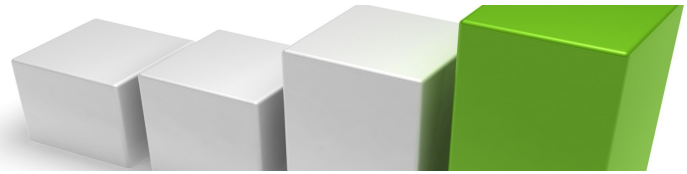
Vorkonfigurieren der CRASER-Firewall und des CRASER-Zertifikates im CR220N und CR230U

1. Allgemeines

ISK-Automation liefert alle Router mit vorkonfigurierter CRASER-Firewall und vorkonfiguriertem CRASER-Zertifikat aus. Sollten Sie dennoch einen Router ohne Vorkonfiguration erhalten haben, so dass Firewall und Zertifikat ergänzt werden müssen, soll diese Checkliste die notwendigen Schritte erläutern:

2. Checkliste zum Vorkonfigurieren der CRASER-Firewall und des CRASER-Zertifikates

1. ISK-Automation liefert ein p12-Zertifikat und eine Firewalldatei für die Subnetkopplung des CR220N/CR230U. Die Dateinamen werden aus einem Firmenkürzel (3Buchstaben), der Projektnummer (z.B. P1 für Projekt 1), der Netzbezeichnung des Fernwartungs-Subnetzes (NET1..63), der globalen Subnetzadresse gebildet.
Die Firma ISK-Automation GmbH würde von uns für Ihr 2.Fernwartungsprojekt, das nur ein Fernwartungs-Subnetz enthält, folgende Dateien bekommen:
p12-Zertifikat für CR220N/CR230U: ISK-P2-NET1(10.2.128.0).p12
Firewalldatei für CR220N/CR230U: ISK-P2-NET1(10.2.128.0).sh
2. Web-Konfiguration des "CR220N" bzw. „CR230U“ aufrufen:
CR220N: <http://192.168.0.126:7777>
CR230U: <http://192.168.0.127:7777>
- login: admin
3. CRASER-Firewalldatei konfigurieren: (siehe Bild 1)
Services → Firewall and NAT:
 - User configured script below: aktiv
 - Button "Durchsuchen" anklicken und die Firewalldatei, die ISK-Automation Ihnen geliefert hat, im Verzeichnisbaum des PCs suchen und öffnen (*.sh).
 - Button "Apply" betätigen und warten, bis die Firewall aktiviert ist.
 - Durch Betätigen des Buttons "Script rules" die geladene Firewalldatei anzeigen lassen.
In der Überschrift befinden sich alle wichtigen Daten zur Subnetkopplung.
 - Firewall-Anzeigefenster schließen.



4. CRASER-Zertifikatdatei konfigurieren: (siehe Bild 2)

VPN → OpenVPN:

- Enable/Disable OpenVPN: aktivieren
- OK-Schalter betätigen.
- "Durchsuchen"-Button betätigen und die Zertifikatdatei, die ISK-Automation Ihnen geliefert hat, im Verzeichnisbaum des PCs suchen und öffnen (*.p12).
- Die Datei mit dem "Import"-Button in den Router laden.
- "Apply" betätigen.
- Der Name der Zertifikatdatei muss jetzt in der Zeile „p12-certificate“ zu lesen sein.
- Durch Betätigen des Buttons "Info", die geladene Zertifikatdatei anzeigen lassen.
- Zertifikat-Anzeigefenster schließen

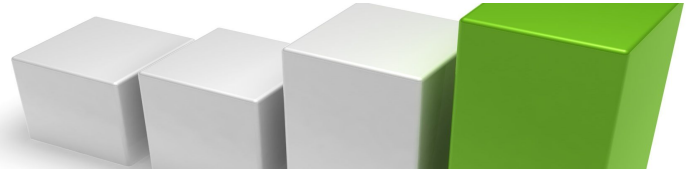
5. OpenVPN-Client deaktivieren. (siehe Bild3)

- Enable/Disable OpenVPN: deaktivieren
- „Apply“ betätigen.

Achtung: Schritt 5 ist wichtig, damit Sie nach dieser Vorkonfiguration mit einem unserer Applikationsberichte:

„CR220N_Fernwartung_DSL-Internetzugang.pdf“ oder
„CR220N_Fernwartung_EXT-Internetzugang oder
„CR230U_Fernwartung_UMTS-Internetzugang.pdf

weiterarbeiten können.



3. Darstellung der zugehörigen Konfigurationsseiten zum Kapitel 2 dieser Doku

Bild1 CRASER-Firewalldatei konfigurieren:

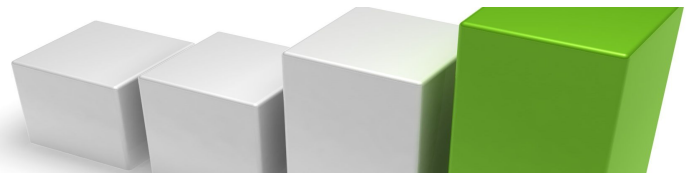
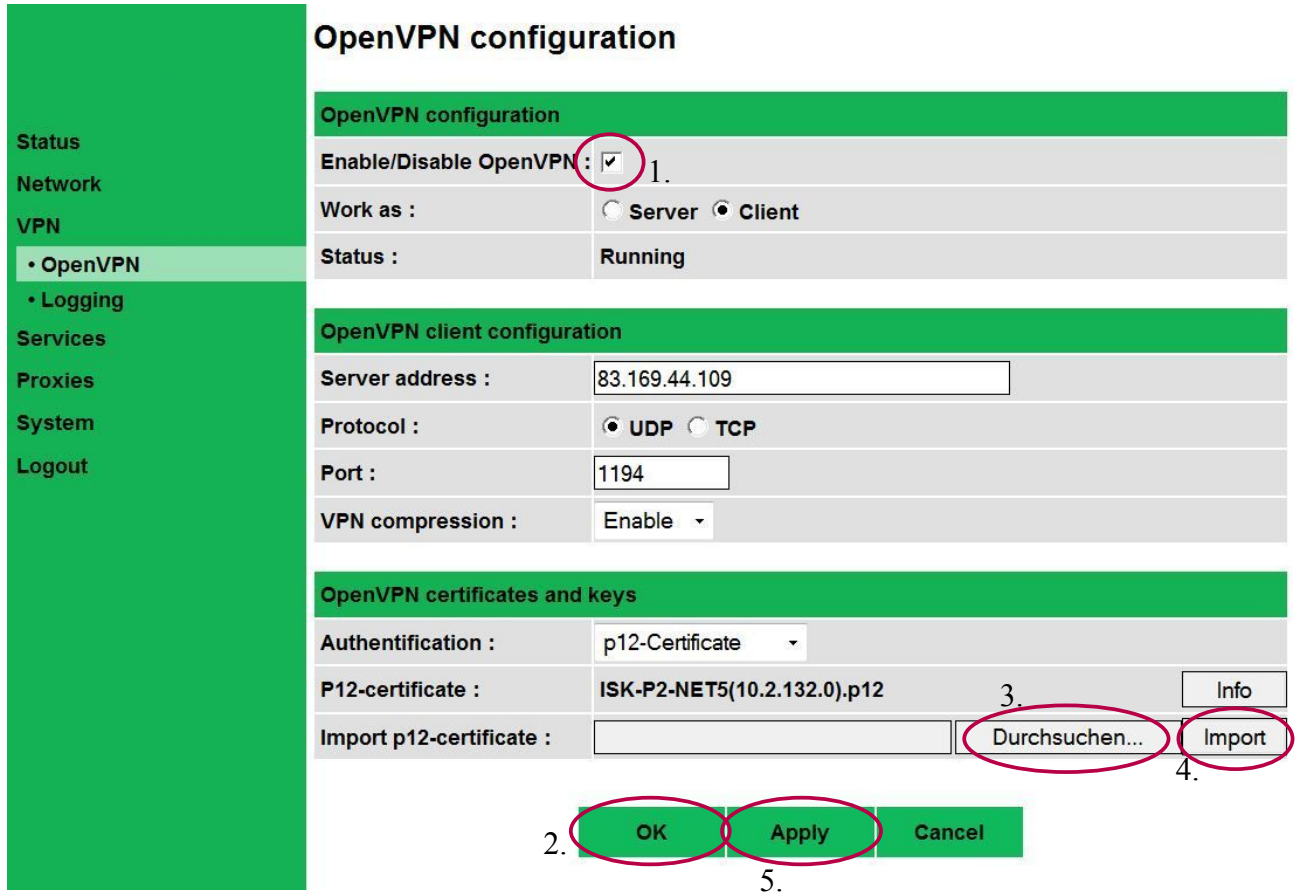


Bild2 CRASER-Zertifikatdatei konfigurieren:



OpenVPN configuration

OpenVPN configuration

Enable/Disable OpenVPN : 1.

Work as : Server Client

Status : Running

OpenVPN client configuration

Server address : 83.169.44.109

Protocol : UDP TCP

Port : 1194

VPN compression : Enable

OpenVPN certificates and keys

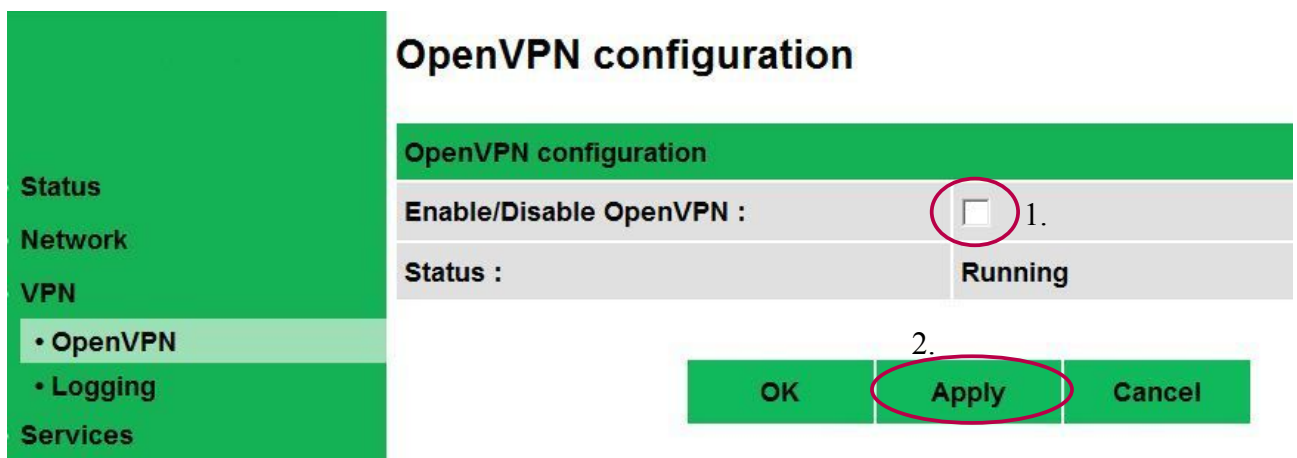
Authentication : p12-Certificate

P12-certificate : ISK-P2-NET5(10.2.132.0).p12 3. Info

Import p12-certificate : Durchsuchen... 4. Import

2. OK 5. Apply Cancel

Bild 3 OpenVPN deaktivieren



OpenVPN configuration

OpenVPN configuration

Enable/Disable OpenVPN : 1.

Status : Running

2. OK Apply Cancel