HowTo – OpenVPN Site-2-Site Static Key

Dieses Beispiel zeigt, wie zwei Netze via OpenVPN unter Verwendung eines Static Key miteinander verbunden werden, um beispielsweise eine **Außenstelle** an eine Firmenzentrale (**Zentrale**) anzubinden.

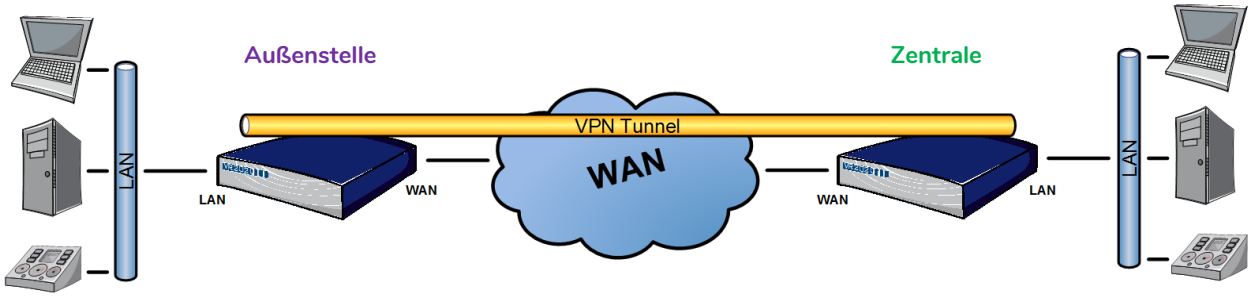

Abbildung 1: Netzplan-Beispiel

Hinweis

- In diesem Beispiel werden zwei VR2020 mittels **WAN**-Schnittstelle direkt miteinander verbunden. Die Verbindung kann natürlich auch über jeden anderen WAN-Weg etabliert werden, so sich die Geräte erreichen können.
- Außenstelle mit ***wechselnder IP*** an Schnittstelle **WAN** und ***192.168.1.50/24*** an **LAN**.
- Zentrale hat die IP ***10.99.99.1*** an Schnittstelle **WAN** und ***192.168.0.50/24*** an **LAN**.

1 Firewall der Zentrale anpassen

Um den Tunnelaufbau und die Datenkommunikation erfolgreich durchführen zu können ist vorab eine Änderung an der Firewall nötig. Diese wird im Menü ***Netzwerk > Firewall*** durchgeführt.

Hier wird auf den Tab **Verkehrsregeln** gewechselt und die bestehende OpenVPN-Regel aktiviert. Dazu wird bei dem Eintrag ***Allow-OpenVPN-Input*** das Häkchen in der Spalte **Aktivieren** gesetzt und die Änderung mit `Speichern & Anwenden` übernommen.

2 Static Key

2.1 Generieren des Key's

Der Key wird auf einem der beiden Router über die Kommandozeile erstellt. Dazu wird in der SSH-Session folgender Befehl ausgeführt:

```
openvpn --genkey --secret /etc/upload/shared-secret.key
```

2.2 Übertragen des Secret Key

Der neu erzeugte Secret Key wird über ein SCP-Programm, wie zum Beispiel WinSCP, auf den lokalen Rechner heruntergeladen.

Um den Key auf dem zweiten Gerät hochzuladen, kann das ***Datei-Upload*** Modul, zu finden unter System verwendet werden.

3 OpenVPN-Server-Konfiguration (Zentrale)

Auf der Konfigurationsseite **Dienste > OpenVPN** wird in dem Eingabefeld ein Name für den Tunnel eingegeben, im Dropdown daneben ***Simple server configuration for a routed point-to-point VPN*** ausgewählt und der Button **Hinzufügen** gedrückt. Die neu angelegte Instanz wird automatisch bearbeitend geöffnet.

3.1 Netzwerk Einstellungen

Hier werden die ***Erweiterten Einstellungen*** geöffnet und dort in die Kategorie **Networking** gewechselt. Im Dropdown **-- Zusätzliches Feld --** wird der Parameter ***route*** ausgewählt und mit **Hinzufügen** angehängt. Der neue Parameter **route** wird mit dem Netz der Außenstelle, im Beispiel ***192.168.1.0 255.255.255.0***, konfiguriert.

Zum Abschluss wird die Konfiguration mit **Speichern** erstellt.

4 OpenVPN-Client-Konfiguration (Außenstelle)

Um den Tunnel auf der Client-Seite hinzuzufügen, wird auf der Konfigurationsseite **Dienste > OpenVPN** im Eingabefeld ein Name für den Tunnel eingegeben, im Dropdown daneben ***Simple client configuration for a routed point-to-point VPN*** ausgewählt und der Button **Hinzufügen** gedrückt.

4.1 Gegenstelle definieren

Auf der sich öffnenden Dialogseite wird bei **remote** die **WAN** IP-Adresse der Zentrale, im Beispiel ***10.99.99.1***, eingegeben und die Konfiguration mit **Speichern** erstellt.

4.2 Netzwerk Einstellungen

Auch am Client werden die ***Erweiterten Einstellungen*** geöffnet und dort in die Kategorie **Networking** gewechselt. Hier wird der Parameter ***route*** ausgewählt im Dropdown **-- Zusätzliches Feld --** ausgewählt und mit **Hinzufügen** angehängt. Danach wird das getunnelte Netz der Zentrale, in diesem Beispiel ***192.168.0.0 255.255.255.0***, bei **route** eingetragen.

Im nächsten Schritt wird im Dropdown der Parameter ***keepalive*** ausgewählt und mit **Hinzufügen** für die Konfiguration übernommen. Die standardmäßig vordefinierten Werte **10 60** sollten für gängige Szenarien ausreichend sein.

Mit dem Button **Speichern** wird die Konfiguration übernommen.

5 Sicherheitseinstellungen

Grundsätzlich würde die vorhergehende Konfiguration für einen Tunnelaufbau schon ausreichen. Um die Datenkommunikation besser abzusichern, werden in den **Erweiterten Einstellungen** unter der Kategorie **Cryptography** noch Authentifizierungs- und Verschlüsselungsalgorithmen auf beiden Seiten (Außenstelle und Zentrale) definiert.

Dazu werden die folgenden Parameter ***auth*** und ***cipher*** hinzugefügt. Dabei wird **auth** mit dem Wert ***SHA256*** und **cipher** mit ***AES-128-CBC*** konfiguriert. Standardmäßig würde hier nur **SHA1** und **BF-CBC** verwendet werden.

6 OpenVPN-Tunnel starten

Um den OpenVPN-Tunnel aufzubauen wird zur **Übersicht** gewechselt und bei dem neu angelegten Tunnel das Häkchen bei **Einschalten** gesetzt.

Die Änderung wird dann durch Klicken auf **Speichern & Anwenden** übernommen. Dabei wird der Tunnel automatisch initiiert.