

Remote Client VPN Traffic zu anderen Standort mittel Site2Site VPN

Was wollen wir?

Wir wollen von einem Externen Netz mittels VPN zum Standort A verbinden und dort Geräte erreichen.

Weiteres besitzen wir einen Standort B welcher zu Standort A mittels Site2Site-VPN verbunden ist.

Wir möchten nun nicht immer mit dem Externen Gerät zum jeweiligen VPN Server des Standort A/B verbinden. sondern das Gerät immer auf Standort A verbinden und dort zum Standort B routen.

Was benötige ich?

Ich erstelle dieses Tutorial mit einer UDM-SE am Standort A sowie einer UDM-Pro am Standort B.

Derzeit wird noch die UDM-SE vorausgesetzt, damit man Wireguard als VPN-Server nutzen kann.

Sobald die UDM-Pro ebenfalls die Firmware v.3.x erhalten hat, kann man auch 2 oder mehr UDM-Pro nutzen.

Hintergrundwissen:

Standort A	Standort B
IP-Bereich: 10.0.0.0/24	IP-Bereich: 10.1.0.0/24
Dienste: Wireguard Client VPN OpenVPN Site2Site	Dienste: OpenVPN Site2Site

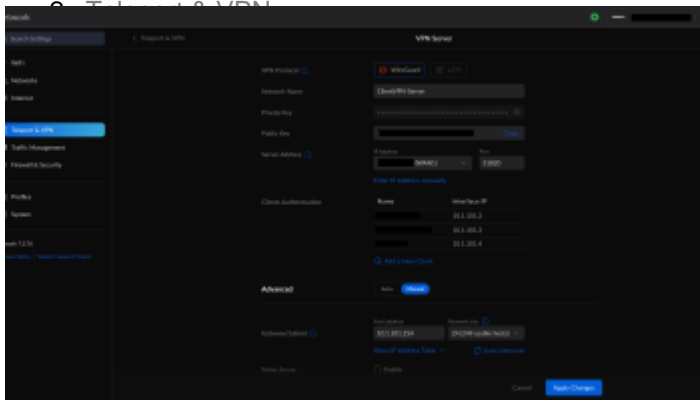
Und wie geht das genau?

Schritt 1:

- Wir erstellen ein Client-VPN um die externen Geräte ins "Heimnetz" zu lassen

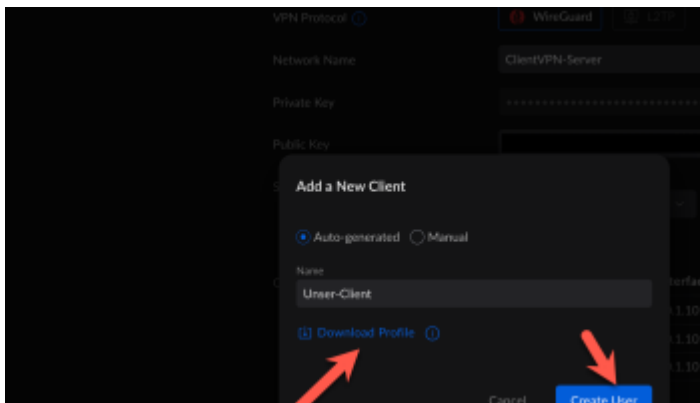
Wir loggen uns also nun in die Unifi-Oberfläche ein und wählen dort die UDM-SE von Standort A aus und begeben uns zu:

1. Settings



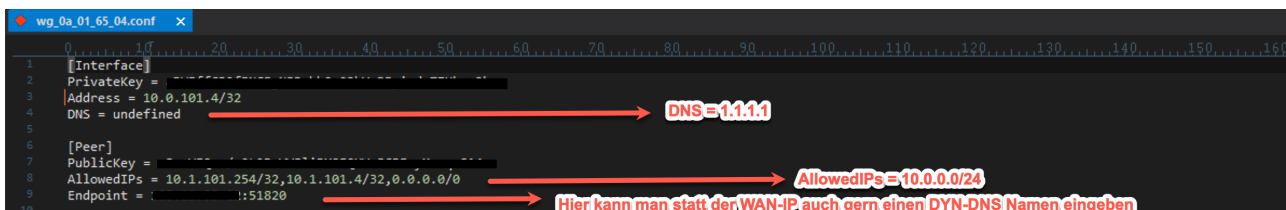
Wir tragen hier nun einen Namen für unseren

Server ein, sowie den IP-Bereich und legen Clients an.



Client anlegen und Profil downloaden

Da UniFi derzeit leider noch einen Fehler im Profil des Clients mit dem DNS - Server hat, müssen wir die heruntergeladene Datei/Profil nun öffnen und etwas editieren:



Hinweis:

Wir leiten mit meiner Konfiguration nur alle Anfragen welche auf die IP-Adressen 10.0.0.0 - 10.255.255.255 lauten durch den VPN-Tunnel.

Wer allen Traffic durch den VPN-Tunnel leiten möchte, muss bei AllowedIPs folgenden Eintrag hinterlegen:

AllowedIPs = 10.0.0.0/8, 0.0.0.0/0

Die Datei speichern wir nun ab und können diese im Wireguard-Client des Laptops importieren.

Somit ist die Konfiguration der Client VPN-Verbindung abgeschlossen und der Client kann sich nun in das Netz von Standort A verbinden und sollte auch alle Geräte erreichen.

Nun geht es weiter mit der Verbindung über Site2Site VPN von Standort A und Standort B

Standort A:

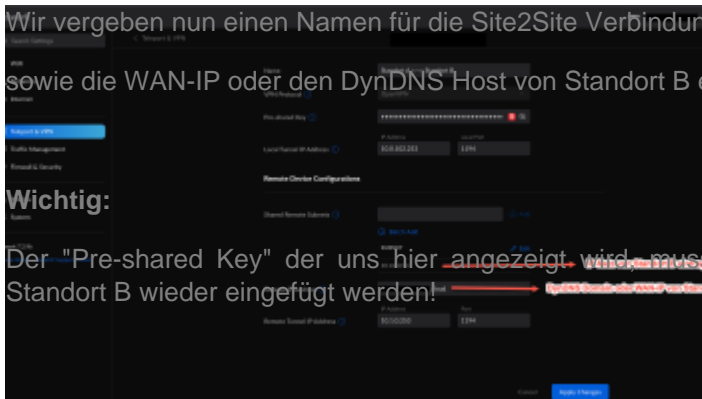
Wir befinden uns immer noch im Unifi Interface vom Standort A und gehen dort nun zum Menü:

1. Settings
2. Teleport & VPN
3. Create Site-to-Site VPN

Wir vergeben nun einen Namen für die Site2Site Verbindung und tragen die IP-Netze vom Standort B sowie die WAN-IP oder den DynDNS Host von Standort B ein

Wichtig:

Der "Pre-shared Key" der uns hier angezeigt wird, muss im nächsten Schritt bei der Konfiguration bei Standort B wieder eingefügt werden!

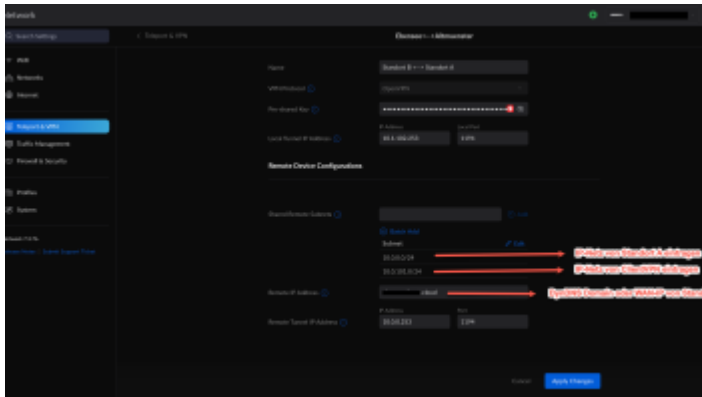


Standort B:

Nachdem wir die Site2Site VPN-Verbindung auf Standort A nun eingerichtet haben, müssen wir dasselbe nun noch für Standort B konfigurieren.

Wir wechseln deshalb nun in das Unifi Interface von Standort B und begeben uns dort wieder zum Menü:

1. Settings
2. Teleport & VPN
3. Create Site-to-Site VPN



Wir vergeben nun einen Namen für die Site2Site Verbindung und tragen die IP-Netze vom Standort A, der ClientVPN-Verbindung

sowie die WAN-IP oder den DynDNS Host von Standort A ein

Wichtig:

Wir setzen nun bei "Pre Shared Key" den kopierten Key von Standort A ein! Sonst kann keine Verbindung aufgebaut werden!

Nun sind wir auch schon Fertig! 😊

Wir sollten nun in der Lage sein, von einem Gerät was Extern über die Client-VPN Verbindung zum Standort A connected, alle Geräte von Standort A sowie auch Standort B erreichen.

Gruß,

RobotSox

Auswählen: _____
Gültige Software-Version Keine Firmware-Relevanz!