VPN ZWISCHEN FRITZBOX UND UBIQUITI UDM PRO (DREAM MACHINE) (STAND: 23.08.2024)

Inhaltsverzeichnis

Anleitungs-Update: 23.08.2024

> Zitat
> Haftungsausschluss
> Ich übernehme keine Haftung für Schäden an euren Systemen!
> Erfahrene Administratoren sollten diese Anleitung umsetzen.
> Anwendung auf eigene Verantwortung!

> Zitat
> Anschluss Voraussetzungen
> Um die Anleitung umsetzen zu können braucht ihr einen Internet Anschluss auf beiden Seiten mit richtiger Öffentlicher IP Adresse, DS-Lite Anschlüsse werden mit dieser Anleitung nicht unterstützt.
> Ebenfalls werden DynDNS sowie MyFritz Dienste benötigt. Die meisten DynDNS Dienste (mit Ausnahme von MyFritz Adressen) sind Kostenlos brauchen aber manuelle Reaktivierungen da diese nach 30-90 Tagen in der Regel "Ablaufen".

Basiseinstellung

VPN-Typ: IPSec

Name: Hier ein Beliebiger Name

Pre-Shared-Key: Gemeinsamer Schlüssel für die FritzBox und die UDM

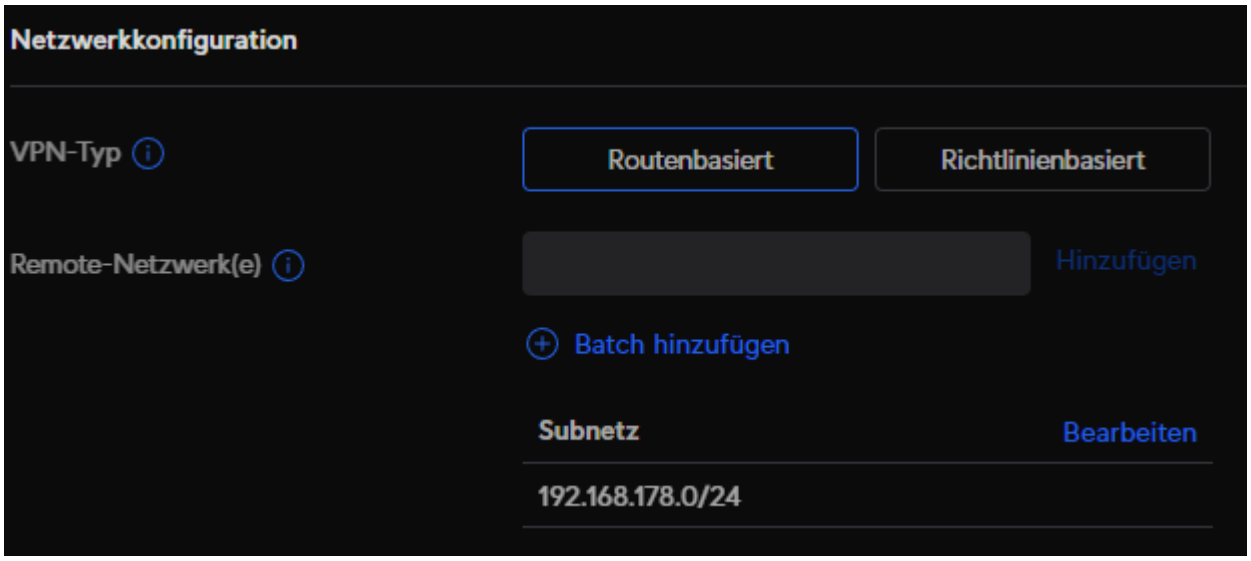
Lokale IP: Hier steht die Öffentliche IP Adresse deines Internet Providers

Remote IP / Host: Die Feste IP, FQDN oder die MyFritz Adresse der Gegenstelle/FritzBox

Netzwerkkonfiguration

VPN Typ: Routenbasiert

Remote Netzwerk(e): Lokales IP Netz der Fritzbox (Default: 192.168.178.0/24)



Erweiterte Einstellung

Erweitert: Manuell

Schlüsselaustausch Version: IKEv1

IKE:

Verschlüsselung: AES-256

Hash: SHA512

DH-Gruppe: 15

Lebenszeit: 28800

ESP:

Verschlüsselung: AES-256

Hash: SHA512

DH-Gruppe: 15

Lebenszeit: 28800

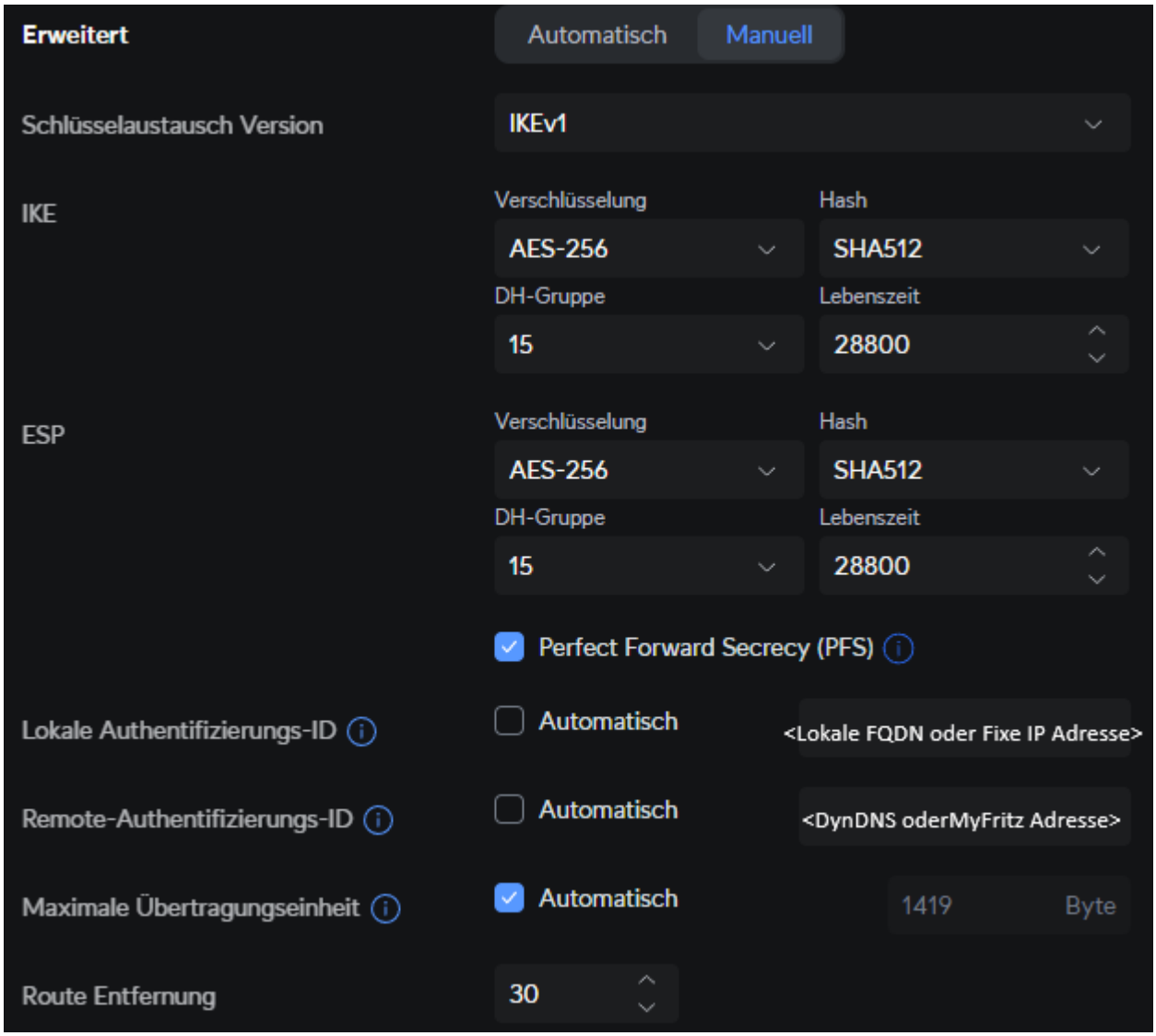
Perfect Forward Secrecy (SPF): Angehakt

> Zitat
> Verschlüsselung Hinweis
> Die hier in dem Artikel gezeigten Verschlüsselungsmethoden sind bereits die höchsten von der FritzBox unterstützten Technologien.

Lokale Authentifizierungs-ID - (Manuell: Haken Weg): <FQDN/DynDNS der UniFi UDM>

Remote-Authentifizierungs-ID- (Manuell: Haken Weg): <FQDN/MyFritz-Adresse der FritzBox>

Route Entfernung: 30



1 Voraussetzungen / Einschränkungen durch die FirtzBox

Quelle: https://avm.de/service/wissens…rmen-VPN-IPSec-verbinden/

Voraussetzungen / Einschränkungen

- Die FRITZ!Box unterstützt VPN-Verbindungen nach dem IPSec-Standard mit ESP, IKEv1 und Pre-Shared Keys. Authentication Header (AH) und Perfect Forward Security (PFS) werden nicht unterstützt.
- Unterstützte IPSec-Algorithmen für IKE-Phase 1:
  - Verschlüsselungsverfahren: AES mit 256, 192, 128 Bit, Triple-DES mit 168 Bit oder DES mit 56 Bit
  - Hash-Algorithmus: SHA2-512, SHA1 oder MD5-96
  - Die FRITZ!Box nutzt beim Schlüsselaustausch über Diffie-Hellman initial 1024 Bit (DH-Gruppe 2). Sie akzeptiert danach aber auch 768, 1536, 2048 und 3072 Bit (DH-Gruppe 1, 5, 14 und 15).
- Unterstützte IPSec-Algorithmen für IKE-Phase 2:
  - Verschlüsselungsverfahren: AES mit 256, 192, 128 Bit, Triple-DES mit 168 Bit oder DES mit 56 Bit
  - Hash-Algorithmus: SHA2-512, SHA1 oder MD5-96
  - Die Diffie-Hellman-Gruppe wird durch IKE-Phase 1 bestimmt
  - Kompression: keine

Diese Anleitung bezieht sich auf FRITZ!OS 7.28 oder neuer. Unter einem älteren FRITZ!OS kann die Einrichtung abweichen oder die Funktion nicht zur Verfügung stehen. Die FRITZ!OS-Version finden Sie in der Benutzeroberfläche auf der Seite "Übersicht".

2 Vorbereitung für der FritzBox:

Man erstellt ne neue Text Datei, Trägt meine Vorlage ein und Lädt diese in der FritzBox unter "Internet" ? "Freigaben" ? VPN (IPSec) als Config hoch:

Angepasst müssen Folgende werte:

Zeile 5, Zeile 7, Zeile 14, Zeile 16, Zeile 19, Zeile 24, Zeile 31-32, Zeile 37-38 und Zeile 42

Zeile 5: Name der VPN Verbindung der in der FirtzBox angezeigt wird.

Zeile 7: keepalive_ip = "<FQDN/DynDNS der UniFi UDM>"; *oder* keepalive_ip = <Ohne "" für Feste IP Adresse der UDM>;

Zeile 14: remotehostname = "<FQDN/DynDNS der UniFi UDM>";

Zeile 16: fqdn = "<FQDN/MyFritz-Adresse der FritzBox>";

Zeile 19: fqdn = "<FQDN/DynDNS der UniFi UDM>";

Zeile 24: key = "<Gemeinsamer Schluessel zwischen FritzBox und UniFi UDM>";

Zeile 31-32: IP Netz inkl. Subnet der FirtzBox

Zeile 37-38: IP Netz inkl. Subnet der UniFi UDM

Zeile 42: accesslist = "permit ip any <IP Netz der UDM> <Subnet, Beispiel: 255.255.255.0>";

VPN Config FritzBox Quelle erweitern

Code

```
vpncfg {

            keepalive_ip = "<Feste IP Adresse der UDM ohne "" oder FQDN/DynDNS der

    }

    }

            }
        }

            }
        }
accesslist="permitipany<IPNetzderUDM>255.255.255.0";
        }

}
//                                                                              EOF
```

Alles anzeigen

Config für das gleichzeitige Verbinden von 2 Netzwerken (Beispiel: LAN und vLAN gleichzeitig)

Hinweis: Wird nicht unbedingt von allen FritzBoxen unterstützt!

Code

```
vpncfg                                                                    {

keepalive_ip="<FesteIPAdressederUDMohne""oderFQDN/DynDNSderUniFiUDMmit"">";

                                                    remotehostname      =      "<FQDN/DynDNS
                                        fqdn         =         "<FQDN/MyFritz-Adresse         de
    }
                                                              fqdn        =        "<FQD
      }

            }
          }

            }{
                                                          ipaddr        =        <2tes
        }
          }
                                                                  phase2ss
accesslist="permitany<IPNetdeUDM>255.255.255.0"",permitany<2tesIPNetdeUDM>255.255.255.0";
          }
ike_forward_rules="udp0.0.0.0:5000.0.0.0:500","udp0.0.0.0:4500.0.0.0:4500";
    }
    // EOF
```

Alles anzeigen

Bekannte Probleme | FAQ:

Problem	Lösung

Verbindung wird nicht aufgebaut	1.) Für diese Lösung reicht ein Neustart der FritzBox. 2.) Prüfe die Parameter in der Konfiguration für die FritzBox. 3.) Der Verbindungsaufbau dauert in der Regel zwischen 5 und 10 Minuten je nach alter der FritzBox
Ich hab kein PING zur gegenstele	1.) Für diese Lösung reicht ein Neustart der FritzBox. 2.) Der Verbindungsaufbau dauert in der Regel zwischen 5 und 10 Minuten je nach alter der FritzBox 3.) Prüfe den "keepalive_ip" Parameter in dem VPN Konfiguration File und entferne diesen ggf. aus der Konfig
Das Gegenüber stehende Netz war kurz erreichbar und jetzt nicht mehr	1.) Für diese Lösung reicht ein Neustart der FritzBox. 2.) Deaktiviere und Aktiviere die IPSec VPN Konfiguration in der UDM 3.) Prüfe den "keepalive_ip" Parameter in dem VPN Konfiguration File und entferne diesen ggf. aus der Konfig
Ich hab die FritzBox und die UDM neu gestartet, aber es geht trotzdem nicht, was kann ich tun?	1.) Bitte achte da drauf ob du ein DS-Lite Anschluss hast, das erfährst du bei deinem Internet Anbieter. 2.) Prüfe auf mögliche Firewall Fehlkonfigurationen 3.) Ist die Konfiguration auf der FritzBox oder UDM Aktiviert? 4.) Prüfe den "keepalive_ip" Parameter in dem VPN Konfiguration File und entferne diesen ggf. aus der Konfig
Die Konfig lässt sich nicht in die FritzBox Importieren	1.) Entferne die komplette Zeile mit keepalive_ip = aus der Konfig und Probiere es erneut 2.) Überprüfe ob du dich nicht ggf. Vertippt hast. 3.) Wechsle mit Notepad++ unter “Bearbeiten” ? “Format Zeilenende” ? von “Windows (CR+LF)” zu “Unix (LF)” und speichere dies erneut ab.

Auswählen:

Gültige Software-Version Keine Firmware-Relevanz!