S2S VPN WireGuard (zwischen FritzBox und Firewall)

Einleitung

Dieses HowTo beschreibt die Konfiguration einer WireGuard Site-to-Site VPN-Verbindung einer Securepoint UTM mit einer Fritz!Box.

Schlüssel hinzufügen

Damit eine Kommunikation zwischen der UTM und der Fritz!Box möglich ist, sind folgende Schlüssel notwendig:

- Schlüssel vom Typ x25519 für die UTM
- x25519 Schlüssel für die Fritz!Box

Von beiden Schlüsseln wird der öffentliche und der private Teil benötigt.

Schlüssel hinzufügen			
Schlüsselverwaltung öffnen unter Authentifizierung Schlüssel Schaltfläche Schlüssel hinzufügen den Dialog öffnen			
Beschriftung	**Wert**	**Beschreibung**	Schlüssel hinzufügen UTMbenutzer@firewall.name.fqdnAuthentifizierungSchlüssel UTM v12.6 Schlüssel-Fritz!Box
Name:	x25519_a.vpn	Eindeutigen Namen vergeben Hier der Schlüsselname für die UTM	
Typ:	X25519	Als Typ **X25519** auswählen	
Dialog mit der Schaltfläche Speichern und schließen schließen.			
Fritz!Box-Schlüssel			

Den oben beschriebenen Vorgang für einen Schlüssel mit dem Namen **x25519_fritzbox-1** wiederholen.

- Den öffentlichen und privaten Teil des Schlüssel für die Fritz!Box **x25519_fritzbox-1** im *.raw*-Format exportieren
- Den Schlüssel **x25519_fritzbox-1** auf der UTM anschließend löschen

Schlüssel UTMbenutzer@firewall.name.fqdnAuthentifizierung
UTM v12.6 Schlüssel Fritzbox-
Der fertige Zustand beider Schlüssel

Auf die Schaltfläche Schlüssel importieren klicken und den **öffentlichen** Teil des Fritz!Box-Schlüssels importieren.

WireGuard-Verbindung hinzufügen

WireGuard-Konfiguration an der UTM

Unter VPN WireGuard auf die Schaltfläche WireGuard Verbindung hinzufügen klicken

Es wird empfohlen die WireGuard-Verbindung über die UTM zu erstellen. Daher sollte der **Schritt 1 - Konfiguration importieren** übersprungen werden.

Beschriftung	Wert	Beschreibung
Datei:	Datei auswählen	Falls die WireGuard-Verbindung über die Fritz!Box erstellt wurde, kann hier die entsprechende Konfigurationsdatei hochgeladen werden. Allgemein trägt die Konfigurationsdatei die Bezeichnung ***wg_config.conf***. Entsprechend wird unter Konfiguration: das Konfigurationsfeld ausgefüllt. • Falls mehrere Peers vorhanden sind, wird bloß der erste Peer übernommen.

WireGuard Verbindung hinzufügen UTMbenutzer@firewall.name.fqdnVPNWireGuard
UTM v12.6 VPN Wireguard Ste
WireGuard Assistent - Schritt 1

Konfiguration:		Falls eine WireGuard-Verbindung über die Fritz!Box erstellt wurde, kann die Konfiguration in dieses Konfigurationsfeld kopiert werden. • Falls mehrere Peers vorhanden sind, wird bloß der erste Peer übernommen. Vorlage einer Konfigurationsdatei zum kopieren

Beschriftung	Wert	Beschreibung
Schnittstelle:	wg1	Name der Schnittstelle, die für die Verbindung angelegt wird (automatische Vorgabe, kann nicht geändert werden)
Name:	wg_s2s_fritzbox	Eindeutiger Name für die Verbindung
IPv4 Adresse:	10.0.0.1/24	IPv4 Adresse für die Netzwerkschnittstelle des Transfernetzes der UTM
IPv6 Adresse:		IPv6 Adresse für die Netzwerkschnittstelle des Transfernetzes der UTM (optional)
Listening Port:	51820Link=	Default-Port für WireGuard Verbindungen
Privater Schlüssel:		
Aus Schlüsseln wählen	x25519_a.vpn	Privater Schlüssel der UTM im Format x25519. Es sind nur solche Schlüssel auswählbar, die auch über einen privaten Schlüsselteil verfügen.
Servernetzwerke global freigeben:		Zusätzliche Netzwerke für die (lokale) Serverseite, auf die der WireGuard-Tunnel der Peers zugreifen können

UTM 12.6 VPN Wireguard Schr

WireGuard Assistent - Schritt 2

Verwende AD Benutzer als Peers:	Aus	Die Verwendung An von AD Benutzern als Peer wird dann empfohlen, wenn diese mit einem AD/LDAP-Server vebunden sind und diese die richtigen Attributseinstellungen vorweisen. Weiterhin muss eine Benutzergruppe auf der UTM mit einer Benutzergruppe im AD/LDAP verknüpft sein und diese die WireGuard-Berechtigung besitzen. Weitere Informationen sind im Wiki-Artikel AD/LDAP-Anbindung zu finden.	UTM 12.6 VPN Wireguard Schr WireGuard Assistent - Schritt 3
Name:	wg_peer_fritzbox-1	Bezeichnung der Gegenstelle für die Fritz!Box	
Peernetzwerke freigeben:	»192.168.178.1/24	Das interne Netz der Fritz!Box, auf das zugegriffen werden soll	
Endpunkt:	d-vpn.spdns.org	Öffentliche DNS auflösbarer FQDN der Fritz!Box	
Endpunkt Port:	51820Link=	Der Listening Port der Fritz!Box	
Öffentlicher Schlüssel:			
Aus Schlüsseln wählen	x25519_fritzbox-1_pub_b64	Den öffentlichen Schlüsselteil der Fritz!Box auswählen • Öffentlicher Schlüssel vorhanden, aber nicht auswählbar? Hinweis anzeigen	
Pre-Shared Key (optional):	…8DmBioPyPNqZ7Rk=	Pre-Shared Key zur weiteren Absicherung der Verbindung	
	Anzeigen Verbergen	Zeigt / Verbirgt den Pre-Shared Key	

Generieren	Erzeugt einen sehr starken Pre-Shared Key • Der Pre-Shared Key muss an beiden Enden der VPN-Verbindung identisch sein!	
In die Zwischenablage kopieren	Kopiert den PSK in die Zwischenablage	
Keepalive:	Aus	Sendet regelmäßig ein Signal. Dadurch werden Verbindungen auf NAT-Routern offen gehalten. Ein Die Aktivierung wird empfohlen.
	25Link= Sekunden	Abstand in Sekunden, in dem ein Signal gesendet wird

Routen zu den Netzwerken des Peers erstellen:	Nein	Aktivierung wird empfohlen. Es werden Routen zu den Netzwerken / Hosts erstellt, die in Schritt 3 unter *Erlaubte IPs* eingetragen wurden mit der Schnittstelle als Gateway, die in Schritt 2 angezeigt wurde.	UTM 12.6 VPN Wireguard Schr WireGuard Assistent - Schritt 4
Zonen erstellen:	Ja	Erzeugt eine neue Zone für die WireGuard Schnittstelle	
Zonenname:	wireguard-wg0-1	Einen Namen für die Zone eintragen	
Netzwerkobjekte für den Peer erstellen:	Ja »wg_peer_fritzbox-1-0	Erzeugt bei Aktivierung Ja Netzwerkobjekte (IPv4 und ggf. IPv6) für die Gegenstelle. Der automatische Vorschlag kann auch geändert werden.	

Regeln zwischen dem Peer und internal-networks erstellen:	Nein	Erzeugt bei Aktivierung autogenerierte Regeln, die die Inbetriebnahme erleichtern. Diese Regeln müssen unbedingt durch eigene Regeln, die nur notwendige Dienste mit notwendigen Netzwerkobjekten erlauben, ersetzt werden.
Mit der Schaltfläche Fertig werden die Einstellungen übernommen.		
Anschließend wird über die Schaltfläche Neustarten Neustarten der WireGuard-Dienst neu gestartet.		

WireGuard-Konfiguration an der Fritz!Box

Den öffentlichen Teil des Schlüssels der UTM **x25519_a.vpn** im *.raw*-Format exportieren.

Eine Konfigurationsdatei mit folgendem Inhalt wird erstellt. Dazu wird eine Datei in einem beliebigem Editor geöffnet.

```
[Interface]
PrivateKey = $PRIVATE_KEY_FRITZBOX
ListenPort = $LISTENPORT_WIREGUARD_FRITZBOX
Address = $LOCAL_IP_FRITZBOX/$NETMASK

[Peer]
PublicKey = $PUBLIC_KEY_UTM
PresharedKey = $PRESHAREDKEY
AllowedIPs = $NETWORK_SECUREPOINT/$NETMASK
Endpoint = $HOSTNAME_UTM:$LISTENPORT_WIREGUARD_UTM
PersistentKeepalive = 1
```

Beschriftung	Wert	Beschreibung	FRITZ!Box-7590 VPN WireGua
PrivateKey =	$PRIVATE_KEY_FRITZBOX	*Private Key* aus dem heruntergeladenem Schlüssel eintragen	Beispiel solch einer Konfigurationsdatei
ListenPort =	$LISTENPORT_WIREGUARD_FRITZBOX	ListenPort der Fritz!Box eintragen Im Beispiel *51378*	

Address =	$LOCAL_IP_FRITZBOX/$NETMASK	Statische IP-Adresse der Fritz!Box im internem Netzwerk mit Netzmaske eintragen Im Beispiel *192.168.178.1/24*
PublicKey =	$PUBLIC_KEY_UTM	Den heruntergeladenem public Key der UTM eintragen
PresharedKey =	$PRESHAREDKEY	Den preshared Key der UTM eintragen
AllowedIPs =	$NETWORK_SECUREPOINT/$NETMASK	Internes Netzwerk / interne Netzwerke / Transfernetzwerk der Securepoint eintragen Im Beispiel 10.0.0.0/24 (aus Schritt 2 - IPv4 Adresse) Mehrere IP-Adressen sind durch ein Komma zu trennen. Beispiel: IPv4 Adresse: 10.0.1.0/24,10.0.2.0/24
Endpoint =	$HOSTNAME_UTM:$LISTENPORT_WIREGUARD_UTM	Hostname der UTM und Endpoint der UTM (aus Schritt 2 - Schnittstelle) eintragen. Beides durch einen Doppelpunkt trennen.
PersistentKeepalive =	1	Abstand in Sekunden, in dem ein Signal gesendet wird (aus Schritt 3 - Peer) Im Beispiel *25*
Falls etwas an der Konfigurationsdatei geändert wird, kann es vorkommen, dass die Fritz!Box die geänderte Konfiguration nicht sofort akzeptiert. Ein Neustart der Fritz!Box ist dann notwendig.		

Im Interface der Fritz!Box anmelden und unter Internet → Freigaben→ Reiter VPN (WireGuard) wechseln.
Dort auf Verbindung hinzufügen klicken.

FRITZ!Box-7590 VPN Wireguard Schritt1.png
Abb.1
Im neuem Fenster auf Benutzerdefinierte Einrichtung klicken und dann auf Weiter >.
FRITZ!Box-7590 VPN Wireguard Schritt2.png
Abb.2
Bei der Frage unter *Benutzerdefinierte Einstellungen festlegen* auf Ja klicken und anschließend auf Weiter >.
FRITZ!Box-7590 VPN Wireguard Schritt3.png

Abb.3

Bei *Name der WireGuard-Verbindung* einen Namen eintragen und über Durchsuchen... die erstellte Konfiguationsdatei auswählen. Dann auf Fertigstellen klicken.

Ggf. kann die Aktivierung der Option *NetBIOS über diese Verbindung zulassen* Probleme z.B. mit SMB oder FTP beheben.

Nach dem automatischem Wechsel auf den Dialog VPN (WireGuard) wird auf Aktualisieren geklickt und die WireGuard-Verbindung ist aktiv.

Sollte unter anderem beim Hochladen der Konfigurationsdatei ein Fehler auftreten, wird unter System → Ereignisse die entsprechende Fehlermeldung angezeigt.

Revision #4
Created 3 December 2024 15:43:05 by Moritz Sarcher
Updated 3 December 2024 15:47:08 by Moritz Sarcher