

Einrichtung des VPN-Clients zum Standort auf USG / ZyWall-Geräten

 support.zyxel.eu/hc/de/articles/360001378833-Einrichtung-des-VPN-Clients-zum-Standort-auf-USG-ZyWall-Geräten

VPNs sind eines der Haupt Konfigurations-Setups auf unseren Geräten. Neben dem üblichen Site-to-Site-Setup können Sie auch Mobilität gewähren, während Sie mit Ihrem Standort verbunden sind, indem Sie einen Client-to-Site konfigurieren. In diesem Handbuch zeigen wir Ihnen, wie Sie dieses spezielle Szenario mit dem ZyWall IPSec VPN-Client einrichten!

Exemplarische Vorgehensweise

Bitte beachten Sie: Alle folgenden Schritte beziehen sich nur auf IKEv1!

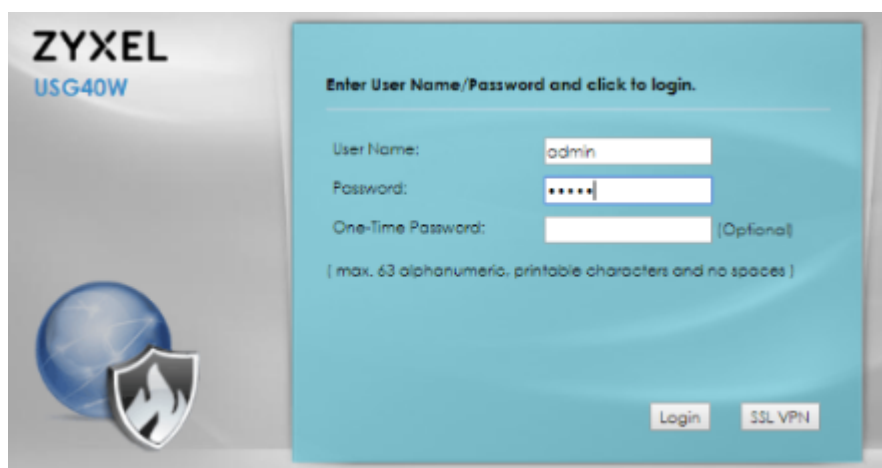
1. VPN Gateway (Phase 1)

2. Konfigurieren des Zyxel IPsec VPN-Clients

3. Anmerkungen

1. VPN Gateway (Phase 1):

1. Melden Sie sich am Gerät an, indem Sie seine IP-Adresse und die Anmeldeinformationen für ein Administratorkonto eingeben (standardmäßig lautet der Benutzername „admin“, das Kennwort lautet „1234“).



2. Fügen Sie unter ein neues VPN-Gateway hinzu:

Konfiguration> VPN> IPSec VPN> VPN Gateway

Bearbeiten Sie die folgenden Einstellungen:

"Show Advanced Settings" (Erweiterte Einstellungen anzeigen), Häkchen bei "Enable" (Aktivieren) setzen, den gewünschten Namen eingeben, die gewünschte WAN-Schnittstelle als "My Address" (Meine Adresse) auswählen, "Dynamic Address for multiple IPs" (Dynamische Adresse für mehrere IPs) markieren und einen Pre-Shared-Schlüssel eingeben.

Add VPN Gateway

Hide Advanced Settings

General Settings

☒ Enable

VPN Gateway Name:

Gateway Settings

My Address

☒ Interface DHCP client -- 192.168.2.107/255.255.255.0

☐ Domain Name / IP

Peer Gateway Address

☐ Static Address Primary Secondary

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: (60-86400 seconds)

☒ Dynamic Address

Authentication

☒ Pre-Shared Key

3. In dieser Anleitung werden die Einstellungen für Phase 1 standardmäßig beibehalten. Sie können diese jedoch auch an Ihre Sicherheitseinstellungen anpassen. Konfigurieren Sie dann den „Negotiation Mode“ auf „Main“.

Phase 1 Settings

SA Life Time: (180 - 3000000 Seconds)

Negotiation Mode:

Proposal

#	Encryption	Authentication
1	DES	MD5

Klicken Sie auf "OK", um die vorgenommenen Änderungen zu übernehmen.

VPN-Verbindung (Phase 2):

1. Navigieren Sie zur Registerkarte „VPN-Verbindung“ und fügen Sie eine neue Verbindung hinzu

Bearbeiten Sie die folgenden Einstellungen:

"Erweiterte Einstellungen anzeigen", Häkchen bei "Aktivieren", gewünschten Namen eingeben, "Anwendungsszenario" auf "Remote-Zugriff (Serverrolle)" setzen und das zuvor erstellte VPN Gateway auswählen

Add VPN Connection

Hide Advanced Settings Create new Object

General Settings

☒ Enable

Connection Name:

☐ Nailed-Up

☐ Enable Replay Detection

☐ Enable NetBIOS broadcast over IPSec

MSS Adjustment

☐ Custom Size (200 - 1460 Bytes)

☒ Auto

VPN Gateway

Application Scenario

☐ Site-to-site

☐ Site-to-site with Dynamic Peer

☒ Remote Access (Server Role)

☐ Remote Access (Client Role)

VPN Gateway: wan1 0.0.0.0 0.0.0.0

2. Wählen Sie unter "Lokale Richtlinie" das Subnetz Ihrer USG aus, auf das die VPN-Clients Zugriff haben sollen. Wählen Sie Ihre gewünschten Vorschläge in den „Phase 2-Einstellungen“ aus und klicken Sie auf „OK“ (erinnern Sie sich daran, so viel wie möglich zu sichern).

Policy

Local policy: INTERFACE SUBNET, 192.168.10.0/24

Phase 2 Setting

SA Life Time: (180 - 3000000 Seconds)

Active Protocol:

Encapsulation:

Proposal

#	Encryption	Authentication
1	DES	SHA1

Perfect Forward Secrecy (PFS):

2. Konfigurieren des ZyWall IPSec VPN-Clients:

1. Die aktuellste Software finden Sie [hier](#)

2. Starten Sie die Software und definieren Sie die Ports in den „IKE V1-Parametern“ (IKE Port = 500, NAT-T-Port = 4500).

The screenshot shows the 'VPN Konfiguration' window with the 'Allgemein' tab selected. The left sidebar shows a tree structure: 'IKE V1' (containing 'Allgemein', 'Ikev1Gateway', and 'Ikev1Tunnel') and 'IKE V2' (containing 'Ikev2Gateway'). The main area displays the following settings:

Lebensdauer (Sek.)			
	Standard	Minimal	Maximal
Authentisierung (IKE)	1800	360	28800
Verschlüsselung (IPsec)	1200	300	28800

☒ **Dead Peer Detection (DPD)**

Intervall (Sek.) Sek.

Max. Wiederholungen

Pause zw. Wiederholungen Sek.

Verschiedenes

Wiederholungen IKE Port

X-Auth Timeout NAT Port

☐ Split Tunnel deaktivieren

3. Geben Sie im Feld „Ikev1Gateway“ die IP-Adresse der USGs-WAN-Schnittstelle ein und geben Sie den Pre-Shared-Key ein. Stellen Sie sicher, dass die Einstellungen mit denen übereinstimmen, die Sie in Ihrem VPN Gateway in Ihrer USG definiert haben.

The screenshot shows the 'VPN Konfiguration' window with the 'Erweiterte Einstellungen' tab selected. The left sidebar shows the tree structure: 'IKE V1' (containing 'Allgemein', 'Ikev1Gateway', and 'Ikev1Tunnel') and 'IKE V2' (containing 'Ikev2Gateway'). The main area displays the following settings:

Adressen

Netzwerk Interface

Remote VPN Gateway

Authentisierung

☒ Preshared Key

Bestätigen

☐ Zertifikat

IKE

Verschlüsselung

Authentisierung

Key Gruppe

4. Konfigurieren Sie nun den VPN-Tunnel: Belassen Sie die „VPN-Client-Adresse“ auf 0.0.0.0 oder geben Sie eine IP-Adresse ein, die nicht lokal mit einem Netzwerk in der USG übereinstimmt. Geben Sie die Subnetzadresse ein, die Sie in Ihren USGs als lokale Richtlinie definiert haben VPN-Verbindung und stellen Sie sicher, dass die Vorschläge mit denen der USG übereinstimmen.

Nun sollten Sie in der Lage sein, den VPN-Tunnel zu öffnen, indem Sie mit der rechten Maustaste auf den VPN-Tunnel links klicken und "Tunnel öffnen" auswählen. Eine grüne Desktop-Benachrichtigung in der rechten unteren Ecke sollte die erfolgreich hergestellte VPN-Verbindung bestätigen.

Beachten Sie, dass Ihre WAN-to-ZyWall Firewall-Regel die Dienste ESP, IKE und NATT zulassen sollten!



Weitere Informationen zu den VPN-Einstellungen und -Algorithmen finden Sie unter:

http://www.zyxel-tech.de/previews/zyw7ow362wmoco/h_vpn_rules_edit_adv.html

Informationen zum Einrichten einer L2TP-Verbindung unter Windows 10 finden Sie unter:

<https://www.youtube.com/watch?v=BYxcjcOxybs>

3. Bitte beachten Sie:

- Testen Sie die VPN-Verbindung nicht im selben Subnetz wie Ihre lokale Richtlinie! Dies führt zu Routingproblemen.

- Sie können die Konfigurationsdatei des IPSec-Clients exportieren und auf verschiedenen Computern bereitstellen.
- Wenn sich Ihr VPN-Tunnel nicht aufbaut, obwohl nach Ihrem Kenntnisstand alles korrekt eingerichtet wurde, blockiert Ihr ISP möglicherweise IKE (Port 500) oder NAT-T (Port 4500). Bitte wenden Sie sich an Ihren ISP, um dies zu klären.
- Wenn kein IPSec-bezogener Datenverkehr auf Ihre WAN-Schnittstelle trifft, blockiert der ISP möglicherweise ESP (Protokoll 50). Bitte wenden Sie sich an Ihren ISP, um dies zu klären.

Copyright © 2021 - Zyxel Support Campus EMEA. Alle Rechte vorbehalten..