

L2TP VPN Roadwarrior

In diesem HowTo wird beschrieben wie Sie eine L2TP (Pre-Shared Key) Verbindung zwischen einem Windows XP / 7 / 8 Client und einem Gatedefender der eSeries herstellen können.

1.) IPSec aktivieren

OpenVPN Server

OpenVPN Client (Gw2Gw)

IPSec/L2TP

VPN Benutzer

>> IPSec L2TP

>> Globale Einstellungen

Aktiv

⊕ Debug Optionen

* Dieses Feld kann leer bleiben

Speichern

>> Verbindungsstatus und -kontrolle

Name	Typ	Gemeinsamer Name	Anmerkung	Status	Aktionen
Hinzufügen					

>> Zertifizierungsstellen

Name	Betreff	Aktionen
Root Zertifikat:	Nicht vorhanden	
Host Zertifikat:	Nicht vorhanden	

Root/Host Zertifikate erstellen

CA Name:

2.) L2TP aktivieren

System Status Netzwerk Dienste Firewall Proxy VPN Hotspot Protokolle

L2TP

OpenVPN Server

OpenVPN Client (Gw2Gw)

IPSec/L2TP

VPN Benutzer

>> IPSec L2TP

L2TP aktivieren

Zone * GREEN

Startadresse des L2TP IP Bereichs

Endadresse des L2TP IP Bereichs

Debugmodus aktivieren

Speichern

* Dieses Feld wird benötigt.

In dem Feld „Startadresse...“ und „Endadresse...“ geben Sie bitte einen freien IP Range aus Ihrem lokalem Netz an. Liegt Ihr Netz z.B. im Range 192.168.1.X wird in den Feldern z.B. 192.168.1.250 – 192.168.1.254 eingetragen. Aus diesem Pool weist der Gatedefender dem Client eine IP Adresse zu.

3.) L2TP Tunnel erstellen

OpenVPN Server	>> IP Sec	L2TP
OpenVPN Client (Gw2Gw)	>> Globale Einstellungen	
IP Sec/L2TP		
VPN Benutzer		

Aktiv

Debug Optionen
* Dieses Feld kann leer bleiben Speichern

>> Verbindungsstatus und -kontrolle

Name	Typ	Gemeinsamer Name	Anmerkung	Status	Aktionen
Hinzufügen					

>> Zertifizierungsstellen

Name	Betreff	Aktionen
Root Zertifikat:	Nicht vorhanden	
Host Zertifikat:	Nicht vorhanden	

Root/Host Zertifikate erstellen

CA Name: Durchsuchen... CA Zertifikat hochladen

OpenVPN Server	>> IP Sec	L2TP
OpenVPN Client (Gw2Gw)	>> Verbindungstyp	
IP Sec/L2TP		
VPN Benutzer		

Verbindungstyp:

- Host-to-Net Virtual Private Network (Roadwarrior)
- Netz-zu-Netz Virtual Private Network
- L2TP Host-to-Net Virtual Private Network (Roadwarrior mit L2TP)

Hinzufügen

4.) L2TP Tunnel einrichten

The screenshot shows the 'Verbindungskonfiguration' (Connection Configuration) page for an L2TP tunnel. The left sidebar contains a menu with 'IPSec/L2TP' selected. The main area has the following fields:

- Name: [Empty text box]
- Lokal: [Empty text box]
- Schnittstelle: Uplink main (dropdown menu)
- Lokales Subnetz: 192.168.160.0/24
- Lokale ID: [Empty text box]
- ID der Gegenseite: [Empty text box]
- Aktiv:
- Gegenstelle: [Empty text box]
- Gegenstelle Host/IP: [Empty text box]
- Optionen: Aktion bei Dead Peer Erkennung: Säubern (dropdown menu)
- Anmerkung: [Empty text box]
- Erweiterte Einstellungen bearbeiten

In dem Feld „lokales Subnetz“ muss der IP Range des lokalen Netzwerks eingetragen werden in diesem Beispiel ist es z.B. 192.168.160.0/24

The screenshot shows the 'Anmeldung' (Authentication) page. The first radio button is selected and highlighted in yellow:

- Einen Pre-Shared-Key verwenden: [Empty text box]
- Eine Zertifikatsanfrage hochladen: [Empty text box] [Durchsuchen...]
- Ein Zertifikat hochladen: [Empty text box]
- PKCS12 Datei hochladen Passwort der PKCS12 Datei: [Empty text box]
- Peer wurde durch IPV4_ADDR, FQDN, USER_FQDN oder DER_ASN1_DN im Remote ID Feld identifiziert
- Generiere ein Zertifikat:
 - Vollständiger Name des Benutzers oder Hosts: [Empty text box]
 - E-Mail-Adresse des Benutzers: [Empty text box]
 - Abteilung des Benutzers: [Empty text box]
 - Name der Organisation: [Empty text box]
 - Stadt: [Empty text box]
 - Land oder Provinz: [Empty text box]
 - Staat: Afghanistan (dropdown menu)
 - Betreffzeile (subjectAltName=email:*,URI:*,DNS:*,RID:*): [Empty text box]
 - Passwort der PKCS12 Datei: [Empty text box]
 - Passwort der PKCS12 Datei:(Bestätigung) [Empty text box]

Tragen Sie in dem Feld „Pre-Shared Key“ bitte einen Schlüssel ein, dieser Schlüssel wird für Herstellung der VPN Verbindung benötigt (siehe Client Konfiguration)

5.) L2TP Tunnel fertig eingerichtet

Bitte drauf achten das der Hacken bei „Aktiv“ gesetzt ist

System Status Netzwerk Dienste Firewall Proxy VPN Hotspot Protokolle

Virtuelles Privates Netzwerk

- OpenVPN Server
- OpenVPN Client (Gw2Gw)
- IP Sec/L2TP**
- VPN Benutzer

>> IP Sec L2TP

>> Globale Einstellungen

Aktiv

Debug Optionen

* Dieses Feld kann leer bleiben

Speichern

>> Verbindungsstatus und -kontrolle

Name	Typ	Gemeinsamer Name	Anmerkung	Status	Aktionen
test	L2TP (PSK)			BEENDET	

Legende: Aktiviert (klicken, um zu deaktivieren) Zertifikat anzeigen Bearbeiten Löschen

Deaktiviert (klicken, um zu aktivieren) Zertifikat herunterladen Neu starten

Hinzufügen

>> Zertifizierungstellen

Name	Betreff	Aktionen
Root Zertifikat:	Nicht vorhanden	
Host Zertifikat:	Nicht vorhanden	

Root/Host Zertifikate erstellen

CA Name:

Das Zurücksetzen der VPN-Konfiguration wird die Root-CA, das Host-Zertifikat und alle weiteren Zertifikate sowie alle zertifikatsbasierten Verbindungen entfernen

Zurücksetzen

6.) VPN User anlegen

OpenVPN Server

OpenVPN Client (Gw2Gw)

IPSec/L2TP

VPN Benutzer

»

Benutzer hinzufügen

Name *
test

Passwort

Passwort bestätigen

Aktiviert

Anmerkung

VPN Protokolle

OpenVPN

L2TP

▼ L2TP Optionen

IPsec Tunnel
test

or * Dieses Feld wird benötigt.

An erster Stelle Vorherig Nächste An letzter Stelle Suche:

<input type="checkbox"/>	Name	Anmerkung	Protokolle	Netzwerke	Status	Aktionen
Keine Einträge zur Ansicht						

7.) VPN User fertig eingerichtet

OpenVPN Server

OpenVPN Client (Gw2Gw)

IPSec/L2TP

VPN Benutzer

»

[Neuen Benutzer hinzufügen](#)

An erster Stelle Vorherig 1 Nächste An letzter Stelle Suche:

<input type="checkbox"/>	Name	Anmerkung	Protokolle	Netzwerke	Status	Aktionen
<input type="checkbox"/>	test		L2TP		Getrennt	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

8.) Konfiguration VPN Verbindung auf dem Client



Wählen Sie eine Verbindungsoption aus:

-  **Verbindung mit dem Internet herstellen**
Richtet eine Drahtlos-, Breitband- oder Wählverbindung mit dem Internet ein.
-  **Ein neues Netzwerk einrichten**
Konfiguriert einen neuen Router oder Zugriffspunkt.
-  **Verbindung mit dem Arbeitsplatz herstellen**
Richtet eine Einwähl- oder VPN-Verbindung mit dem Arbeitsplatz ein.
-  **Wählverbindung einrichten**
Stellt die Verbindung mit dem Internet über eine Wählverbindung her.

Weiter

Abbrechen



Möchten Sie eine bestehende Verbindung verwenden?

- Nein, eine neue Verbindung erstellen**
- Ja, eine bestehende Verbindung auswählen

Weiter

Abbrechen

Wie möchten Sie eine Verbindung herstellen?

- **Die Internetverbindung (VPN) verwenden**
Verbindung über ein VPN-Netzwerk (VPN=Virтуelles privates Netzwerk) durch das Internet herstellen.



- **Direkt wählen**
Direkte Verbindung durch Wählen einer Telefonnummer herstellen, ohne das Internet zu verwenden.



[Was ist eine VPN-Verbindung?](#)

Abbrechen

Geben Sie die Internetadresse zum Herstellen einer Verbindung ein.

Diese Adresse können Sie vom Netzwerkadministrator erhalten.

Internetadresse:

Zielname:

- Eine Smartcard verwenden
- Anderen Benutzern erlauben, diese Verbindung zu verwenden
Erlaubt jedem, der Zugang zu diesem Computer hat, diese Verbindung zu verwenden.
- Jetzt nicht verbinden, nur für spätere Verwendung einrichten

Weiter

Abbrechen

Geben Sie den Benutzernamen und das Kennwort ein.

Benutzername:

Kennwort:

Zeichen anzeigen

Dieses Kennwort speichern

Domäne (optional):

Erstellen

Abbrechen

Eigenschaften von Test L2TP

Algemein | Optionen | Sicherheit | Netzwerk | Freigabe

VPN-Typ:
Automatisch

Datenverschlüsselung:
Erforderlich (Verbindung trennen, falls Server dies ablehnt)

Authentifizierung

Extensible-Authentication-Protokoll (EAP) verwenden

Folgende Protokolle zulassen
EAP-MSCHAPv2 wird für den IKEv2 VPN-Typ verwendet.
Wählen Sie eines dieser Protokolle für andere VPN-Typen aus.

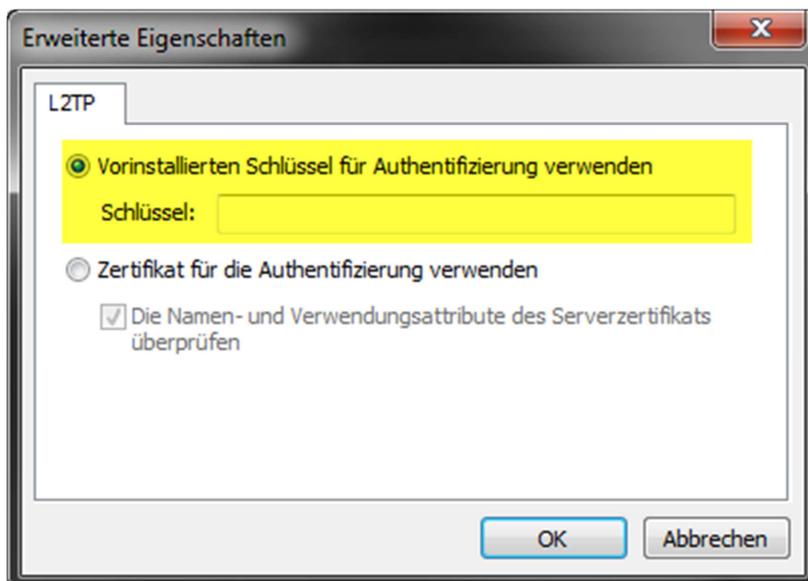
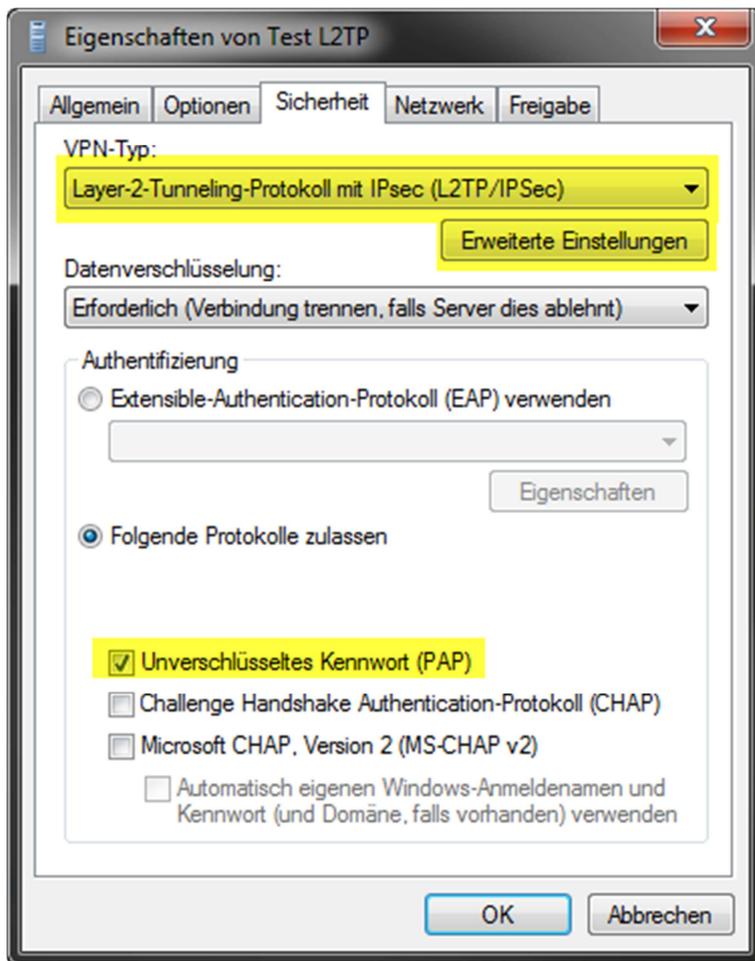
Unverschlüsseltes Kennwort (PAP)

Challenge Handshake Authentication-Protokoll (CHAP)

Microsoft CHAP, Version 2 (MS-CHAP v2)

Automatisch eigenen Windows-Anmeldenamen und Kennwort (und Domäne, falls vorhanden) verwenden

Die standard VPN Einstellungen müssen wie folgt angepasst werden:



In dem Feld „Schlüssel“ tragen Sie bitte den zuvor konfigurierten Pre-Shared Key ein.