

VPN Verbindung Draytek

NCP Clientsoftware (Lancom) zu
Draytek Vigor VPN Router

Hier beschreiben wir die Einrichtung einer VPN Verbindung über IPsec von einem NCP Client zu einem Draytek Vigor Router mit VPN Unterstützung.

Als zweites schauen wir uns die Konfiguration des Draytek Routers an:

1. Als erstes müssen wir ein Einwahlprofil für einen Benutzer einrichten. Hierzu klicken Sie auf der linken Seite auf das Menü „**VPN und externe Einwahl**“ und dort ins Untermenü „**IPsec-Konfiguration**“
2. Hier legen wir einen Pre-Shared-Key an. Dieser kann und sollte Ein Mix aus Buchstaben, Zahlen und Sonderzeichen enthalten. Diesen Kes müssen sie wiederholen, damit dieser auch Identisch ist. Je umfangreicher der Key, desto sicherer die Verbindung. Den Key müssen Sie sich notieren, da dieser bei der Clientkonfiguration später wieder benötigt wird. Alle anderen Einstellungen für die IPsec-Verbindung entnehmen Sie dem Bild unten. Wenn alle Einstellungen getätigt wurden, klicken Sie auf OK.

VPN-IKE/IPsec-Konfiguration
Einwahl-Einstellungen für externe Benutzer oder LAN-zu-LAN-Clients mit dynamischen IPs

IKE-Authentifizierungsmethode	
Einwahl-Zertifikat	Ohne ▼
Pre-Shared-Key	
Pre-Shared-Key	
Pre-Shared-Key bestätigen	
IPsec-Sicherheitsmethode	
☒ Mittel (AH) Daten werden authentifiziert, aber nicht verschlüsselt.	
☐ Hoch (ESP) ☒ DES ☒ 3DES ☒ AES Daten werden sowohl authentifiziert als auch verschlüsselt.	

OK Abbrechen

3. Nun wechseln Sie im Linken Menü auf „Externe Benutzer“. Hier müssen Sie einen neuen Benutzer anlegen, in dem Sie diesem einen eindeutigen Benutzernamen geben. Tragen Sie diesen unter Punkt 1 ein und unter Punkt 2 ein Passwort für den Benutzer. Weiter muss im Bereich „Einwahl zulassen über“ die Methode „**IPsec**“ aktiviert sein. Bei der IKE-Authentifizierungsmethode setzen Sie den Hacken bei „**Pre-Shared-Key**“ wobei nun der zuvor vergebene Key für den Benutzer aktiviert wird. Alle anderen Einstellungen sind individuell je nach Gegebenheiten in Ihrer Firma zu setzen. Wenn alle Einstellungen durchgeführt sind speichern Sie die Angaben mit OK

VPN und externe Einwahl >> Externe-Benutzer

Index-Nr. 1

Benutzerkonto und Authentifizierung ☒ aktiv Max. Leerlaufzeit 300 Sekunden		Benutzername 1 Passwort (bis zu 19 Zeichen) 2 ☐ Mobile One-Time Passwords (mOTP) aktivieren PIN-Code Secret
Einwahl zulassen über ☒ PPTP ☒ IPsec ☒ L2TP mit IPsec erforderlich ☒ SSL ☒ Fernzugriff definieren IP des externen Benutzers oder Peer-ID NetBIOS-Name durchlassen ☒ ja ☐ nein Multicast via VPN ☐ ja ☒ nein (z.B. für IGMP, IP-Kameras, DHCP-Relay, etc.)		IKE-Authentifizierungsmethode ☒ Pre-Shared Key IKE Pre-Shared Key ☐ Digitale Signatur (X.509) ohne
Subnetz LAN 1 ☐ Statische IP-Adresse zuweisen 0.0.0.0		IPsec-Methode ☒ Mittel (AH) Hoch (ESP) ☒ DES ☒ 3DES ☒ AES Local-ID (optional)

4. Zum Abschluss müssen noch schauen, dass der Benutzer auch aktiviert ist:

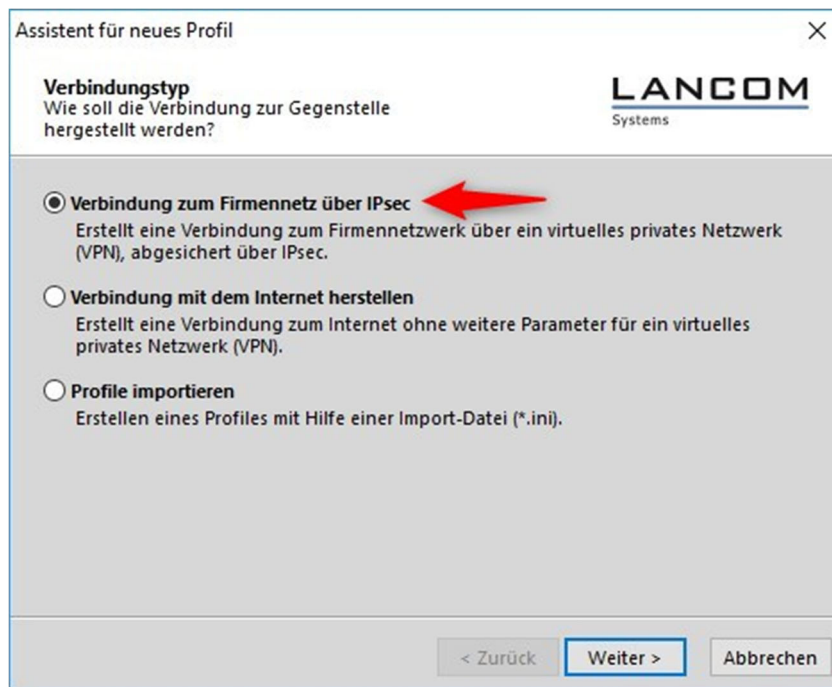
Profile externer Benutzer:

[Auf Werkseinstellungen zurücksetzen](#)

Index	Benutzer	Aktiv	Status	Index	Benutzer	Aktiv	Status
1.		☒	LAN1-DHCP	17.	???	☐	---
2.		☒	LAN1-DHCP	18.	???	☐	---
3.	???	☐	---	19.	???	☐	---

Als zweites schauen wir uns die Konfiguration des NCP VPN Clients an:

1. Starten Sie den NCP VPN Client und wählen Sie im Reiter „**Konfiguration**“ die Option „**Profile**“. Klicken Sie nun im sich öffnenden Fenster „**Hinzufügen / Import**“. Anschließend öffnet sich das unten abgebildete Fenster. Hier gehen Sie auf „**Verbindung zum Firmennetz über IPsec**“ und klicken dann auf Weiter.



2. Geben Sie der neuen Verbindung einen Namen. In unserem Beispiel: **VPN zu Draytek Vigor**
Klicken Sie dann auf Weiter.

The screenshot shows the 'Assistent für neues Profil' window for LANCOM Systems. The title is 'Name des Profils'. The instruction says: 'Geben Sie hier einen unverwechselbaren Namen für das Profil ein.' Below this, a note states: 'Der Name des Profils darf jedes alphanumerische und numerische Zeichen beinhalten und, Leerzeichen eingerechnet, bis zu 39 Zeichen lang sein.' There is a yellow star icon next to the 'Profil-Name:' label. The text input field contains 'VPN zu Draytek Vigor', which is highlighted in yellow. A red arrow points to the end of the text in the input field. At the bottom, there are three buttons: '< Zurück', 'Weiter >' (highlighted with a blue border), and 'Abbrechen'.

3. Wählen Sie das geeignete Verbindungsmedium aus. Klicken Sie dann auf Weiter.

The screenshot shows the 'Assistent für neues Profil' window for LANCOM Systems. The title is 'Verbindungsmedium'. The instruction says: 'Auswahl des Mediums, über das die Verbindung hergestellt werden soll.' Below this, a note states: 'Wählen Sie das Medium, über das die Verbindung hergestellt werden soll. Das Verbindungsmedium wird für jedes Profil eigens eingestellt, vorausgesetzt Sie haben die entsprechende Hardware angeschlossen und in Ihrem System installiert. Soll z. B. das Internet über Modem genutzt werden, stellen Sie unter Verbindungsmedium "Modem" ein und wählen anschließend das gewünschte Modem aus.' There is a globe icon next to the 'Verbindungsmedium:' label. The dropdown menu shows 'LAN (over IP)', which is highlighted in yellow. A red arrow points to the dropdown arrow. At the bottom, there are three buttons: '< Zurück', 'Weiter >' (highlighted with a blue border), and 'Abbrechen'.

- Geben Sie im Feld Gateway (Tunnel-Endpunkt) die IP-Adresse oder den DynDNS Namen des VPN-Servers ein, zu dem die Verbindung aufgebaut werden soll. Klicken Sie dann auf Weiter.

- Im nächsten Fenster wählen Sie den Austausch-Modus. Dieser muss auf „Main Mode (IKEv1)“ gesetzt sein. Alle weiteren Menüpunkte bleiben leer bzw. deaktiviert. Klicken Sie dann auf Weiter.

6. Wählen Sie Als Typ **"Fully Qualified Domain Name"** als lokale Identität (ID) geben Sie einen Namen oder ein DDNS in das ID-Feld ein. In diesem Beispiel haben wir **a.b.c** als lokale ID eingerichtet. Geben Sie das von Ihnen im Router angegebene Passwort in das Feld **Shared Secret** ein und bestätigen Sie es, indem Sie dasselbe Passwort ein zweites Mal in das Feld **Shared Secret (Wiederholung)** eingeben. Klicken Sie dann auf Weiter.

7. Zuweisung der IP-Adressen Wählen Sie eine lokale IP-Adresse aus oder Sie lassen sich eine Lokale IP-Adresse zuweisen, wie in unserem Beispiel dargestellt. Klicken Sie dann auf Weiter.

8. Wählen Sie nun das IPsec Split Tunneling den Netzwerkbereich des entfernten Netzwerks aus. Geben Sie hier das entfernte VPN-Netzwerk und die Netzwerkmaske ein. Anschließend Klicken Sie auf „**Fertigstellen (Finish)**“ um die bisher vorgenommenen Einstellungen abzuschließen.

Assistent für neues Profil

IPsec-Konfiguration - Split Tunneling
Welche entfernten IP-Netzwerke sollen über den Tunnel erreicht werden ?

Hier können die entfernten Netzwerke eingetragen werden, die über den Tunnel erreicht werden sollen. Ohne Einträge wird immer der Tunnel benutzt.

Entfernte IP-Netzwerke	Entfernte IP-Netzmasken
192.168.0.0	255.255.255.0

Hinzufügen
Bearbeiten
Löschen

< Zurück Fertigstellen Abbrechen

9. Wählen Sie nun das soeben erstellte Profil aus und klicken Sie auf die Schaltfläche Bearbeiten.

VPN Profile

Verfügbare Profile

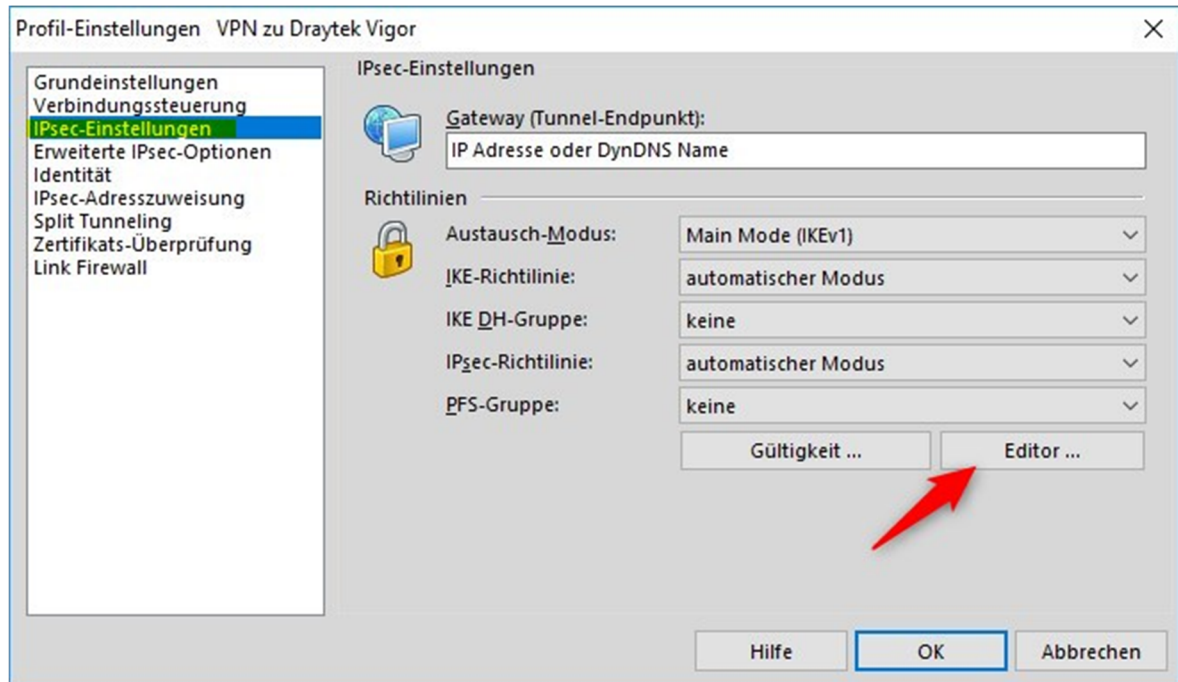
Gruppe:
Alle Profile anzeigen Gruppieren

Profil-Name	Verbindungsmedium	Autom. M...	Standard
	automatisch	☐	☐
	automatisch	☐	☐
	automatisch	☐	☐
	automatisch	☐	☐
VPN zu Draytek Vigor	LAN	☒	☐
	automatisch	☐	☐

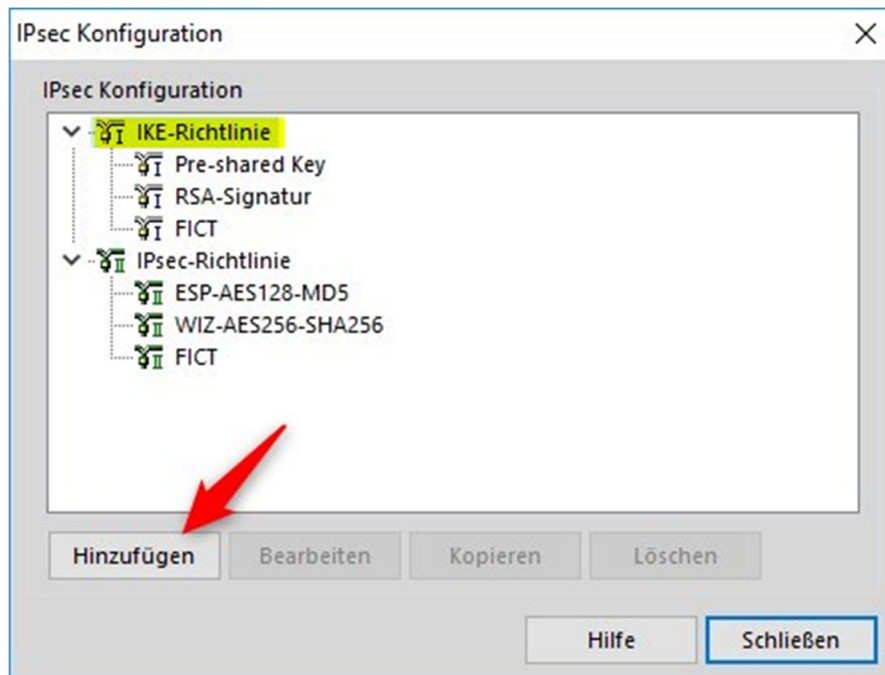
Hinzufügen / Import Bearbeiten Kopieren Löschen Export

Hilfe OK Abbrechen

10. Wählen Sie auf der Registerkarte links **"IPSec-Einstellungen"** und anschließend rechts unten **„Editor“** aus. Hier müssen zwei Regeln für die Verbindung festgelegt werden.



11. Wählen Sie als erstes **IKE-Richtlinie** aus und klicken Sie unten auf die Schaltfläche **„Hinzufügen“**.



12. Geben Sie nun der IKE-Richtlinie einen Namen. Diese Regel wird für die „Phase I“ verwendet. Wählen Sie AES nicht als Verschlüsselung, ohne sicherzustellen, dass Ihr Vigor-Router AES in Phase I unterstützt. Wenn der Router dies unterstützt, wählen Sie als Authentisierung „**Pre-shared Key**“ aus, als Verschlüsselung „**Triple DES**“ und als Hash „**MD5**“ aus. Abschließend klicken Sie auf „Hinzufügen“ und auf OK.

IKE-Richtlinie

Name :

Authentisierung	Verschlüsselung	Hash
Pre-shared Key	Triple DES	MD5

Authentisierung :

Verschlüsselung:

Hash:

13. Wählen Sie als zweites nun **IPSec-Richtlinie** aus und klicken Sie unten auf die Schaltfläche „Hinzufügen“.

IPsec Konfiguration

IPsec Konfiguration

- ✓ IKE-Richtlinie
 - Pre-shared Key
 - RSA-Signatur
 - FICT
- ✓ **IPsec-Richtlinie**
 - ESP-AES128-MD5
 - WIZ-AES256-SHA256
 - FICT

14. Geben Sie nun der IPsec-Richtlinie einen Namen. Diese Regel wird für die „Phase II“ verwendet. Wählen Sie AES nicht als Verschlüsselung, ohne sicherzustellen, dass Ihr Vigor-Router AES in Phase II unterstützt. Wenn der Router dies unterstützt, wählen Sie als Protokoll „**ESP**“ aus, als Verschlüsselung „**Triple DES**“ und als Authentisierung „**MD5**“ aus. Abschließend klicken Sie auf „Hinzufügen“ und auf OK.

IPsec-Richtlinie

Name: Richtliniennamen

Protokoll	Verschlüsselung	Authentisierung
ESP	Triple DES	MD5

Protokoll: ESP

Verschlüsselung: Triple DES

Authentisierung: MD5

Hinzufügen

Entfernen

Hilfe OK Abbrechen

15. Sie haben jetzt 2 neue Einträge mit den von Ihnen vergebenen Namen. In unserem Fall heißen beide Regeln „FICT“. Klicken Sie nun auf die Schaltfläche „**Schließen**“.

IPsec Konfiguration

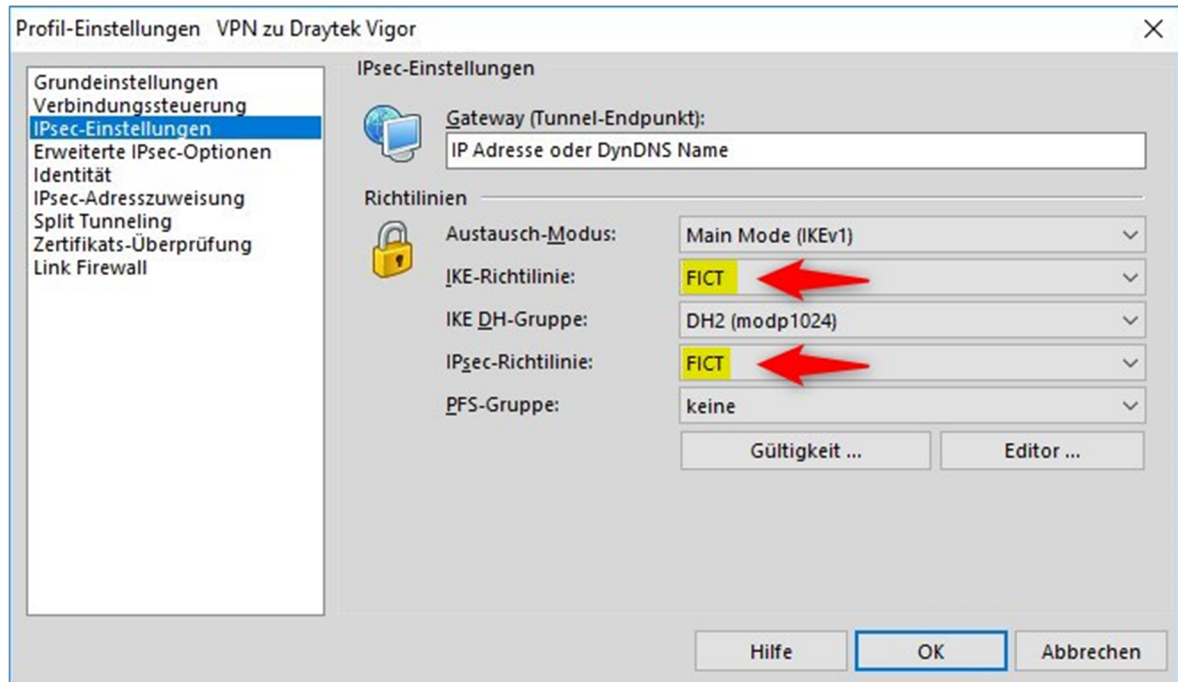
IPsec Konfiguration

- ✓ IKE-Richtlinie
 - Pre-shared Key
 - RSA-Signatur
 - FICT
- ✓ IPsec-Richtlinie
 - ESP-AES128-MD5
 - WIZ-AES256-SHA256
 - FICT

Hinzufügen Bearbeiten Kopieren Löschen

Hilfe Schließen

16. Wählen Sie nun abschließend die zwei neu angelegten Regeln als IKE-Richtlinie und IPSec-Richtlinie aus. Dann klicken Sie auf „OK“.



17. Nun befinden Sie sich wieder auf der Verbindungsoberfläche des NCP-VPN Clients und können sich mit dem entfernten Netzwerk verbinden.