



## ALL-VPN10

VPN Tunnel aufbauen mit dem NCP Secure Entry Client (IPSec)



Hilfestellung

In dieser Hilfestellung wird Ihnen Schritt für Schritt erklärt wie Sie einen VPN Tunnel zwischen dem *NCP Secure Entry Client* und dem ALL-VPN10 aufbauen.

Den *NCP Secure Entry Client* können Sie sich auf [www.ncp-e.com](http://www.ncp-e.com) herunterladen.

Grundsätzlich können Sie den Client 30 Tage lang kostenlos testen. Nach Ablauf dieser Frist müssen Sie die Software mit einem Lizenzschlüssel freischalten, um ihn weiterhin nutzen zu können.

## A Konfiguration des ALL-VPN10

Navigieren Sie auf der Weboberfläche des Routers zu *VPN -> Client to Gateway*

Home

Network

Internet Filter

QoS

IP/DHCP

PPPoE Server

E-Bulletin&ARP-Binding

Firewall

Advanced Function

System Tool

Port Management

**VPN**

Summary

Gateway to Gateway

**Client to Gateway**

PPTP Setup

VPN Pass Through

Smart Link VPN

Log

Client to Gateway

Tunnel(s) No.: 1

Tunnel(s) Name: test

Interface: WAN 1

Enabled: ☒

Local VPN Group Setting

Local Security Gateway Type: IP Only

IP Address: 188 . 174 . 185 . 74

Local Security Group Type: Subnet

IP Address: 192 . 168 . 1 . 0

Subnet Mask: 255 . 255 . 255 . 0

Remote VPN Group Setting

Remote Security Gateway Type: Dynamic IP + Domain Name(FQDN) Authentication

Domain Name: 1

IPSec Setting

Keying Mode: IKE with Preshared Key

Phase1 DHGroup: Group 1

Phase1 Encryption: DES

Phase1 Authentication: MD5

Phase1 SA Life Time: 28800 seconds

Perfect Forward Secrecy: ☒

Phase2 DHGroup: Group 1

Phase2 Encryption: DES

Phase2 Authentication: MD5

Phase2 SA Life Time: 3600 seconds

Preshared Key: 12345

Advanced -

Advanced

☒ Aggressive Mode

☐ Compress (Support IP Payload Compression Protocol(IPComp))

☐ Keep-Alive

☐ AH Hash Algorithm MD5

☒ NAT Traversal

☒ Dead Peer Detection(DPD) Enable Automatic Version Check Every 10 seconds

Apply

Cancel

Die IP Adresse wird automatisch vom Router ausgefüllt  
- bitte nicht ändern -

Stellen Sie hier das LAN-seitige Subnetz Ihres ALL-VPN10 ein

© ALLNET GmbH München 2013 - Alle Rechte vorbehalten

Die Punkte *Client to Gateway*, *Local VPN Group Setting* und *Remote VPN Group Setting* können bei Ihnen unter Umständen abweichen.

Bei *IPSec Setting* und *Advanced* stellen Sie bitte alles genauso ein wie in diesem Beispiel. **Ausnahme** ist der *Preshared Key*! Hier geben Sie bitte einen Schlüssel ein, der nur Ihnen bekannt ist.

Um die Einstellungen zu übernehmen klicken Sie auf "Apply".

Die Konfiguration des Routers ist somit abgeschlossen.

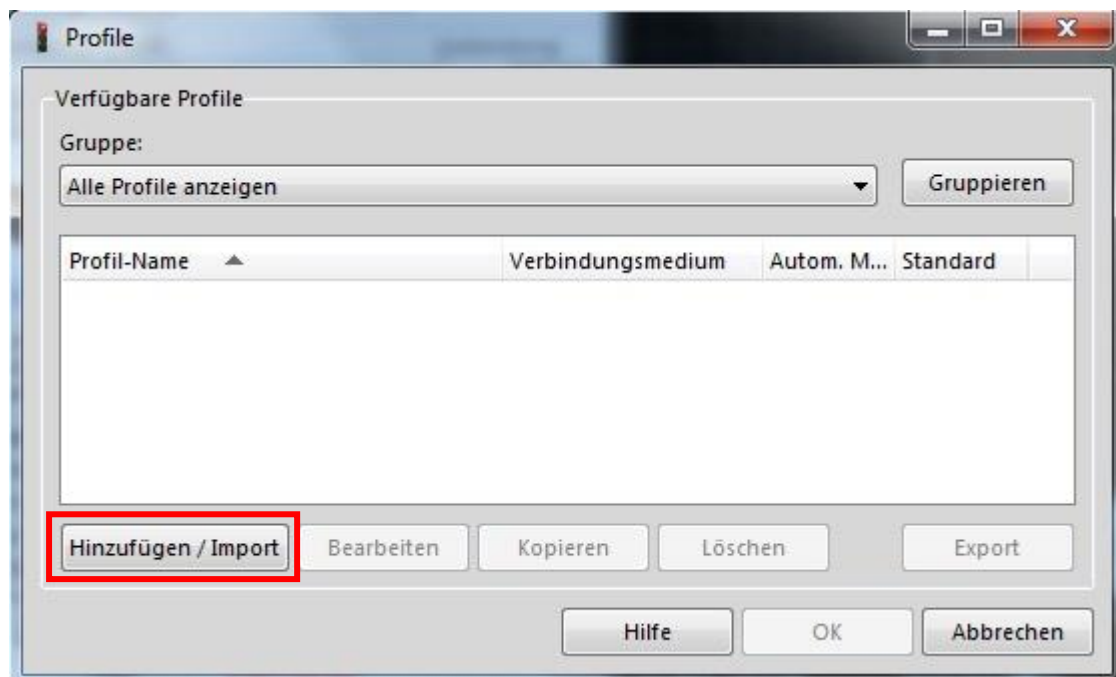
## B Konfiguration des NCP Secure Entry Client

Starten Sie den NCP Secure Entry Client.

Öffnen Sie *Konfiguration -> Profile*



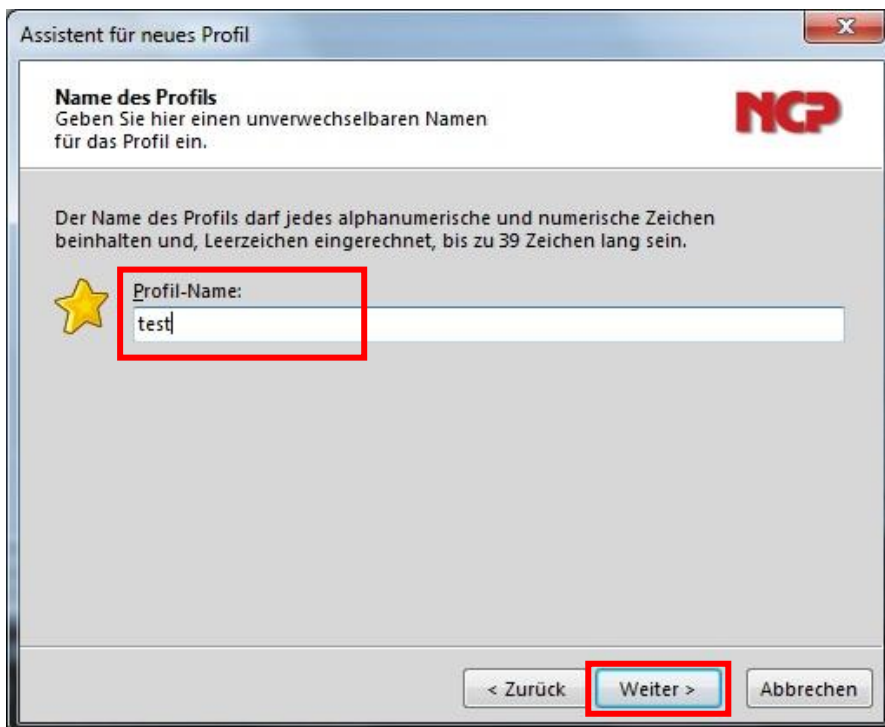
Klicken Sie auf *Hinzufügen/Import*



Wählen Sie *Verbindung zum Firmennetz über IPsec* und klicken Sie auf *Weiter*.



Geben Sie einen frei wählbaren *Profil-Namen* ein und klicken Sie auf *Weiter*.



Wählen Sie hier Ihr Verbindungsmedium aus und klicken Sie auf *Weiter*.

**Assistent für neues Profil**

**Verbindungsmedium**  
Auswahl des Mediums, über das die Verbindung hergestellt werden soll.

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.

**Verbindungsmedium:** LAN (over IP)

< Zurück   **Weiter >**   Abbrechen

Bei Gateway tragen Sie die DDNS Adresse bzw. die statische IP-Adresse Ihres ALL-VPN10 ein und klicken auf *Weiter*.

**Assistent für neues Profil**

**VPN Gateway-Parameter**  
Zu welchem Tunnel-Endpunkt soll die Verbindung aufgebaut werden?

Geben Sie an dieser Stelle den Namen (z.B. vpnserver.musterfirma.de) oder die offizielle IP-Adresse (z.B. 212.10.17.29) an, über die das VPN-Gateway erreichbar ist. Bei erweiterter Authentisierung (XAUTH) kann der Benutzername und das Passwort für die Authentisierung angegeben werden. Werden keine Authentisierungsdaten angegeben, werden diese beim Verbindungsaufbau abgefragt.

**Gateway (Tunnel-Endpunkt):**  
test.dyndns.org

☐ Erweiterte Authentisierung (XAUTH)

**Benutzername:**  
\_\_\_\_\_

**Passwort:** \_\_\_\_\_ **Passwort (Wiederholung):** \_\_\_\_\_

< Zurück   **Weiter >**   Abbrechen



Wählen Sie folgende Parameter aus und klicken Sie auf *Weiter*.

Assistent für neues Profil

**IPsec-Konfiguration**  
Konfiguration der grundlegenden Parameter für IPsec

Hier können sie grundlegende Parameter für IPsec angeben. Für die Richtlinien der IPsec-Verhandlung wird die Einstellung "Automatischer Modus" verwendet. Sollen bestimmte IKE / IPsec-Richtlinien verwendet werden, müssen diese anschließend in den Profil-Einstellungen definiert und zugewiesen werden.

★ Austausch-Modus:  
Aggressive Mode (IKEv1)

PFS-Gruppe:  
DH-Gruppe 1 (768 Bit)

☐ Benutze IPsec-Kompression

< Zurück Weiter > Abbrechen

**Wichtig:** Ihr *Pre-shared Key* und Ihre *lokale Identität* müssen identisch mit den Parametern von Ihrem ALL-VPN10 sein. Klicken Sie auf *Weiter*.

Assistent für neues Profil

**IPsec-Konfiguration - Pre-shared Key**  
Gemeinsamer Schlüssel für die IPsec

Werden für die Authentisierung keine Zertifikate verwendet, wird für die Datenverschlüsselung ein gemeinsamer Schlüssel benötigt, der auf beiden Seiten (VPN Client und VPN Gateway) hinterlegt sein muss. Für die IKE ID muss je nach ausgewähltem IKE ID-Typ der zugehörige String eingetragen werden.

Pre-shared Key

Shared Secret: ..... Shared Secret (Wiederholung): .....

Lokale Identität (IKE)

Typ: Fully Qualified Domain Name

ID: 1

< Zurück Weiter > Abbrechen

siehe **ALL-VPN10**:

<- IP Sec Setting -> Preshared Key

<- Remote VPN Group Setting



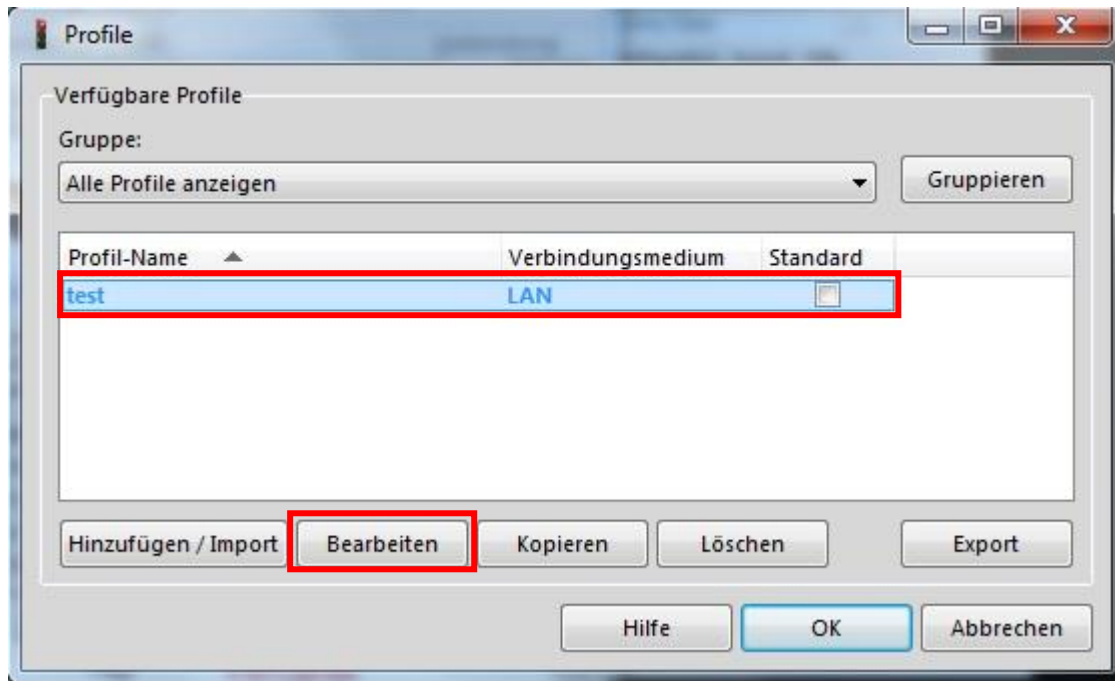
Wählen Sie hier *Lokale IP-Adresse verwenden* und klicken auf *Weiter*.

The screenshot shows the 'Assistent für neues Profil' window with the title 'IPsec-Konfiguration - IP-Adressen'. The subtitle is 'Welche IP-Adressen sollen verwendet werden?'. The NCP logo is in the top right. The main text explains that the user should specify the IP address for the client and that dynamic assignment requires 'IKE Config Mode verwenden'. It also mentions the option to specify DNS or WINS servers. Below this, there is a section for 'IP-Adressen-Zuweisung' with a dropdown menu set to 'Lokale IP-Adresse verwenden'. Below that is a text field for 'IP-Adresse' containing '0.0.0.0'. Further down is a section for 'DNS / WINS Server' with text fields for 'DNS Server' and 'WINS Server', both containing '0.0.0.0'. At the bottom, there are three buttons: '< Zurück', 'Weiter >', and 'Abbrechen'. The 'Weiter >' button is highlighted with a red rectangle.

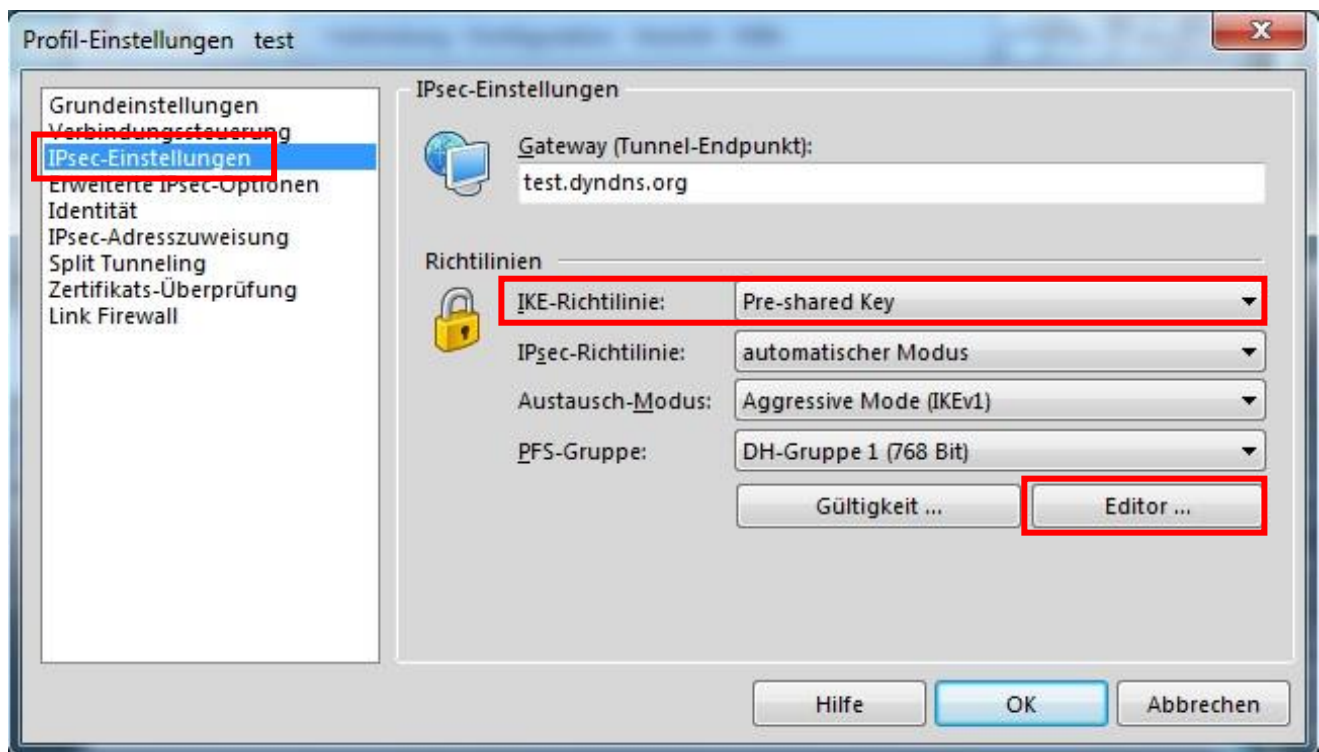
Abschließend klicken Sie auf *Fertigstellen*.

The screenshot shows the 'Assistent für neues Profil' window with the title 'Firewall-Einstellungen'. The subtitle is 'Welche Einstellungen sollen für die Firewall verwendet werden?'. The NCP logo is in the top right. The main text explains that the user should activate the desired firewall option and that Stateful Inspection activation prevents accepting packets from other hosts. It also mentions the option to deactivate NetBIOS over IP. Below this, there is a section for 'Firewall' with a dropdown menu set to 'aus'. Below that is a checkbox for 'Ausschließlich Kommunikation im Tunnel' which is unchecked, and a checkbox for 'NetBIOS über IP' which is checked. At the bottom, there are three buttons: '< Zurück', 'Fertigstellen', and 'Abbrechen'. The 'Fertigstellen' button is highlighted with a red rectangle.

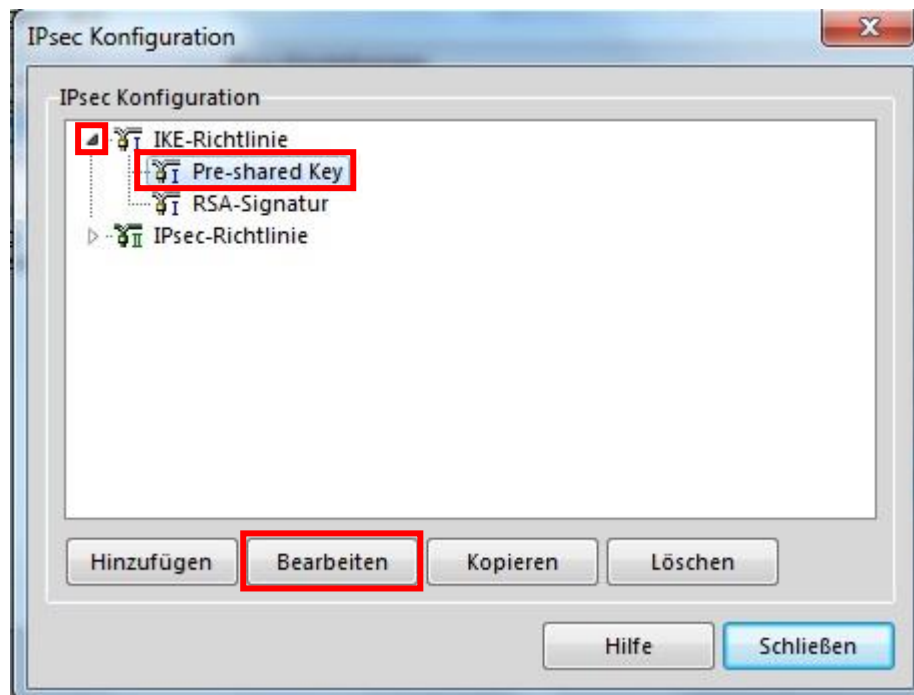
Markieren Sie Ihr gerade angelegtes Profil und klicken Sie auf *Bearbeiten*.



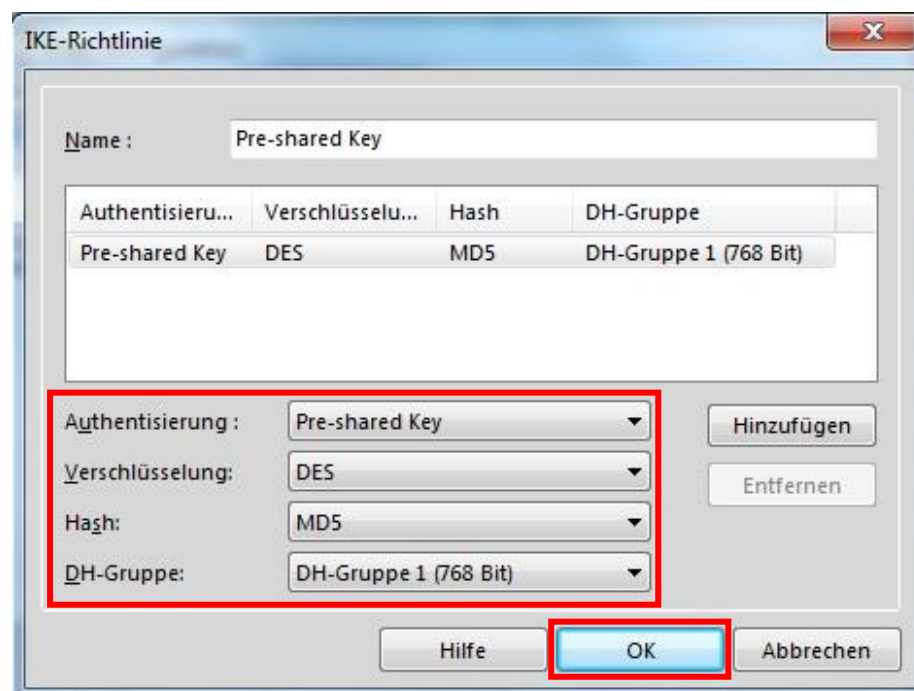
Bei *IPSec-Einstellungen* wählen Sie *Pre-shared Key* aus und klicken dann auf *Editor ...*.



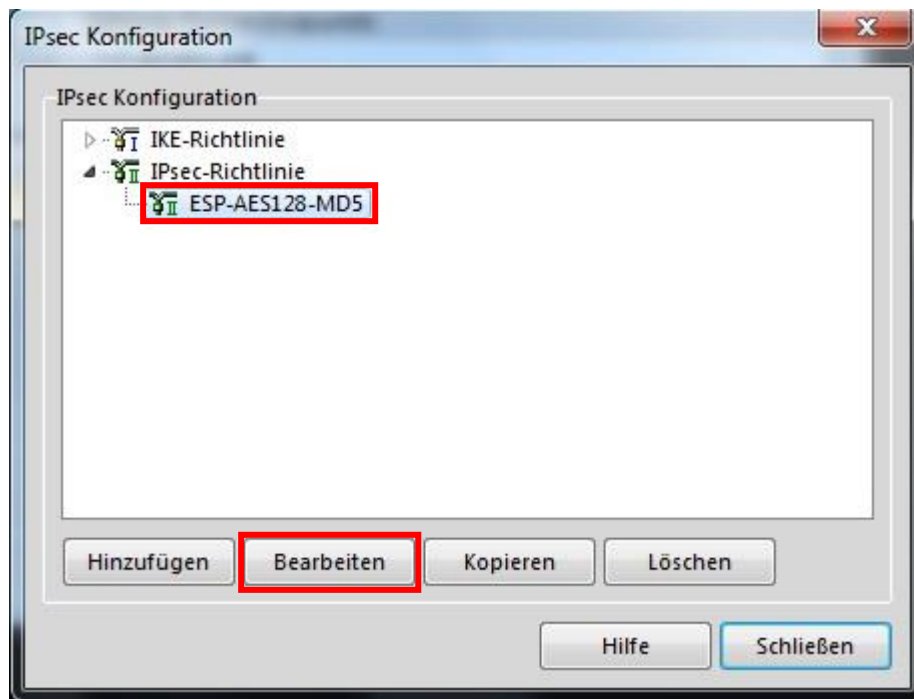
Klicken Sie auf das kleine Dreieck damit die Auswahl sich öffnet. Markieren Sie *Pre-shared Key* und klicken auf *Bearbeiten*.



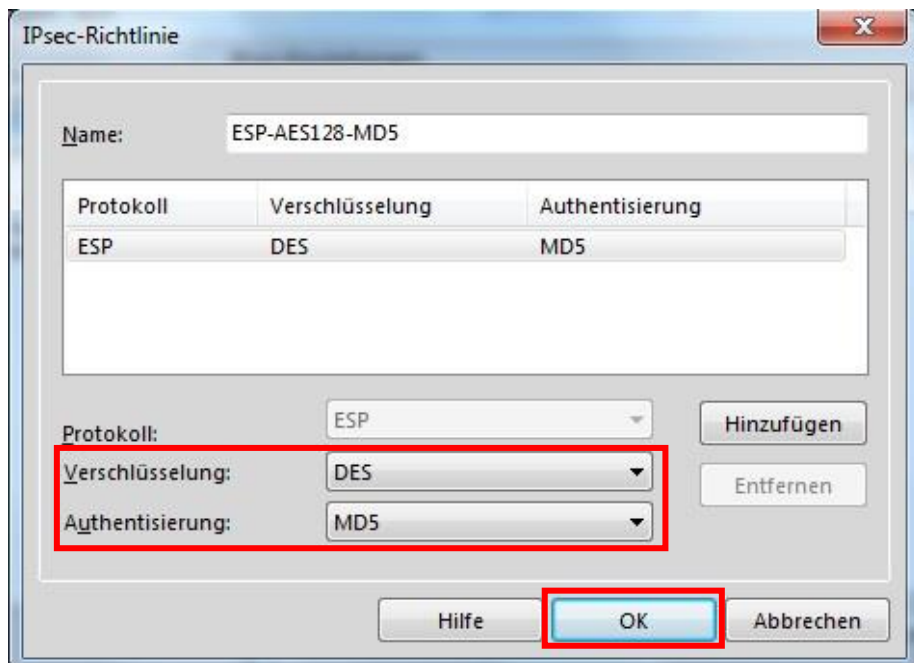
Übernehmen Sie folgende Parameter und klicken auf *OK*.



Markieren Sie *ESP-AES128-MD5* und klicken auf *Bearbeiten*.

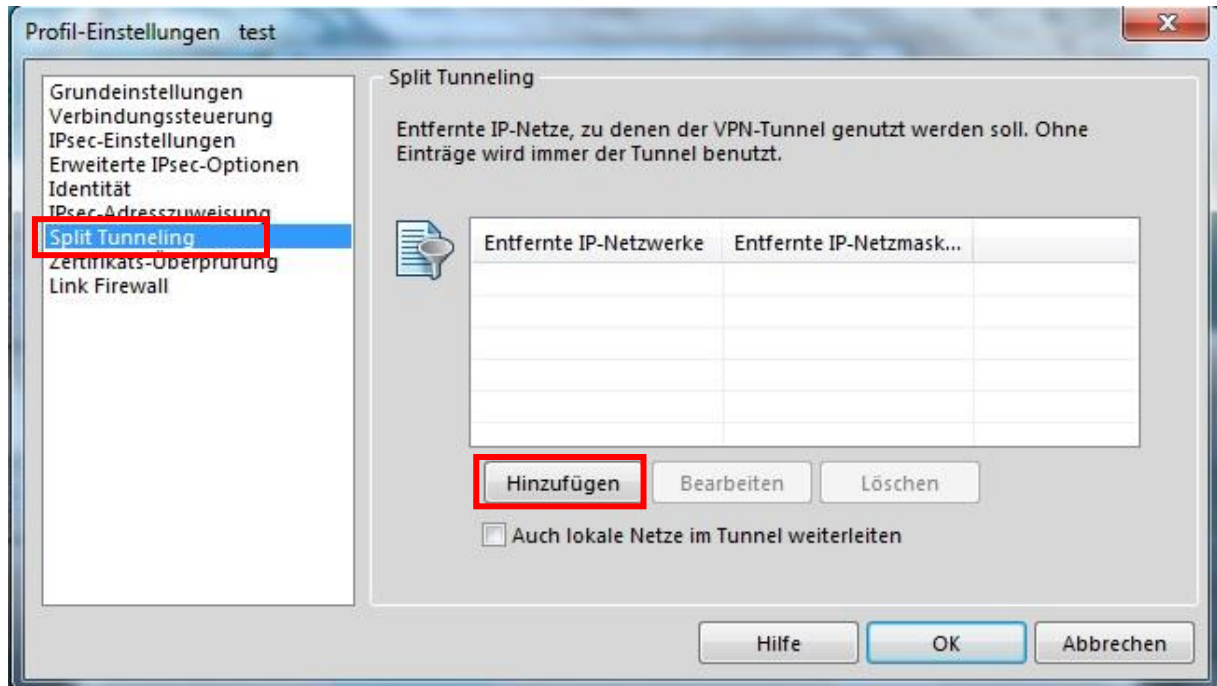


Übernehmen Sie folgende Parameter und klicken auf *OK*.

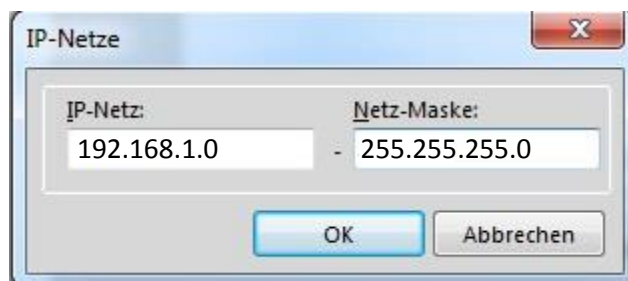


Klicken Sie auf *Schließen*.

Klicken Sie auf *Split Tunneling* und dann auf *Hinzufügen*.



Stellen Sie hier das LAN-seitige Subnetz Ihres ALL-VPN10 ein und klicken auf *OK*.



siehe **ALL-VPN10**:

<- Local VPN Group Setting ->  
Local Security Group Type

Klicken Sie auf *OK* -> *OK*

## C VPN Tunnel öffnen

Wählen Sie als *Verbindungs-Profil* das so eben erstellte Profil aus und klicken auf den Schieber unter *Verbindung*.



Jetzt sind Sie via IPSec mit Ihrem ALL-VPN10 verbunden:

