NETGEAR®

VPN-Beispielkonfigurationen

für die Router-Modelle

FVS114
FVS318v1, v2, v3
FVM318
FVS328
FVS338
FVL328
FWAG114
FWG114Pv1, v2
FVX538

sowie die **ProSafe VPN Client Software**

August 2005

Inhaltsverzeichnis

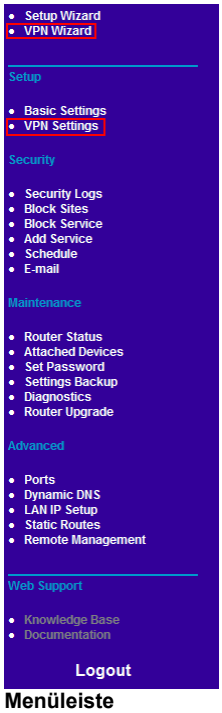
16.BEISPIELKONFIGURATION
PROSAFE VPN CLIENT ZU FVL328 MIT DYNAMISCHER WAN-IP

Vorwort

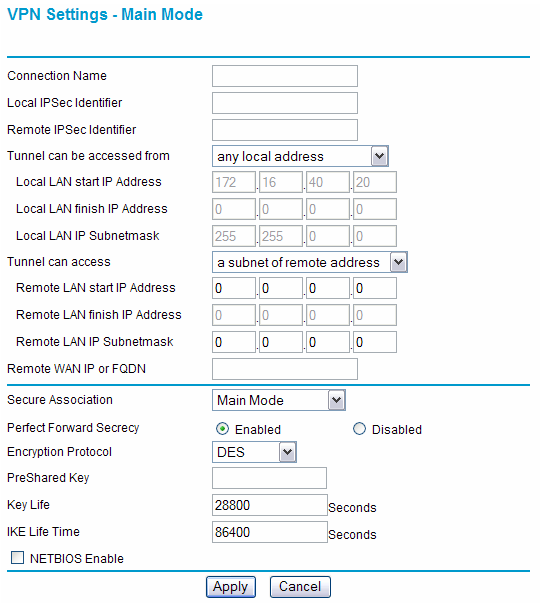
In dieser Anleitung werden die Beispielkonfigurationen anhand der Routermodelle FVS318v2 bzw. v2 und FVL328 beschrieben.

Es gibt bei Netgear VPN Routern 2 verschiedene Menüstrukturen für die VPN Konfiguration.

Einteiliges Menü



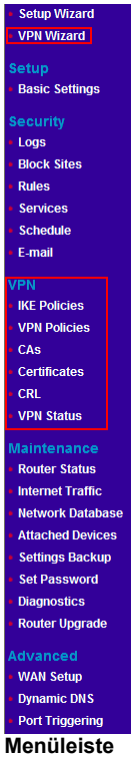
Menüleiste



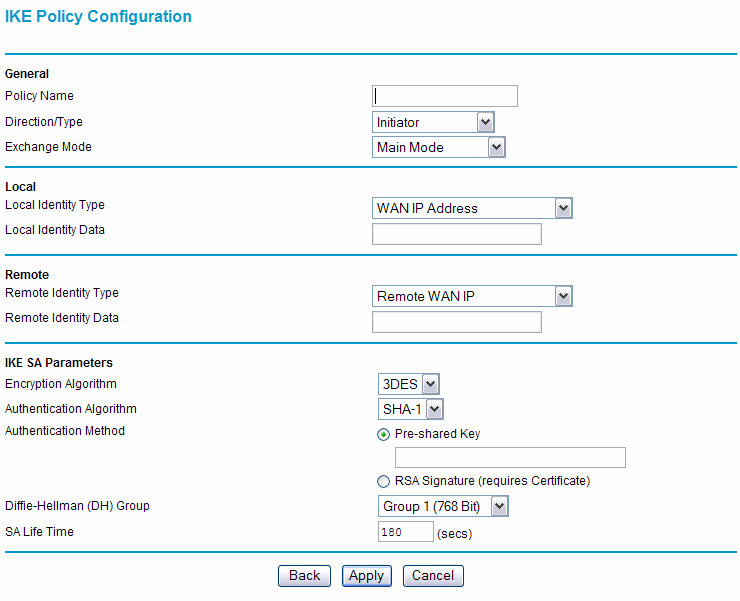
Menü VPN Settings

Diese Menüpunkte finden Sie bei den Modellen FVS318v1, FVS318v2 und FVM318 vor. Beide Phasen der VPN Verbindung werden in einem einzigen Menü konfiguriert. Die Anleitung für den FVS318v1 gilt auch für den FVS318v2 und den FVM318.

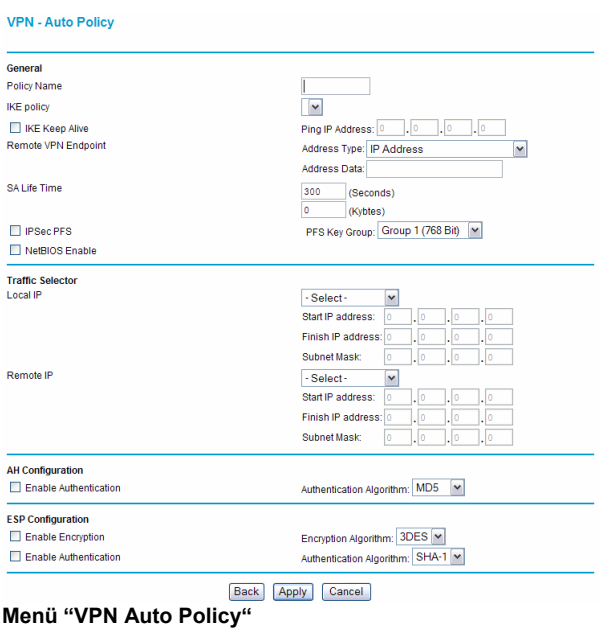
Zweigeteiltes Menü



Menüleiste



Menü “IKE Policy Konfiguration“



Menü “VPN Auto Policy“

Diese Menüpunkte finden Sie bei den folgenden Modellen:

FVS318v3, FVS328, FVS338, FVL328, FWG114Pv1 und v2, FWAG114, FVS114, FVS124G und FVX538.

Hier werden die beiden Phasen des VPNs getrennt voneinander konfiguriert.

Die Phase 1 wird in den IKE Policies festgelegt, die Phase 2 in den VPN Policies.

1. Beispielkonfiguration

FVS318v1 mit fester WAN-IP-Adresse
zu
FVS318v1 mit fester WAN-IP-Adresse

1.1. Übersicht

Standort A:

FVS318v1 (Firmware 2.4)

FVS318v1 LAN-Seite: 192.168.0.1
FVS318v1 WAN-Seite: 217.232.56.129

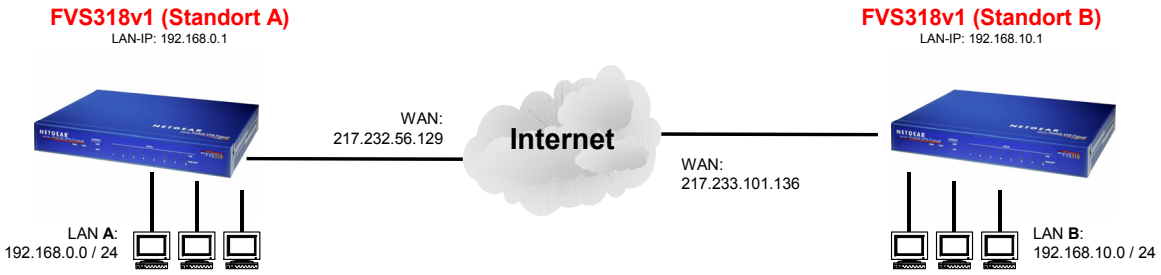
Netzwerkadresse: 192.168.0.0/24
Test-PC im Netzwerk: 192.168.0.2

Standort B:

FVS318v1 (Firmware 2.4)

FVS318v1 LAN-Seite: 192.168.10.1
FVS318v1 WAN-Seite: 217.233.101.136

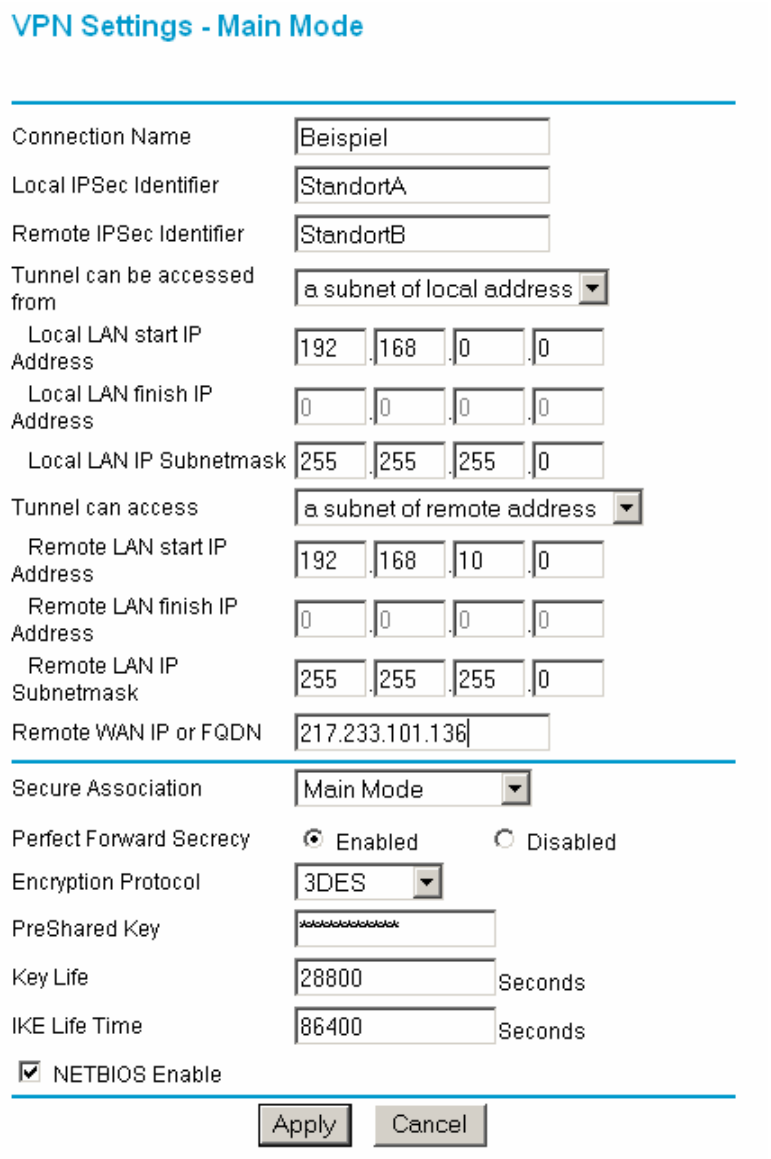
Netzwerkadresse: 192.168.10.0/24
Test-PC im Netzwerk: 192.168.10.2



1.2. Konfiguration des Routers an Standort A

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links oben auf den Menüpunkt **VPN Settings**.
- Aktivieren Sie den Punkt vor der 1 und klicken Sie auf **Edit**.
- Konfigurieren Sie die Verbindung wie in Abb. 1.2.1 gezeigt.

Abb. 1.2.1

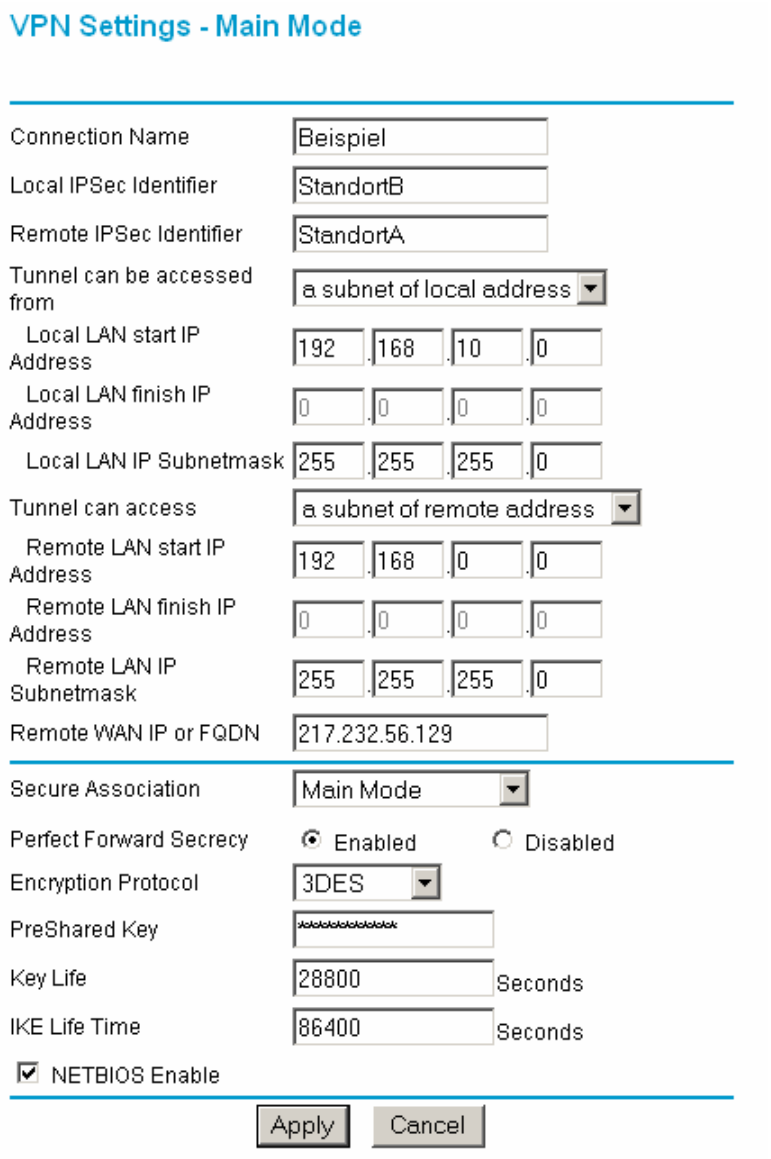


- Klicken Sie auf Apply um die Einstellungen zu speichern.

1.3. Konfiguration des Routers an Standort B

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links oben auf den Menüpunkt **VPN Settings**.
- Aktivieren Sie den Punkt vor der 1 und klicken Sie auf **Edit**.
- Konfigurieren Sie die Verbindung wie in Abb. 1.3.1 gezeigt.

Abb. 1.3.1



- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

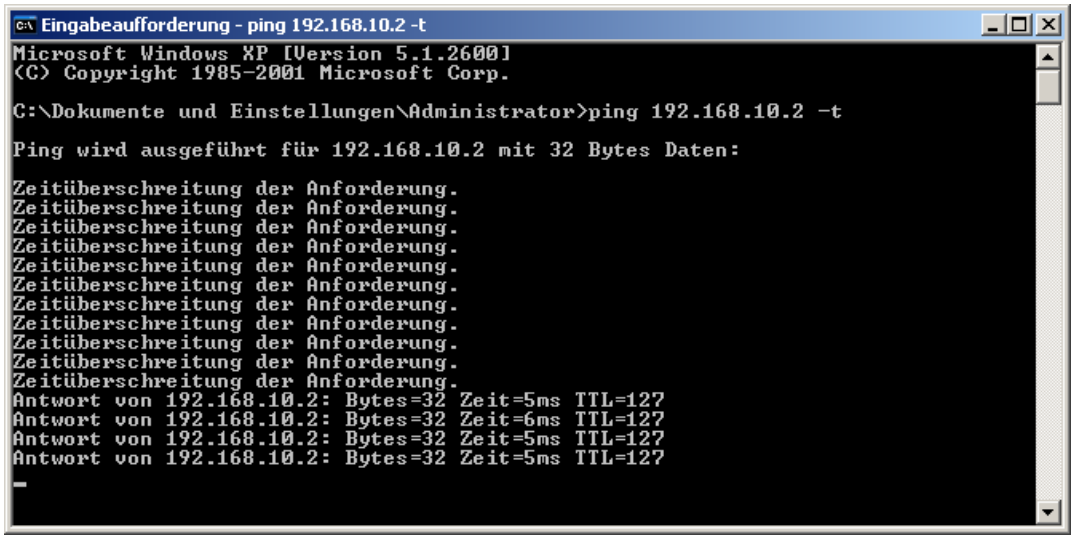
1.4. Testen der Verbindung

Um die Verbindung zu testen, versuchen Sie beispielsweise von einem PC an Standort A (z.B. 192.168.0.2) einen PC an Standort B (z.B. 192.168.10.2) zu erreichen:

Hinweis:	- Bei beiden PCs muss der jeweils lokale Router als Gateway verwendet werden: - Der PC an Standort A (192.168.**0**.2) verwendet als Gateway seinen lokalen Router 192.168.**0**.1. - Der PC an Standort B (192.168.**10**.2) verwendet als Gateway seinen lokalen Router 192.168.**10**.1.

- Klicken Sie in Windows links unten auf **Start** und **Ausführen...**
- Geben Sie **cmd** ein (Windows 95/98/ME: **command**) und klicken Sie auf **OK**
- Geben Sie folgenden Befehl ein: **ping 192.168.10.2 –t** (siehe Abb. 1.4.1)

Abb. 1.4.1



- Bei richtiger Konfiguration wird die VPN-Verbindung innerhalb einiger Sekunden aufgebaut (siehe Abb. 1.4.1).
- Der VPN Status des FVS318v1 (**Show VPN Status** im Menü **Router Status**) zeigt ebenfalls eine etablierte VPN-Verbindung (siehe Abb. 1.4.2).

Abb. 1.4.2

IPSec Connection Status

Status	Connection Name	Remote IP	Virtual Network	Type	State	Drop
Active	Beispiel	217.233.101.136	192.168.10.0/24	ESP(3DES-CBC SHA-1)	[P1:M-Estab.] [P2:Q-Estab.]	Drop

2. Beispielkonfiguration

FVS318v1 mit dynamischer WAN-IP-Adresse
zu
FVS318v1 mit fester WAN-IP-Adresse

2.1. Übersicht

Standort A:

FVS318 (Firmware 2.4)

FVS318v1 LAN-Seite: 192.168.0.1
FVS318v1 WAN-Seite: standorta.dyndns.org

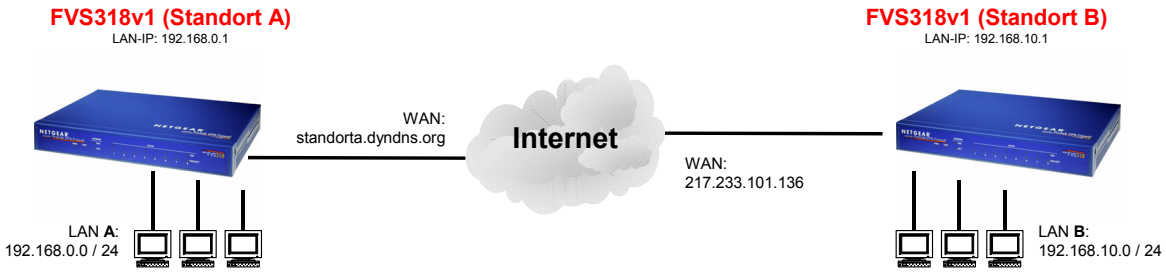
Netzwerkadresse: 192.168.0.0/24
Test-PC im Netzwerk: 192.168.0.2

Standort B:

FVS318v1 (Firmware 2.4)

FVS318v1 LAN-Seite: 192.168.10.1
FVS318v1 WAN-Seite: 217.233.101.136

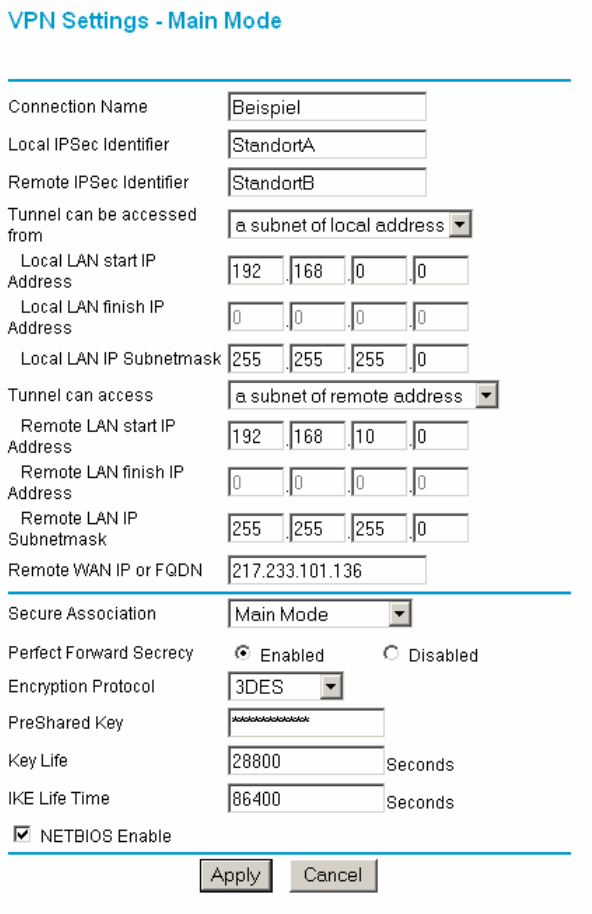
Netzwerkadresse: 192.168.10.0/24
Test-PC im Netzwerk: 192.168.10.2



2.2. Konfiguration des Routers an Standort A

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links oben auf den Menüpunkt **VPN Settings**.
- Aktivieren Sie den Punkt vor der 1 und klicken Sie auf **Edit**.
- Konfigurieren Sie die Verbindung wie in Abb. 2.2.1 gezeigt.

Abb. 2.2.1

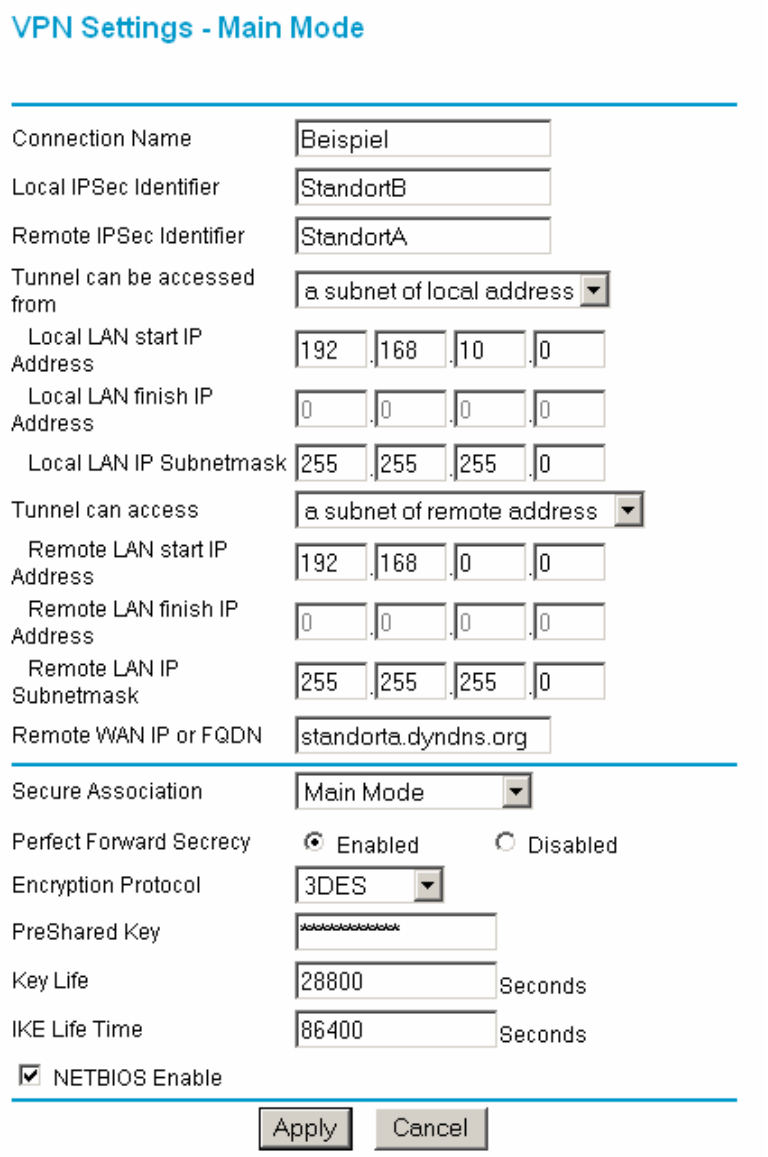


- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

2.3. Konfiguration des Routers an Standort B

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links oben auf den Menüpunkt **VPN Settings**.
- Aktivieren Sie den Punkt vor der 1 und klicken Sie auf **Edit**.
- Konfigurieren Sie die Verbindung wie in Abb. 2.3.1 gezeigt.

Abb. 2.3.1



- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

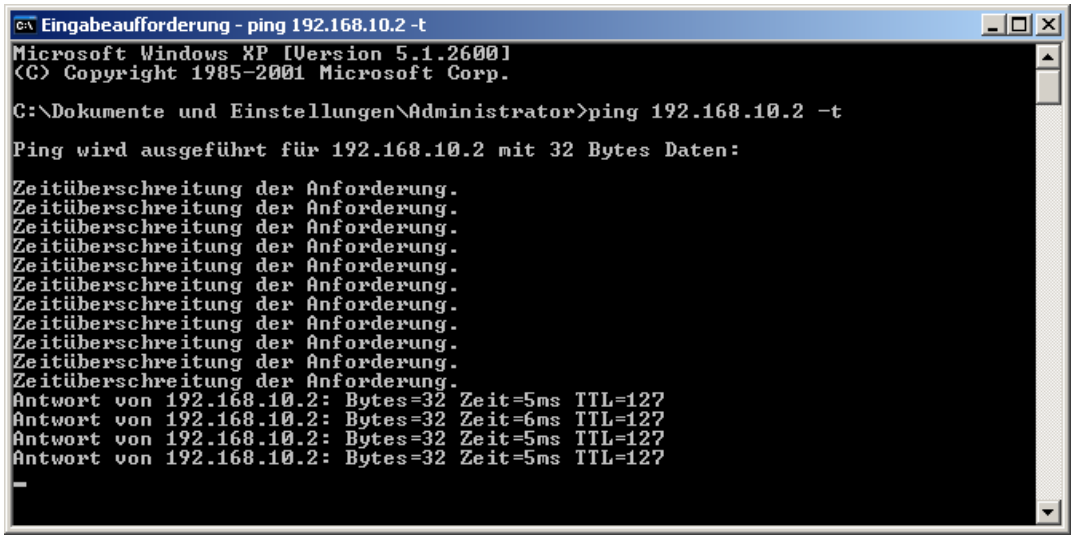
2.4. Testen der Verbindung

Um die Verbindung zu testen, versuchen Sie beispielsweise von einem PC an Standort A (z.B. 192.168.0.2) einen PC an Standort B (z.B. 192.168.10.2) zu erreichen:

Hinweis:	- Bei beiden PCs muss der jeweils lokale Router als Gateway verwendet werden: - Der PC an Standort A (192.168.**0**.2) verwendet als Gateway seinen lokalen Router 192.168.**0**.1. - Der PC an Standort B (192.168.**10**.2) verwendet als Gateway seinen lokalen Router 192.168.**10**.1.

- Klicken Sie in Windows links unten auf **Start** und **Ausführen...**
- Geben Sie **cmd** ein (Windows 95/98/ME: **command**) und klicken Sie auf **OK**
- Geben Sie folgenden Befehl ein: **ping 192.168.10.2 –t** (siehe Abb. 2.4.1)

Abb. 2.4.1



- Bei richtiger Konfiguration wird die VPN-Verbindung innerhalb einiger Sekunden aufgebaut (siehe Abb. 2.4.1).
- Der VPN Status des FVS318v1 (**Show VPN Status** im Menü **Router Status**) zeigt ebenfalls eine etablierte VPN-Verbindung (siehe Abb. 2.4.2).

Abb. 2.4.2

IPSec Connection Status

Status	Connection Name	Remote IP	Virtual Network	Type	State	Drop
Active	Beispiel	217.233.101.136	192.168.10.0/24	ESP(3DES-CBC SHA-1)	[P1:M-Estab.] [P2:Q-Estab.]	Drop

3. Beispielkonfiguration

FVS318v1 mit dynamischer WAN-IP-Adresse
zu
FVS318v1 mit dynamischer WAN-IP-Adresse

3.1. Übersicht

Standort A:

FVS318v1 (Firmware 2.4)

FVS318v1 LAN-Seite: 192.168.0.1
FVS318v1 WAN-Seite: standorta.dyndns.org

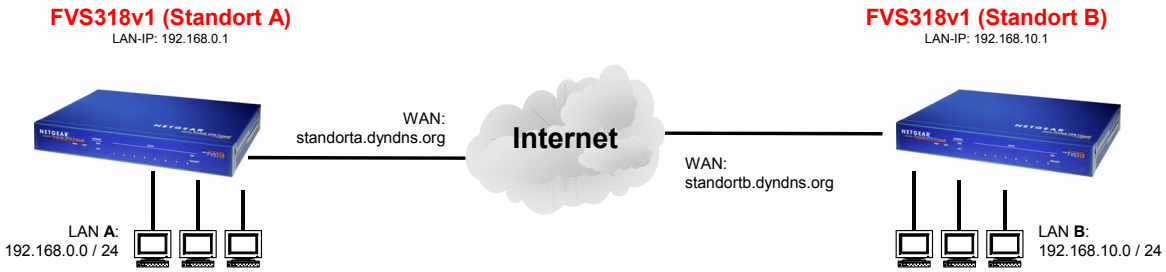
Netzwerkadresse: 192.168.0.0/24
Test-PC im Netzwerk: 192.168.0.2

Standort B:

FVS318 (Firmware 2.4)

FVS318v1 LAN-Seite: 192.168.10.1
FVS318v1 WAN-Seite: standortb.dyndns.org

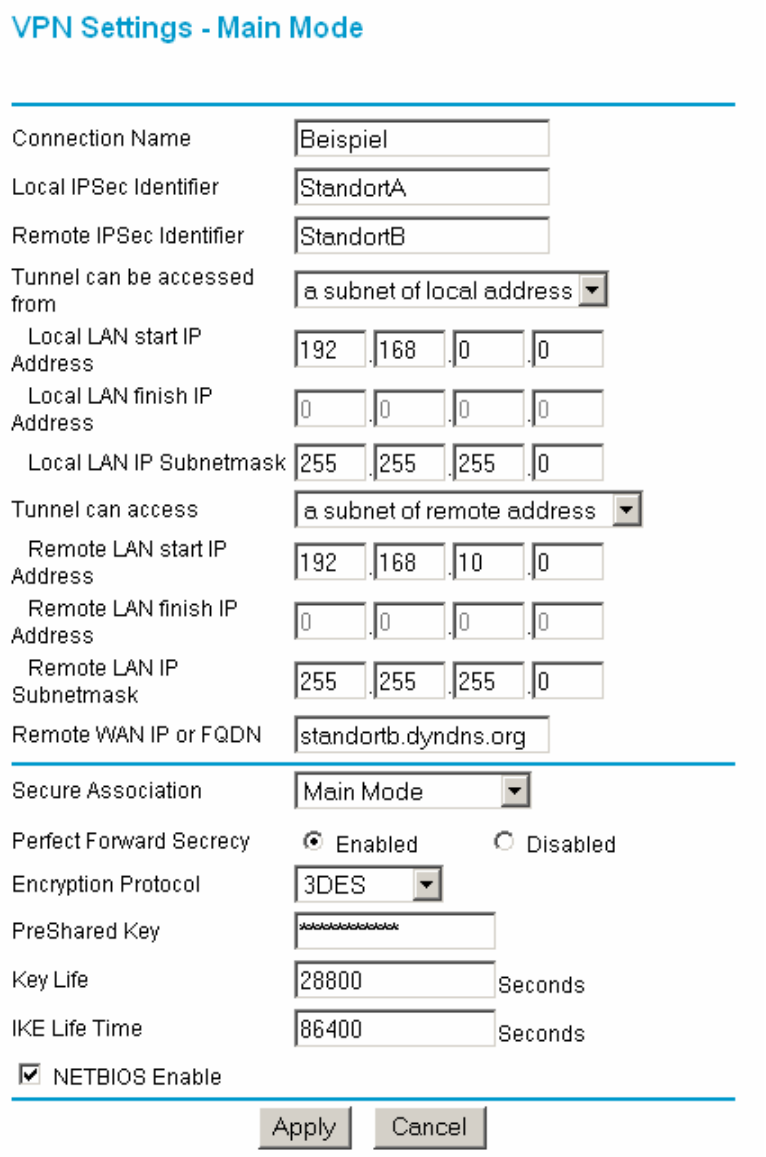
Netzwerkadresse: 192.168.10.0/24
Test-PC im Netzwerk: 192.168.10.2



3.2. Konfiguration des Routers an Standort A

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links oben auf den Menüpunkt **VPN Settings**.
- Aktivieren Sie den Punkt vor der 1 und klicken Sie auf **Edit**.
- Konfigurieren Sie die Verbindung wie in Abb. 3.2.1 gezeigt.

Abb. 3.2.1

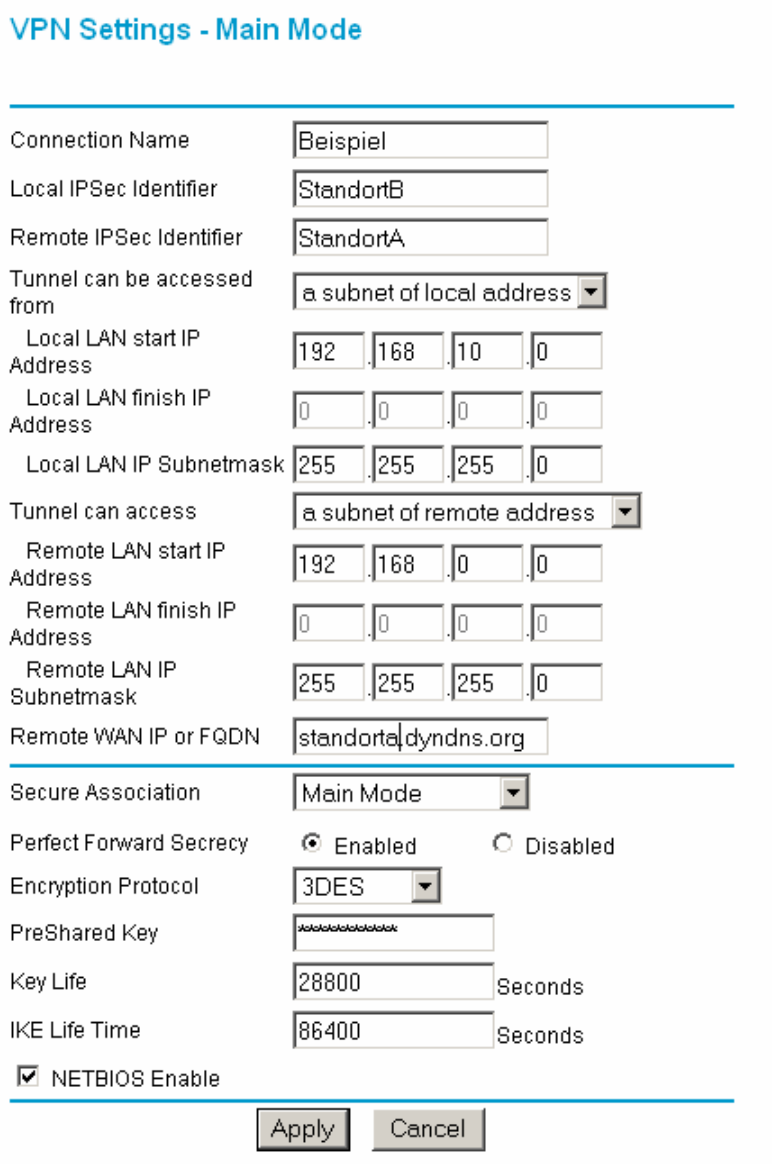


- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

3.3. Konfiguration des Routers an Standort B

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links oben auf den Menüpunkt **VPN Settings**.
- Aktivieren Sie den Punkt vor der 1 und klicken Sie auf **Edit**.
- Konfigurieren Sie die Verbindung wie in Abb. 3.3.1 gezeigt.

Abb. 3.3.1



- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

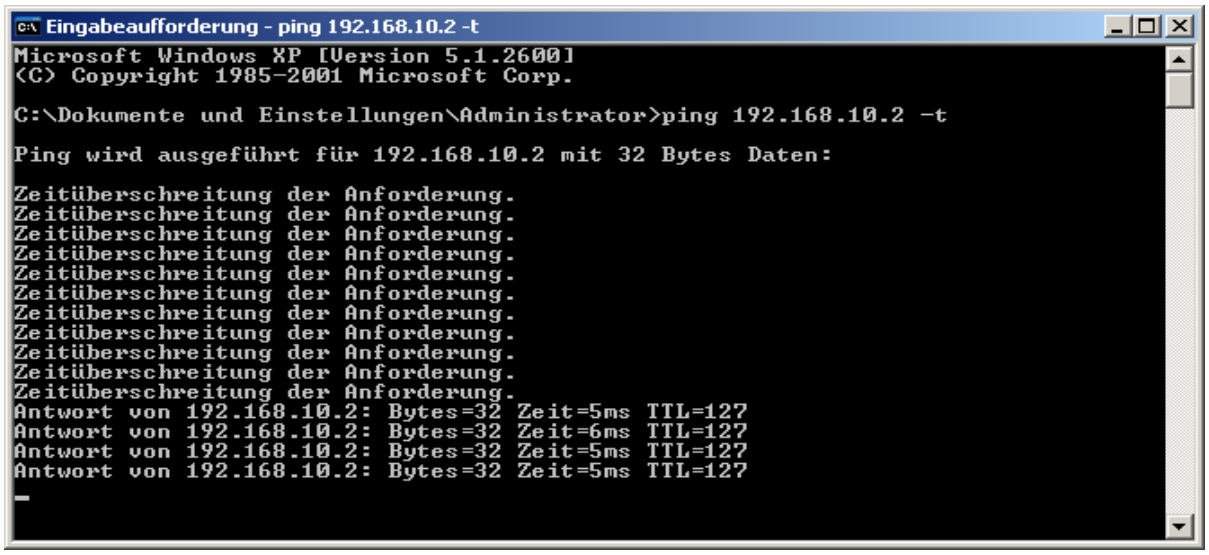
3.4. Testen der Verbindung

Um die Verbindung zu testen, versuchen Sie beispielsweise von einem PC an Standort A (z.B. 192.168.0.2) einen PC an Standort B (z.B. 192.168.10.2) zu erreichen:

Hinweis:	- Bei beiden PCs muss der jeweils lokale Router als Gateway verwendet werden: - Der PC an Standort A (192.168.0.2) verwendet als Gateway seinen lokalen Router 192.168.0.1. - Der PC an Standort B (192.168.**10**.2) verwendet als Gateway seinen lokalen Router 192.168.**10**.1.

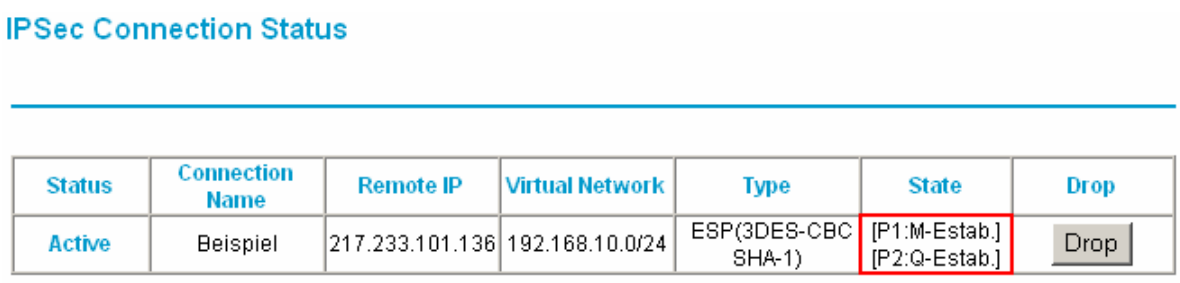
- Klicken Sie in Windows links unten auf **Start** und **Ausführen...**
- Geben Sie **cmd** ein (Windows 95/98/ME: **command**) und klicken Sie auf **OK**
- Geben Sie folgenden Befehl ein: **ping 192.168.10.2 –t** (siehe Abb. 3.4.1)

Abb. 3.4.1



- Bei richtiger Konfiguration wird die VPN-Verbindung innerhalb einiger Sekunden aufgebaut (siehe Abb. 3.4.1).
- Der VPN Status des FVS318v1 (**Show VPN Status** im Menü **Router Status**) zeigt ebenfalls eine etablierte VPN-Verbindung (siehe Abb. 3.4.2).

Abb. 3.4.2



4. Beispielkonfiguration

FVL328 mit fester WAN-IP-Adresse
zu
FVL328 mit fester WAN-IP-Adresse

4.1. Übersicht

Standort A:

FVL328 (Firmware 2.0 Release 08)

FVL328 LAN-Seite: 192.168.0.1
FVL328 WAN-Seite: 217.232.56.129

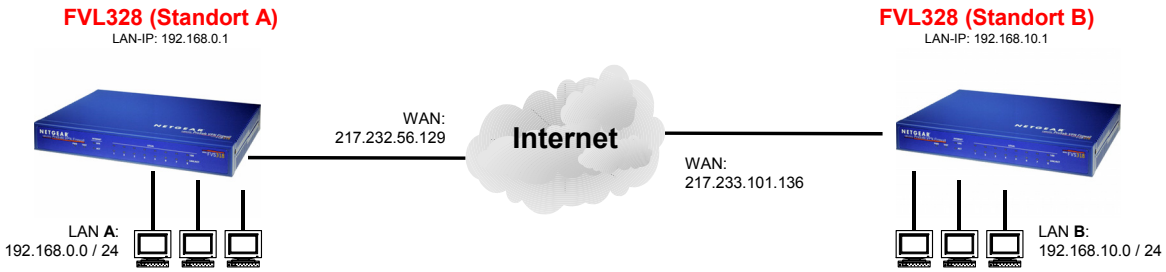
Netzwerkadresse: 192.168.0.0/24
Test-PC im Netzwerk: 192.168.0.2

Standort B:

FVL328 (Firmware 2.0 Release 08)

FVL328 LAN-Seite: 192.168.10.1
FVL328 WAN-Seite: 217.233.101.136

Netzwerkadresse: 192.168.10.0/24
Test-PC im Netzwerk: 192.168.10.2

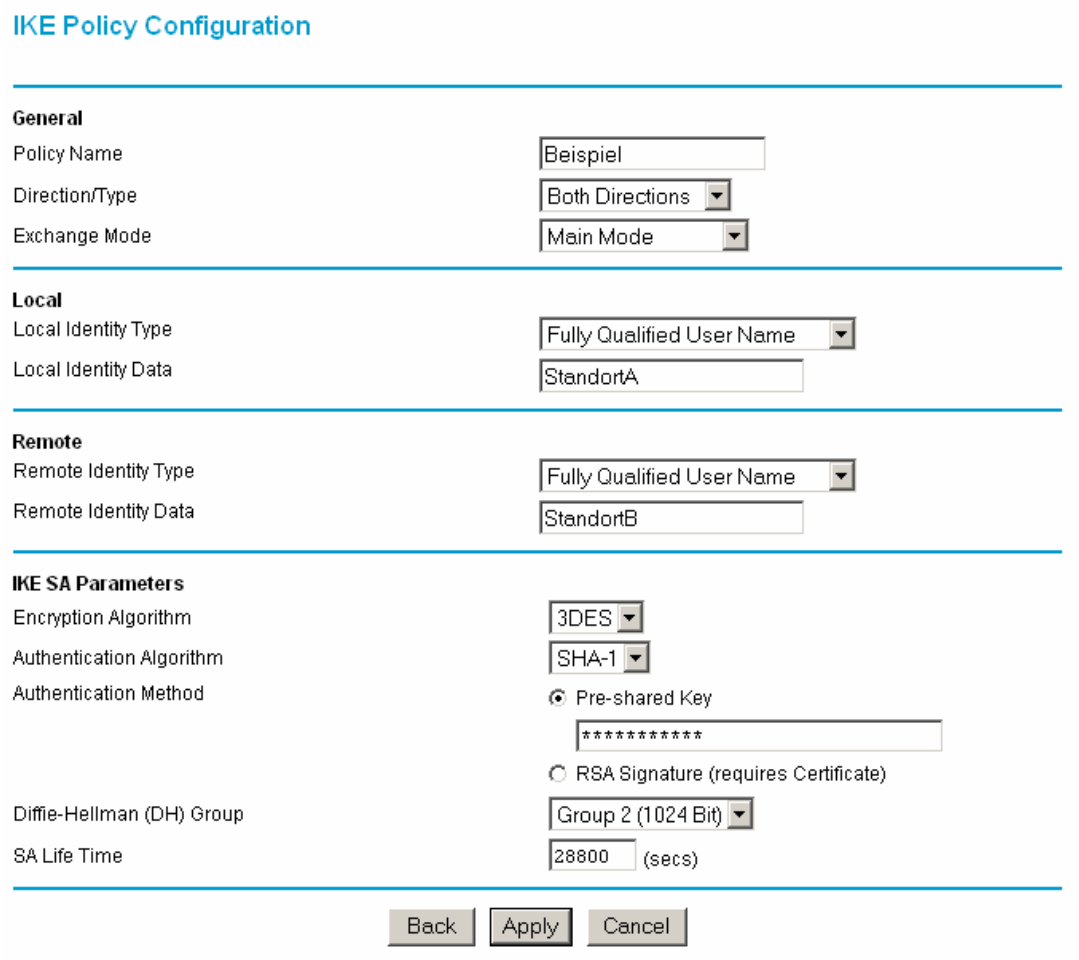


4.2. Konfiguration des Routers an Standort A

Schritt 1: Erstellen der IKE-Policy (Phase 1)

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links auf den Menüpunkt **IKE Policies**.
- Klicken Sie dort auf den Button **Add** um eine IKE-Policy zu erstellen.
- Konfigurieren Sie die IKE-Policy wie in Abb. 4.2.1 gezeigt.

Abb. 4.2.1

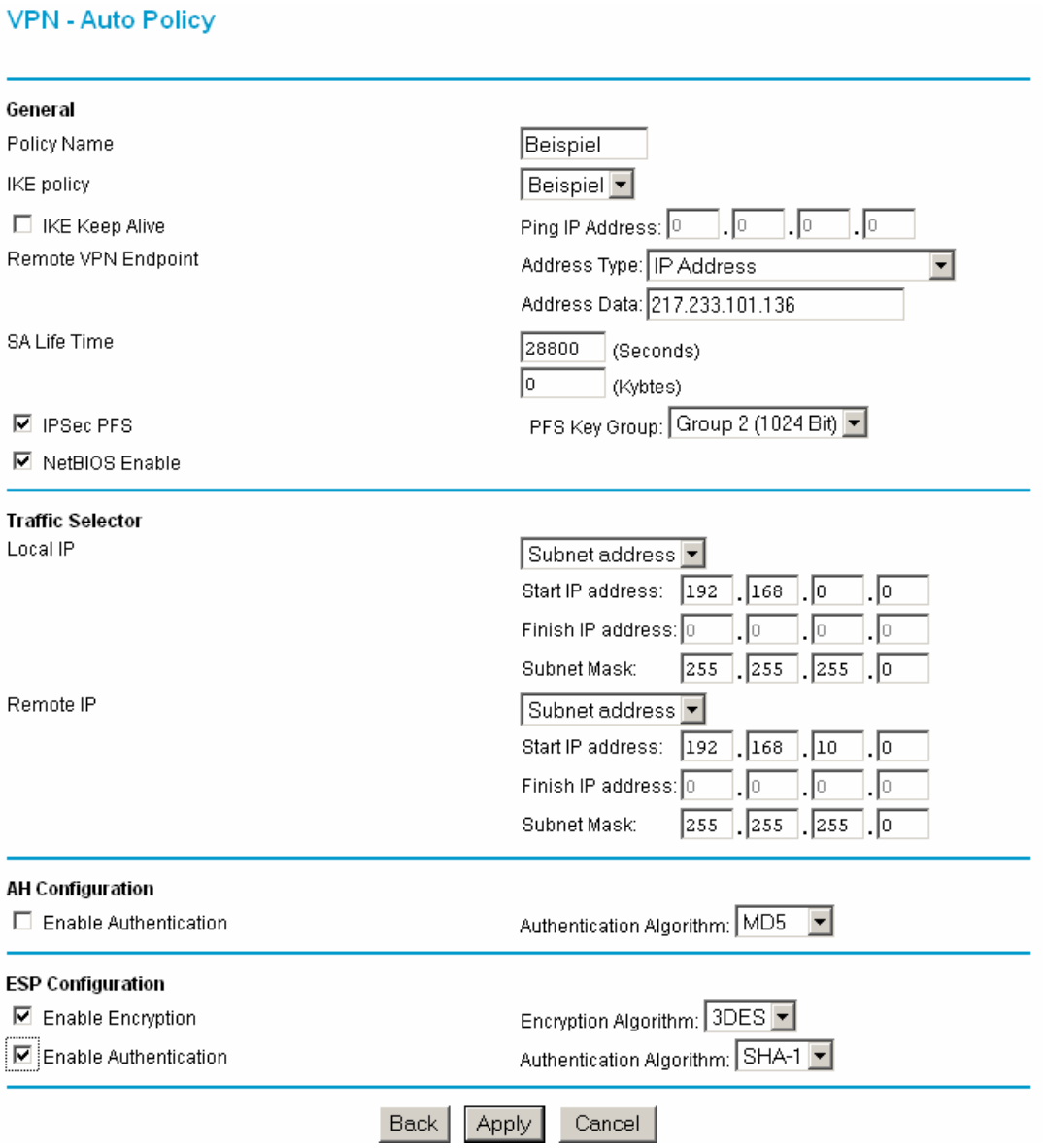


- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

Schritt 2: Erstellen der VPN-Policy (Phase 2)

- Klicken Sie links auf den Menüpunkt **VPN Policies**.
- Um eine VPN-Policy zu erstellen, klicken Sie auf **Add Auto Policy**.
- Konfigurieren Sie die VPN-Policy wie in Abb. 4.2.2 gezeigt.
  ! Bei dem Punkt **IKE policy** wählen Sie die in Schritt 1 erstellte IKE Policy.

Abb. 4.2.2



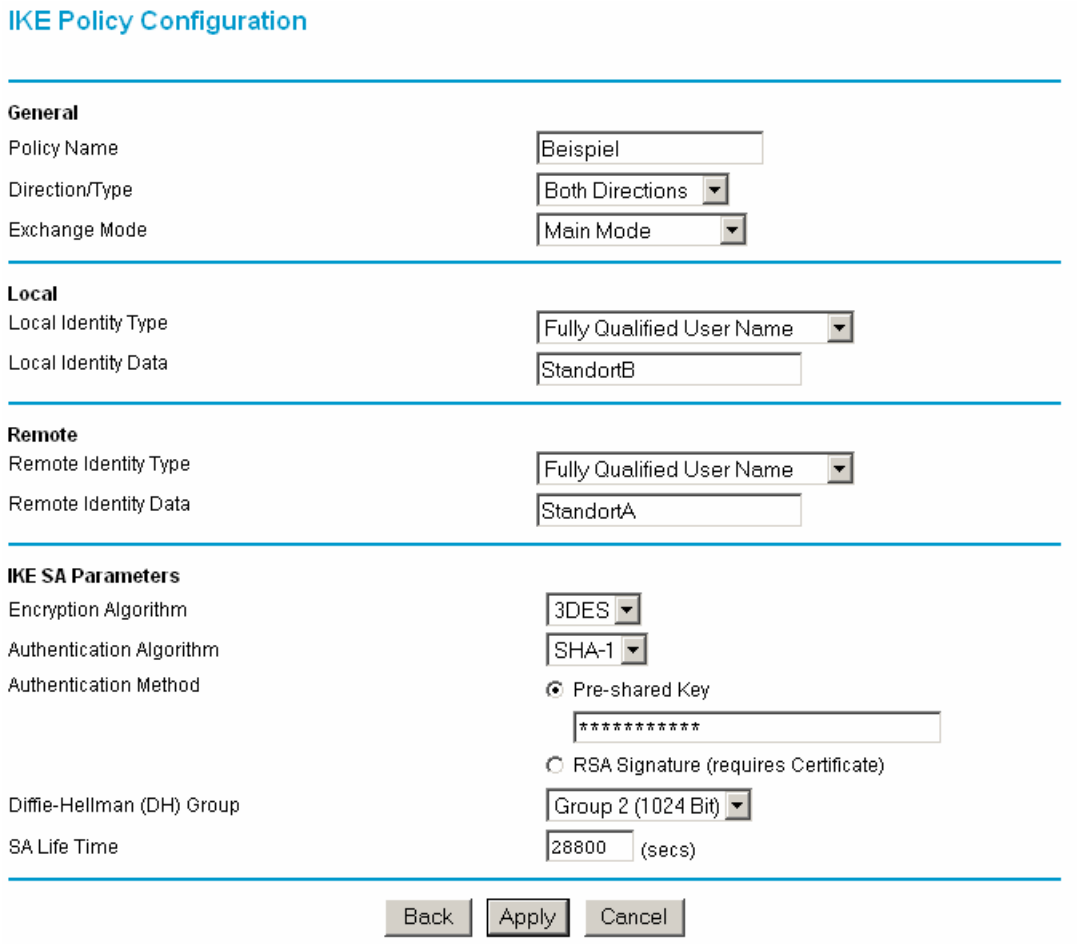
- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

4.3. Konfiguration des Routers an Standort B

Schritt 1: Erstellen der IKE-Policy (Phase 1)

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links auf den Menüpunkt **IKE Policies**.
- Klicken Sie dort auf den Button **Add** um eine IKE-Policy zu erstellen.
- Konfigurieren Sie die IKE-Policy wie in Abb. 4.3.1 gezeigt.

Abb. 4.3.1

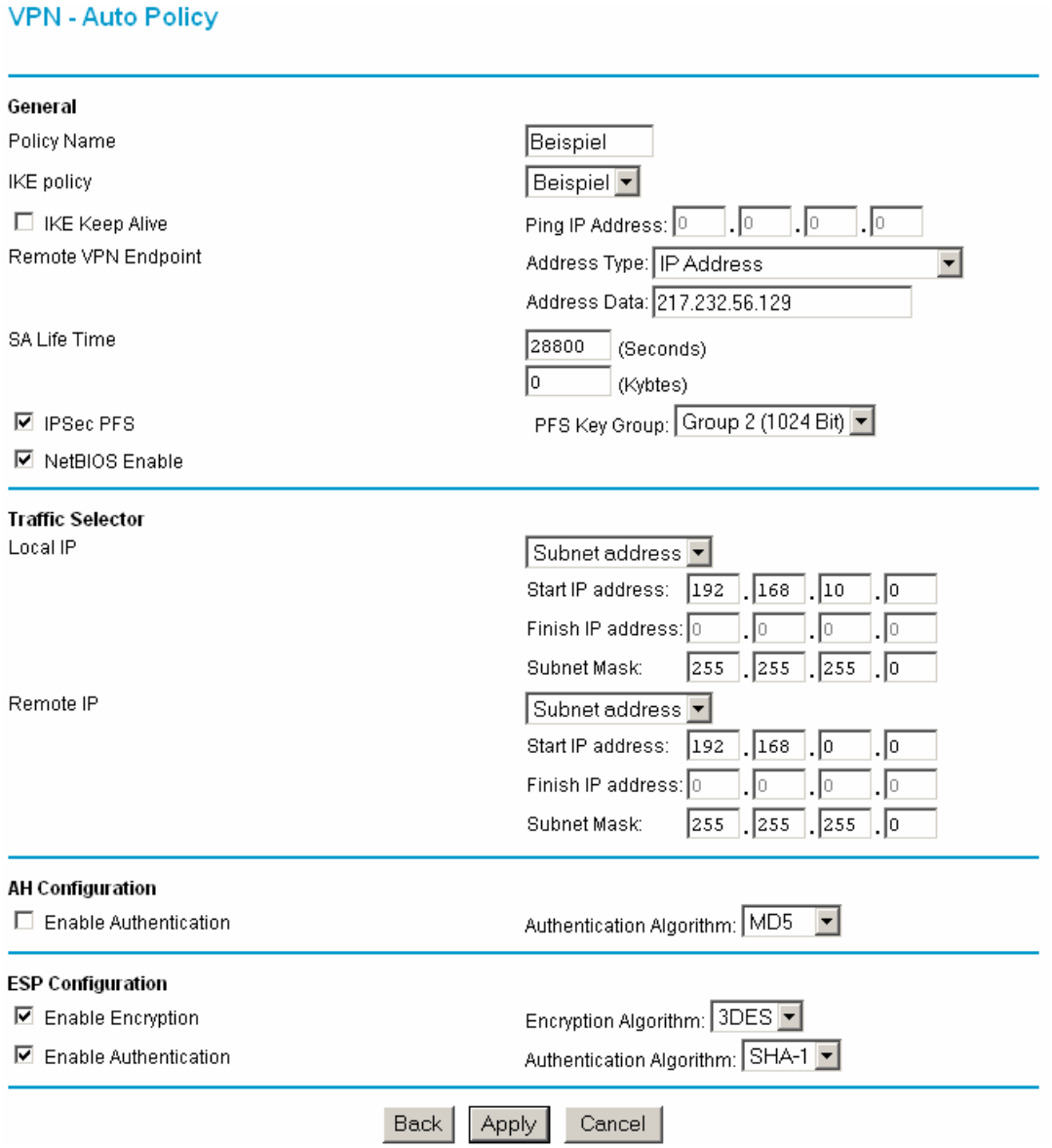


- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

Schritt 2: Erstellen der VPN-Policy (Phase 2)

- Klicken Sie links auf den Menüpunkt **VPN Policies**.
- Um eine VPN-Policy zu erstellen, klicken Sie auf **Add Auto Policy**.
- Konfigurieren Sie die VPN-Policy wie in Abb. 4.3.2 gezeigt.
  ! Bei dem Punkt **IKE policy** wählen Sie die in Schritt 1 erstellte IKE Policy.

Abb. 4.3.2



- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

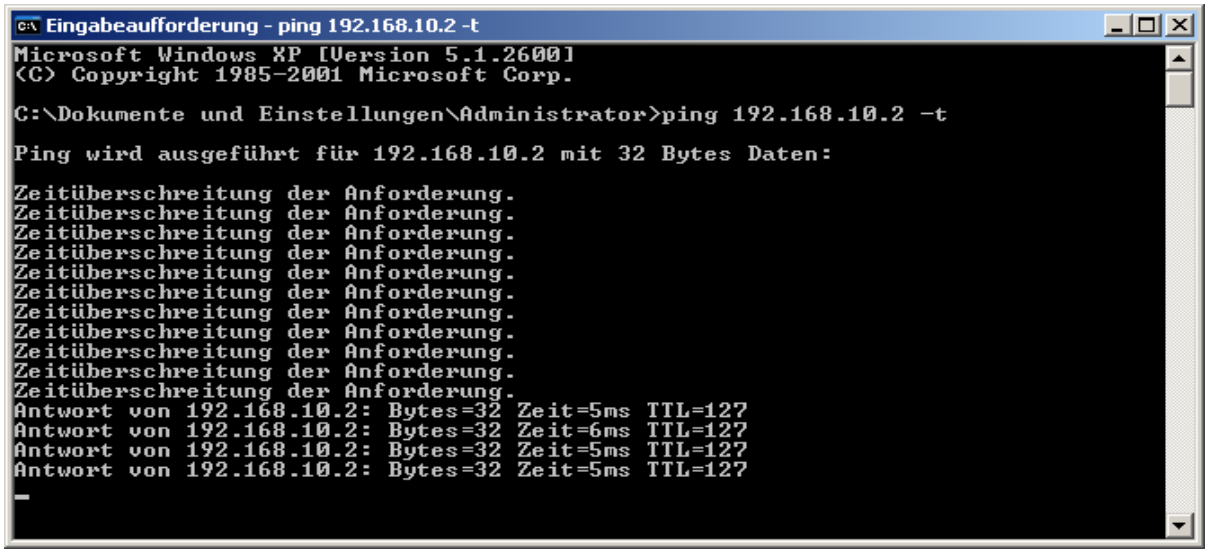
4.4. Testen der Verbindung

Um die Verbindung zu testen, versuchen Sie beispielsweise von einem PC an Standort A (z.B. 192.168.0.2) einen PC an Standort B (z.B. 192.168.10.2) zu erreichen:

Hinweis:	- Bei beiden PCs muss der jeweils lokale Router als Gateway verwendet werden: - Der PC an Standort A (192.168.**0**.2) verwendet als Gateway seinen lokalen Router 192.168.**0**.1. - Der PC an Standort B (192.168.**10**.2) verwendet als Gateway seinen lokalen Router 192.168.**10**.1.

- Klicken Sie in Windows links unten auf **Start** und **Ausführen...**
- Geben Sie **cmd** ein (Windows 95/98/ME: **command**) und klicken Sie auf **OK**
- Geben Sie folgenden Befehl ein: **ping 192.168.10.2 –t** (siehe Abb. 4.4.1)

Abb. 4.4.1



- Bei richtiger Konfiguration wird die VPN-Verbindung innerhalb einiger Sekunden aufgebaut (siehe Abb. 4.4.1).

- Der VPN Status des FVL328 (Menüpunkt **VPN Status** in der Router-Konfiguration) zeigt ebenfalls eine etablierte VPN-Verbindung

5. Beispielkonfiguration

FVL328 mit dynamischer WAN-IP-Adresse
zu
FVL328 mit fester WAN-IP-Adresse

5.1. Übersicht

Standort A:

FVL328 (Firmware 2.0 Release 08)

FVL328 LAN-Seite: 192.168.0.1
FVL328 WAN-Seite: standorta.dyndns.org

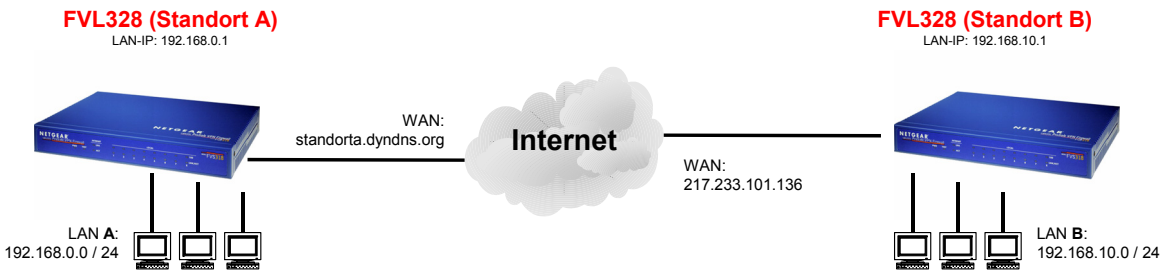
Netzwerkadresse: 192.168.0.0/24
Test-PC im Netzwerk: 192.168.0.2

Standort B:

FVL328 (Firmware 2.0 Release 08)

FVL328 LAN-Seite: 192.168.10.1
FVL328 WAN-Seite: 217.233.101.136

Netzwerkadresse: 192.168.10.0/24
Test-PC im Netzwerk: 192.168.10.2

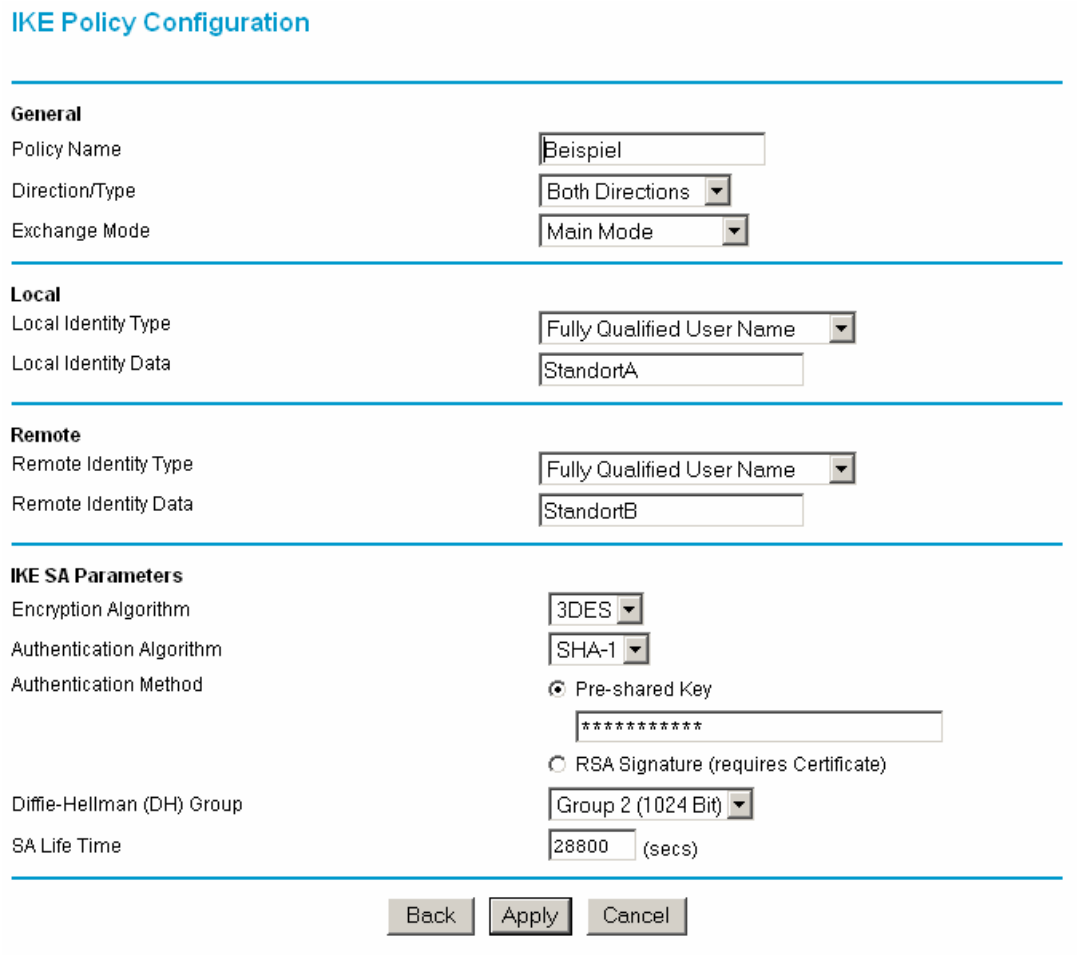


5.2. Konfiguration des Routers an Standort A

Schritt 1: Erstellen der IKE-Policy (Phase 1)

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links auf den Menüpunkt **IKE Policies**.
- Klicken Sie dort auf den Button **Add** um eine IKE-Policy zu erstellen.
- Konfigurieren Sie die IKE-Policy wie in Abb. 5.2.1 gezeigt.

Abb. 5.2.1

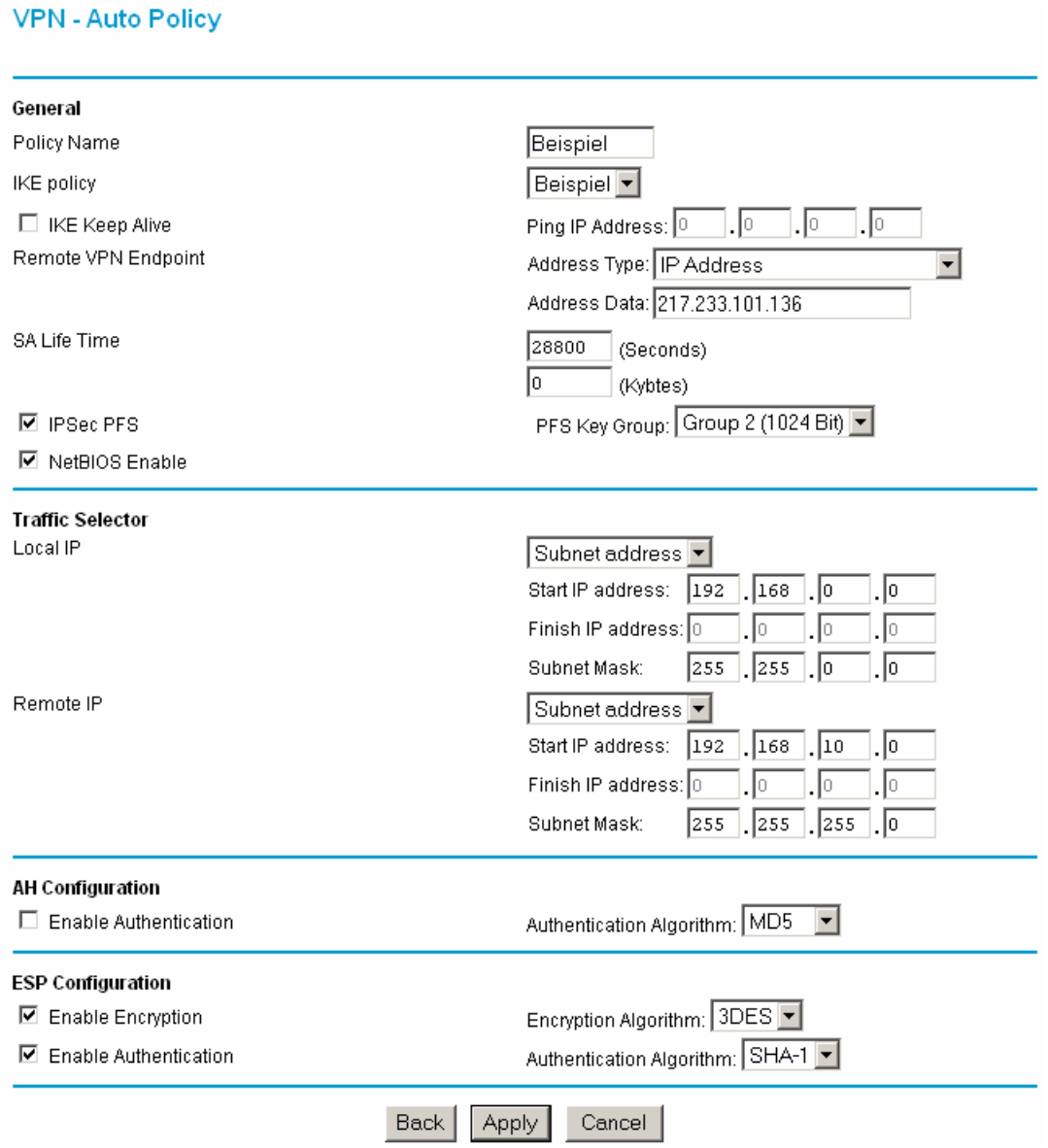


- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

Schritt 2: Erstellen der VPN-Policy (Phase 2)

- Klicken Sie links auf den Menüpunkt **VPN Policies**.
- Um eine VPN-Policy zu erstellen, klicken Sie auf **Add Auto Policy**.
- Konfigurieren Sie die VPN-Policy wie in Abb. 5.2.2 gezeigt.
  ! Bei dem Punkt **IKE policy** wählen Sie die in Schritt 1 erstellte IKE Policy.

Abb. 5.2.2



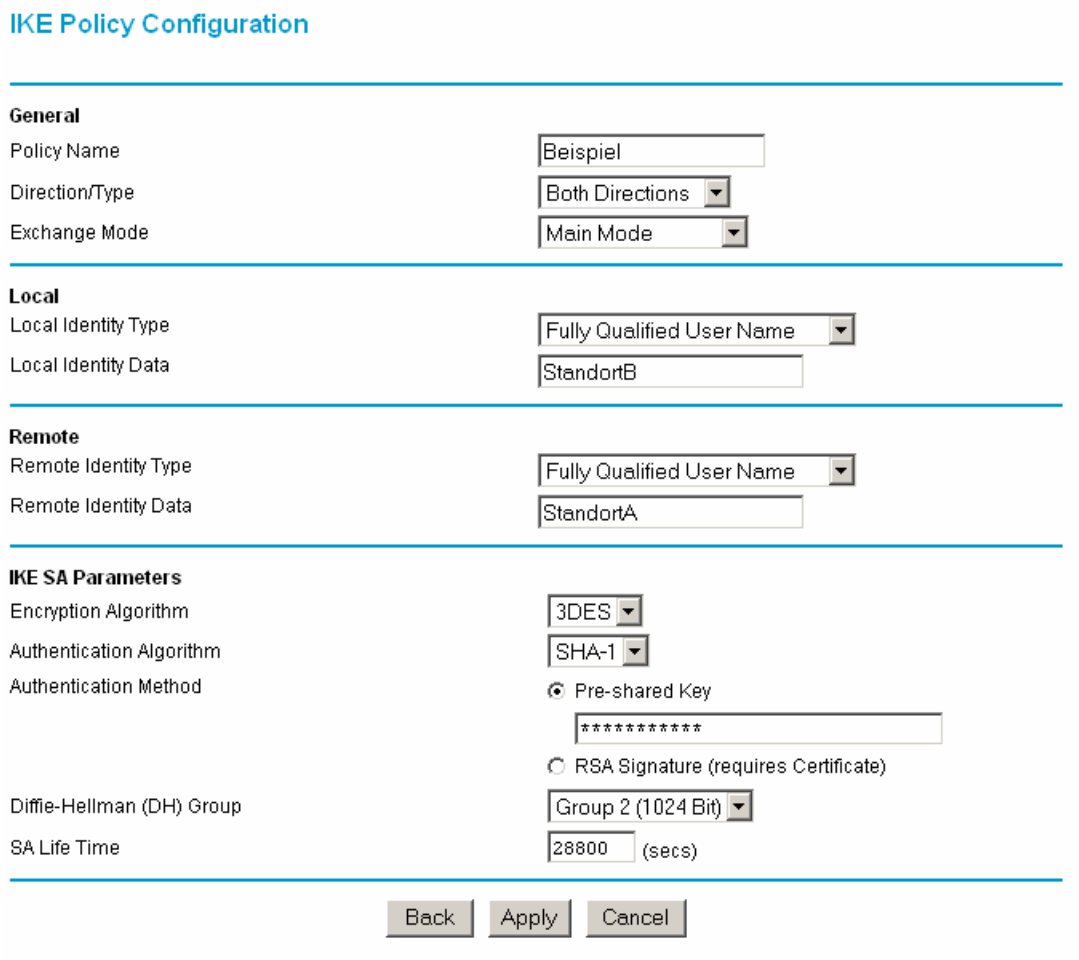
- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

5.3. Konfiguration des Routers an Standort B

Schritt 1: Erstellen der IKE-Policy (Phase 1)

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links auf den Menüpunkt **IKE Policies**.
- Klicken Sie dort auf den Button **Add** um eine IKE-Policy zu erstellen.
- Konfigurieren Sie die IKE-Policy wie in Abb. 5.3.1 gezeigt.

Abb. 5.3.1

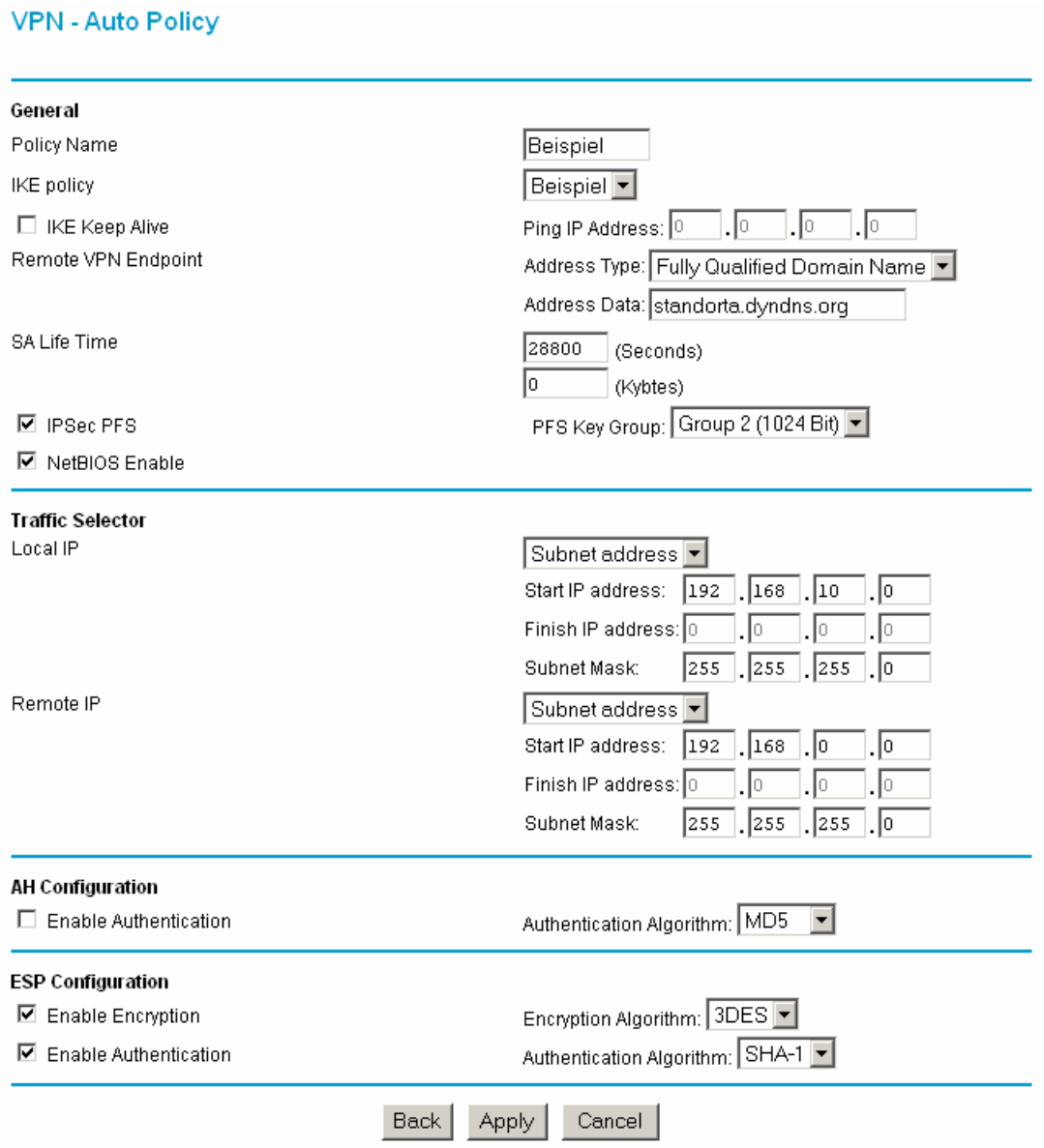


- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

Schritt 2: Erstellen der VPN-Policy (Phase 2)

- Klicken Sie links auf den Menüpunkt **VPN Policies**.
- Um eine VPN-Policy zu erstellen, klicken Sie auf **Add Auto Policy**.
- Konfigurieren Sie die VPN-Policy wie in Abb. 5.3.2 gezeigt.
  ! Bei dem Punkt **IKE policy** wählen Sie die in Schritt 1 erstellte IKE Policy.

Abb. 5.3.2



- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

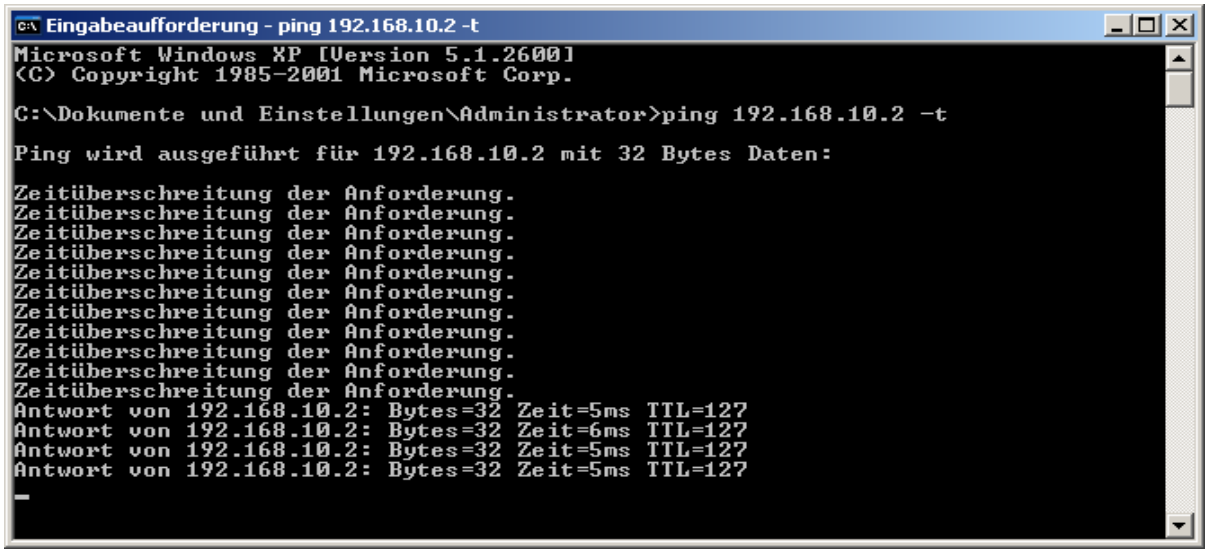
5.4. Testen der Verbindung

Um die Verbindung zu testen, versuchen Sie beispielsweise von einem PC an Standort A (z.B. 192.168.0.2) einen PC an Standort B (z.B. 192.168.10.2) zu erreichen:

Hinweis:	- Bei beiden PCs muss der jeweils lokale Router als Gateway verwendet werden: - Der PC an Standort A (192.168.**0**.2) verwendet als Gateway seinen lokalen Router 192.168.**0**.1. - Der PC an Standort B (192.168.**10**.2) verwendet als Gateway seinen lokalen Router 192.168.**10**.1.

- Klicken Sie in Windows links unten auf **Start** und **Ausführen...**
- Geben Sie **cmd** ein (Windows 95/98/ME: **command**) und klicken Sie auf **OK**
- Geben Sie folgenden Befehl ein: **ping 192.168.10.2 –t** (siehe Abb. 5.4.1)

Abb. 5.4.1



- Bei richtiger Konfiguration wird die VPN-Verbindung innerhalb einiger Sekunden aufgebaut (siehe Abb. 5.4.1).

- Der VPN Status des FVL328 (Menüpunkt **VPN Status** in der Router-Konfiguration) zeigt ebenfalls eine etablierte VPN-Verbindung.

6. Beispielkonfiguration

FVL328 mit dynamischer WAN-IP-Adresse
zu
FVL328 mit dynamischer WAN-IP-Adresse

6.1. Übersicht

Standort A:

FVL328 (Firmware 2.0 Release 08)

FVL328 LAN-Seite: 192.168.0.1
FVL328 WAN-Seite: standorta.dyndns.org

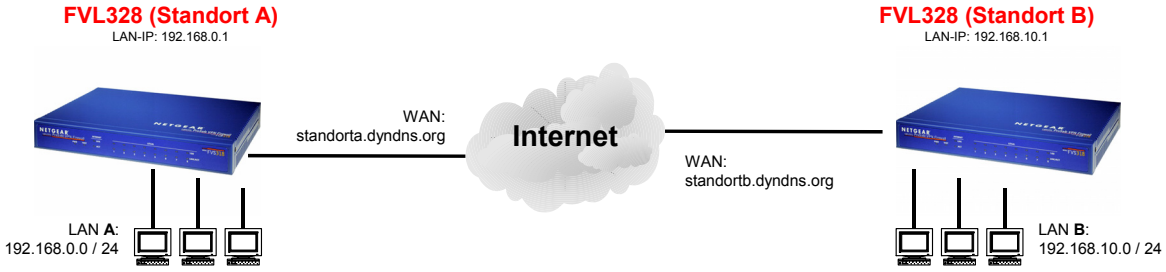
Netzwerkadresse: 192.168.0.0/24
Test-PC im Netzwerk: 192.168.0.2

Standort B:

FVL328 (Firmware 2.0 Release 08)

FVL328 LAN-Seite: 192.168.10.1
FVL328 WAN-Seite: standortb.dyndns.org

Netzwerkadresse: 192.168.10.0/24
Test-PC im Netzwerk: 192.168.10.2

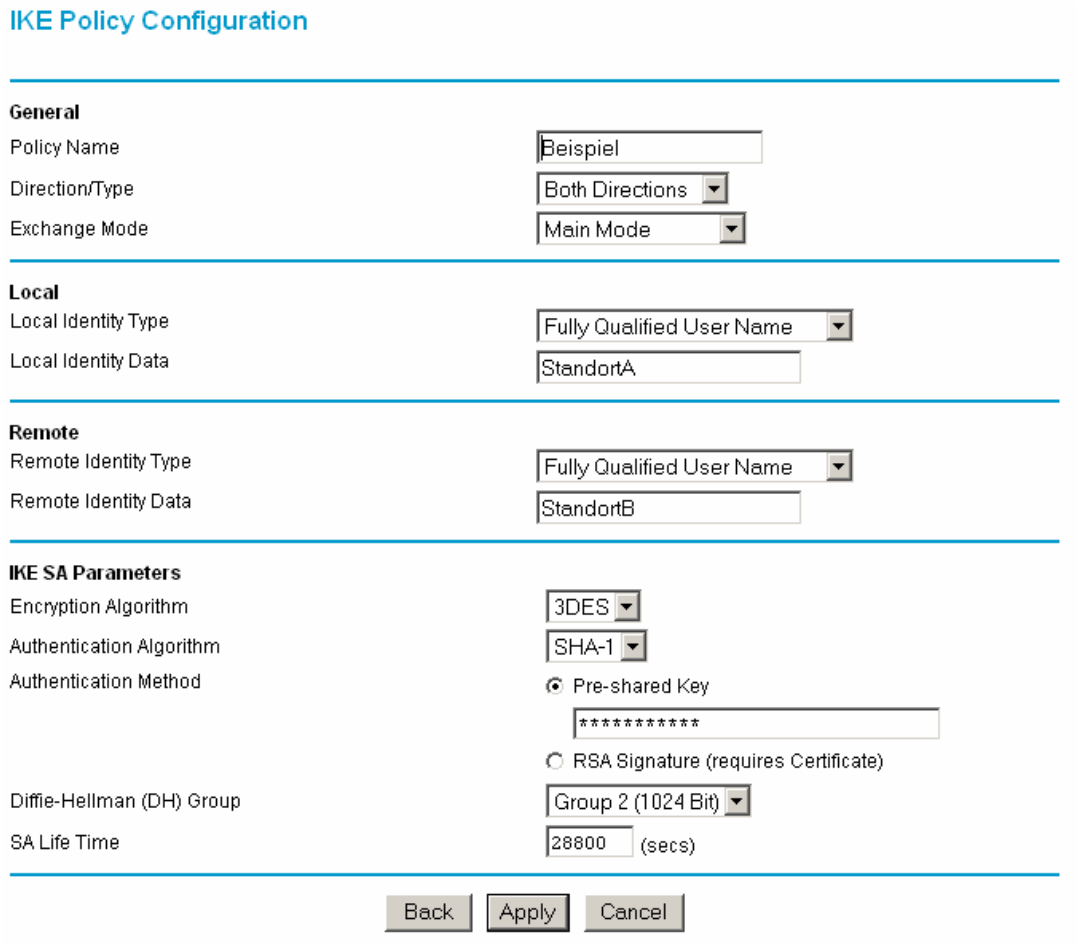


6.2. Konfiguration des Routers an Standort A

Schritt 1: Erstellen der IKE-Policy (Phase 1)

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links auf den Menüpunkt **IKE Policies**.
- Klicken Sie dort auf den Button **Add** um eine IKE-Policy zu erstellen.
- Konfigurieren Sie die IKE-Policy wie in Abb. 6.2.1 gezeigt.

Abb. 6.2.1

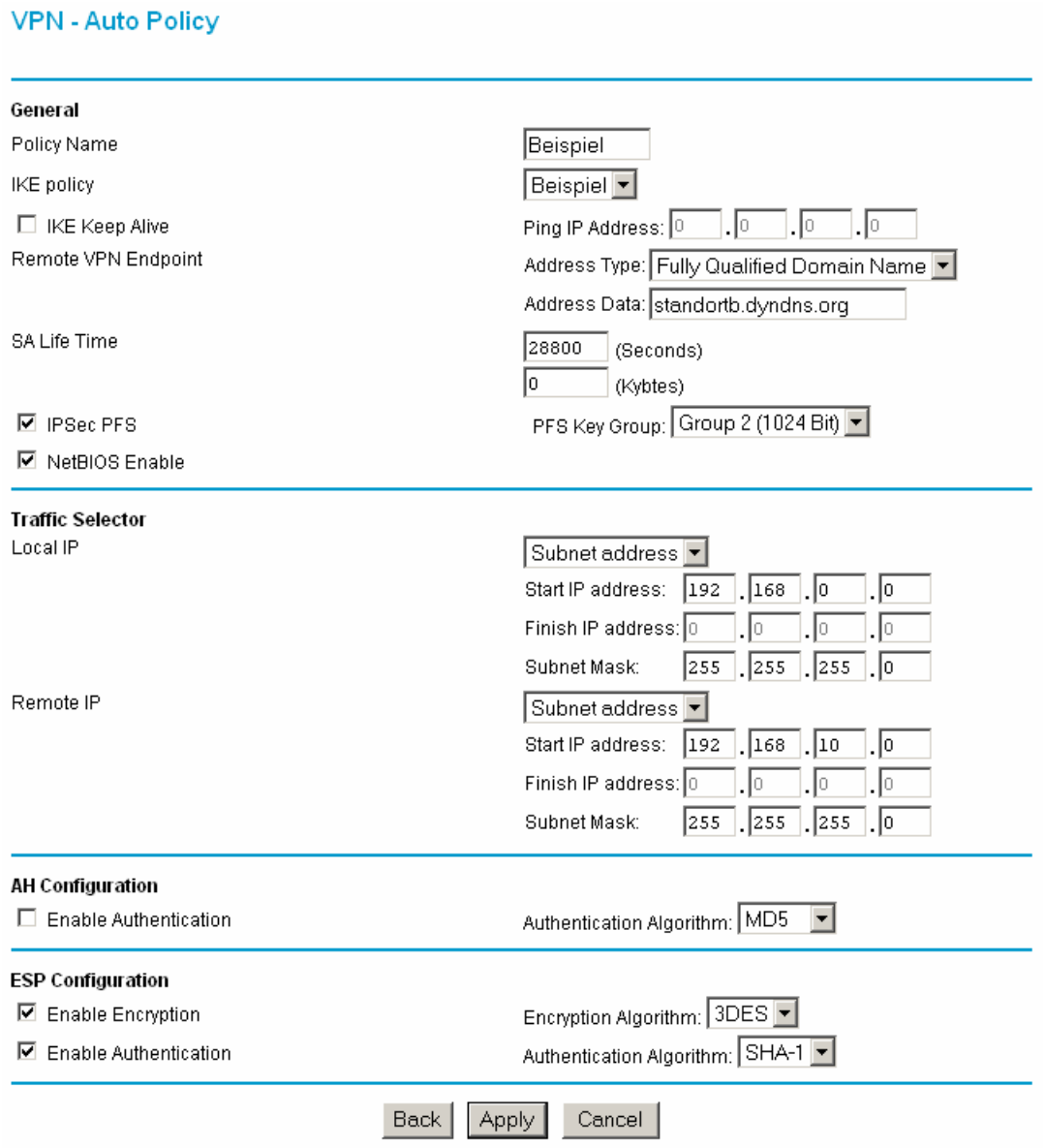


- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

Schritt 2: Erstellen der VPN-Policy (Phase 2)

- Klicken Sie links auf den Menüpunkt **VPN Policies**.
- Um eine VPN-Policy zu erstellen, klicken Sie auf **Add Auto Policy**.
- Konfigurieren Sie die VPN-Policy wie in Abb. 6.2.2 gezeigt.
  ! Bei dem Punkt **IKE policy** wählen Sie die in Schritt 1 erstellte IKE Policy.

Abb. 6.2.2



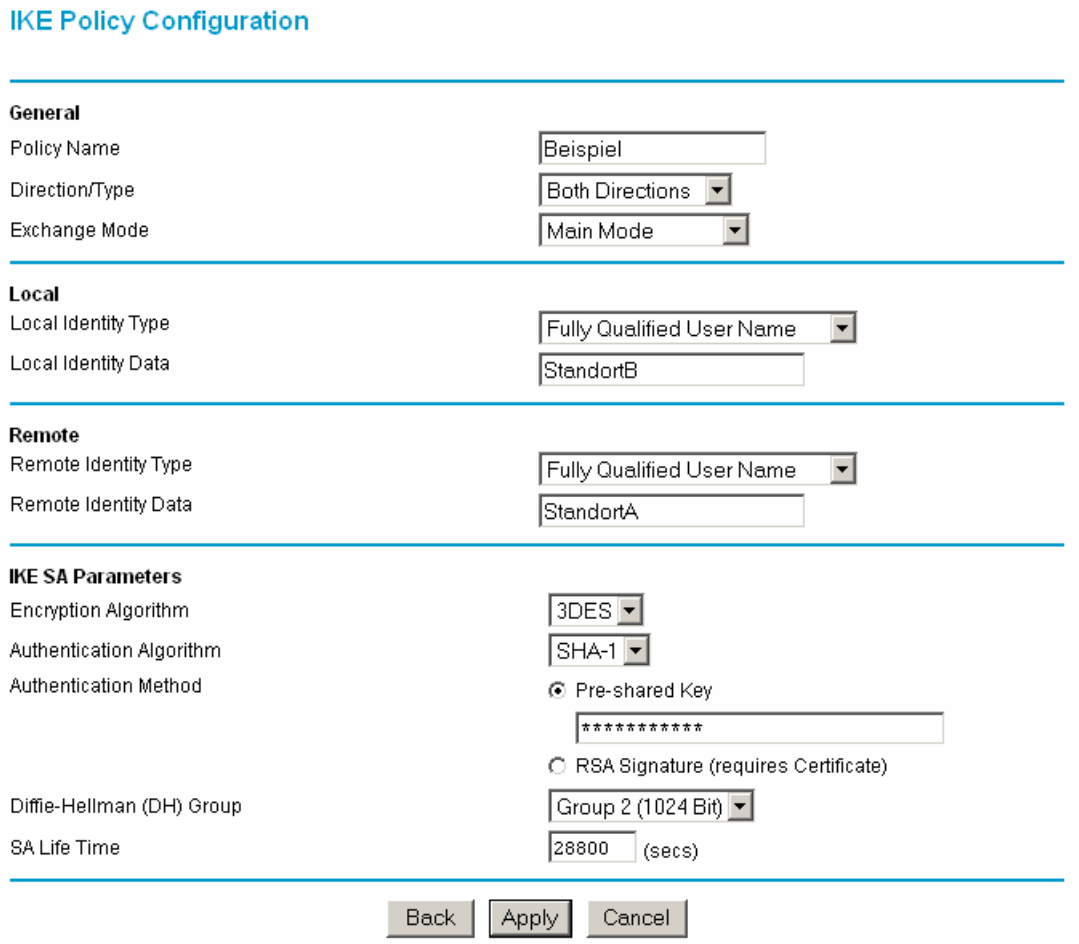
- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

6.3. Konfiguration des Routers an Standort B

Schritt 1: Erstellen der IKE-Policy (Phase 1)

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links auf den Menüpunkt **IKE Policies**.
- Klicken Sie dort auf den Button **Add** um eine IKE-Policy zu erstellen.
- Konfigurieren Sie die IKE-Policy wie in Abb. 6.3.1 gezeigt.

Abb. 6.3.1

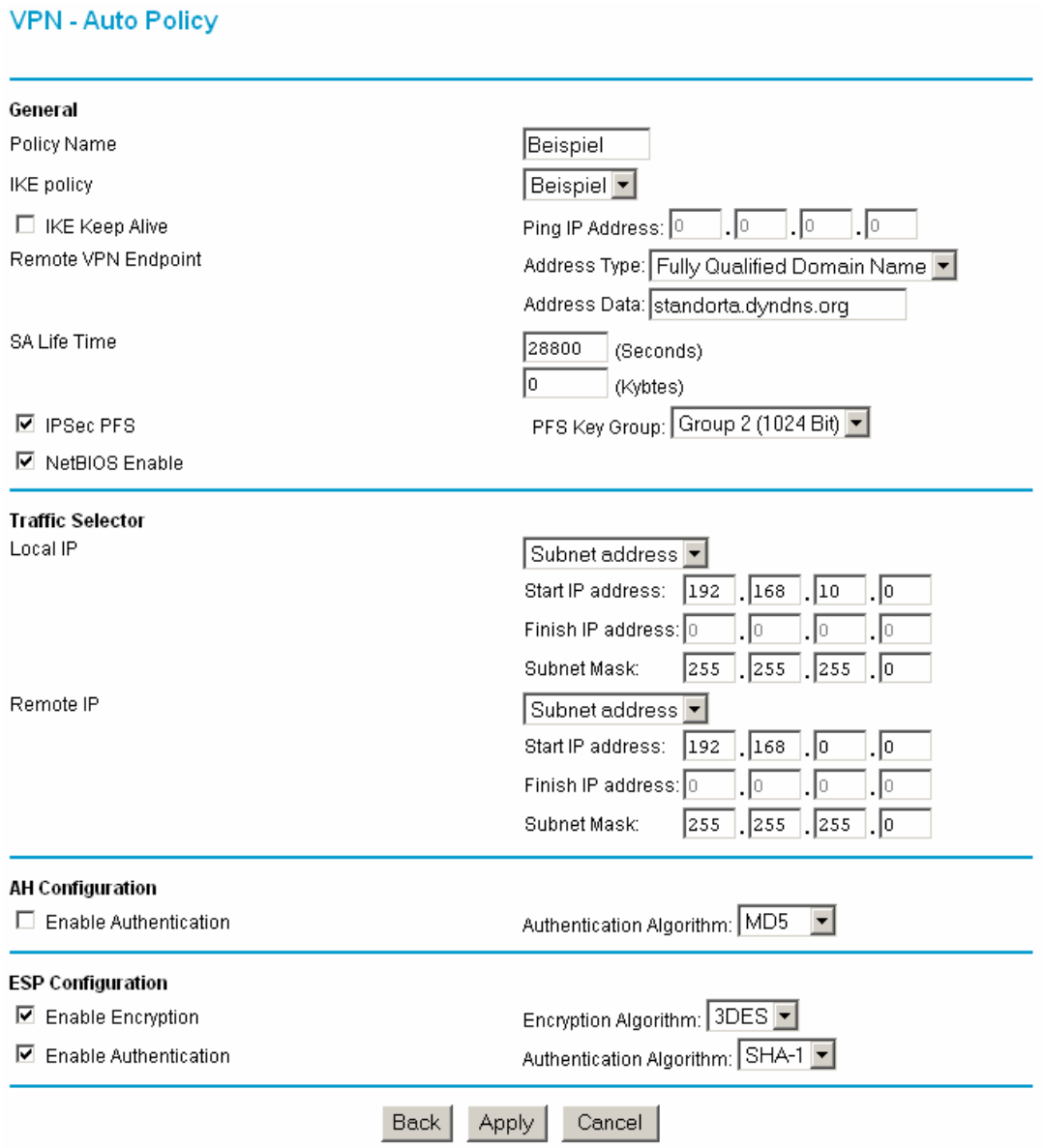


- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

Schritt 2: Erstellen der VPN-Policy (Phase 2)

- Klicken Sie links auf den Menüpunkt **VPN Policies**.
- Um eine VPN-Policy zu erstellen, klicken Sie auf **Add Auto Policy**.
- Konfigurieren Sie die VPN-Policy wie in Abb. 6.3.2 gezeigt.
  ! Bei dem Punkt **IKE policy** wählen Sie die in Schritt 1 erstellte IKE Policy.

Abb. 6.3.2



- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

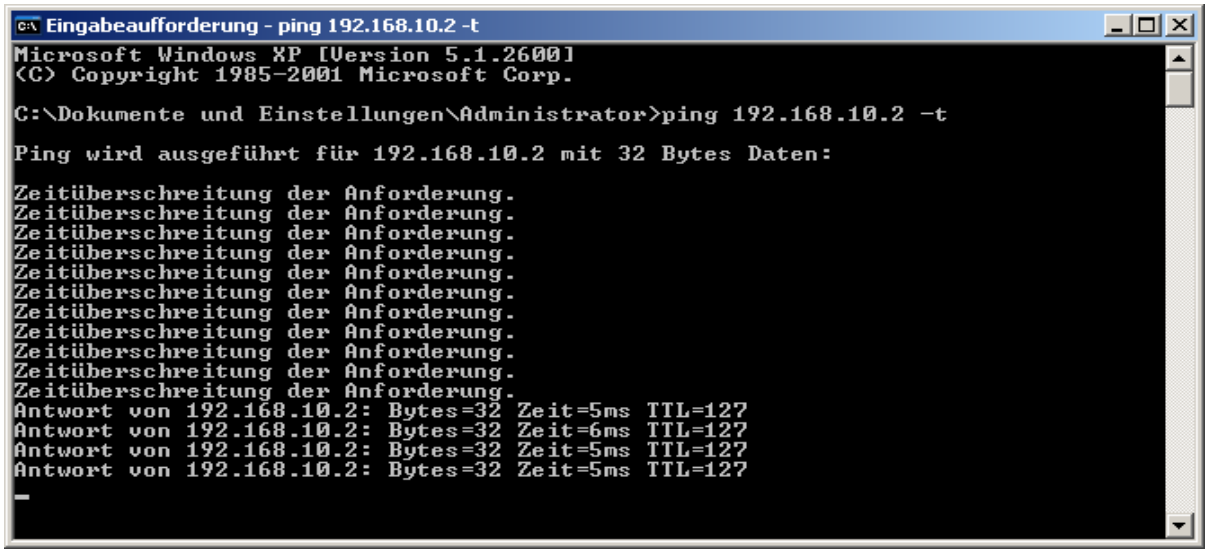
6.4. Testen der Verbindung

Um die Verbindung zu testen, versuchen Sie beispielsweise von einem PC an Standort A (z.B. 192.168.0.2) einen PC an Standort B (z.B. 192.168.10.2) zu erreichen:

Hinweis:	- Bei beiden PCs muss der jeweils lokale Router als Gateway verwendet werden: - Der PC an Standort A (192.168.**0**.2) verwendet als Gateway seinen lokalen Router 192.168.**0**.1. - Der PC an Standort B (192.168.**10**.2) verwendet als Gateway seinen lokalen Router 192.168.**10**.1.

- Klicken Sie in Windows links unten auf **Start** und **Ausführen...**
- Geben Sie **cmd** ein (Windows 95/98/ME: **command**) und klicken Sie auf **OK**
- Geben Sie folgenden Befehl ein: **ping 192.168.10.2 –t** (siehe Abb. 6.4.1)

Abb. 6.4.1



- Bei richtiger Konfiguration wird die VPN-Verbindung innerhalb einiger Sekunden aufgebaut (siehe Abb. 6.4.1).

- Der VPN Status des FVL328 (Menüpunkt **VPN Status** in der Router-Konfiguration) zeigt ebenfalls eine etablierte VPN-Verbindung.

7. Beispielkonfiguration

FVS318v1 mit fester WAN-IP-Adresse
zu
FVL328 mit fester WAN-IP-Adresse

7.1. Übersicht

Standort A:

FVS318v1 (Firmware 2.4)

FVS318v1 LAN-Seite: 192.168.0.1
FVS318v1 WAN-Seite: 217.232.56.129

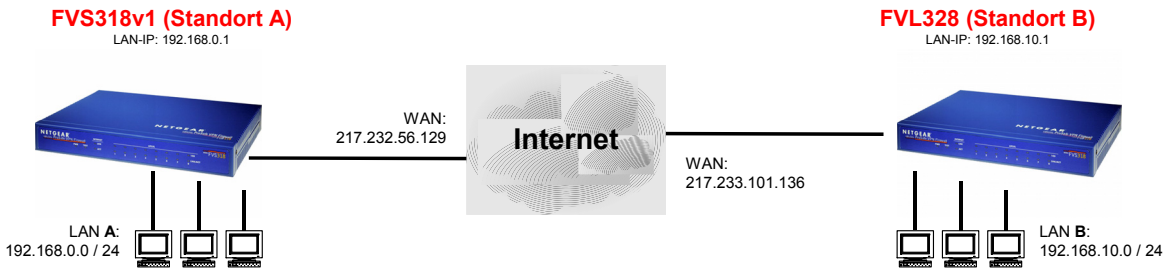
Netzwerkadresse: 192.168.0.0/24
Test-PC im Netzwerk: 192.168.0.2

Standort B:

FVL328 (Firmware 2.0 Release 08)

FVL328 LAN-Seite: 192.168.10.1
FVL328 WAN-Seite: 217.233.101.136

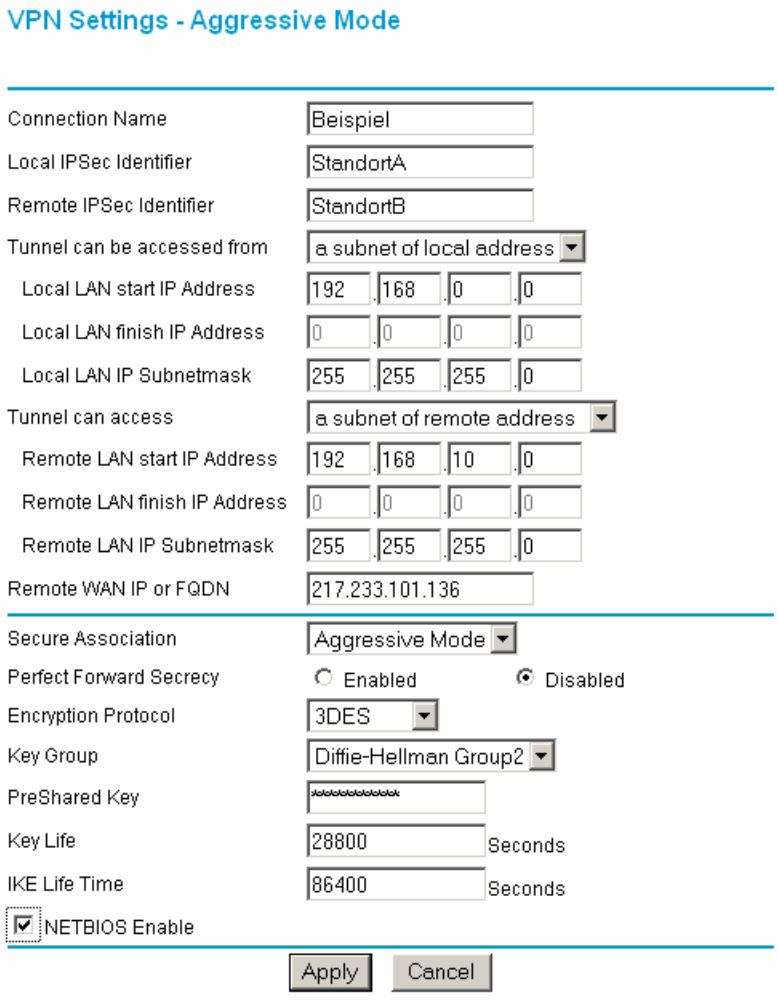
Netzwerkadresse: 192.168.10.0/24
Test-PC im Netzwerk: 192.168.10.2



7.2. Konfiguration des Routers an Standort A

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links oben auf den Menüpunkt **VPN Settings**.
- Aktivieren Sie den Punkt vor der 1 und klicken Sie auf **Edit**.
- Konfigurieren Sie die Verbindung wie in Abb. 7.2.1 gezeigt.

Abb. 7.2.1



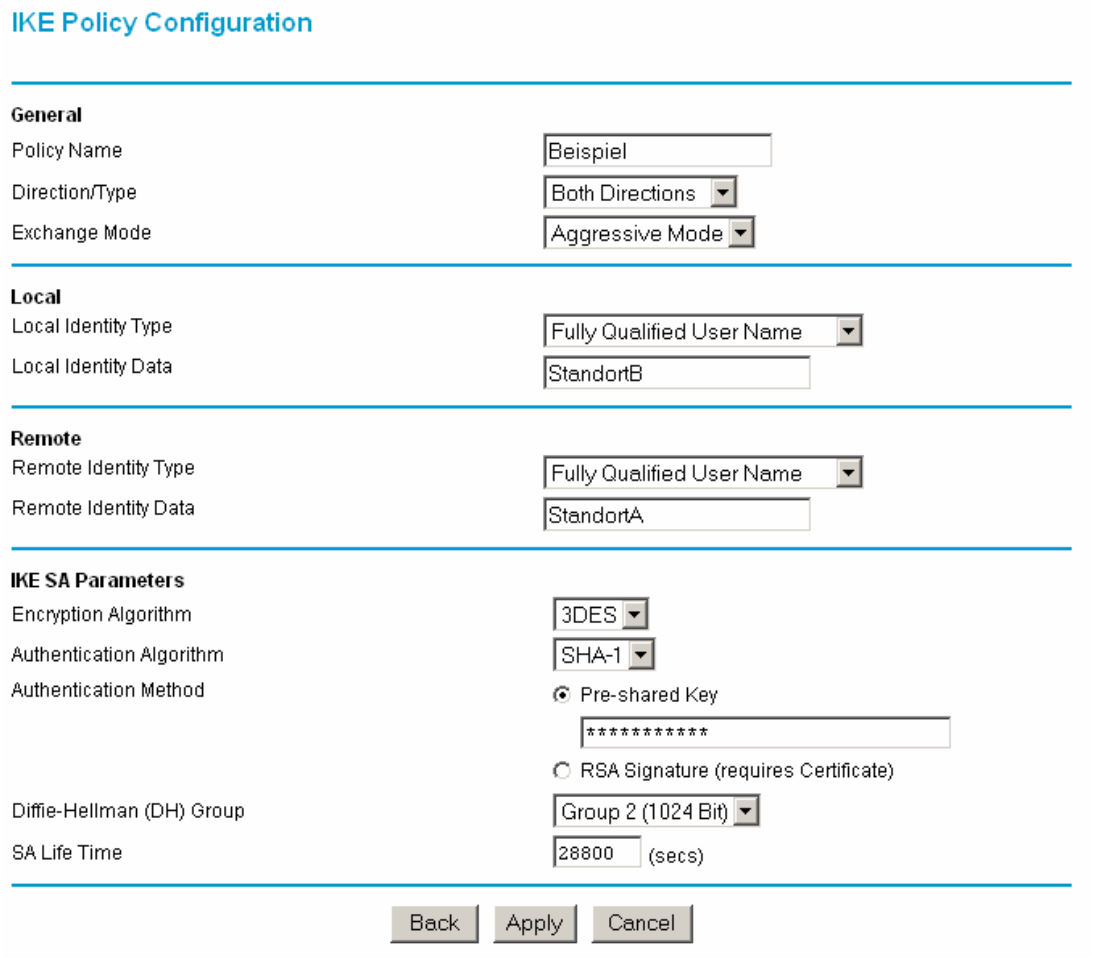
- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

7.3. Konfiguration des Routers an Standort B

Schritt 1: Erstellen der IKE-Policy (Phase 1)

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links auf den Menüpunkt **IKE Policies**.
- Klicken Sie dort auf den Button **Add** um eine IKE-Policy zu erstellen.
- Konfigurieren Sie die IKE-Policy wie in Abb. 7.3.1 gezeigt.

Abb. 7.3.1

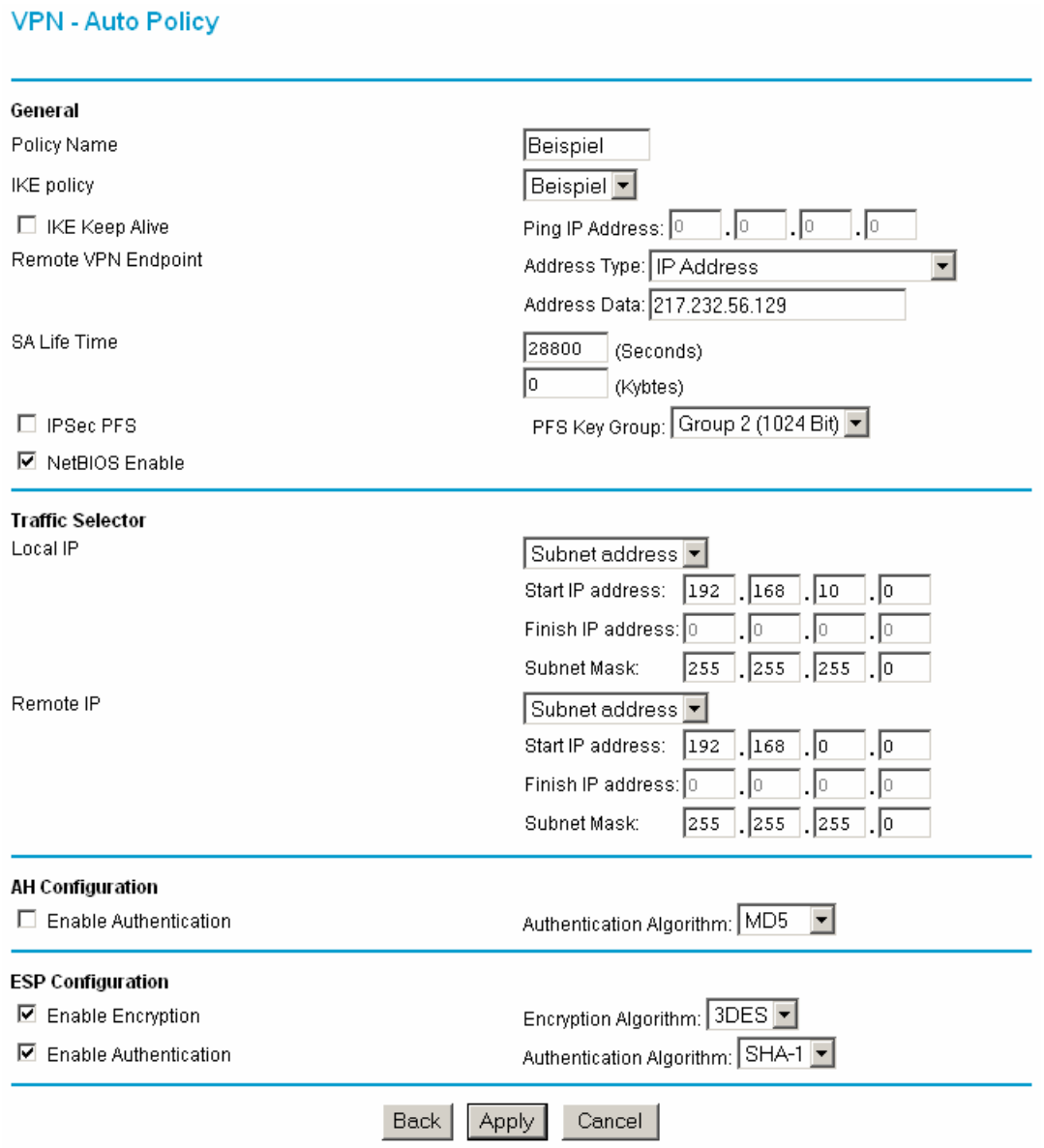


- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

Schritt 2: Erstellen der VPN-Policy (Phase 2)

- Klicken Sie links auf den Menüpunkt **VPN Policies**.
- Um eine VPN-Policy zu erstellen, klicken Sie auf **Add Auto Policy**.
- Konfigurieren Sie die VPN-Policy wie in Abb. 7.3.2 gezeigt.
  ! Bei dem Punkt **IKE policy** wählen Sie die in Schritt 1 erstellte IKE-Policy.

Abb. 7.3.2



- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

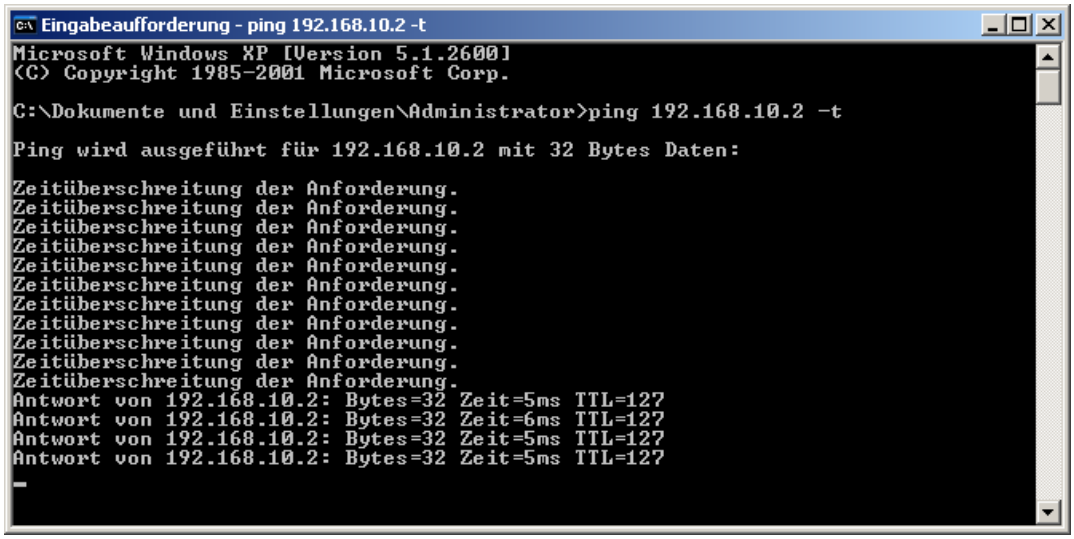
7.4. Testen der Verbindung

Um die Verbindung zu testen, versuchen Sie beispielsweise von einem PC an Standort A z.B. 192.168.0.2) einen PC an Standort B (z.B. 192.168.10.2) zu erreichen:

Hinweis:	- Bei beiden PCs muss der jeweils lokale Router als Gateway verwendet werden: - Der PC an Standort A (192.168.**0**.2) verwendet als Gateway seinen lokalen Router 192.168.**0**.1. - Der PC an Standort B (192.168.**10**.2) verwendet als Gateway seinen lokalen Router 192.168.**10**.1.

- Klicken Sie in Windows links unten auf **Start** und **Ausführen...**
- Geben Sie **cmd** ein (Windows 95/98/ME: **command**) und klicken Sie auf **OK**
- Geben Sie folgenden Befehl ein: **ping 192.168.10.2 –t** (siehe Abb. 7.4.1)

Abb. 7.4.1



- Bei richtiger Konfiguration wird die VPN-Verbindung innerhalb einiger Sekunden aufgebaut (siehe Abb. 7.4.1).

- Der VPN Status des FVS318 (**Show VPN Status** im Menü **Router Status**) zeigt ebenfalls eine etablierte VPN-Verbindung (siehe Abb. 7.4.2).

Abb. 7.4.2

IPSec Connection Status

Status	Connection Name	Remote IP	Virtual Network	Type	State	Drop
Active	Beispiel	217.233.101.136	192.168.10.0/24	ESP(DES-CBC MD5)	[P1:M-Estab.] [P2:Q-Estab.]	Drop

8. Beispielkonfiguration

FVS318v1 mit dynamischer WAN-IP-Adresse
zu
FVL328 mit fester WAN-IP-Adresse

8.1. Übersicht

Standort A:

FVS318v1 (Firmware 2.4)

FVS318 LAN-Seite: 192.168.0.1
FVS318 WAN-Seite: standorta.dyndns.org

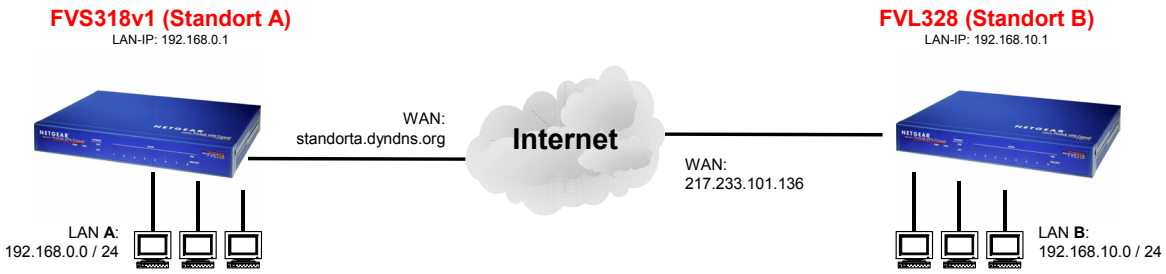
Netzwerkadresse: 192.168.0.0/24
Test-PC im Netzwerk: 192.168.0.2

Standort B:

FVL328 (Firmware 2.0 Release 08)

FVL328 LAN-Seite: 192.168.10.1
FVL328 WAN-Seite: 217.233.101.136

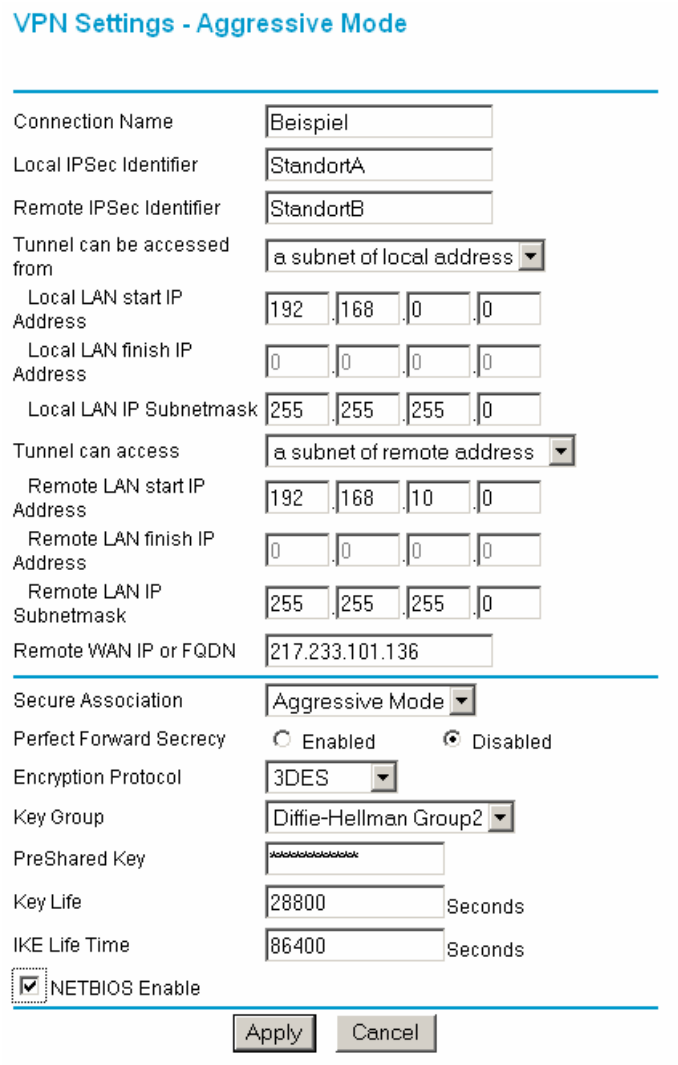
Netzwerkadresse: 192.168.10.0/24
Test-PC im Netzwerk: 192.168.10.2



8.2. Konfiguration des Routers an Standort A

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links oben auf den Menüpunkt **VPN Settings**.
- Aktivieren Sie den Punkt vor der 1 und klicken Sie auf **Edit**.
- Konfigurieren Sie die Verbindung wie in Abb. 8.2.1 gezeigt.

Abb. 8.2.1



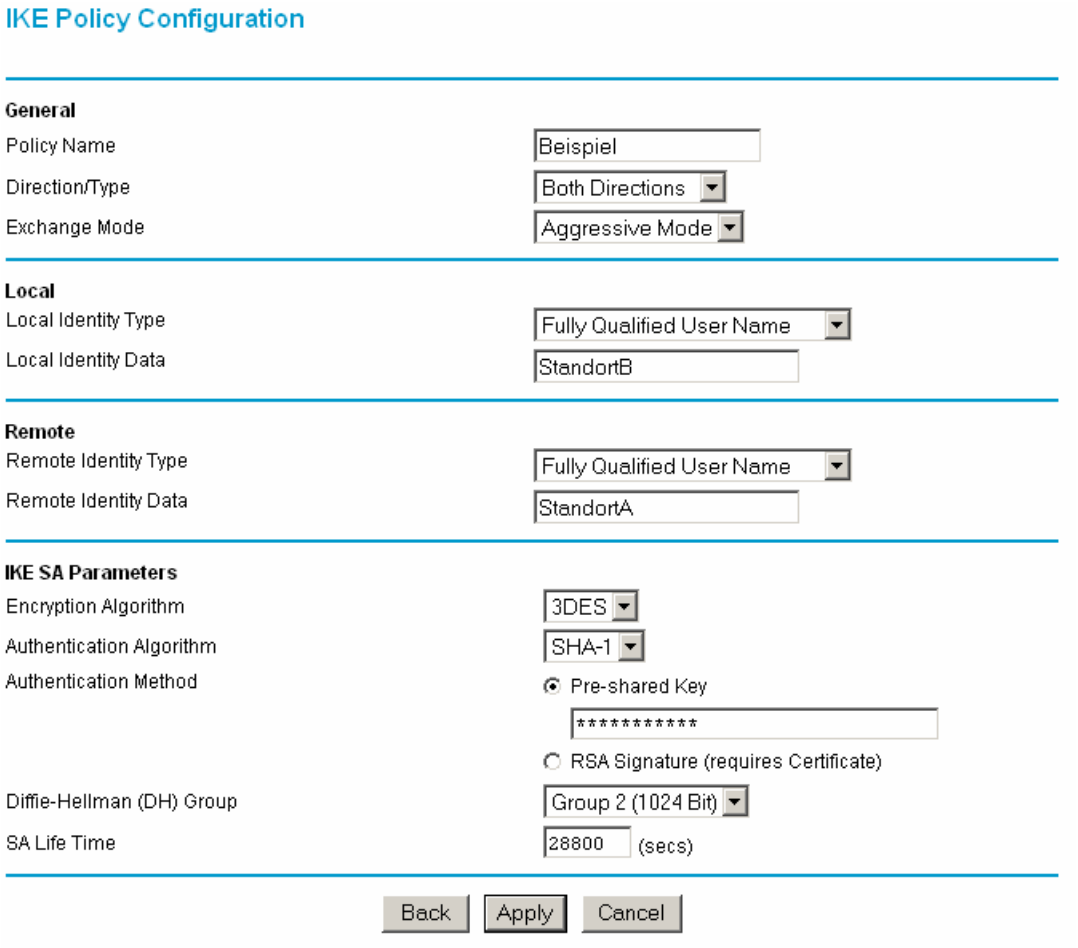
- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

8.3. Konfiguration des Routers an Standort B

Schritt 1: Erstellen der IKE-Policy (Phase 1)

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links auf den Menüpunkt **IKE Policies**.
- Klicken Sie dort auf den Button **Add** um eine IKE-Policy zu erstellen.
- Konfigurieren Sie die IKE-Policy wie in Abb. 8.3.1 gezeigt.

Abb. 8.3.1

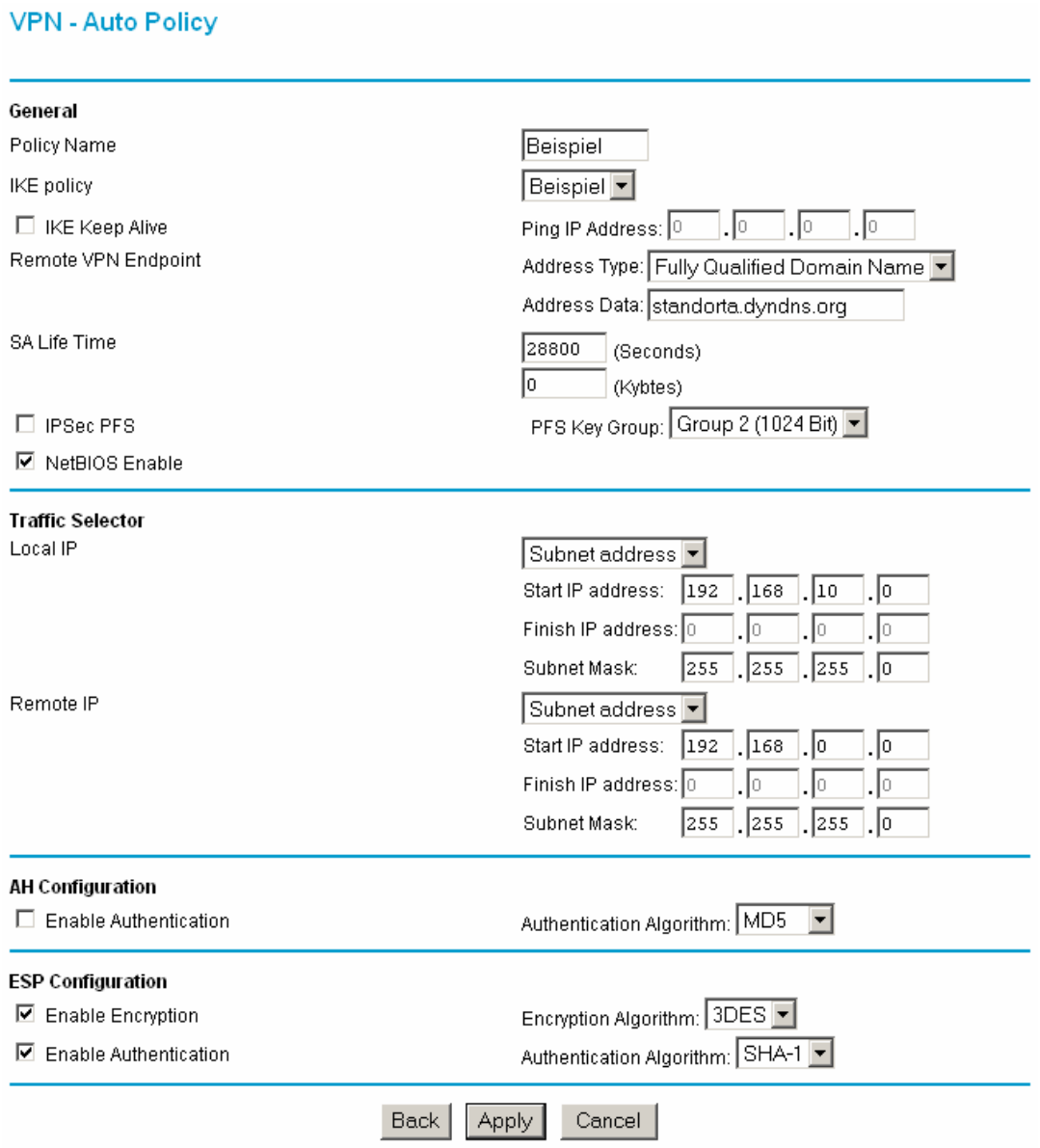


- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

Schritt 2: Erstellen der VPN-Policy (Phase 2)

- Klicken Sie links auf den Menüpunkt **VPN Policies**.
- Um eine VPN-Policy zu erstellen, klicken Sie auf **Add Auto Policy**.
- Konfigurieren Sie die VPN-Policy wie in Abb. 8.3.2 gezeigt.
  ! Bei dem Punkt **IKE policy** wählen Sie die in Schritt 1 erstellte IKE-Policy.

Abb. 8.3.2



- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

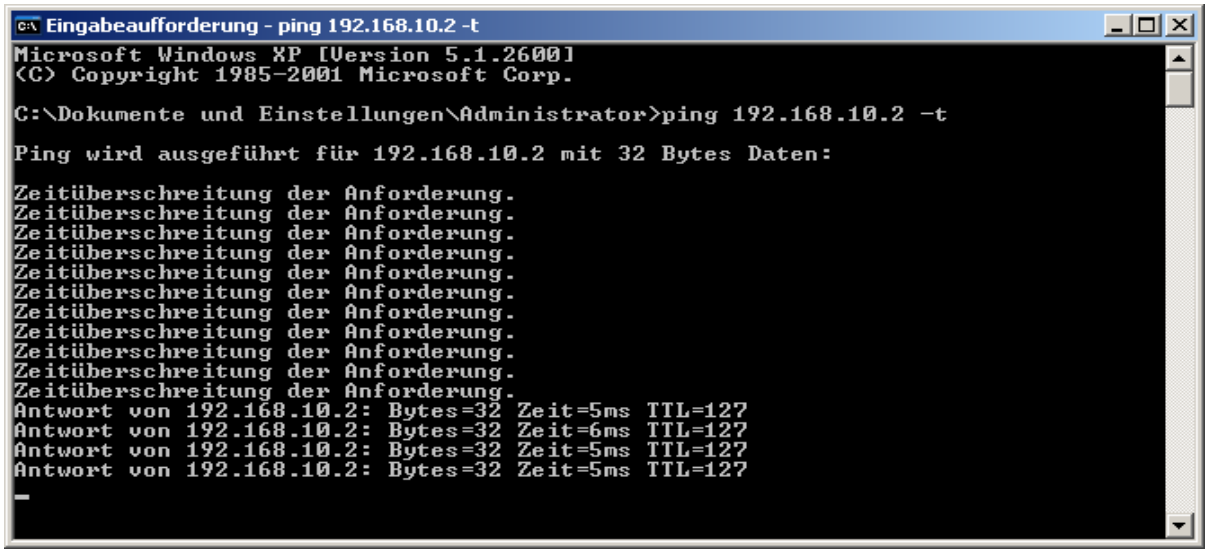
8.4. Testen der Verbindung

Um die Verbindung zu testen, versuchen Sie beispielsweise von einem PC an Standort A (z.B. 192.168.0.2) einen PC an Standort B (z.B. 192.168.10.2) zu erreichen:

Hinweis:	- Bei beiden PCs muss der jeweils lokale Router als Gateway verwendet werden: - Der PC an Standort A (192.168.**0**.2) verwendet als Gateway seinen lokalen Router 192.168.**0**.1. - Der PC an Standort B (192.168.**10**.2) verwendet als Gateway seinen lokalen Router 192.168.**10**.1.

- Klicken Sie in Windows links unten auf **Start** und **Ausführen...**
- Geben Sie **cmd** ein (Windows 95/98/ME: **command**) und klicken Sie auf **OK**
- Geben Sie folgenden Befehl ein: **ping 192.168.10.2 –t** (siehe Abb. 8.4.1)

Abb. 8.4.1



- Bei richtiger Konfiguration wird die VPN-Verbindung innerhalb einiger Sekunden aufgebaut (siehe Abb. 8.4.1).

- Der VPN Status des FVS318 (**Show VPN Status** im Menü **Router Status**) zeigt ebenfalls eine etablierte VPN-Verbindung (siehe Abb. 8.4.2).

Abb. 8.4.2

IPSec Connection Status

Status	Connection Name	Remote IP	Virtual Network	Type	State	Drop
Active	Beispiel	217.233.101.136	192.168.10.0/24	ESP(DES-CBC MD5)	[P1:M-Estab.] [P2:Q-Estab.]	Drop

9. Beispielkonfiguration

FVS318v1 mit fester WAN-IP-Adresse
zu
FVL328 mit dynamischer WAN-IP-Adresse

9.1. Übersicht

Standort A:

FVS318v1 (Firmware 2.4)

FVS318 LAN-Seite: 192.168.0.1
FVS318 WAN-Seite: 217.232.56.129

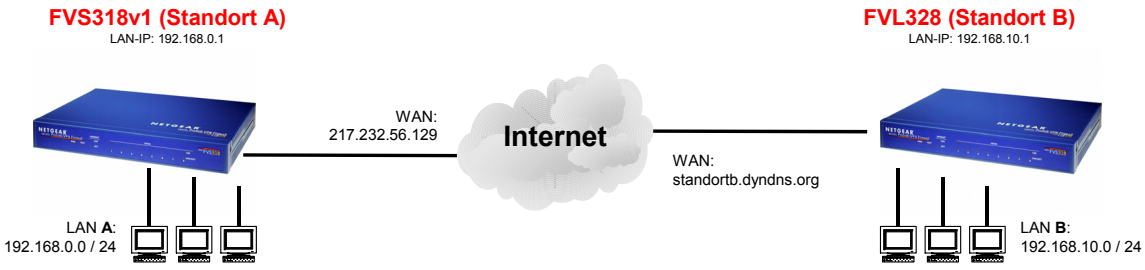
Netzwerkadresse: 192.168.0.0/24
Test-PC im Netzwerk: 192.168.0.2

Standort B:

FVL328 (Firmware 2.0 Release 08)

FVL328 LAN-Seite: 192.168.10.1
FVL328 WAN-Seite: standortb.dyndns.org

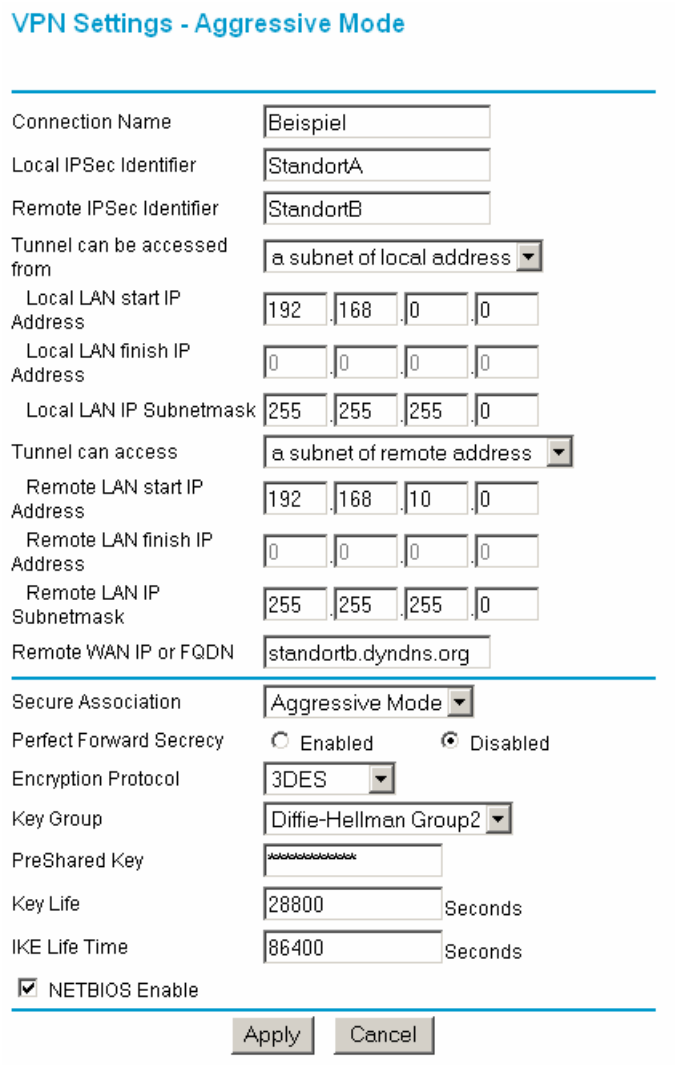
Netzwerkadresse: 192.168.10.0/24
Test-PC im Netzwerk: 192.168.10.2



9.2. Konfiguration des Routers an Standort A

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links oben auf den Menüpunkt **VPN Settings**.
- Aktivieren Sie den Punkt vor der 1 und klicken Sie auf **Edit**.
- Konfigurieren Sie die Verbindung wie in Abb. 9.2.1 gezeigt.

Abb. 9.2.1



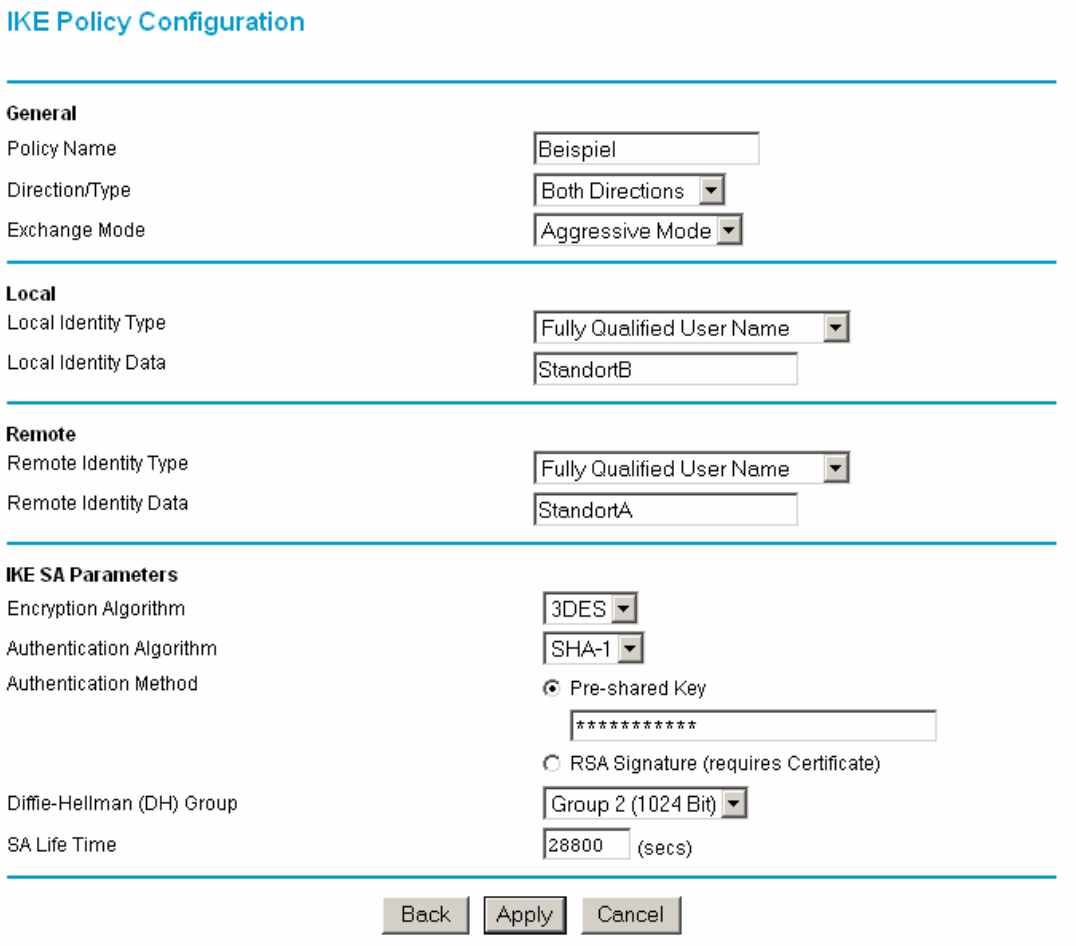
- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

9.3. Konfiguration des Routers an Standort B

Schritt 1: Erstellen der IKE-Policy (Phase 1)

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links auf den Menüpunkt **IKE Policies**.
- Klicken Sie dort auf den Button **Add** um eine IKE-Policy zu erstellen.
- Konfigurieren Sie die IKE-Policy wie in Abb. 9.3.1 gezeigt.

Abb. 9.3.1

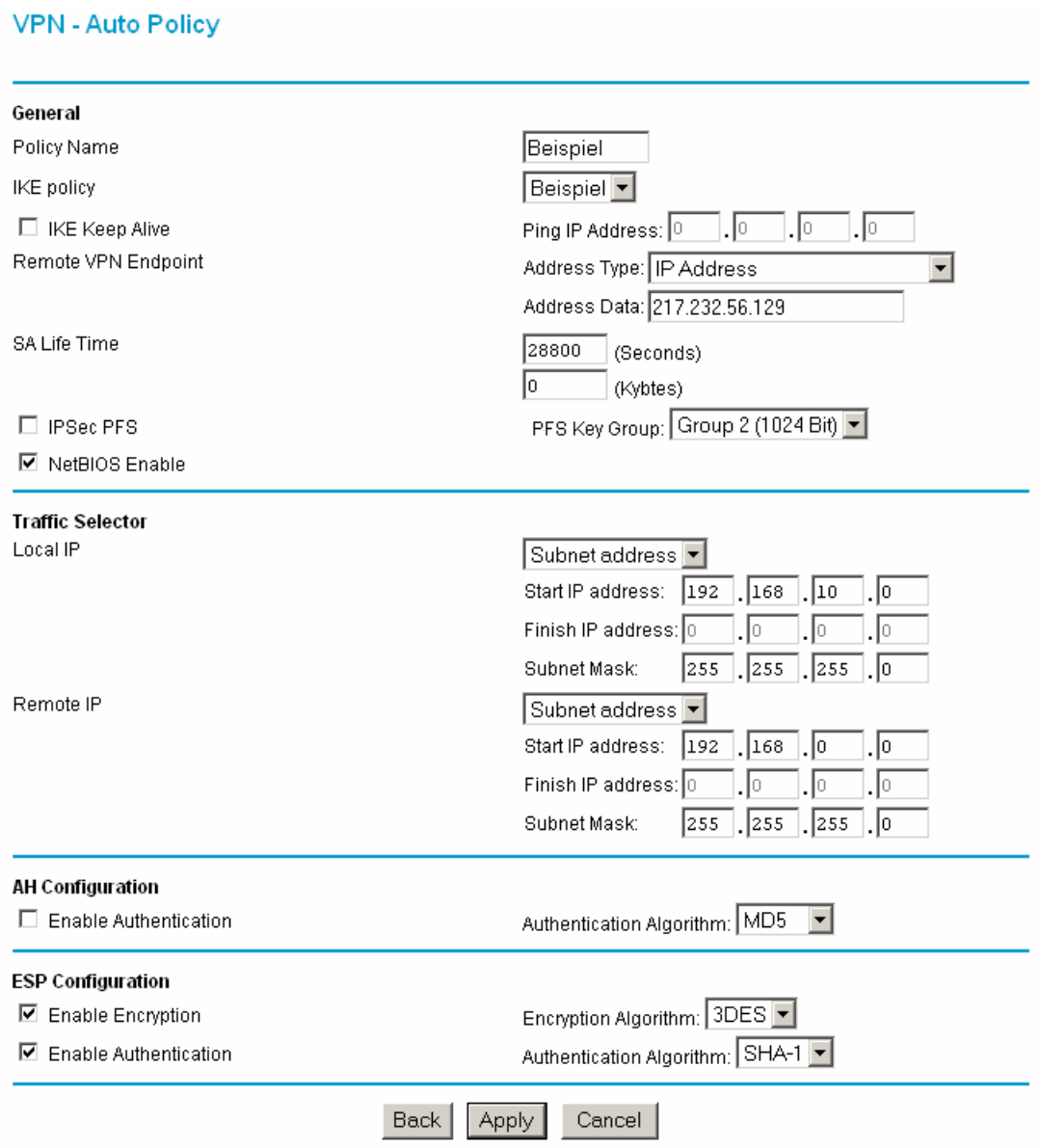


- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

Schritt 2: Erstellen der VPN-Policy (Phase 2)

- Klicken Sie links auf den Menüpunkt **VPN Policies**.
- Um eine VPN-Policy zu erstellen, klicken Sie auf **Add Auto Policy**.
- Konfigurieren Sie die VPN-Policy wie in Abb. 9.3.2 gezeigt.
  ! Bei dem Punkt **IKE policy** wählen Sie die in Schritt 1 erstellte IKE-Policy.

Abb. 9.3.2



- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

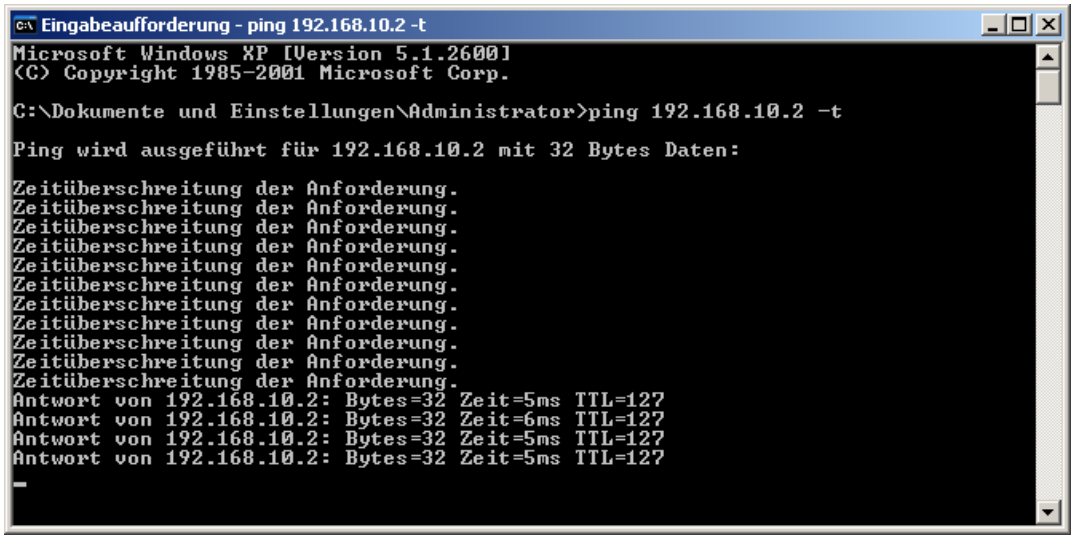
9.4. Testen der Verbindung

Um die Verbindung zu testen, versuchen Sie beispielsweise von einem PC an Standort A (z.B. 192.168.0.2) einen PC an Standort B (z.B. 192.168.10.2) zu erreichen:

Hinweis:	- Bei beiden PCs muss der jeweils lokale Router als Gateway verwendet werden: - Der PC an Standort A (192.168.**0**.2) verwendet als Gateway seinen lokalen Router 192.168.**0**.1. - Der PC an Standort B (192.168.**10**.2) verwendet als Gateway seinen lokalen Router 192.168.**10**.1.

- Klicken Sie in Windows links unten auf **Start** und **Ausführen...**
- Geben Sie **cmd** ein (Windows 95/98/ME: **command**) und klicken Sie auf **OK**
- Geben Sie folgenden Befehl ein: **ping 192.168.10.2 –t** (siehe Abb. 9.4.1)

Abb. 9.4.1



- Bei richtiger Konfiguration wird die VPN-Verbindung innerhalb einiger Sekunden aufgebaut (siehe Abb. 9.4.1).

- Der VPN Status des FVS318 (**Show VPN Status** im Menü **Router Status**) zeigt ebenfalls eine etablierte VPN-Verbindung (siehe Abb. 9.4.2).

Abb. 9.4.2

IPSec Connection Status

Status	Connection Name	Remote IP	Virtual Network	Type	State	Drop
Active	Beispiel	217.233.101.136	192.168.10.0/24	ESP(DES-CBC MD5)	[P1:M-Estab.] [P2:Q-Estab.]	Drop

10. Beispielkonfiguration

FVS318 mit dynamischer WAN-IP-Adresse
zu
FVL328 mit dynamischer WAN-IP-Adresse

10.1. Übersicht

Standort A:

FVS318v1 (Firmware 2.4)

FVS318v1 LAN-Seite: 192.168.0.1
FVS318v1 WAN-Seite: standorta.dyndns.org

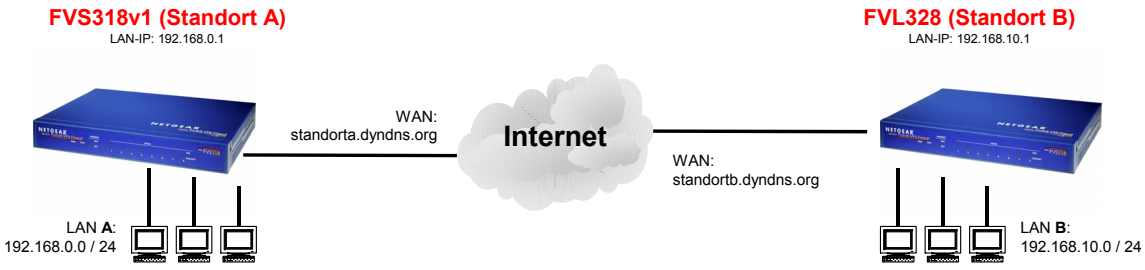
Netzwerkadresse: 192.168.0.0/24
Test-PC im Netzwerk: 192.168.0.2

Standort B:

FVL328 (Firmware 2.0 Release 08)

FVL328 LAN-Seite: 192.168.10.1
FVL328 WAN-Seite: standortb.dyndns.org

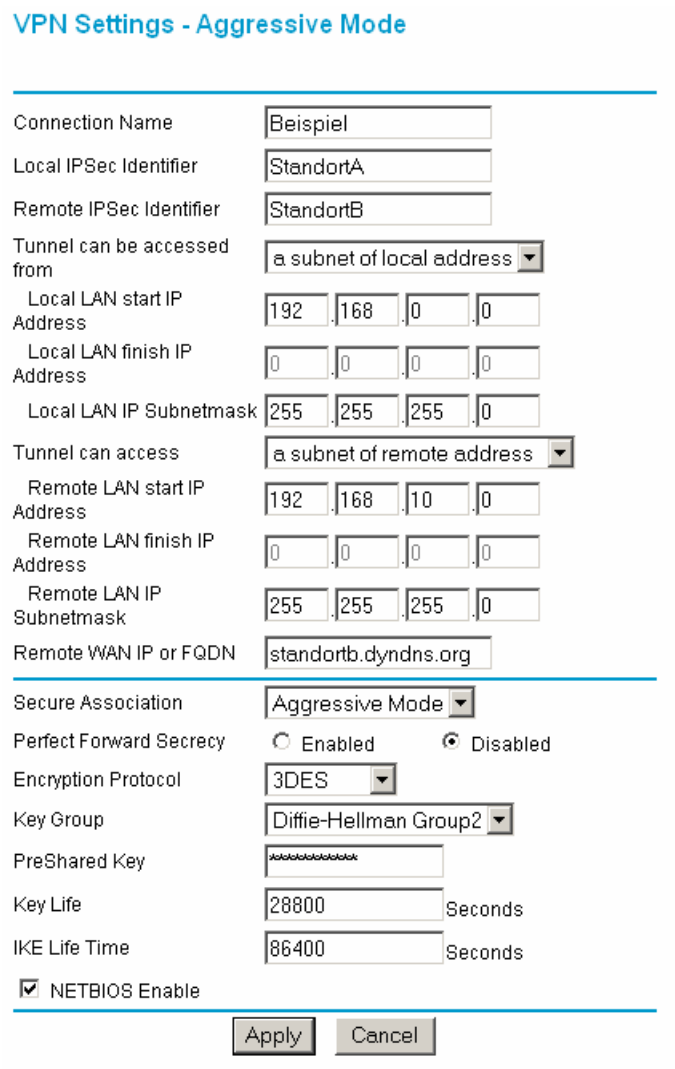
Netzwerkadresse: 192.168.10.0/24
Test-PC im Netzwerk: 192.168.10.2



10.2. Konfiguration des Routers an Standort A

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links oben auf den Menüpunkt **VPN Settings**.
- Aktivieren Sie den Punkt vor der 1 und klicken Sie auf **Edit**.
- Konfigurieren Sie die Verbindung wie in Abb. 10.2.1 gezeigt.

Abb. 10.2.1



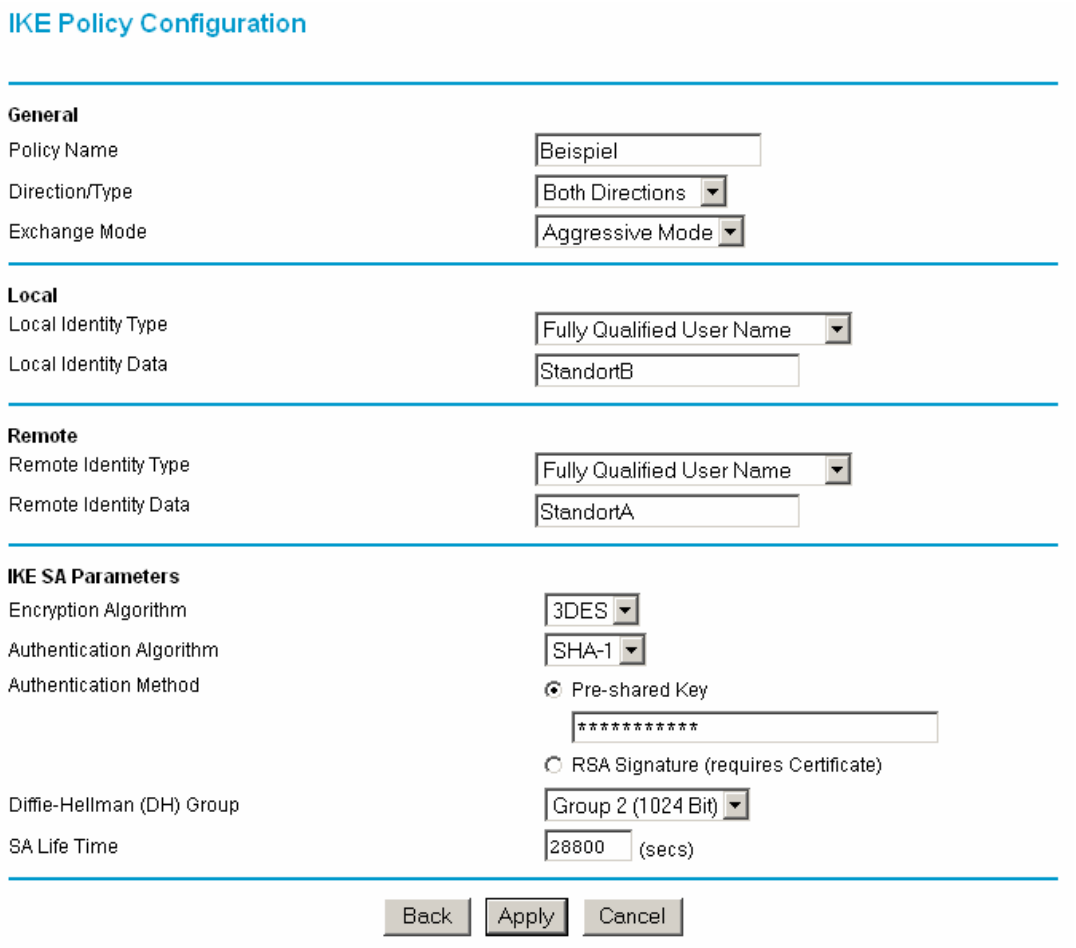
- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

10.3. Konfiguration des Routers an Standort B

Schritt 1: Erstellen der IKE-Policy (Phase 1)

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links auf den Menüpunkt **IKE Policies**.
- Klicken Sie dort auf den Button **Add** um eine IKE-Policy zu erstellen.
- Konfigurieren Sie die IKE-Policy wie in Abb. 10.3.1 gezeigt.

Abb. 10.3.1

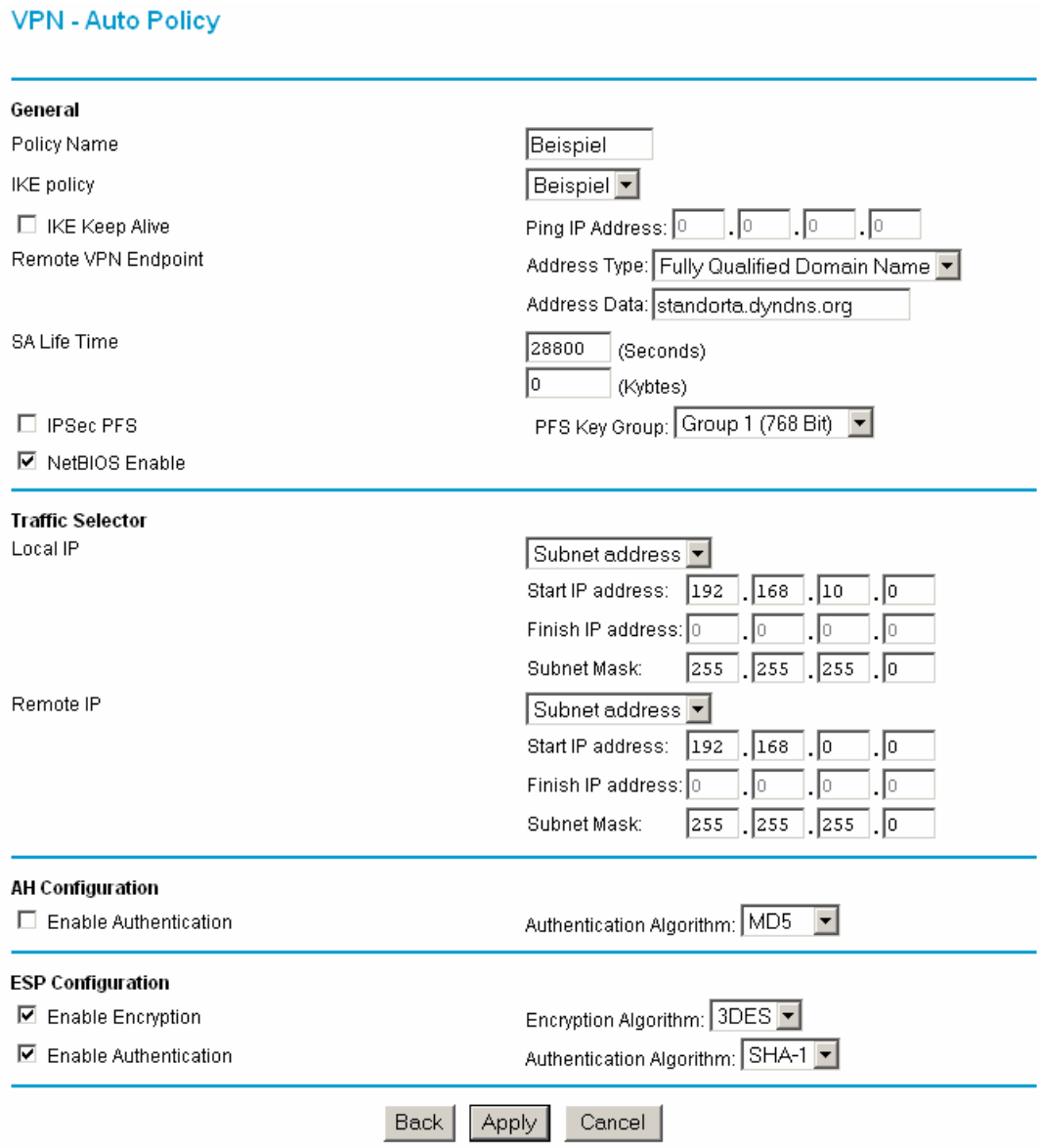


- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

Schritt 2: Erstellen der VPN-Policy (Phase 2)

- Klicken Sie links auf den Menüpunkt **VPN Policies**.
- Um eine VPN-Policy zu erstellen, klicken Sie auf **Add Auto Policy**.
- Konfigurieren Sie die VPN-Policy wie in Abb. 10.3.2 gezeigt.
  ! Bei dem Punkt **IKE policy** wählen Sie die in Schritt 1 erstellte IKE-Policy.

Abb. 10.3.2



- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

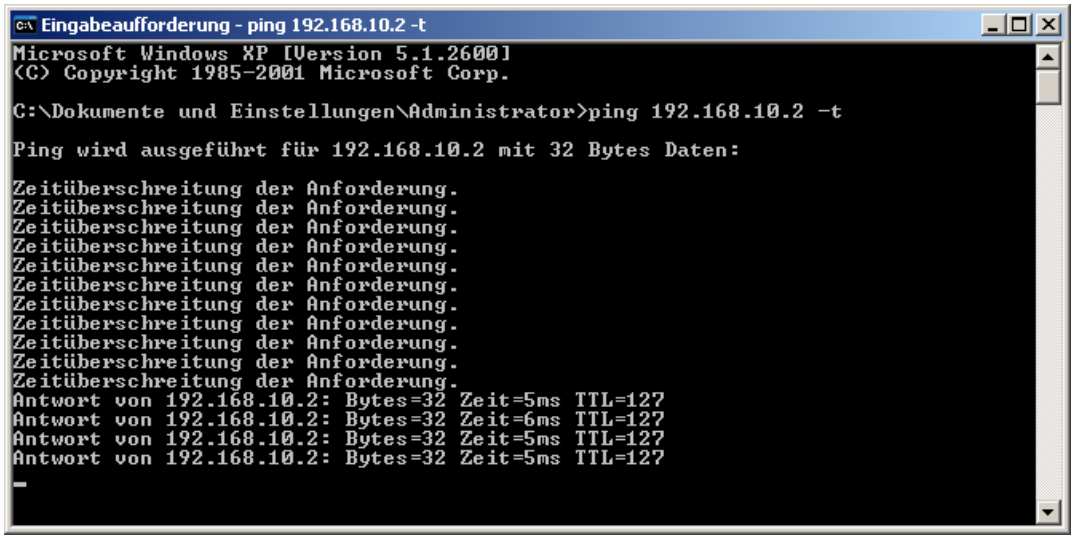
10.4. Testen der Verbindung

Um die Verbindung zu testen, versuchen Sie beispielsweise von einem PC an Standort A (z.B. 192.168.0.2) einen PC an Standort B (z.B. 192.168.10.2) zu erreichen:

Hinweis:	- Bei beiden PCs muss der jeweils lokale Router als Gateway verwendet werden: - Der PC an Standort A (192.168.**0**.2) verwendet als Gateway seinen lokalen Router 192.168.**0**.1. - Der PC an Standort B (192.168.**10**.2) verwendet als Gateway seinen lokalen Router 192.168.**10**.1.

- Klicken Sie in Windows links unten auf **Start** und **Ausführen...**
- Geben Sie **cmd** ein (Windows 95/98/ME: **command**) und klicken Sie auf **OK**
- Geben Sie folgenden Befehl ein: **ping 192.168.10.2 –t** (siehe Abb. 10.4.1)

Abb. 10.4.1



- Bei richtiger Konfiguration wird die VPN-Verbindung innerhalb einiger Sekunden aufgebaut (siehe Abb. 10.4.1).

- Der VPN Status des FVS318 (**Show VPN Status** im Menü **Router Status**) zeigt ebenfalls eine etablierte VPN-Verbindung (siehe Abb. 10.4.2).

Abb. 10.4.2

IPSec Connection Status

Status	Connection Name	Remote IP	Virtual Network	Type	State	Drop
Active	Beispiel	217.233.101.136	192.168.10.0/24	ESP(DES-CBC MD5)	[P1:M-Estab.] [P2:Q-Estab.]	Drop

11. Beispielkonfiguration

ProSafe VPN Client Software
zu
FVS318v1 mit fester WAN-IP-Adresse

11.1. Übersicht

Standort A:

FVS318v1 (Firmware 2.4)

FVS318v1 LAN-Seite: 192.168.0.1
FVS318v1 WAN-Seite: 217.232.56.129

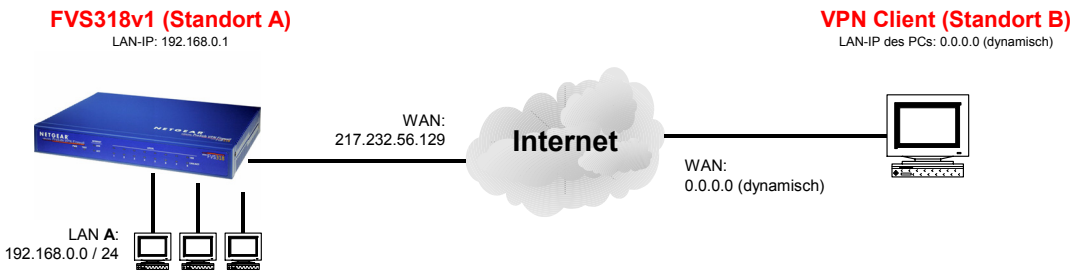
Netzwerkadresse: 192.168.0.0/24
Test-PC im Netzwerk: 192.168.0.2

Standort B:

ProSafe VPN Client Software (Ver.: 10.5.1 Build 8)

WAN-Seite des VPN-Client-PCs: 0.0.0.0 (dynamisch)

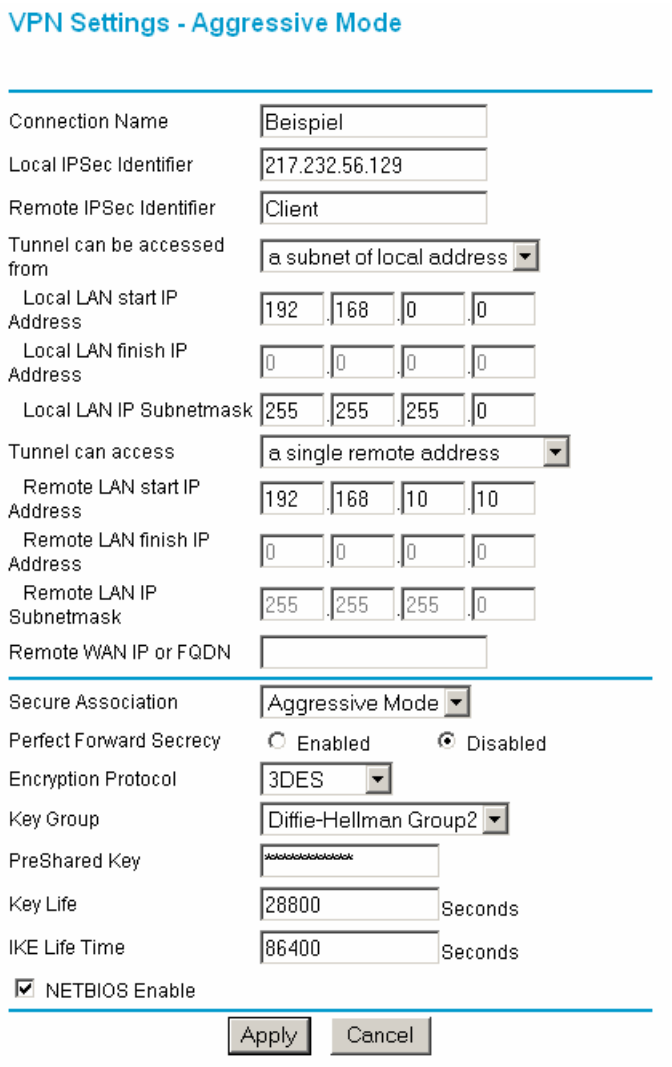
LAN-Seite des VPN-Client-PCs: 0.0.0.0 (dynamisch)



11.2. Konfiguration des Routers an Standort A

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links oben auf den Menüpunkt **VPN Settings**.
- Aktivieren Sie den Punkt vor der 1 und klicken Sie auf **Edit**.
- Konfigurieren Sie die Verbindung wie in Abb. 11.2.1 gezeigt.
  ! Im Feld **Local IPSec Identifier** tragen Sie die WAN-IP-Adresse des FVS318 ein (in diesem Beispiel: 217.232.56.129).

Abb. 11.2.1



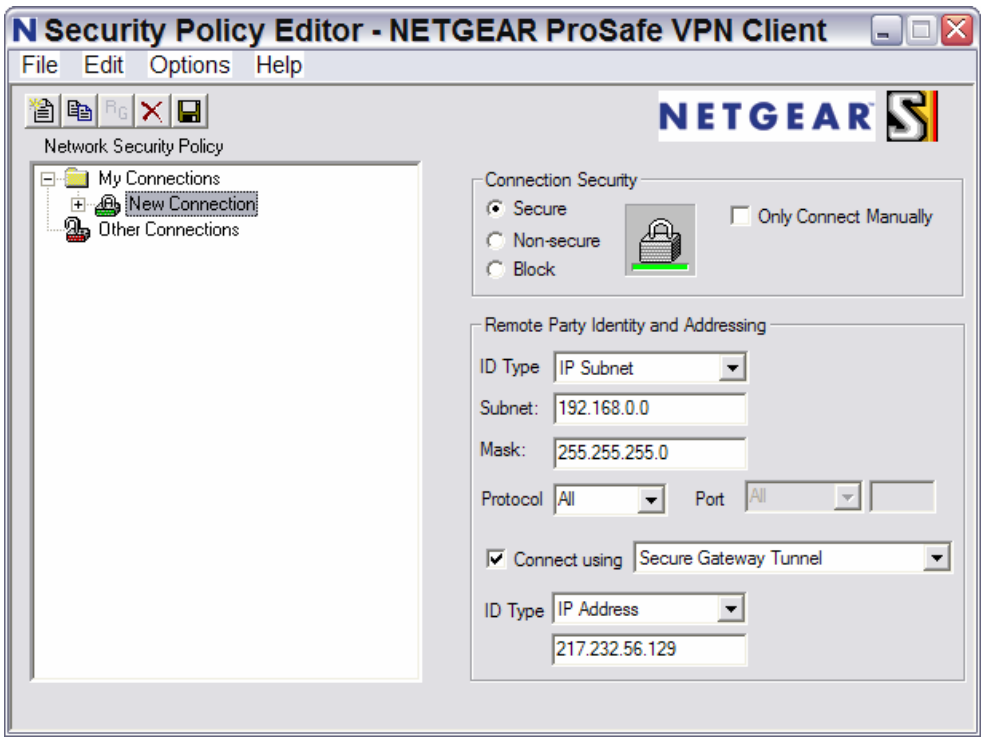
- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

11.3. Konfiguration des ProSafe VPN Client (Standort B)

- Starten Sie den Security Policy Editor mit einem Doppelklick auf das Symbol des ProSafe VPN Client in der Taskleiste:
  

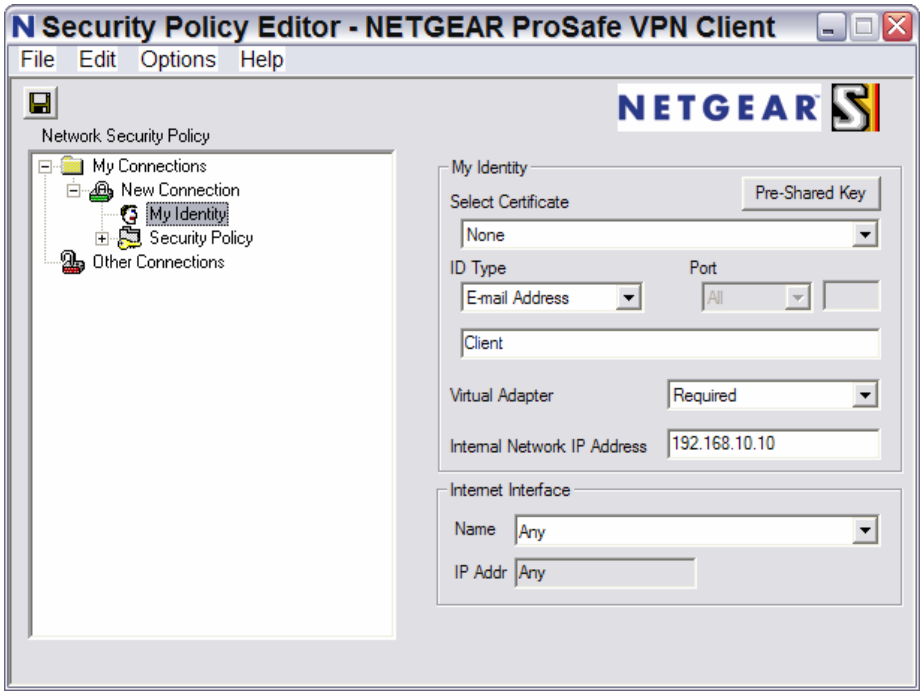
- Klicken Sie auf **Edit** –> **Add** -> **Connection** um eine neue Verbindung zu erstellen.
- Um die Eingabe einer IP-Adresse für den Virtual Adapter zu ermöglichen, aktivieren Sie im Security Policy Editor unter **Options** -> **Global Policy Settings** die Option **Allow to Specify Internal Network Address**.
- Konfigurieren Sie die Verbindung wie in Abb. 11.3.1 gezeigt.
  ! Im **unteren** Feld **ID Type** wählen Sie **IP Address** und tragen darunter die WAN-IP-Adresse des FVS318 ein (in diesem Beispiel: 217.232.56.129).

Abb. 11.3.1



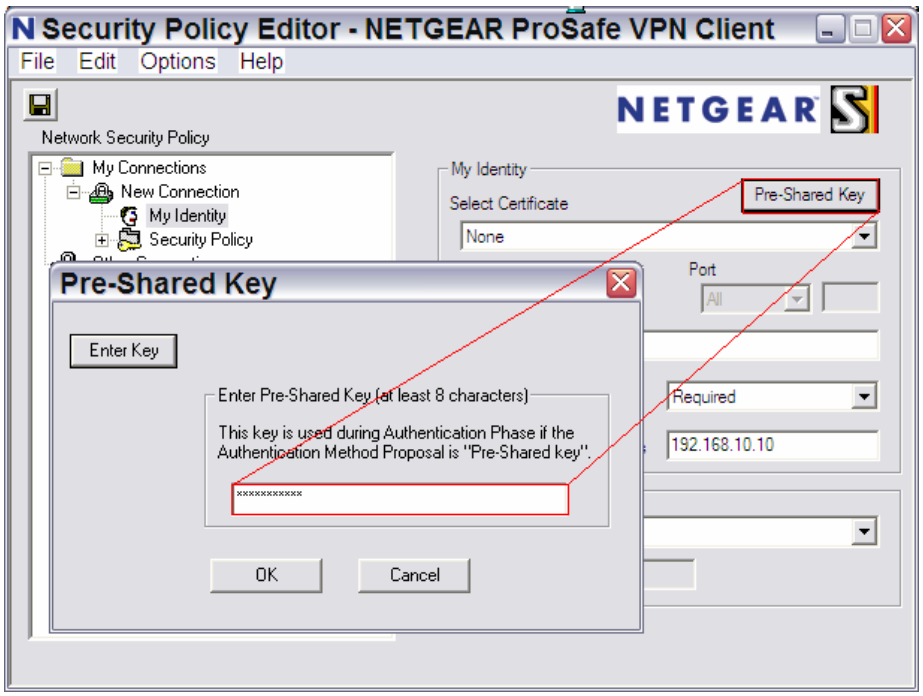
- Konfigurieren Sie die Option **My Identity** wie in Abb. 11.3.2 gezeigt.

Abb. 11.3.2



- Um den Pre-Shared Key einzutragen, klicken Sie rechts oben auf **Pre-Shared Key**. In dem erschienenen Fenster klicken Sie auf **Enter Key** und geben den Pre-Shared Key ein (siehe Abb. 11.3.3).

Abb. 11.3.3



- Konfigurieren Sie die Verbindung wie in den folgenden drei Abb. gezeigt.

Abb. 11.3.4

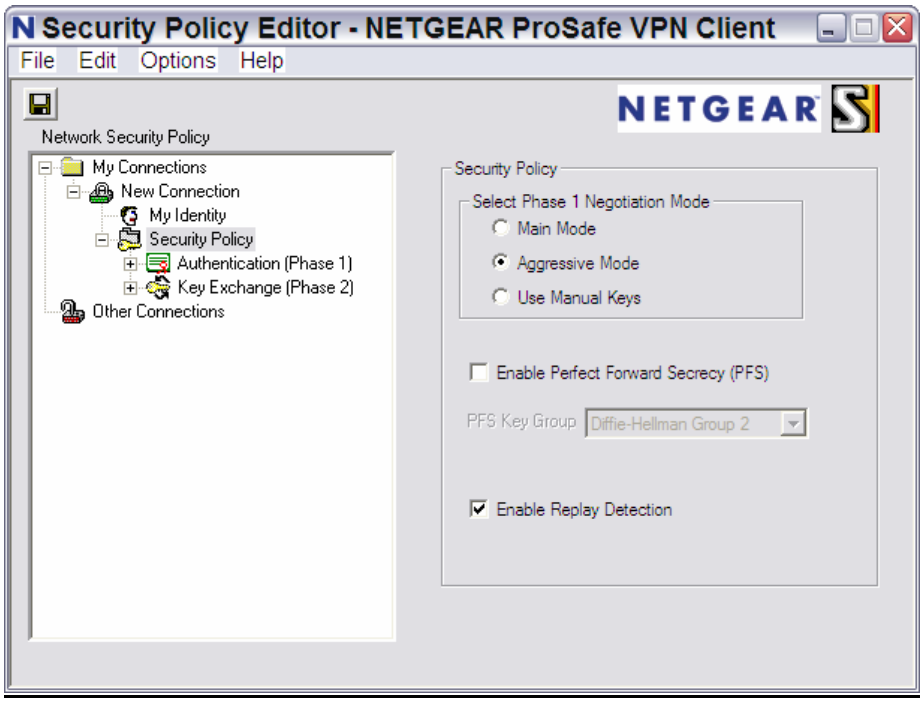


Abb. 11.3.5

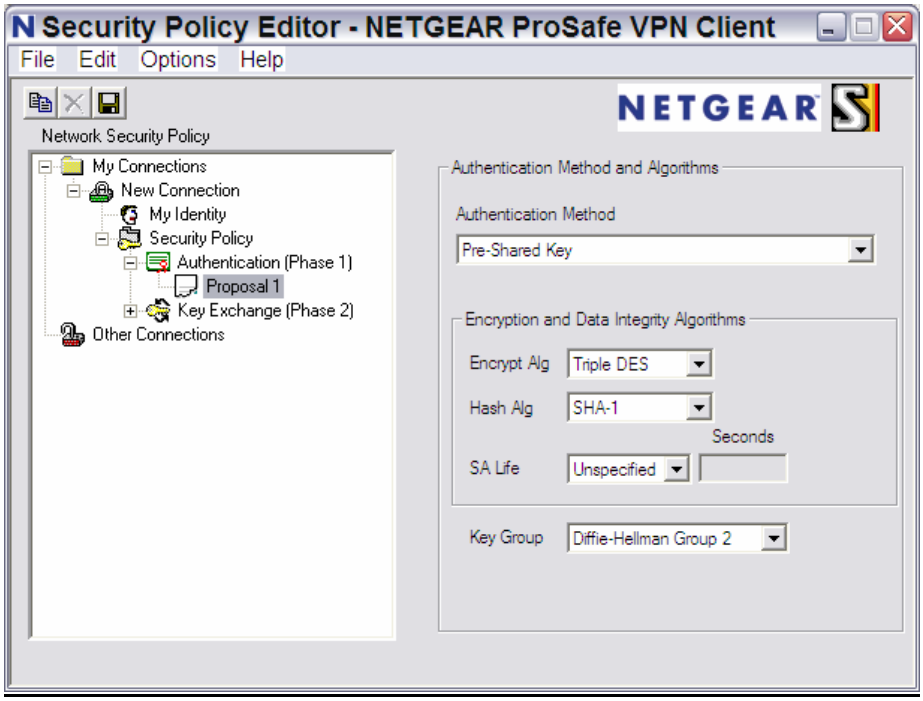
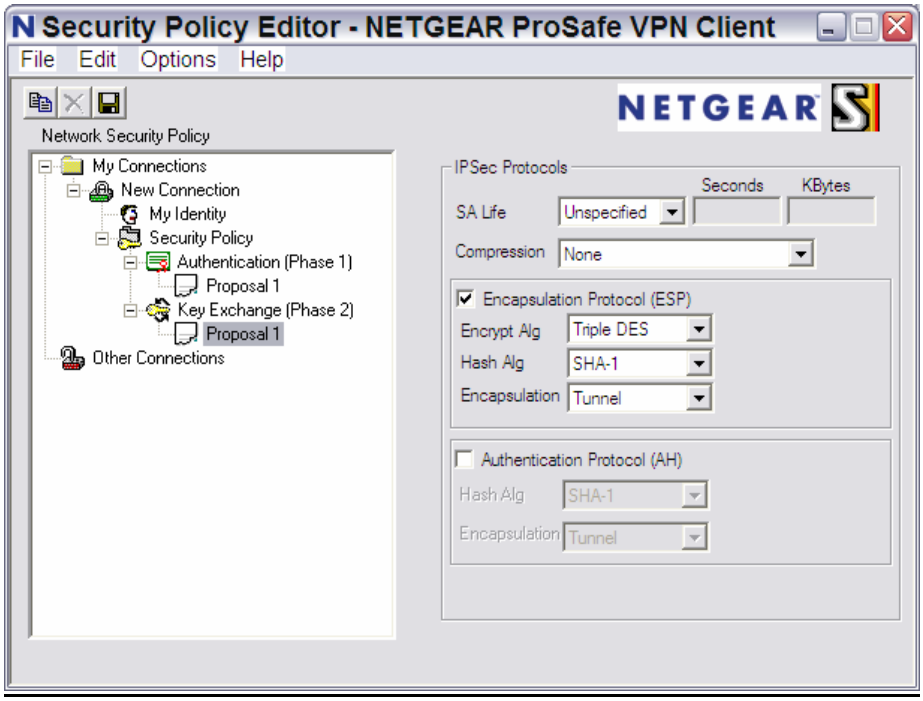


Abb. 11.3.6



- Klicken Sie links oben auf **File** -> **Save** um die erstellte Verbindung zu speichern.

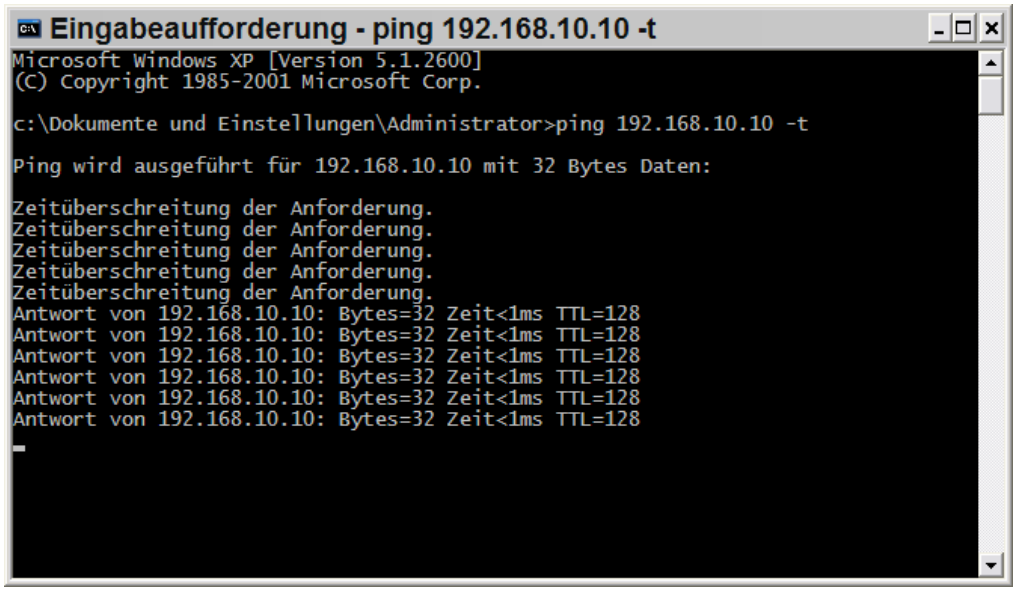
11.4. Testen der Verbindung

Um die Verbindung zu testen, versuchen Sie von dem PC mit dem VPN Client an Standort B einen PC an Standort A (z.B. 192.168.0.2) zu erreichen:

Hinweis:	Um den PC im Netzwerk an Standort A erreichen zu können, muss dort der lokale FVS318 als Standardgateway verwendet werden. Für dieses Beispiel gilt: Der PC an Standort A (192.168.**0**.2) verwendet als Gateway seinen lokalen Router 192.168.**0**.1.

- Klicken Sie in Windows links unten auf **Start** und **Ausführen...**
- Geben Sie **cmd** ein (Windows 95/98/ME: **command**) und klicken Sie auf **OK**
- Geben Sie folgenden Befehl ein: **ping 192.168.10.10 –t** (siehe Abb. 11.4.1)

Abb. 11.4.1



- Bei richtiger Konfiguration wird die VPN-Verbindung innerhalb einiger Sekunden aufgebaut (siehe Abb. 11.4.1).

12. Beispielkonfiguration

ProSafe VPN Client Software (hinter einem NAT-Router)
zu
FVS318v1 mit fester WAN-IP-Adresse

12.1. Übersicht

Standort A:

FVS318 (Firmware 2.4)

FVS318v1 LAN-Seite: 192.168.0.1
FVS318v1 WAN-Seite: 217.232.56.129

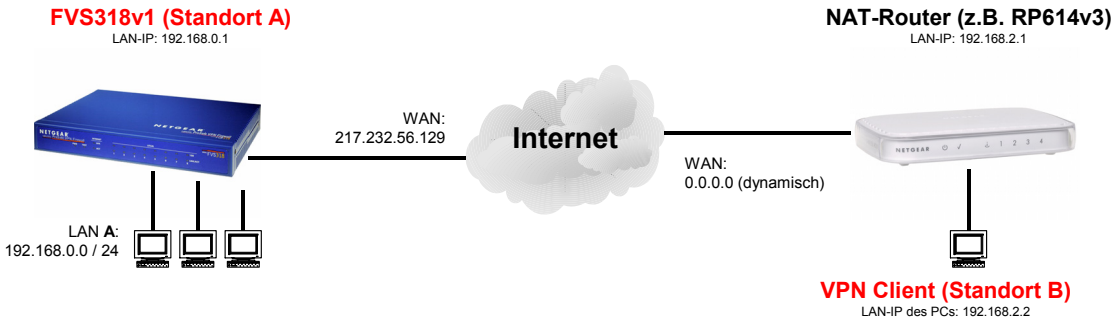
Netzwerkadresse: 192.168.0.0/24
Test-PC im Netzwerk: 192.168.0.2

Standort B:

ProSafe VPN Client Software (Ver.: 10.5.1 Build 8)

NAT-Router LAN-Seite: 192.168.2.1
NAT-Router WAN-Seite: 0.0.0.0 (dynamisch)

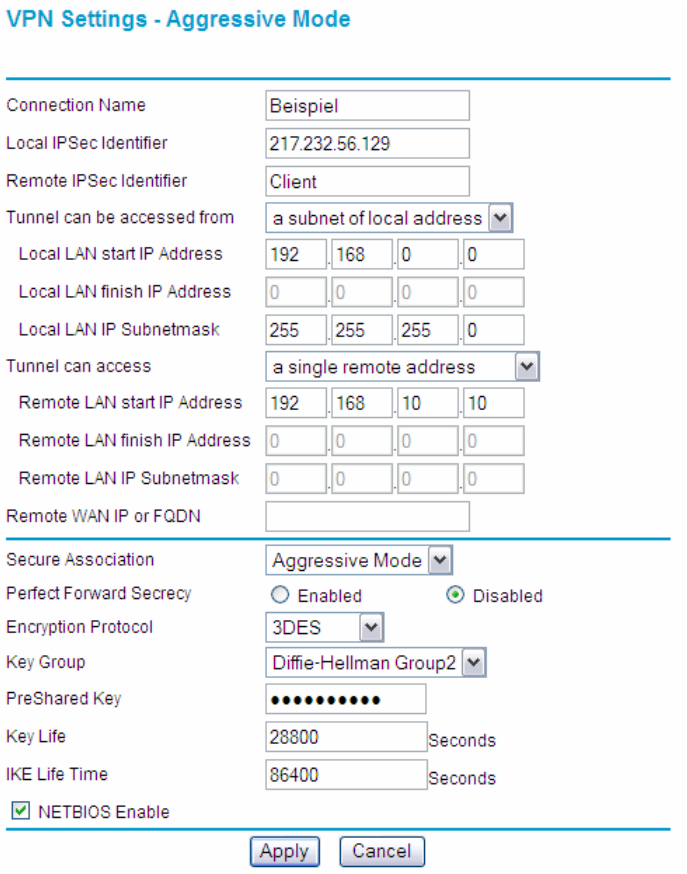
PC mit ProSafe VPN Client Software: 192.168.2.2



12.2. Konfiguration des Routers an Standort A

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links oben auf den Menüpunkt **VPN Settings**.
- Aktivieren Sie den Punkt vor der 1 und klicken Sie auf **Edit**.
- Konfigurieren Sie die Verbindung wie in Abb. 12.2.1 gezeigt.
  ! Im Feld **Local IPSec Identifier** tragen Sie die WAN-IP-Adresse des FVS318 ein (in diesem Beispiel: 217.232.56.129).

Abb. 12.2.1



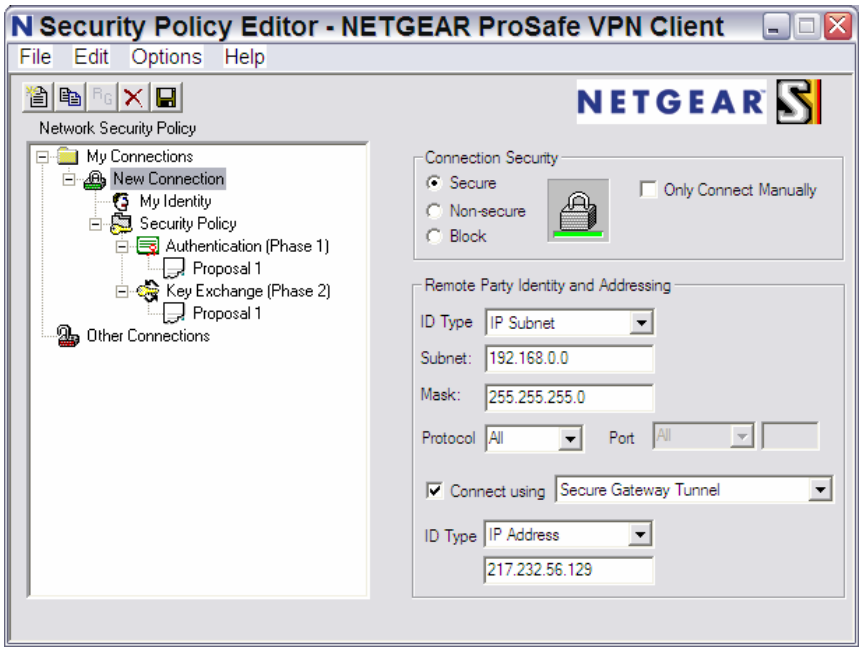
- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

12.3. Konfiguration des ProSafe VPN Client (Standort B)

- Starten Sie den Security Policy Editor mit einem Doppelklick auf das Symbol des ProSafe VPN Client in der Taskleiste:
  

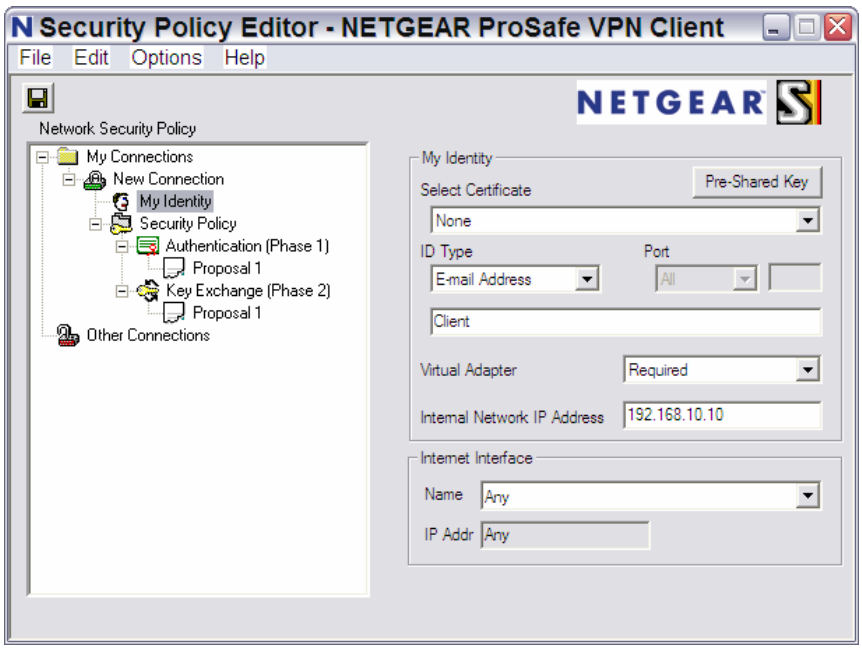
- Klicken Sie auf **Edit** –> **Add** -> **Connection** um eine neue Verbindung zu erstellen.
- Um die Eingabe einer IP-Adresse für den Virtual Adapter zu ermöglichen, aktivieren Sie im Security Policy Editor unter **Options** -> **Global Policy Settings** die Option **Allow to Specify Internal Network Address**.
- Konfigurieren Sie die Verbindung wie in Abb. 12.3.1 gezeigt.
  ! Im **unteren** Feld **ID Type** wählen Sie **IP Address** und tragen darunter die WAN-IP-Adresse des FVS318 ein (in diesem Beispiel: 217.232.56.129).

Abb. 12.3.1



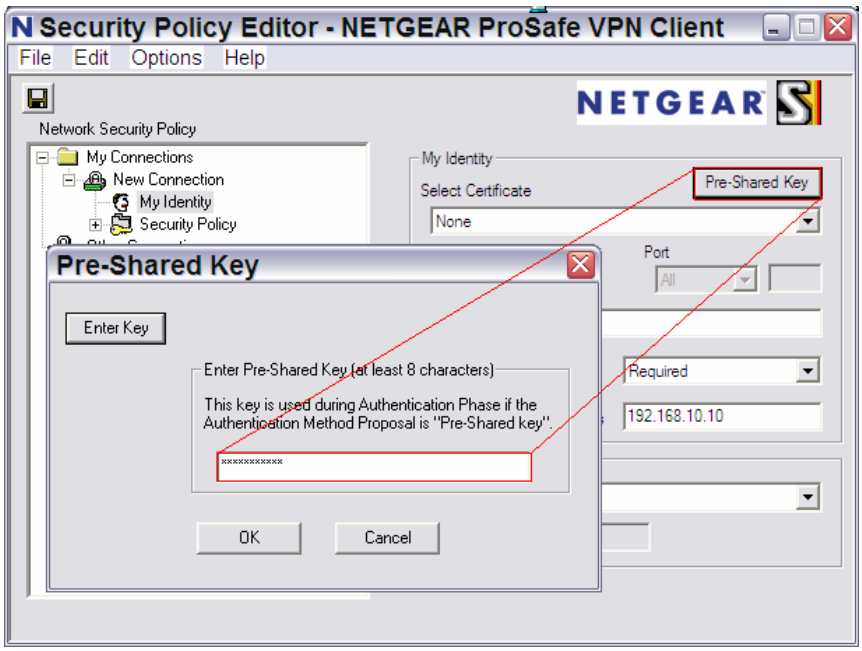
- Konfigurieren Sie die Option **My Identity** wie in Abb. 12.3.2 gezeigt.
  ! Bei **Internet Interface** wählen Sie “Any“ aus und vergeben Sie eine IP-Adresse für den Virtual Adapter (in diesem Beispiel 192.168.10.10). Der Virtual Adapter muß dabei auf **Required** stehen.

Abb. 12.3.2



- Um den Pre-Shared Key einzutragen, klicken Sie rechts oben auf **Pre-Shared Key**. In dem erschienenen Fenster klicken Sie auf **Enter Key** und geben den Pre-Shared Key ein (siehe Abb. 12.3.3).

Abb. 12.3.3



- Konfigurieren Sie die Verbindung wie in den folgenden drei Abb. gezeigt.

Abb. 12.3.4

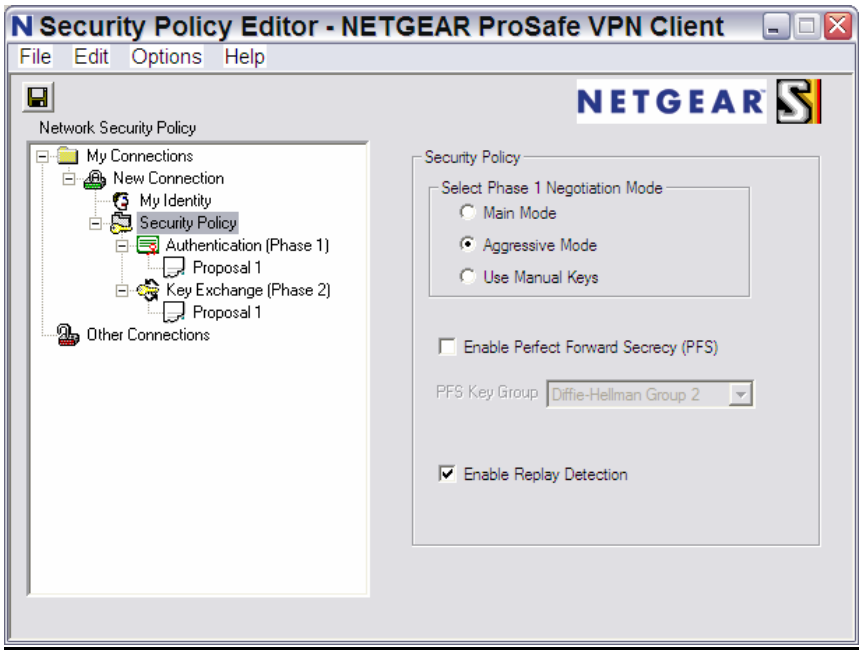


Abb. 12.3.5

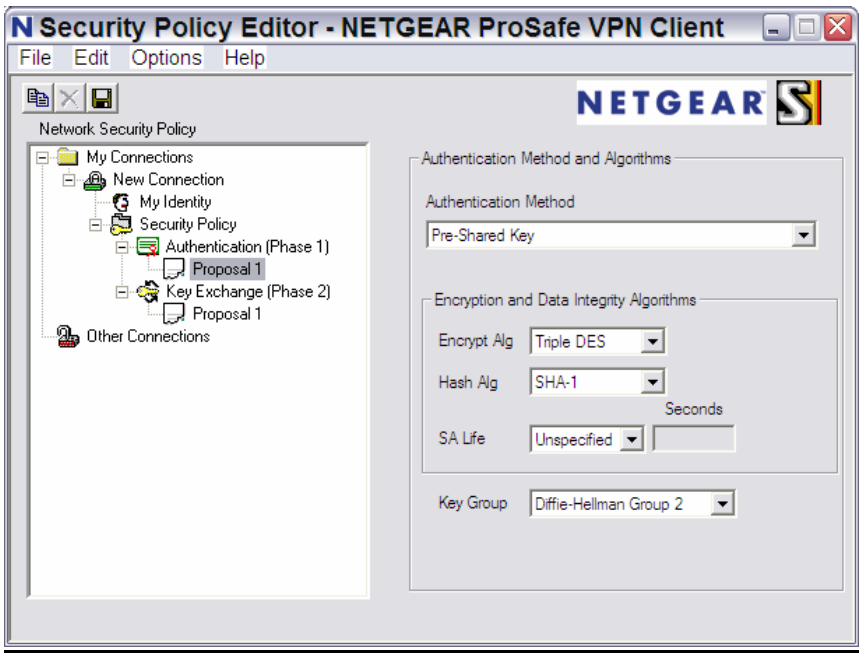
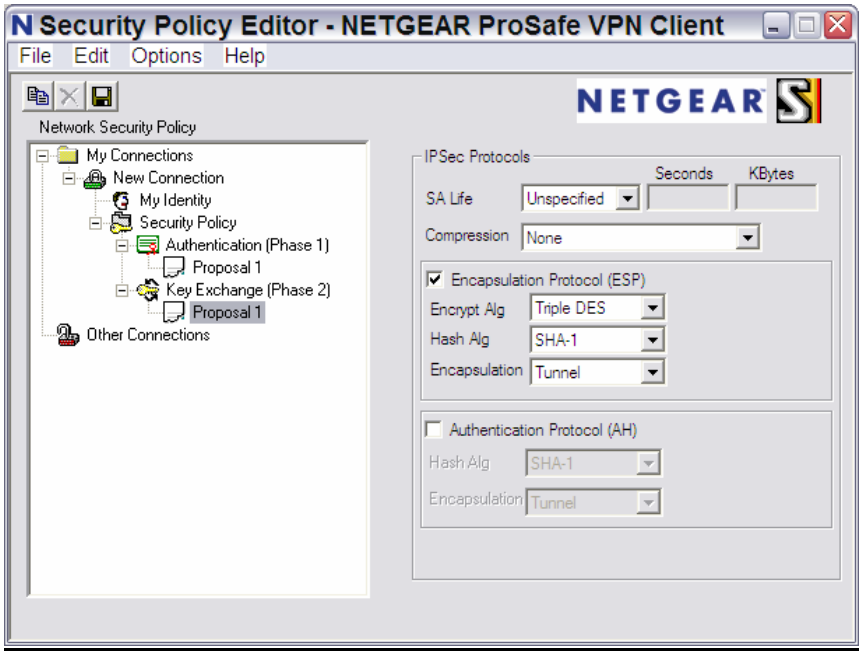


Abb. 12.3.6



- Klicken Sie links oben auf **File** -> **Save** um die erstellte Verbindung zu speichern.

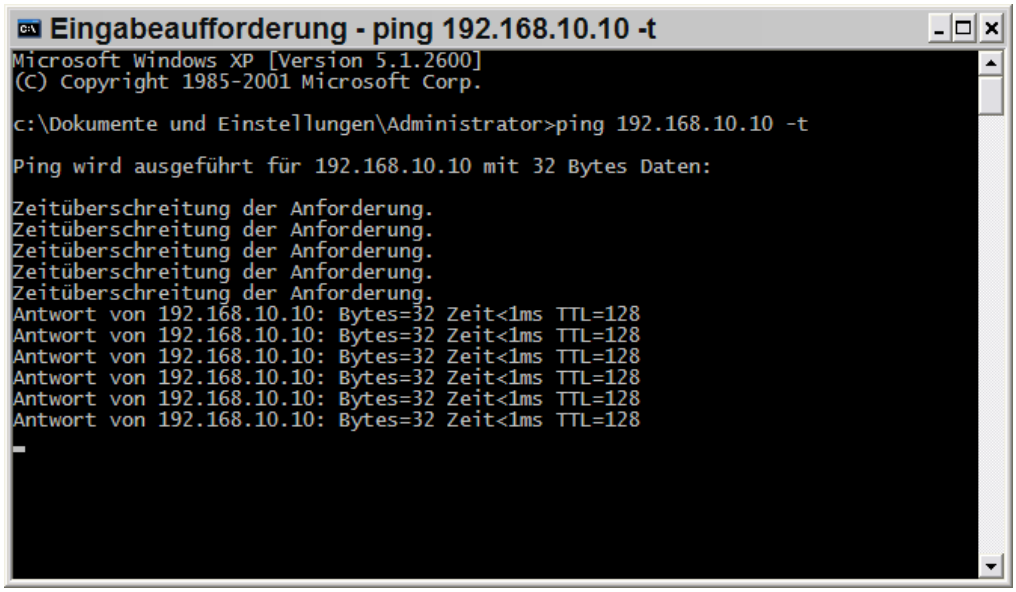
12.4. Testen der Verbindung

Um die Verbindung zu testen, versuchen Sie von dem PC mit dem VPN Client an Standort B (192.168.2.2 bzw. 192.168.10.10 auf dem Virtual Adapter) einen PC an Standort A (z.B. 192.168.0.2) zu erreichen:

Hinweis:	- Bei beiden PCs muss der jeweils lokale Router als Gateway verwendet werden: - Der PC an Standort A (192.168.**0**.2) verwendet als Gateway seinen lokalen Router 192.168.**0**.1. - Der PC an Standort B (192.168.**2**.2) verwendet als Gateway seinen lokalen Router 192.168.**2**.1.

- Klicken Sie in Windows links unten auf **Start** und **Ausführen...**
- Geben Sie **cmd** ein (Windows 95/98/ME: **command**) und klicken Sie auf **OK**
- Geben Sie folgenden Befehl ein: **ping 192.168.10.10 –t** (siehe Abb. 12.4.1)

Abb. 12.4.1



- Bei richtiger Konfiguration wird die VPN-Verbindung innerhalb einiger Sekunden aufgebaut (siehe Abb. 12.4.1).

13. Beispielkonfiguration

ProSafe VPN Client Software
zu
FVS318v1 mit dynamischer WAN-IP-Adresse

13.1. Übersicht

Standort A:

FVS318v1 (Firmware 2.4)

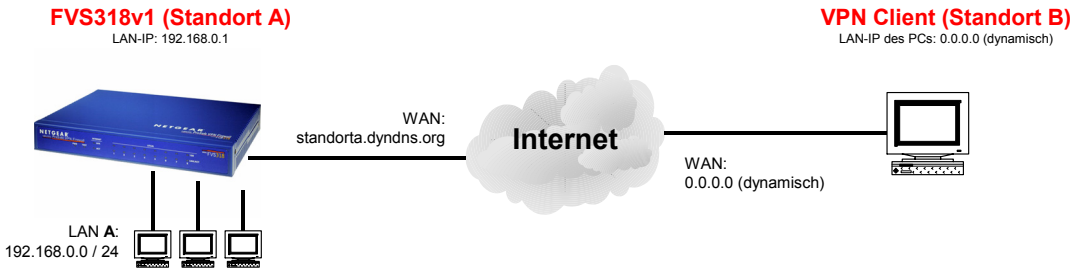
FVS318v1 LAN-Seite: 192.168.0.1
FVS318v1 WAN-Seite: standorta.dyndns.org

Netzwerkadresse: 192.168.0.0/24
Test-PC im Netzwerk: 192.168.0.2

Standort B:

ProSafe VPN Client Software (Ver.: 10.5.1 Build 8)

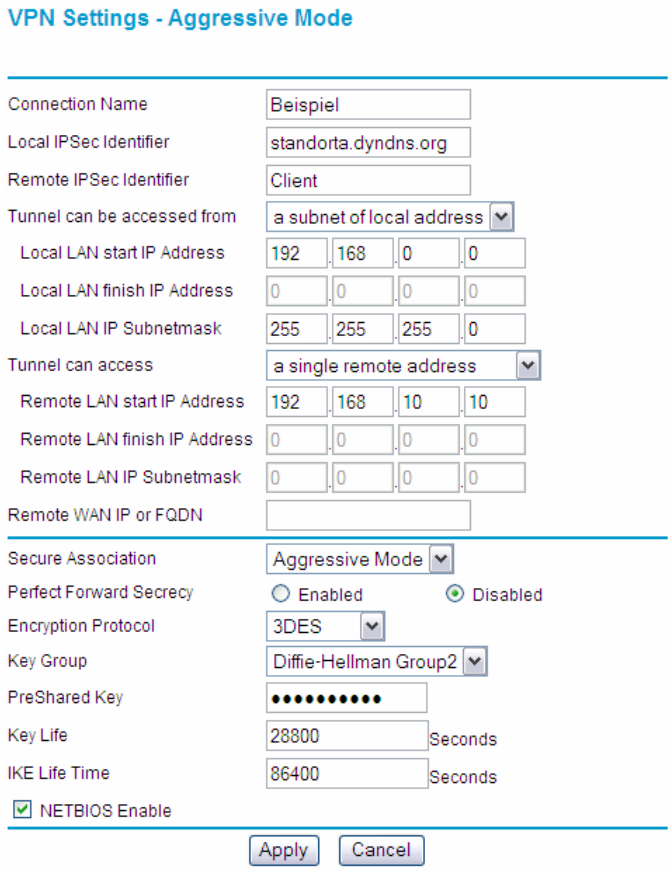
WAN-Seite des VPN-Client-PCs: 0.0.0.0 (dynamisch)
LAN-Seite des VPN-Client-PCs: 0.0.0.0 (dynamisch)



13.2. Konfiguration des Routers an Standort A

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links oben auf den Menüpunkt **VPN Settings**.
- Aktivieren Sie den Punkt vor der 1 und klicken Sie auf **Edit**.
- Konfigurieren Sie die Verbindung wie in Abb. 13.2.1 gezeigt.
  ! Im Feld **Local IPSec Identifier** tragen Sie die DynDNS-Namen des FVS318 ein (in diesem Beispiel: standorta.dyndns.org).

Abb. 13.2.1



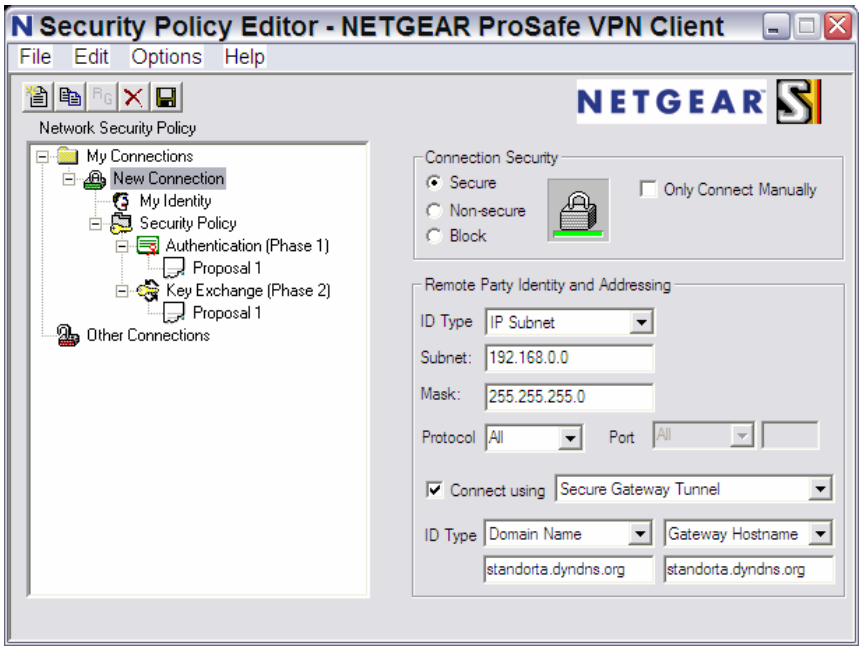
- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

13.3. Konfiguration des ProSafe VPN Client (Standort B)

- Starten Sie den Security Policy Editor mit einem Doppelklick auf das Symbol des ProSafe VPN Client in der Taskleiste:
  

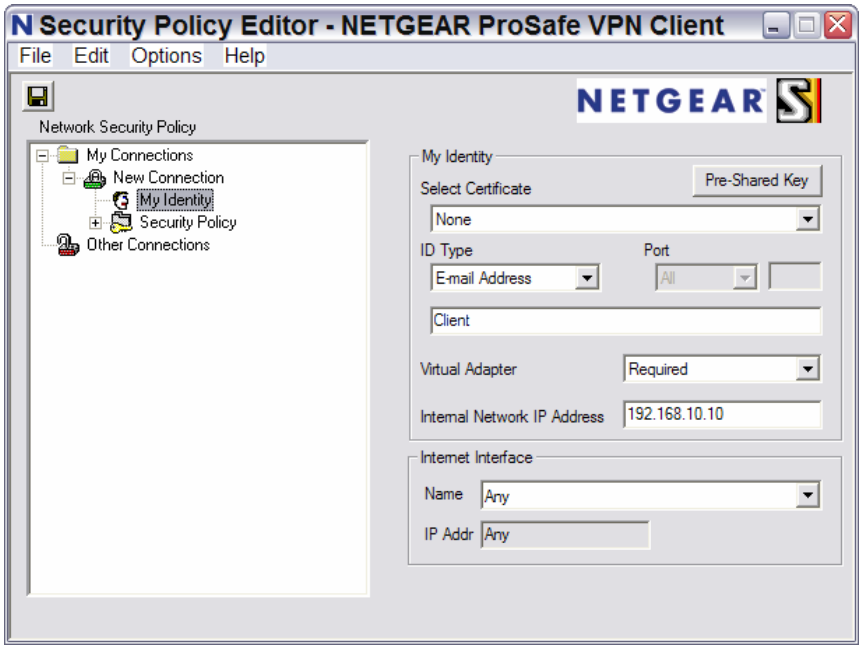
- Klicken Sie auf **Edit** –> **Add** -> **Connection** um eine neue Verbindung zu erstellen.
- Um die Eingabe einer IP-Adresse für den Virtual Adapter zu ermöglichen, aktivieren Sie im Security Policy Editor unter **Options** -> **Global Policy Settings** die Option **Allow to Specify Internal Network Address**.
- Konfigurieren Sie die Verbindung wie in Abb. 13.3.1 gezeigt.
  ! Im **unteren** Feld **ID Type** wählen Sie **Domain Name** und tragen darunter den DynDNS-Namen des FVS318 ein (in diesem Beispiel: standorta.dyndns.org). Rechts daneben wählen Sie **Gateway Hostname** und tragen darunter ebenfalls den DynDNS-Namen des FVS318 ein (in diesem Beispiel: standorta.dyndns.org).

Abb. 13.3.1



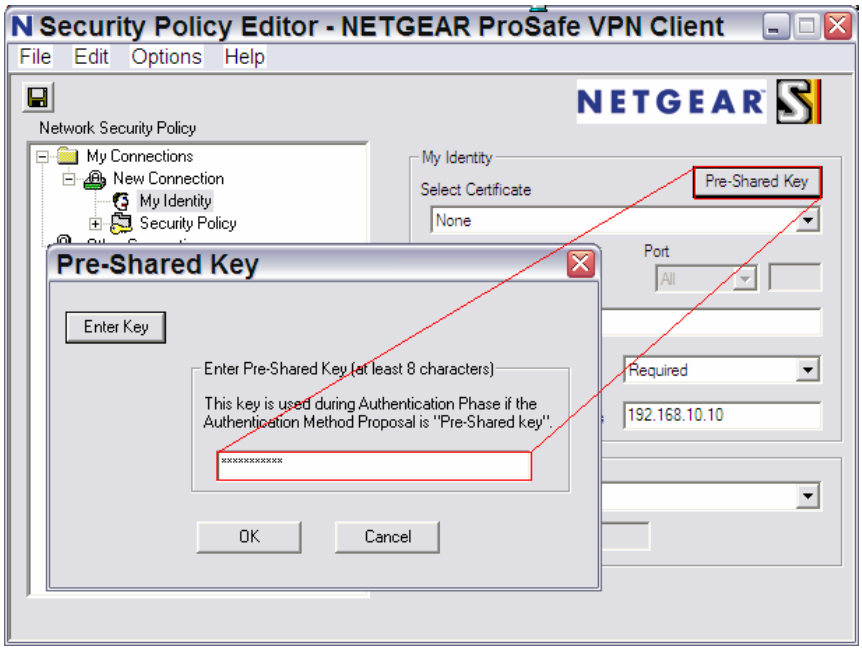
- Konfigurieren Sie die Option **My Identity** wie in Abb. 13.3.2 gezeigt.

Abb. 13.3.2



- Um den Pre-Shared Key einzutragen, klicken Sie rechts oben auf **Pre-Shared Key**. In dem erschienenen Fenster klicken Sie auf **Enter Key** und geben den Pre-Shared Key ein (siehe Abb. 13.3.3).

Abb. 13.3.3



- Konfigurieren Sie die Verbindung wie in den folgenden drei Abb. gezeigt.

Abb. 13.3.4

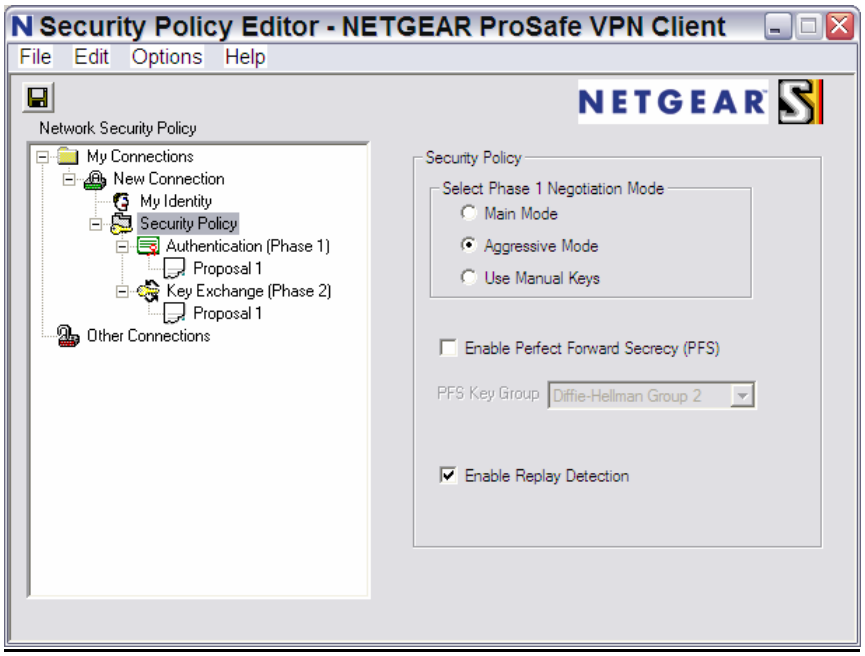


Abb. 13.3.5

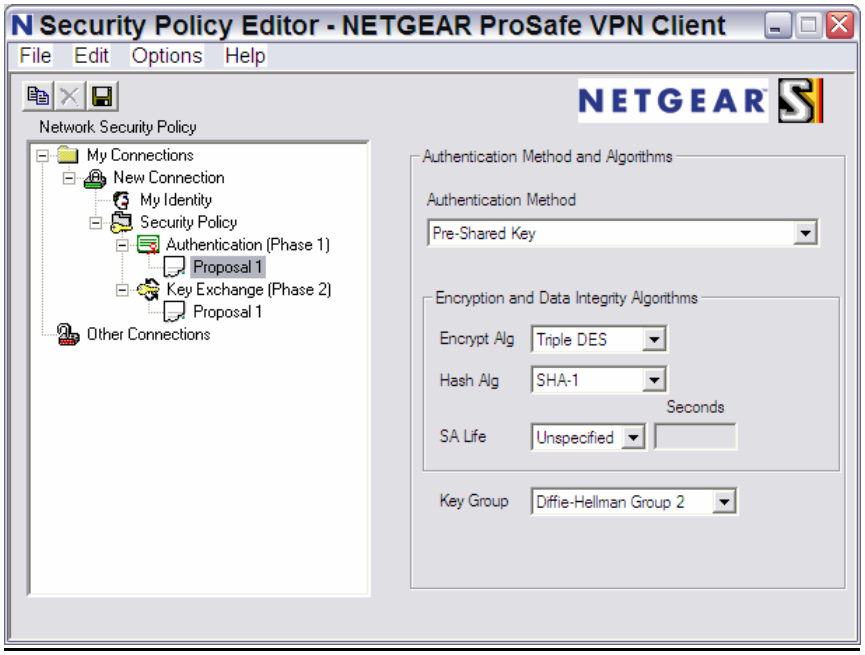
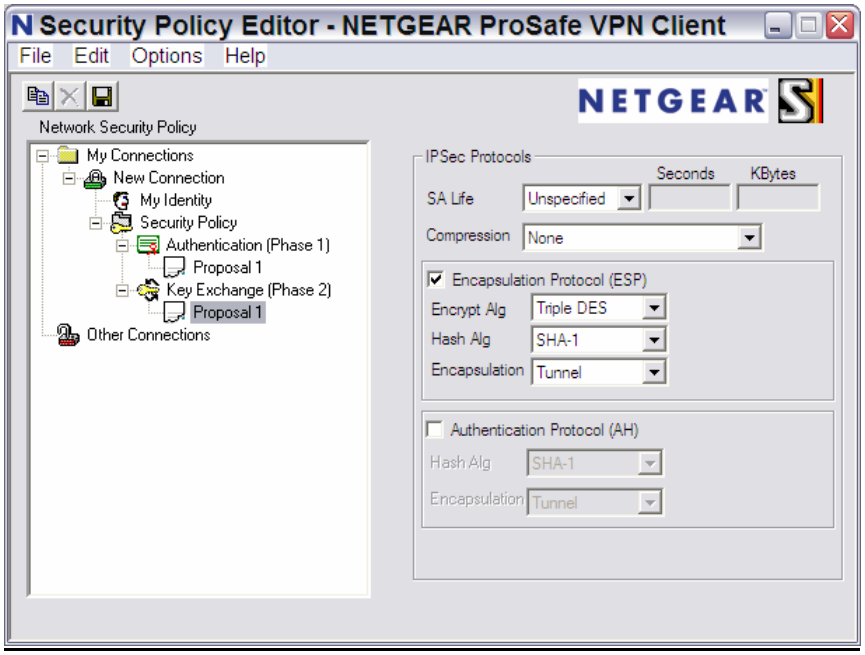


Abb. 13.3.6



- Klicken Sie links oben auf **File** -> **Save** um die erstellte Verbindung zu speichern.

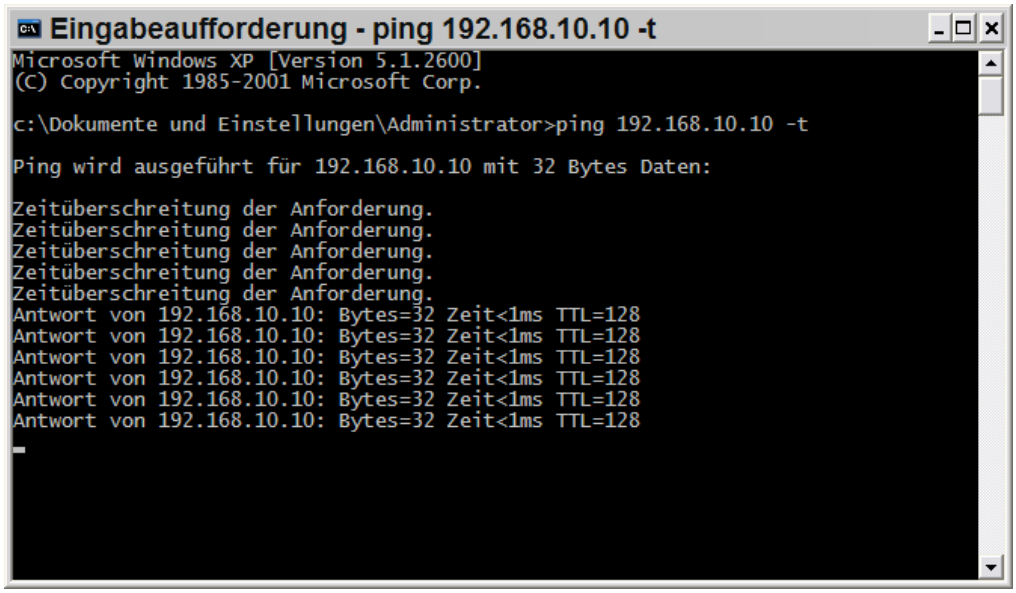
13.4. Testen der Verbindung

Um die Verbindung zu testen, versuchen Sie von dem PC mit dem VPN Client an Standort B einen PC an Standort A (z.B. 192.168.0.2) zu erreichen:

Hinweis:	Um den PC im Netzwerk an Standort A erreichen zu können, muss dort der lokale FVS318 als Standardgateway verwendet werden. Für dieses Beispiel gilt: Der PC an Standort A (192.168.**0**.2) verwendet als Gateway seinen lokalen Router 192.168.**0**.1.

- Klicken Sie in Windows links unten auf **Start** und **Ausführen...**
- Geben Sie **cmd** ein (Windows 95/98/ME: **command**) und klicken Sie auf **OK**
- Geben Sie folgenden Befehl ein: **ping 192.168.10.10 –t** (siehe Abb. 13.4.1)

Abb. 13.4.1



- Bei richtiger Konfiguration wird die VPN-Verbindung innerhalb einiger Sekunden aufgebaut (siehe Abb. 13.4.1).

14. Beispielkonfiguration

ProSafe VPN Client Software (hinter einem NAT-Router)
zu
FVS318v1 mit dynamischer WAN-IP-Adresse

14.1. Übersicht

Standort A:

FVS318v1 (Firmware 2.4)

FVS318v1 LAN-Seite: 192.168.0.1
FVS318v1 WAN-Seite: standorta.dyndns.org

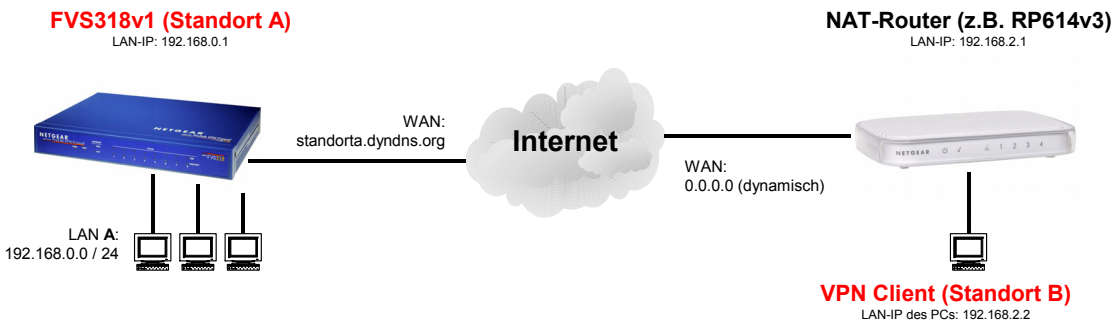
Netzwerkadresse: 192.168.0.0/24
Test-PC im Netzwerk: 192.168.0.2

Standort B:

ProSafe VPN Client Software (Ver.: 10.5.1 Build 8)

NAT-Router LAN-Seite: 192.168.2.1
NAT-Router WAN-Seite: 0.0.0.0 (dynamisch)

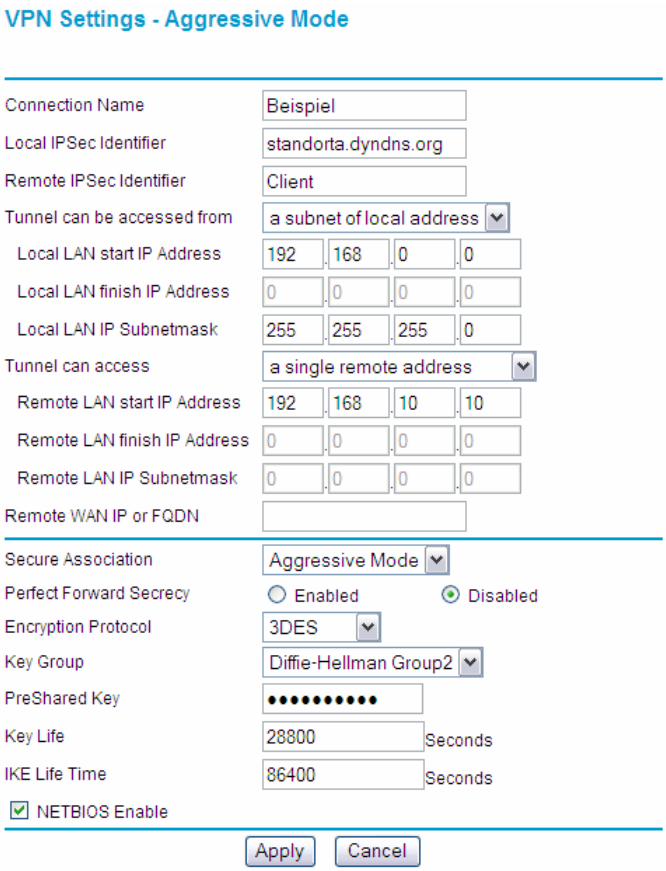
PC mit ProSafe VPN Client Software: 192.168.2.2



14.2. Konfiguration des Routers an Standort A

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links oben auf den Menüpunkt **VPN Settings**.
- Aktivieren Sie den Punkt vor der 1 und klicken Sie auf **Edit**.
- Konfigurieren Sie die Verbindung wie in Abb. 14.2.1 gezeigt.
  ! Im Feld **Local IPSec Identifier** tragen Sie die DynDNS-Namen des FVS318 ein (in diesem Beispiel: standorta.dyndns.org).

Abb. 14.2.1



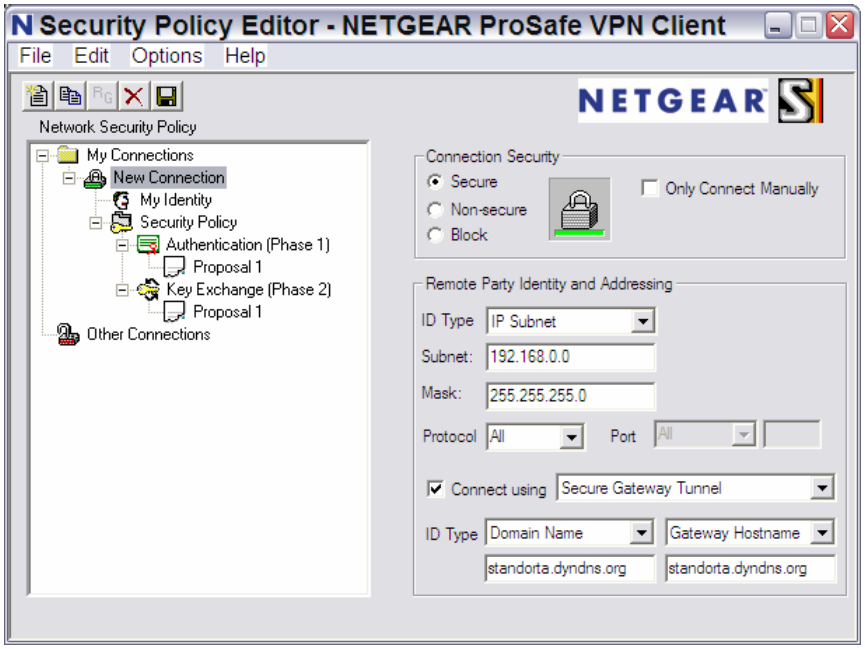
- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

14.3. Konfiguration des ProSafe VPN Client (Standort B)

- Starten Sie den Security Policy Editor mit einem Doppelklick auf das Symbol des ProSafe VPN Client in der Taskleiste:
  

- Klicken Sie auf **Edit** –> **Add** -> **Connection** um eine neue Verbindung zu erstellen.
- Um die Eingabe einer IP-Adresse für den Virtual Adapter zu ermöglichen, aktivieren Sie im Security Policy Editor unter **Options** -> **Global Policy Settings** die Option **Allow to Specify Internal Network Address**.
- Konfigurieren Sie die Verbindung wie in Abb. 14.3.1 gezeigt.
  ! Im **unteren** Feld **ID Type** wählen Sie **Domain Name** und tragen darunter den DynDNS-Namen des FVS318 ein (in diesem Beispiel: standorta.dyndns.org).
  Rechts daneben wählen Sie **Gateway Hostname** und tragen darunter ebenfalls den DynDNS-Namen des FVS318 ein (in diesem Beispiel: standorta.dyndns.org).

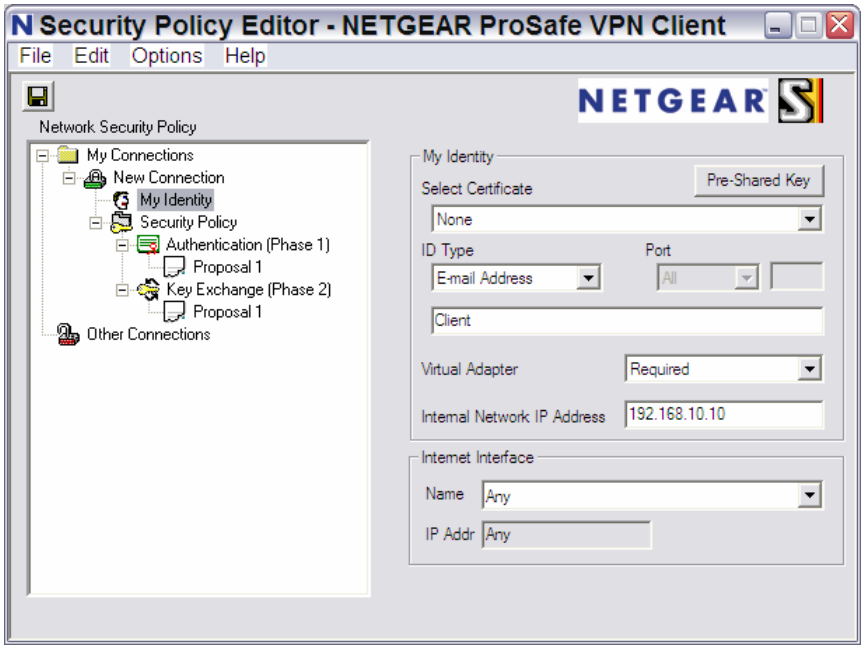
Abb. 14.3.1



- Konfigurieren Sie die Option **My Identity** wie in Abb. 14.3.2 gezeigt.

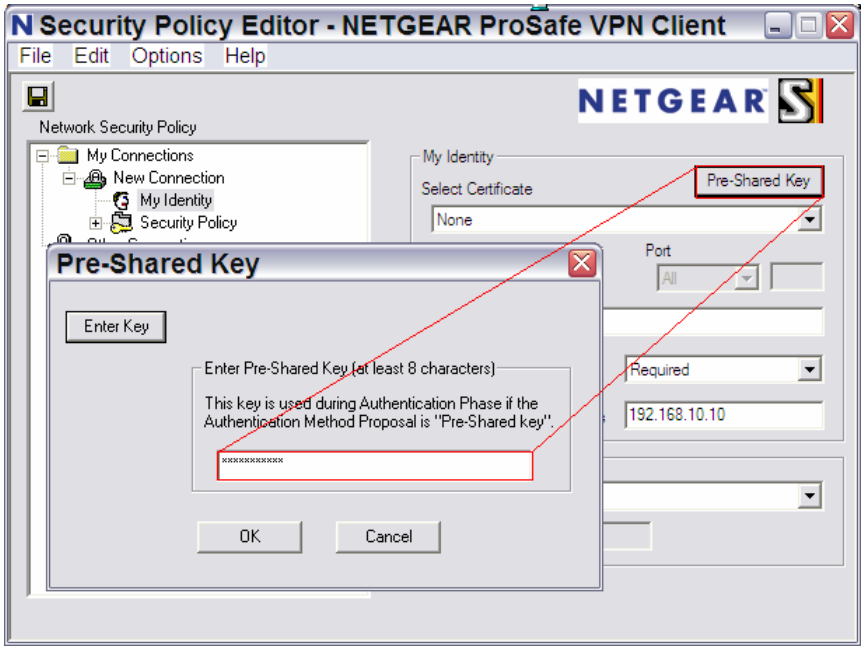
  ! Bei **Internet Interface** wählen Sie “Any“ aus und vergeben Sie eine IP-Adresse für den Virtual Adapter (in diesem Beispiel 192.168.10.10). Der Virtual Adapter muß dabei auf **Required** stehen.

Abb. 14.3.2



- Um den Pre-Shared Key einzutragen, klicken Sie rechts oben auf **Pre-Shared Key**. In dem erschienenen Fenster klicken Sie auf **Enter Key** und geben den Pre-Shared Key ein (siehe Abb. 14.3.3).

Abb. 14.3.3



- Konfigurieren Sie die Verbindung wie in den folgenden drei Abb. gezeigt.

Abb. 14.3.4

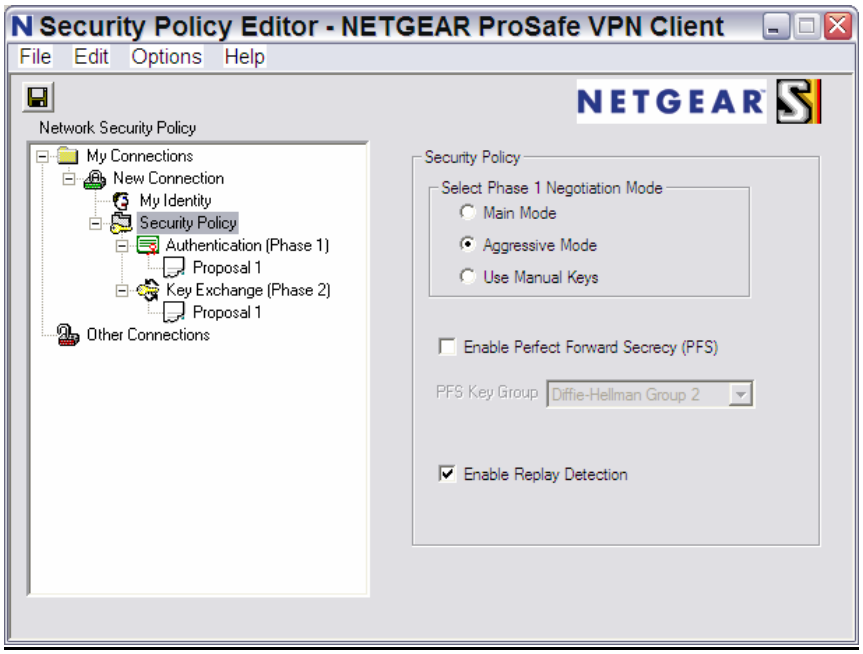


Abb. 14.3.5

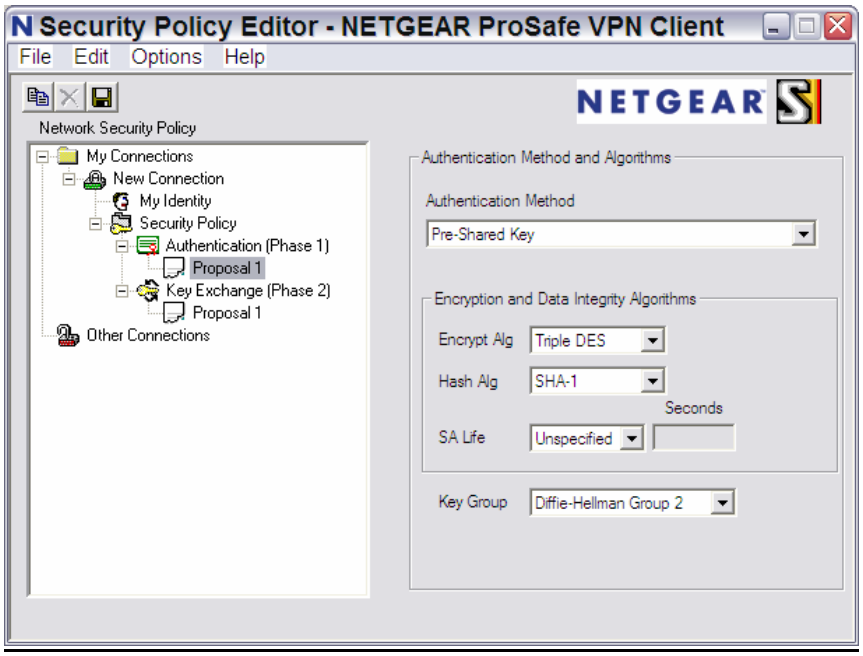
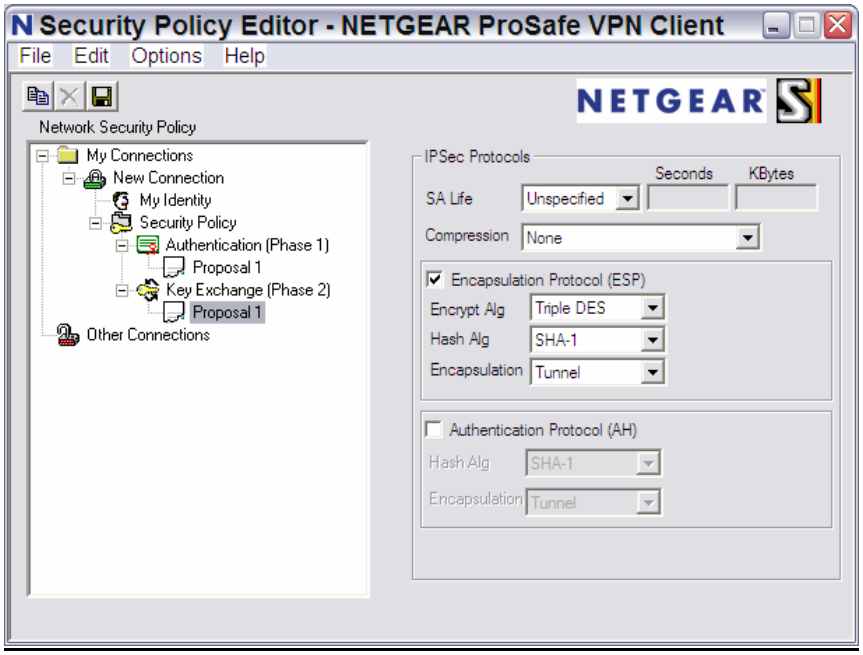


Abb. 14.3.6



- Klicken Sie links oben auf **File** -> **Save** um die erstellte Verbindung zu speichern.

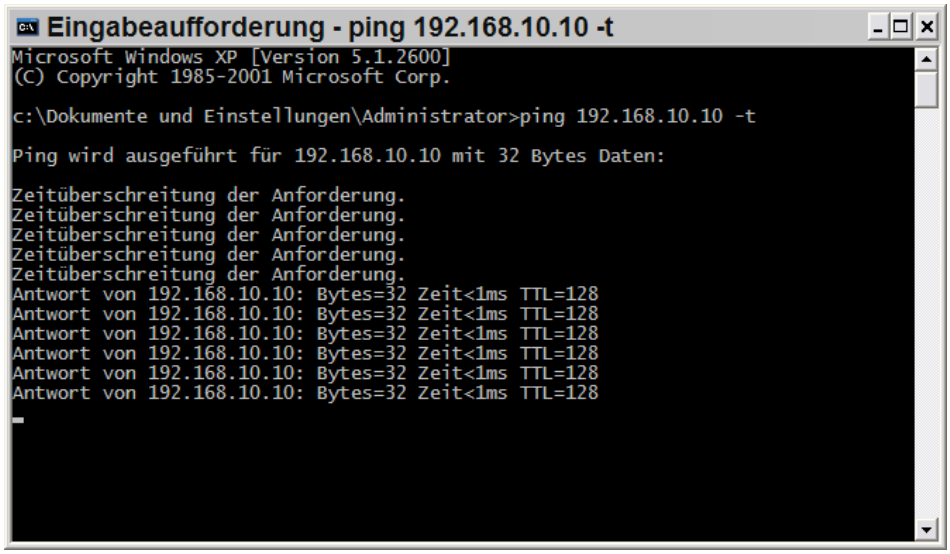
14.4. Testen der Verbindung

Um die Verbindung zu testen, versuchen Sie von dem PC mit dem VPN Client an Standort B (192.168.2.2) einen PC an Standort A (z.B. 192.168.0.2) zu erreichen:

Hinweis:	- Bei beiden PCs muss der jeweils lokale Router als Gateway verwendet werden: - Der PC an Standort A (192.168.**0**.2) verwendet als Gateway seinen lokalen Router 192.168.**0**.1. - Der PC an Standort B (192.168.**2**.2) verwendet als Gateway seinen lokalen Router 192.168.**2**.1.

- Klicken Sie in Windows links unten auf **Start** und **Ausführen...**
- Geben Sie **cmd** ein (Windows 95/98/ME: **command**) und klicken Sie auf **OK**
- Geben Sie folgenden Befehl ein: **ping 192.168.10.10 –t** (siehe Abb. 14.4.1)

Abb. 14.4.1



- Bei richtiger Konfiguration wird die VPN-Verbindung innerhalb einiger Sekunden aufgebaut (siehe Abb. 14.4.1).

15. Beispielkonfiguration

ProSafe VPN Client Software
zu
FVL328 mit fester WAN-IP-Adresse

15.1. Übersicht

Standort A:

FVL328 (Firmware 2.0 Release 08)

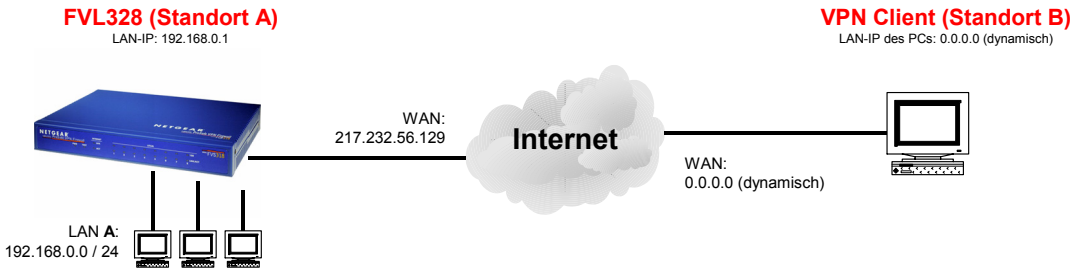
FVL328 LAN-Seite: 192.168.0.1
FVL328 WAN-Seite: 217.232.56.129

Netzwerkadresse: 192.168.0.0/24
Test-PC im Netzwerk: 192.168.0.2

Standort B:

ProSafe VPN Client Software (Ver.: 10.5.1 Build 8)

WAN-Seite des VPN-Client-PCs: 0.0.0.0 (dynamisch)
LAN-Seite des VPN-Client-PCs: 0.0.0.0 (dynamisch)

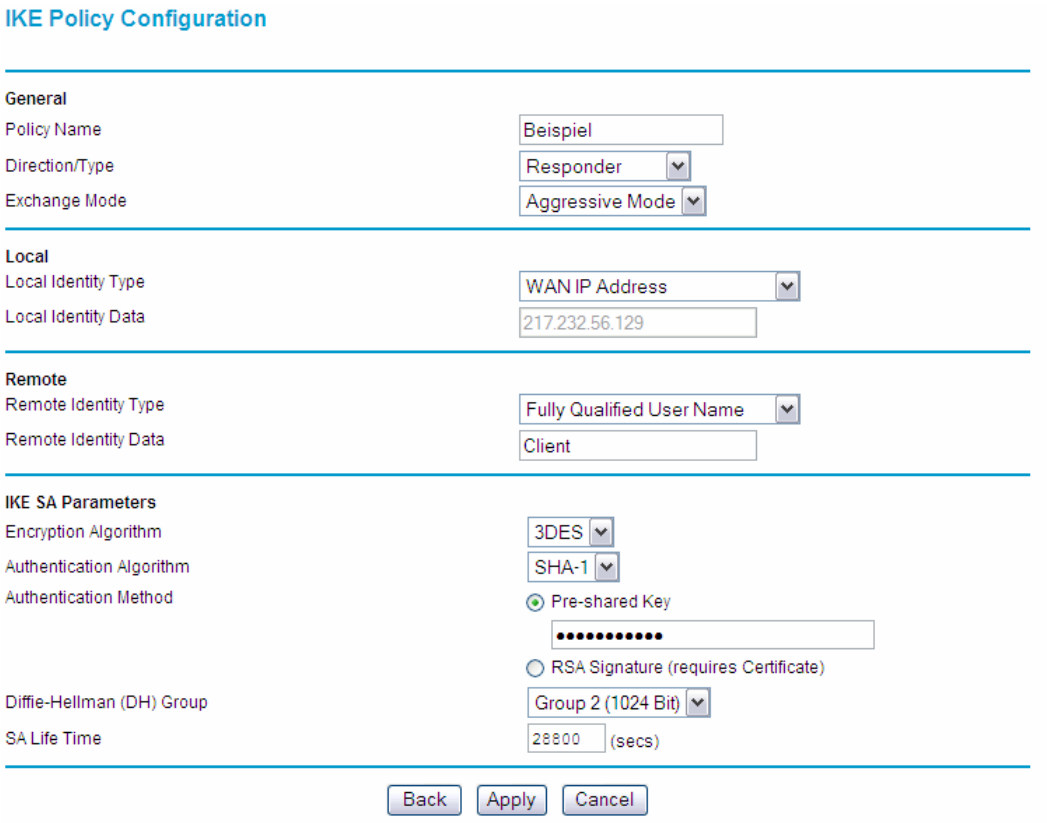


15.2. Konfiguration des Routers an Standort A

Schritt 1: Erstellen der IKE-Policy (Phase 1)

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links auf den Menüpunkt **IKE Policies**.
- Klicken Sie dort auf den Button **Add** um eine IKE-Policy zu erstellen.
- Konfigurieren Sie die IKE-Policy wie in Abb. 15.2.1 gezeigt.

Abb. 15.2.1

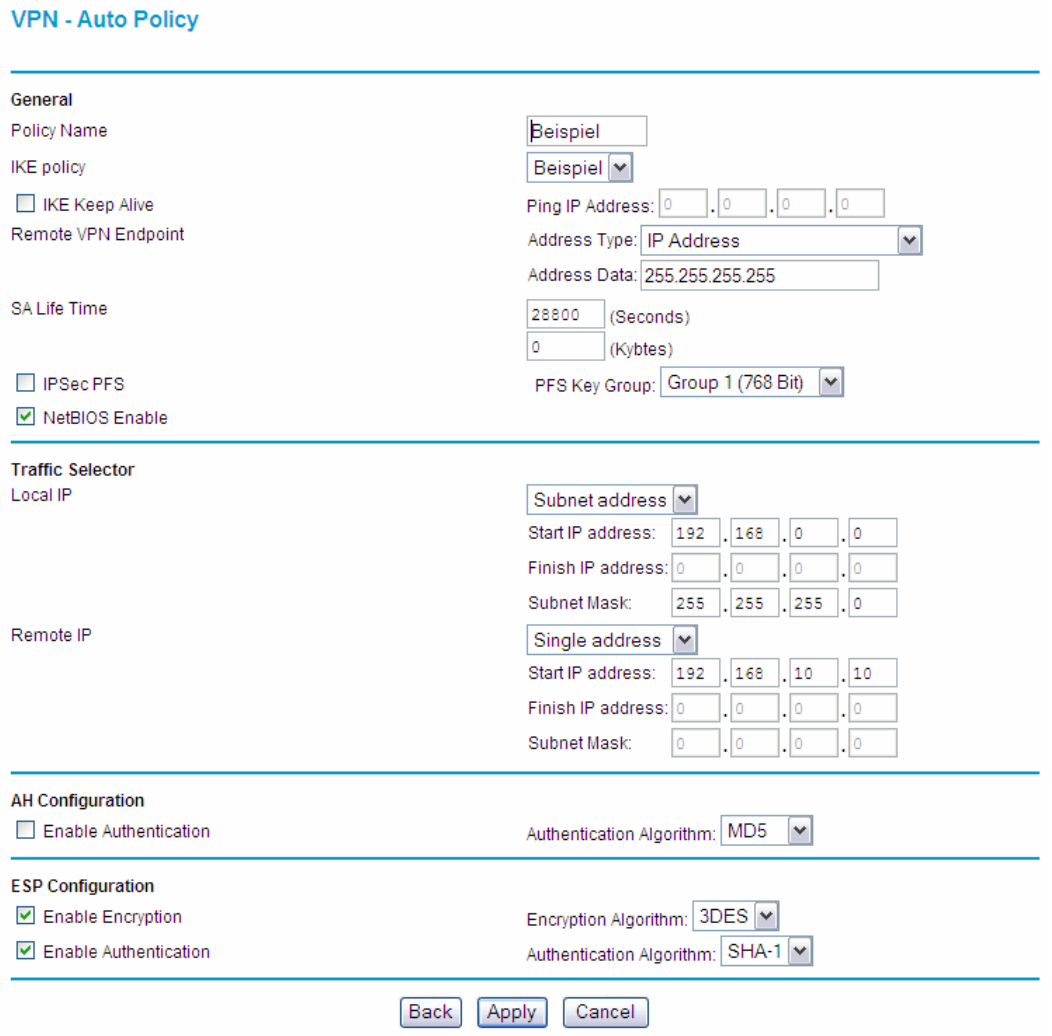


- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

Schritt 2: Erstellen der VPN-Policy (Phase 2)

- Klicken Sie links auf den Menüpunkt **VPN Policies**.
- Um eine VPN-Policy zu erstellen, klicken Sie auf **Add Auto Policy**.
- Konfigurieren Sie die VPN-Policy wie in Abb. 15.2.2 gezeigt.
  ! Bei dem Punkt **IKE policy** wählen Sie die in Schritt 1 erstellte IKE Policy.
  ! Lassen Sie das Feld **Address Data** bei **Remote VPN Endpoint** leer. Nach dem Speichern wird automatisch die 255.255.255.255 eingetragen.

Abb. 15.2.2



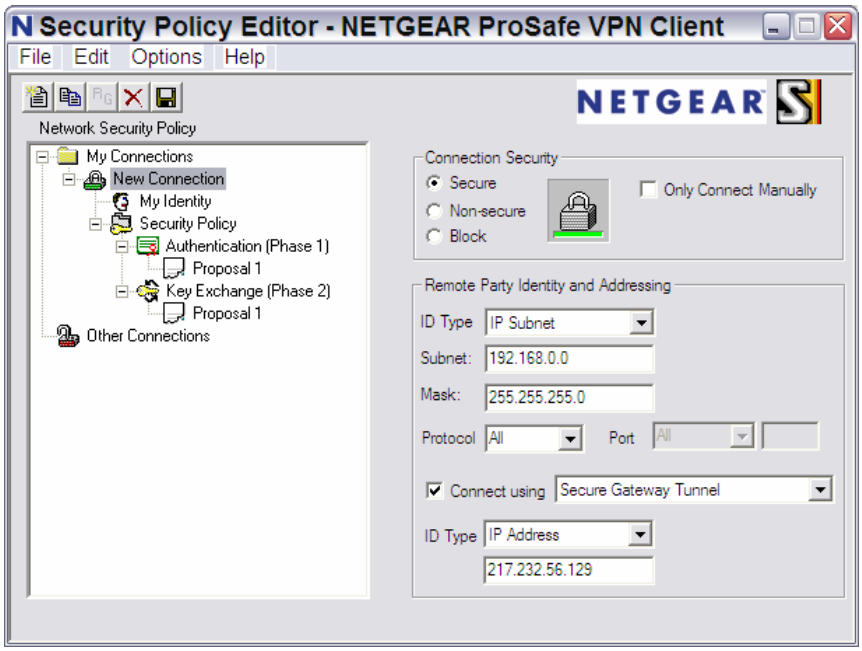
- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

15.3. Konfiguration des ProSafe VPN Client (Standort B)

- Starten Sie den Security Policy Editor mit einem Doppelklick auf das Symbol des ProSafe VPN Client in der Taskleiste:
  

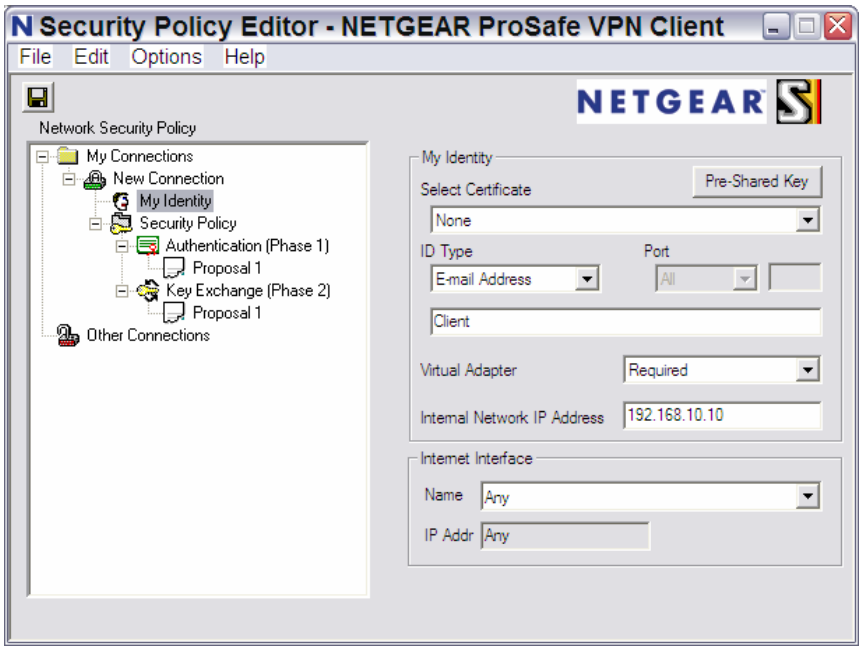
- Klicken Sie auf **Edit** –> **Add** -> **Connection** um eine neue Verbindung zu erstellen.
- Um die Eingabe einer IP-Adresse für den Virtual Adapter zu ermöglichen, aktivieren Sie im Security Policy Editor unter **Options** -> **Global Policy Settings** die Option **Allow to Specify Internal Network Address**.
- Konfigurieren Sie die Verbindung wie in Abb. 15.3.1 gezeigt.
  ! Im **unteren** Feld **ID Type** wählen Sie **IP Address** und tragen darunter die WAN-IP-Adresse des FVL328 ein (in diesem Beispiel: 217.232.56.129).

Abb. 15.3.1



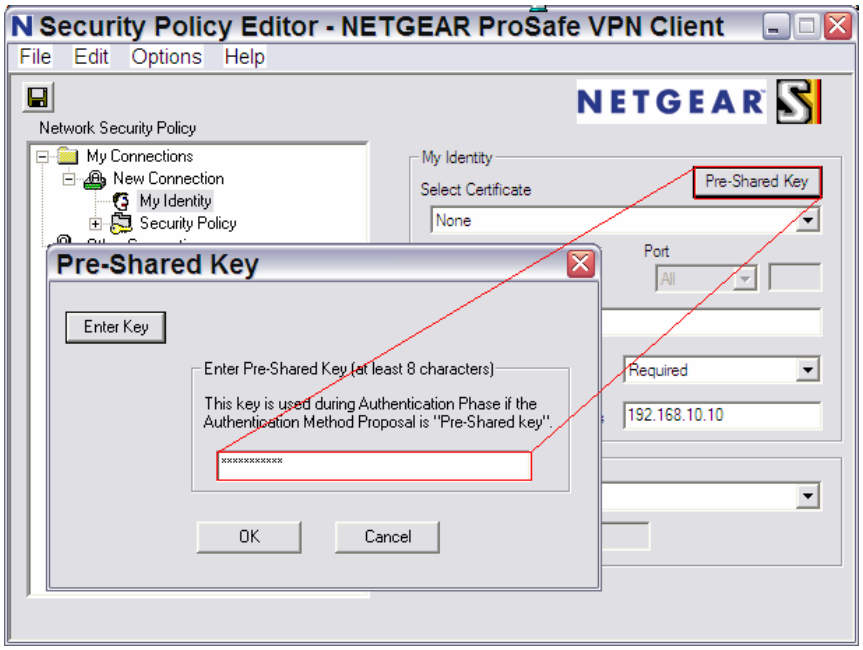
- Konfigurieren Sie die Option **My Identity** wie in Abb. 15.3.2 gezeigt.

Abb. 15.3.2



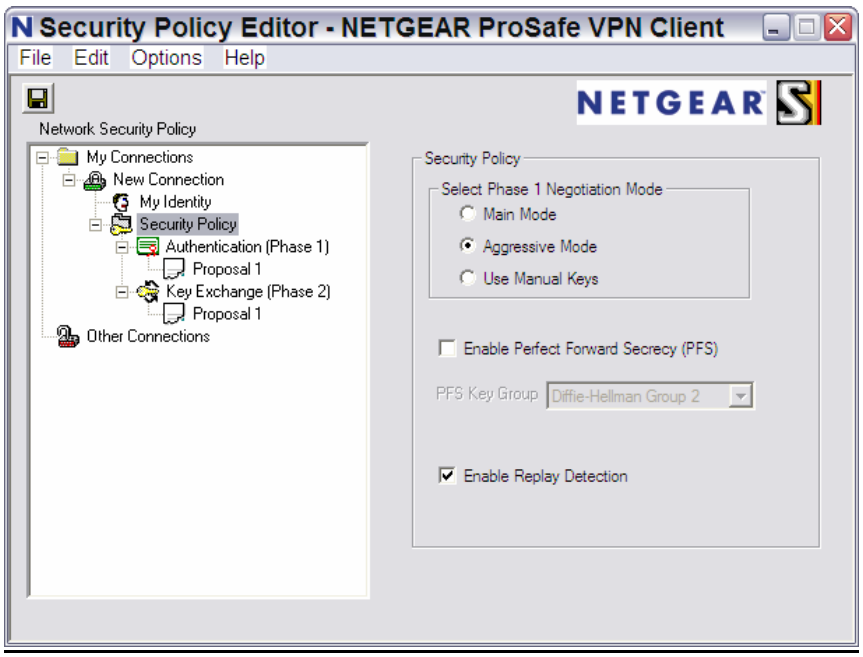
- Um den Pre-Shared Key einzutragen, klicken Sie rechts oben auf **Pre-Shared Key**. In dem erschienenen Fenster klicken Sie auf **Enter Key** und geben den Pre-Shared Key ein (siehe Abb. 15.3.3).

Abb. 15.3.3



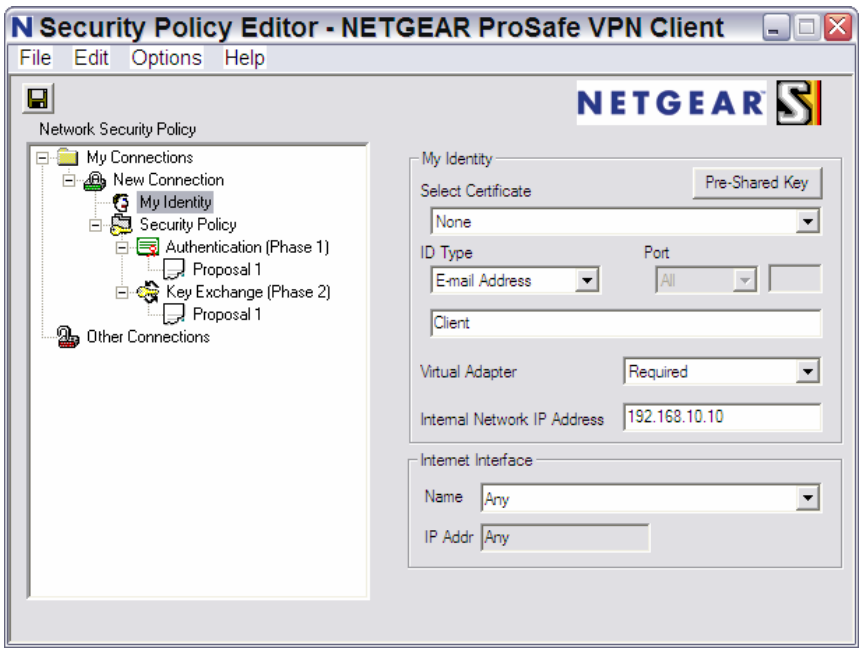
- Konfigurieren Sie die Option **Security Policy** wie in Abb. 15.3.4 gezeigt.
  ! Achten Sie darauf, dass der Punkt vor **Aggressive Mode** gesetzt ist.

Abb. 15.3.4



- Wechseln Sie **nochmals** auf die Option **My Identity** und ändern den **ID Type** auf **E-mail Address** (siehe Abb. 15.3.5).
- Im Feld darunter tragen Sie **Client** ein.

Abb. 15.3.5



- Konfigurieren Sie die Verbindung wie in den folgenden zwei Abb. gezeigt.

Abb. 15.3.6

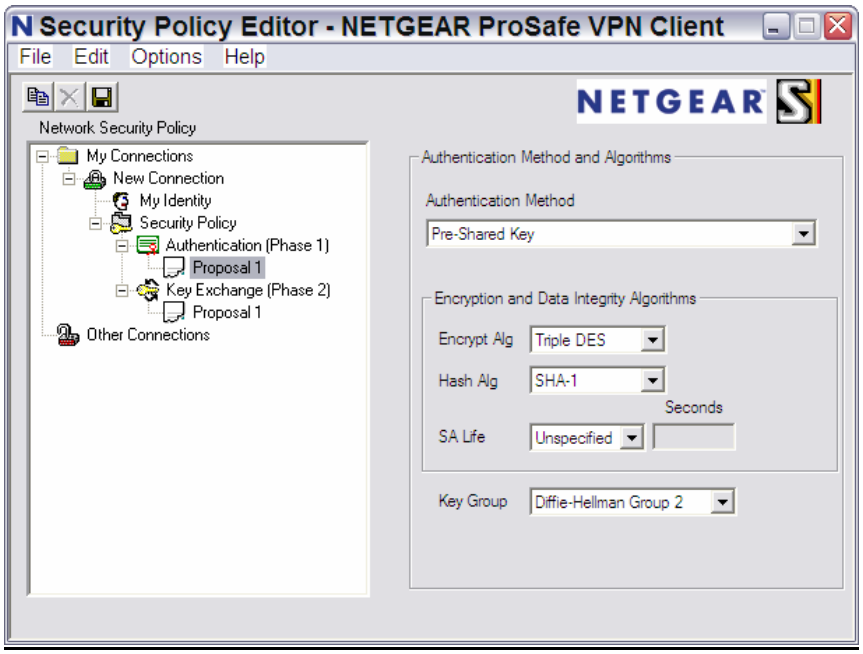
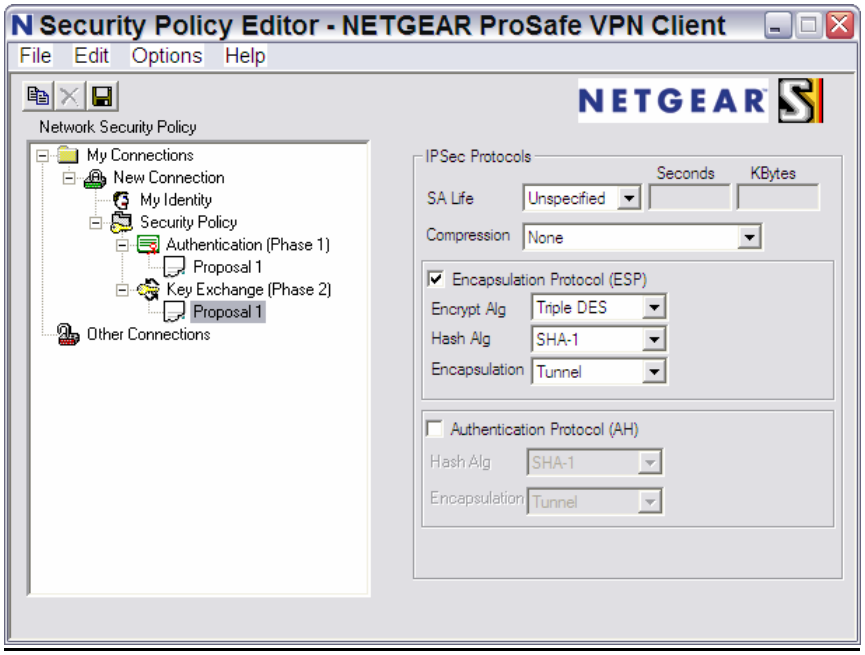


Abb. 15.3.7



- Klicken Sie links oben auf **File** -> **Save** um die erstellte Verbindung zu speichern.

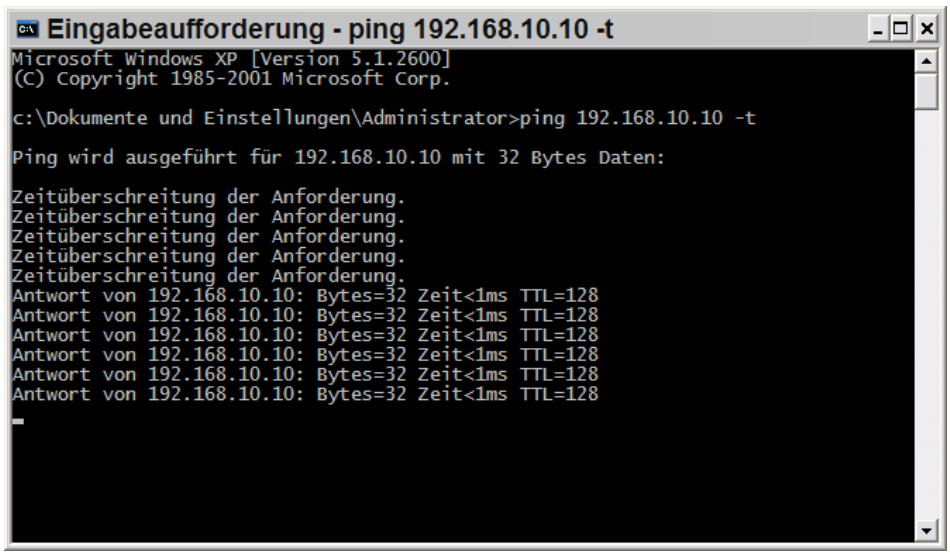
15.4. Testen der Verbindung

Um die Verbindung zu testen, versuchen Sie von dem PC mit dem VPN Client an Standort B einen PC an Standort A (z.B. 192.168.0.2) zu erreichen:

Hinweis:	- Um den PC im Netzwerk an Standort A erreichen zu können, muss dort der lokale FVL328 als Standardgateway verwendet werden. Für dieses Beispiel gilt: Der PC an Standort A (192.168.**0**.2) verwendet als Gateway seinen lokalen Router 192.168.**0**.1.

- Klicken Sie in Windows links unten auf **Start** und **Ausführen...**
- Geben Sie **cmd** ein (Windows 95/98/ME: **command**) und klicken Sie auf **OK**
- Geben Sie folgenden Befehl ein: **ping 192.168.0.2 –t** (siehe Abb. 15.4.1)

Abb. 15.4.1



- Bei richtiger Konfiguration wird die VPN-Verbindung innerhalb einiger Sekunden aufgebaut (siehe Abb. 15.4.1).

- Der VPN Status des FVL328 (Menüpunkt **VPN Status** in der Router-Konfiguration) zeigt ebenfalls eine etablierte VPN-Verbindung (siehe Abb. 15.4.2).

Abb. 15.4.2

IPSec Connection Status

#	Policy Name	Endpoint	Tx (KBytes)	State	Action
1	Beispiel	255.255.255.255	2400	Phase 1: M-ESTABLISHED / Phase 2: ESTABLISHED	Drop

16. Beispielkonfiguration

ProSafe VPN Client Software
zu
FVL328 mit dynamischer WAN-IP-Adresse

16.1. Übersicht

Standort A:

FVL328 (Firmware 2.0 Release 08)

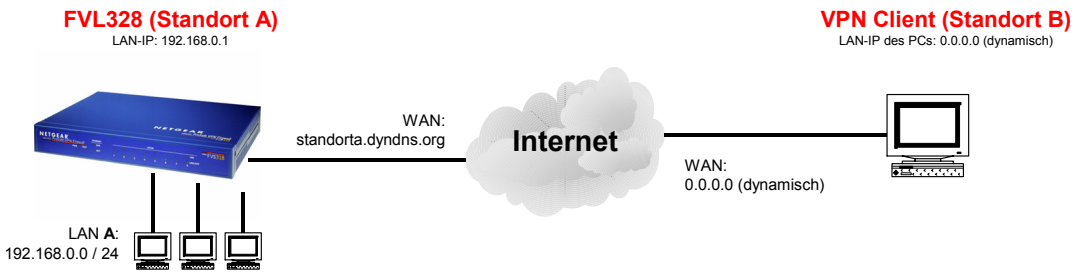
FVL328 LAN-Seite: 192.168.0.1
FVL328 WAN-Seite: standorta.dyndns.org

Netzwerkadresse: 192.168.0.0/24
Test-PC im Netzwerk: 192.168.0.2

Standort B:

ProSafe VPN Client Software (Ver.: 10.5.1 Build 8)

WAN-Seite des VPN-Client-PCs: 0.0.0.0 (dynamisch)
LAN-Seite des VPN-Client-PCs: 0.0.0.0 (dynamisch)

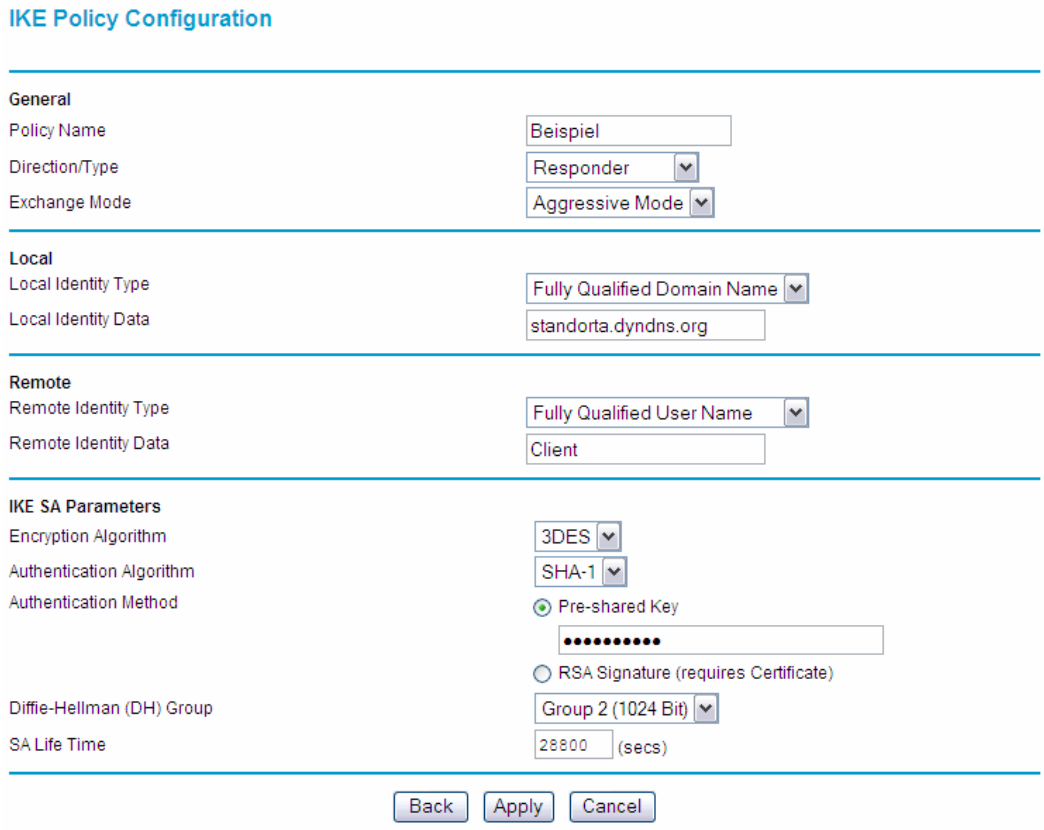


16.2. Konfiguration des Routers an Standort A

Schritt 1: Erstellen der IKE-Policy (Phase 1)

- Starten Sie die Router-Konfigurationsoberfläche.
- Klicken Sie links auf den Menüpunkt **IKE Policies**.
- Klicken Sie dort auf den Button **Add** um eine IKE-Policy zu erstellen.
- Konfigurieren Sie die IKE-Policy wie in Abb. 16.2.1 gezeigt.

Abb. 16.2.1

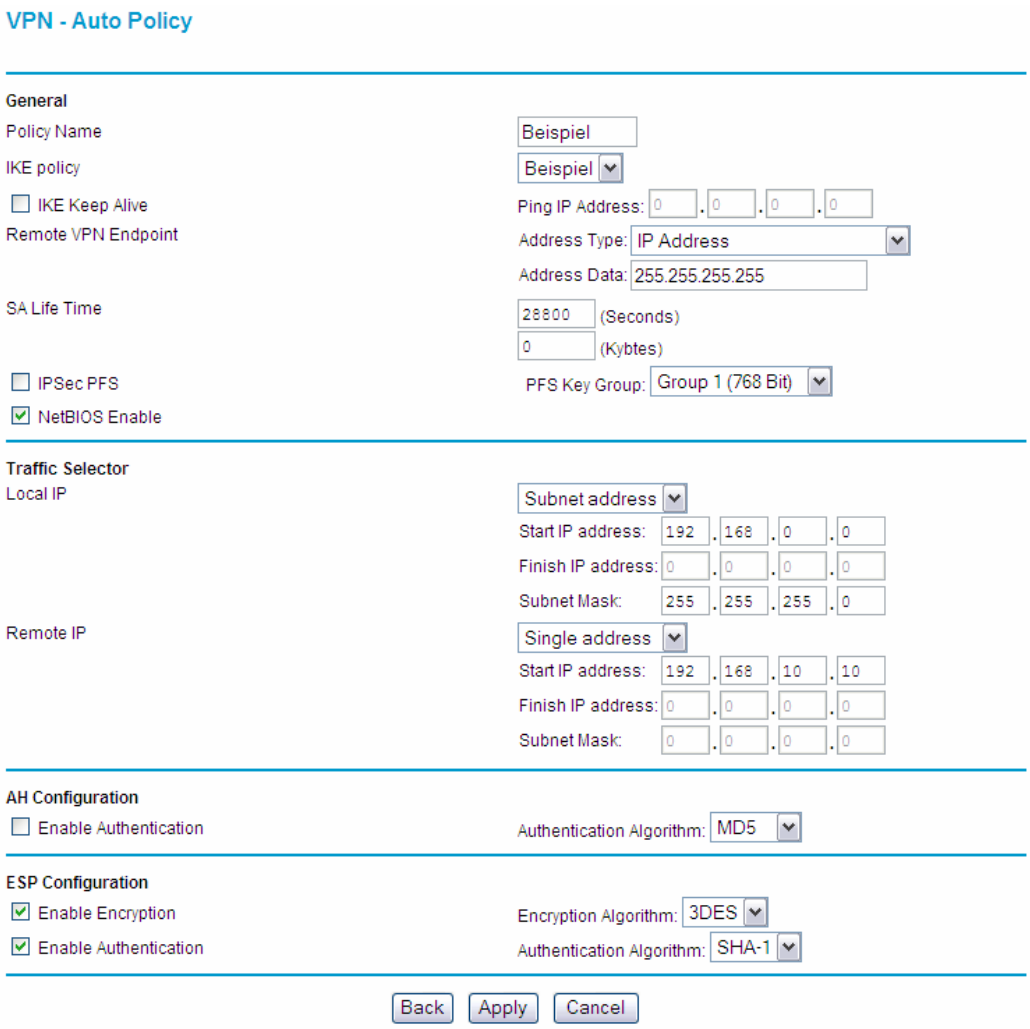


- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

Schritt 2: Erstellen der VPN-Policy (Phase 2)

- Klicken Sie links auf den Menüpunkt **VPN Policies**.
- Um eine VPN-Policy zu erstellen, klicken Sie auf **Add Auto Policy**.
- Konfigurieren Sie die VPN-Policy wie in Abb. 16.2.2 gezeigt.
  ! Bei dem Punkt **IKE policy** wählen Sie die in Schritt 1 erstellte IKE Policy.

Abb. 16.2.2



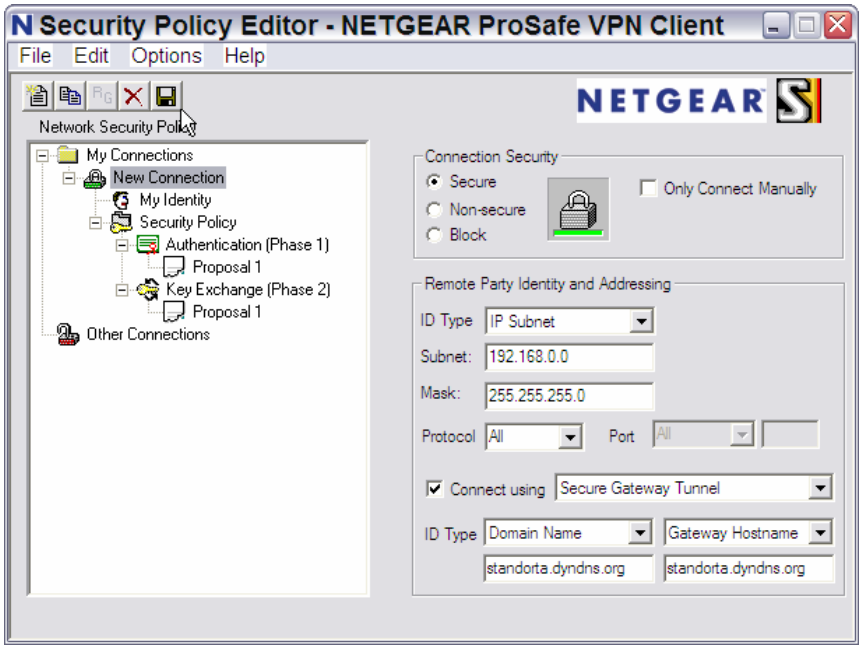
- Klicken Sie auf **Apply** um die Einstellungen zu speichern.

16.3. Konfiguration des ProSafe VPN Client (Standort B)

- Starten Sie den Security Policy Editor mit einem Doppelklick auf das Symbol des ProSafe VPN Client in der Taskleiste:
  

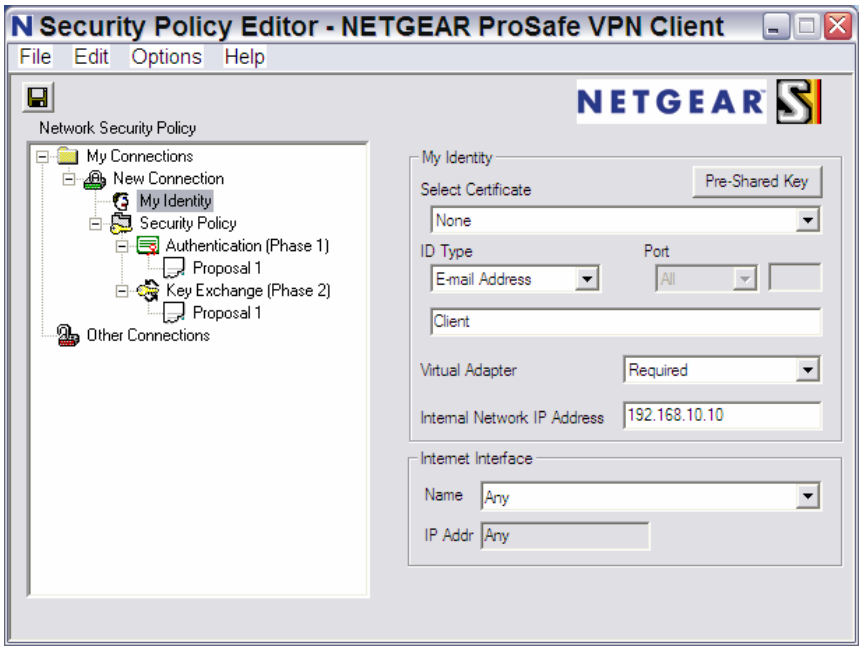
- Klicken Sie auf **Edit** –> **Add** -> **Connection** um eine neue Verbindung zu erstellen.
- Konfigurieren Sie die Verbindung wie in Abb. 16.3.1 gezeigt.
  ! Im **unteren** Feld **ID Type** wählen Sie **Domain Name** und tragen darunter den DynDNS-Namen des FVL328 ein (in diesem Beispiel: standorta.dyndns.org).
  Rechts daneben wählen Sie **Gateway Hostname** und tragen darunter ebenfalls den DynDNS-Namen des FVL328 ein (in diesem Beispiel: standorta.dyndns.org).

Abb. 16.3.1



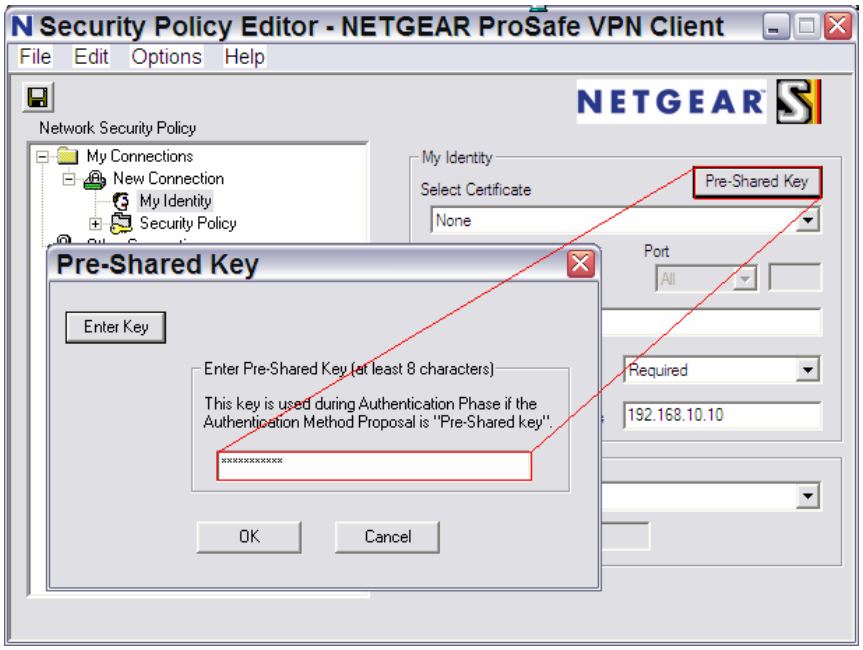
- Konfigurieren Sie die Option **My Identity** wie in Abb. 16.3.2 gezeigt.

Abb. 16.3.2



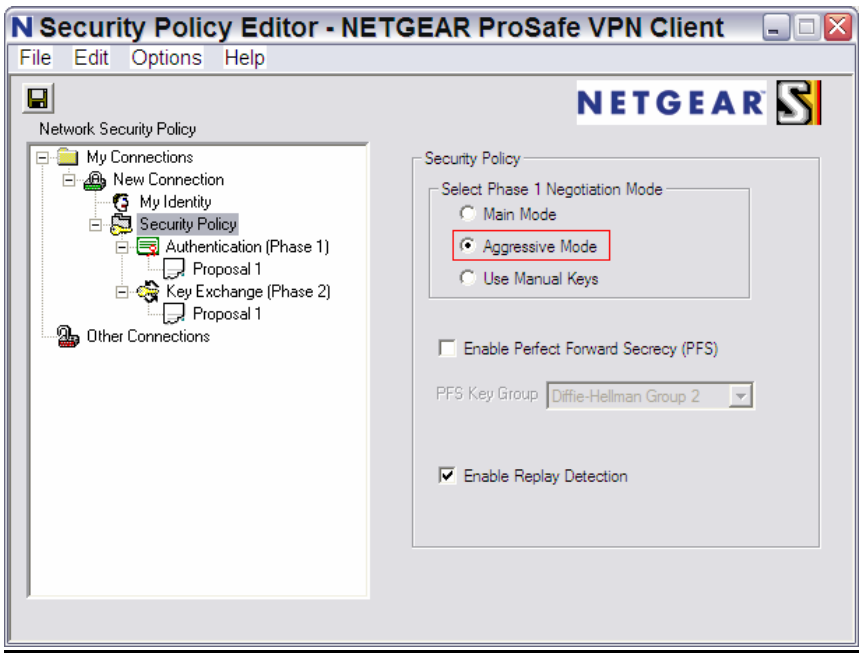
- Um den Pre-Shared Key einzutragen, klicken Sie rechts oben auf **Pre-Shared Key**. In dem erschienenen Fenster klicken Sie auf **Enter Key** und geben den Pre-Shared Key ein (siehe Abb. 16.3.3).

Abb. 16.3.3



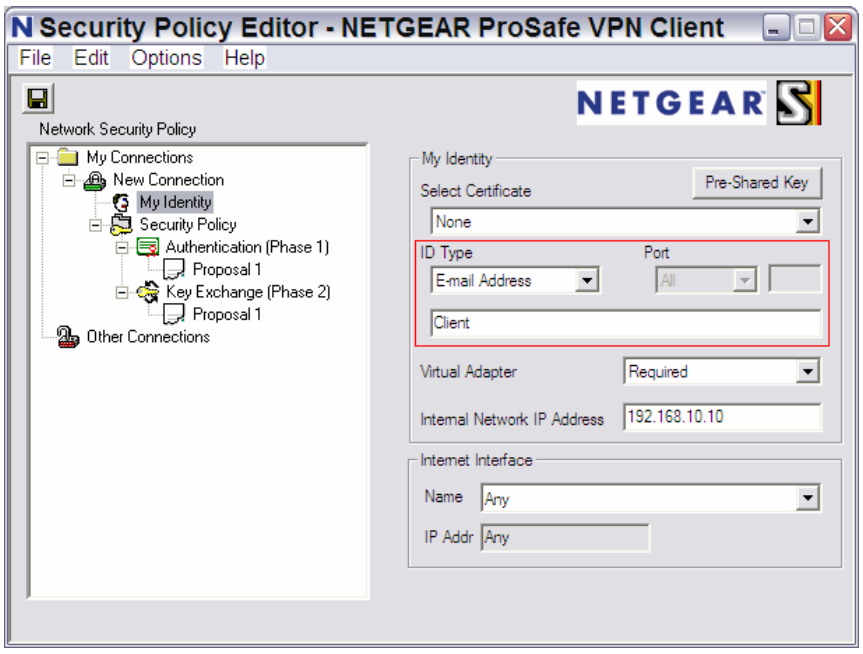
- Konfigurieren Sie die Option **Security Policy** wie in Abb. 16.3.4 gezeigt.
  ! Achten Sie darauf, dass der Punkt vor **Aggressive Mode** gesetzt ist.

Abb. 16.3.4



- Wechseln Sie **nochmals** auf die Option **My Identity** und ändern den **ID Type** auf **E-mail Address** (siehe Abb. 16.3.5).
- Im Feld darunter tragen Sie **Client** ein.

Abb. 16.3.5



- Konfigurieren Sie die Verbindung wie in den folgenden zwei Abb. gezeigt.

Abb. 16.3.6

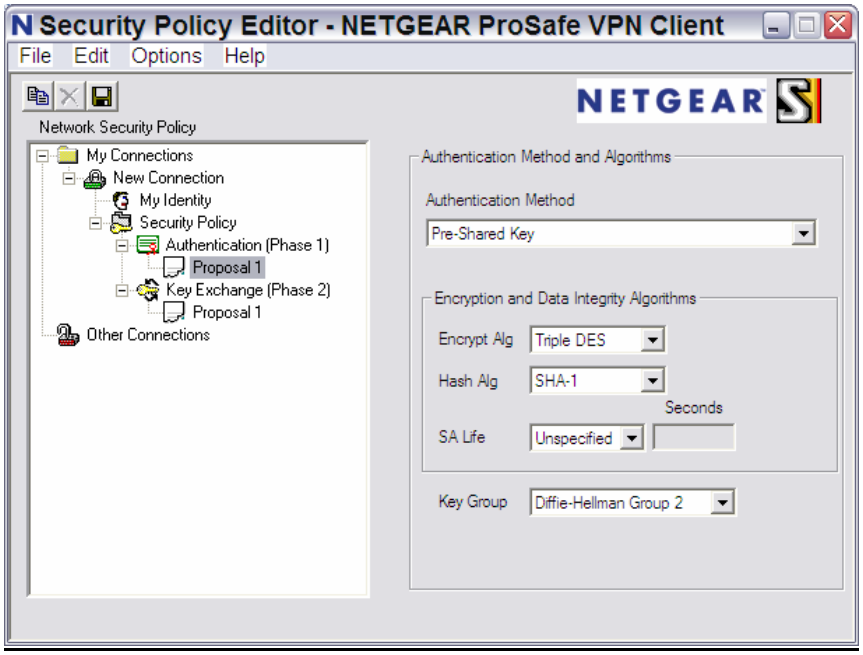
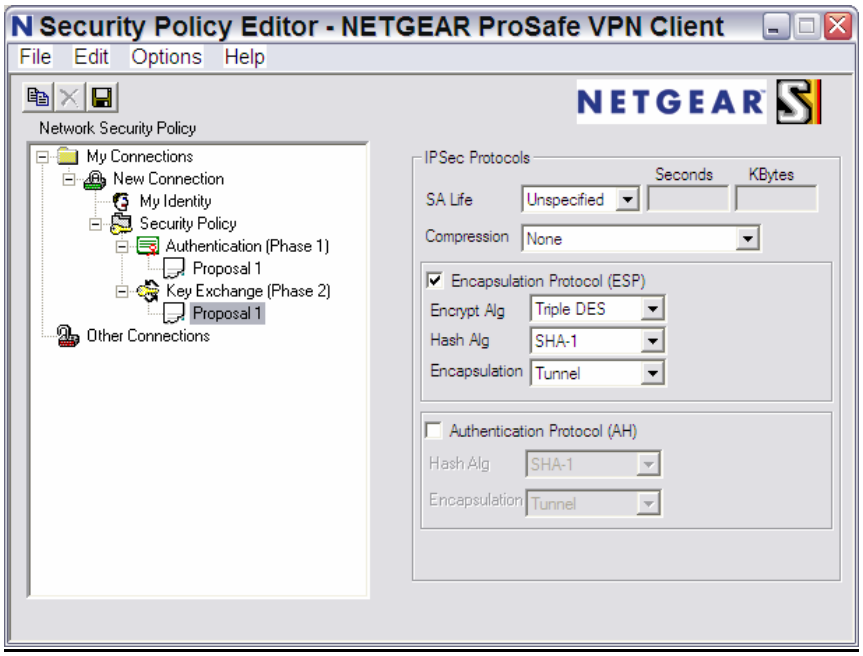


Abb. 16.3.7



- Klicken Sie links oben auf **File** -> **Save** um die erstellte Verbindung zu speichern.

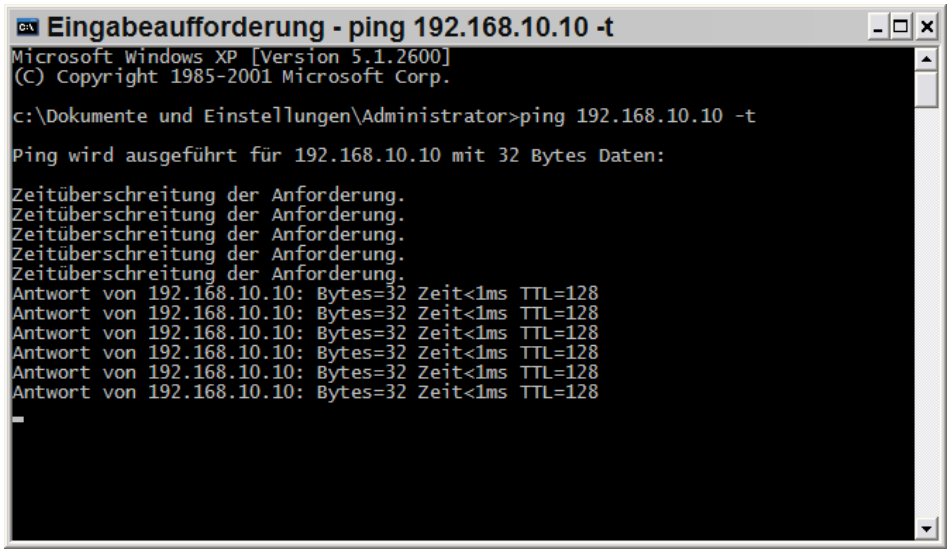
16.4. Testen der Verbindung

Um die Verbindung zu testen, versuchen Sie von dem PC mit dem VPN Client an Standort B (192.168.2.2) einen PC an Standort A (z.B. 192.168.0.2) zu erreichen:

Hinweis:	- Um den PC im Netzwerk an Standort A erreichen zu können, muss dort der lokale FVL328 als Standardgateway verwendet werden. Für dieses Beispiel gilt: Der PC an Standort A (192.168.**0**.2) verwendet als Gateway seinen lokalen Router 192.168.**0**.1.

- Klicken Sie in Windows links unten auf **Start** und **Ausführen...**
- Geben Sie **cmd** ein (Windows 95/98/ME: **command**) und klicken Sie auf **OK**
- Geben Sie folgenden Befehl ein: **ping 192.168.10.10 –t** (siehe Abb. 16.4.1)

Abb. 16.4.1



- Bei richtiger Konfiguration wird die VPN-Verbindung innerhalb einiger Sekunden aufgebaut (siehe Abb. 16.4.1).
- Der VPN Status des FVL328 (Menüpunkt **VPN Status** in der Router-Konfiguration) zeigt ebenfalls eine etablierte VPN-Verbindung (siehe Abb. 16.4.2).

Abb. 16.4.2