



**VPN Konfigurationsanleitung für folgende Modelle:**  
FVS338, FVX538, DGFV338, DG834/B/G/GB und ältere Router (vertreten durch FVS318v3)

Stand: 09/2009

Diese Anleitung beschreibt die Konfiguration einer VPN-Verbindung zwischen Routern unter Verwendung unterschiedlicher Firmwares. Zusätzlich enthält die Anleitung die Konfiguration eines ProSafe VPN-Clients in Verbindung mit verschiedenen Routern.

Diese Anleitung setzt voraus, dass die beteiligten Router direkt eine offizielle IP-Adresse besitzen und nicht hinter etwaigen vorhandenen anderen Routern laufen (z.B. FritzBox).

## **Contents:**

### **1.1 Client to FVX538/FVS338/DGFV338**

#### **1.1.1 with ModeConfig**

#### **1.1.2 without ModeConfig**

### **1.2 Client to old Routermodels (FVS318v3 as example)**

### **1.3 Client to DG834/B/G/GB**

## **2. Router to Router**

### **2.1 FVX538/FVS338/DGFV338 to FVX538/FVS338/DGFV338**

### **2.2 FVX538/FVS338/DGFV338 to older models (FVS318v3 as example)**

### **2.3 FVX538/FVS338/DGFV338 to DG834/B/G/GB**

## 1.1 Client to FVX538/FVS338/DGFV338

### 1.1.1 with ModeConfig\_(using the DGFV338 as example)

Picture 1.1.1.1:

**NETGEAR**  
PROSAFE

NETGEAR ProSafe VPN Wireless ADSL Gateway DGFV338

Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout

Policies | VPN Wizard | Certificates | Mode Config | VPN Client | Connection Status

**Add Mode Config Record**

**Client Pool** help

Record Name: ClientModeConfig

<b>First Pool:</b>	Starting IP	10	0	0	1	Ending IP	10	0	0	25
<b>Second Pool:</b>	Starting IP	0	0	0	0	Ending IP	0	0	0	0
<b>Third Pool:</b>	Starting IP	0	0	0	0	Ending IP	0	0	0	0
<b>WINS Server:</b>	Primary	0	0	0	0	Secondary	0	0	0	0
<b>DNS Server:</b>	Primary	0	0	0	0	Secondary	0	0	0	0

**Traffic Tunnel Security Level** help

PFS Key Group: DH Group 2 (1024 bit)

SA Lifetime: 28800 Seconds

Encryption Algorithm: 3DES

Integrity Algorithm: SHA-1

Local IP Address: 192.168.0.0

Local Subnet Mask: 255.255.255.0

Apply Reset

Picture 1.1.1.2:

Add New VPN Policy

Operation succeeded.

**Mode Config Record** ? help

Do you want to use Mode Config Record?  
 Yes  No

Select Mode Config Record: ClientModeConfig

**General** ? help

Policy Name: ClientModeConfig  
Direction / Type: Responder  
Exchange Mode: Aggressive

**Local** ? help

Select Local Gateway:  ADSL  Ethernet  
Identifier Type: FQDN  
Identifier: fvs\_local.com

**Remote** ? help

Identifier Type: FQDN  
Identifier: fvs\_remote.com

**IKE SA Parameters** ? help

Encryption Algorithm: 3DES  
Authentication Algorithm: SHA-1  
Authentication Method:  Pre-shared key  RSA-Signature  
Pre-shared key: 12345678 (Key Length 8-49 Char)  
Diffie-Hellman (DH) Group: Group 2 (1024 bit)  
SA-Lifetime (sec): 28800

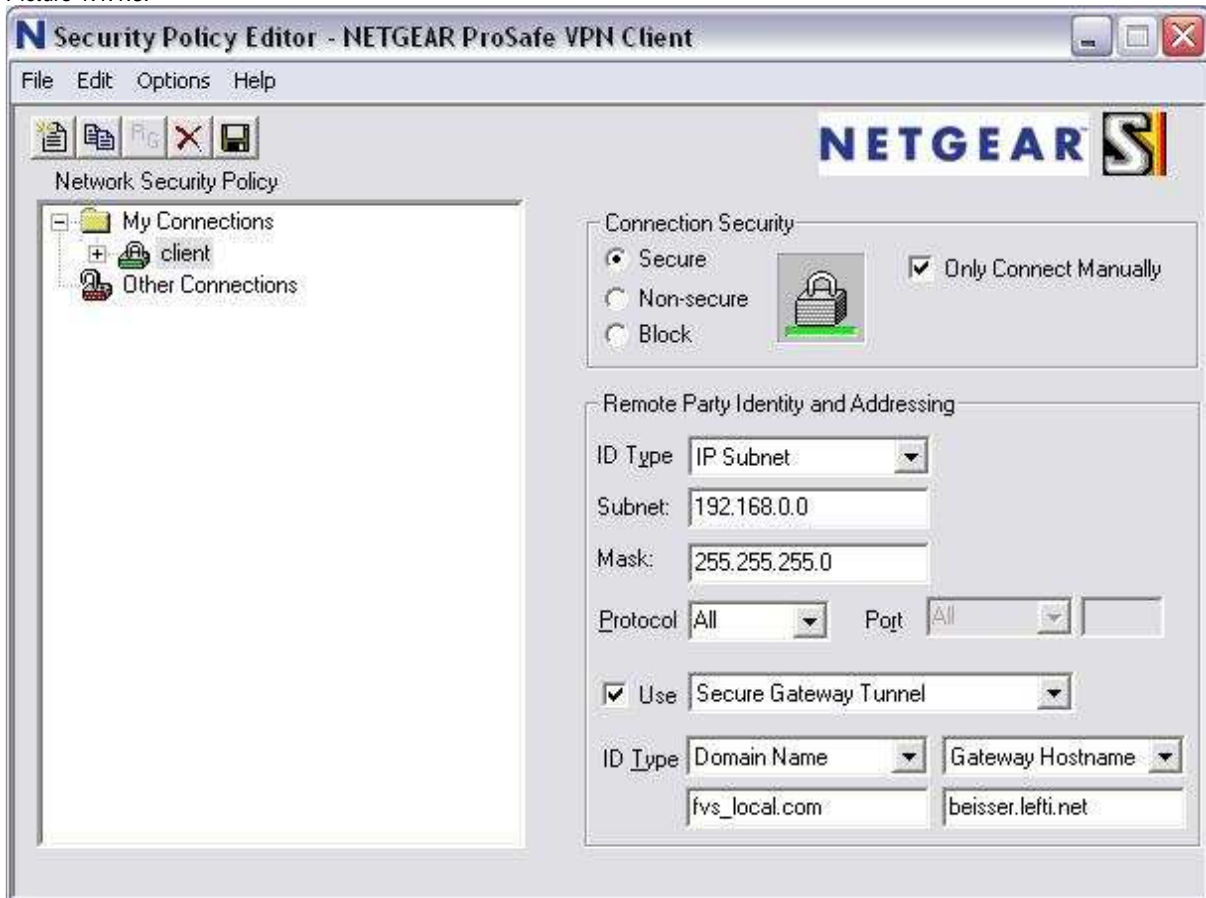
**Extended Authentication** ? help

**XAUTH Configuration**

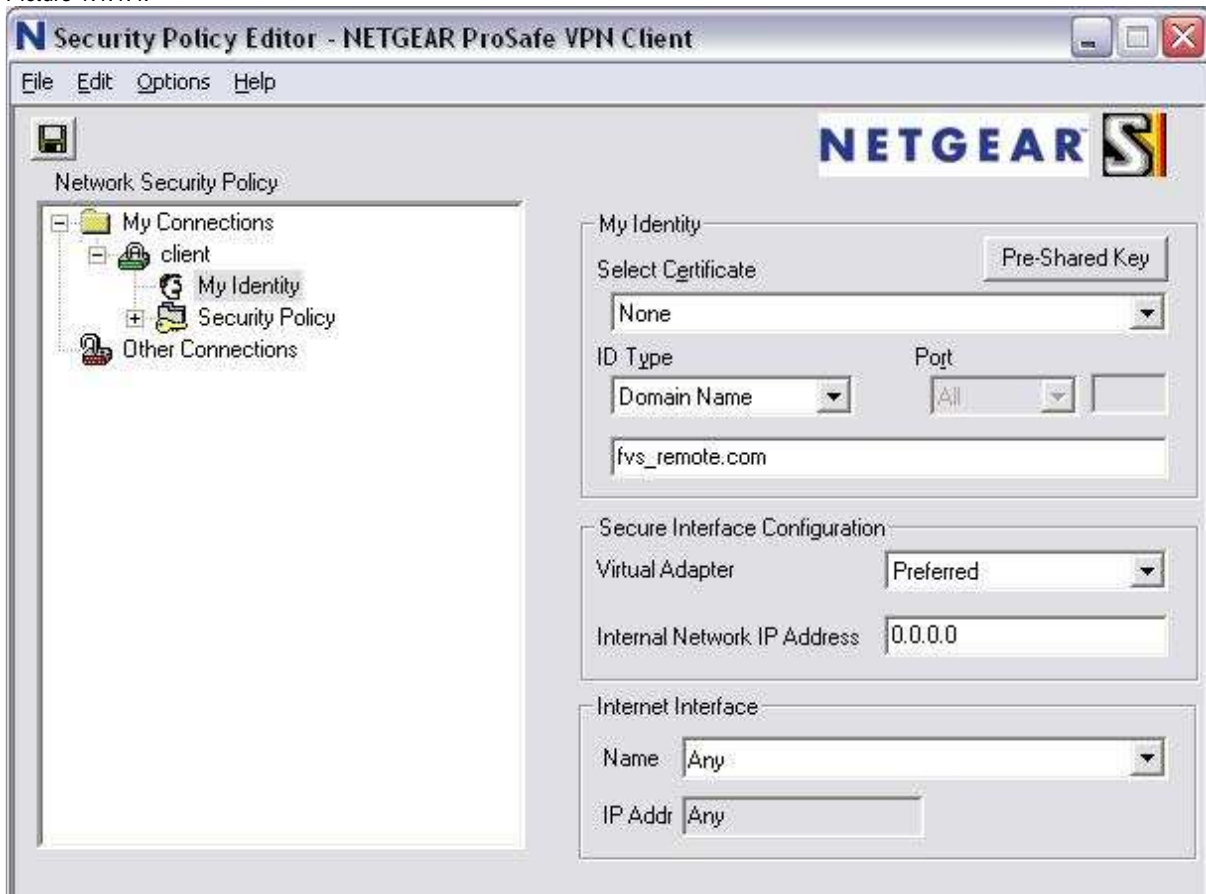
None  
 Edge Device  
 IPsec Host

Authentication Type: User Database  
Username:   
Password:

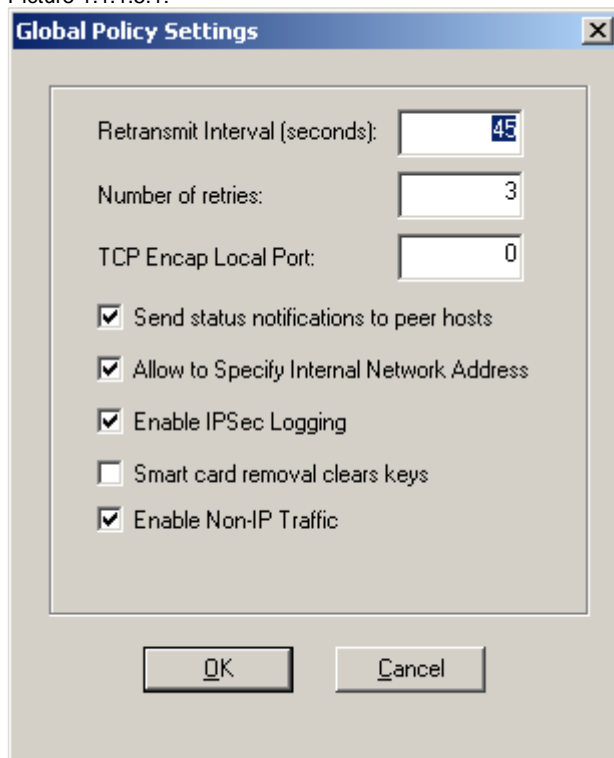
Picture 1.1.1.3:



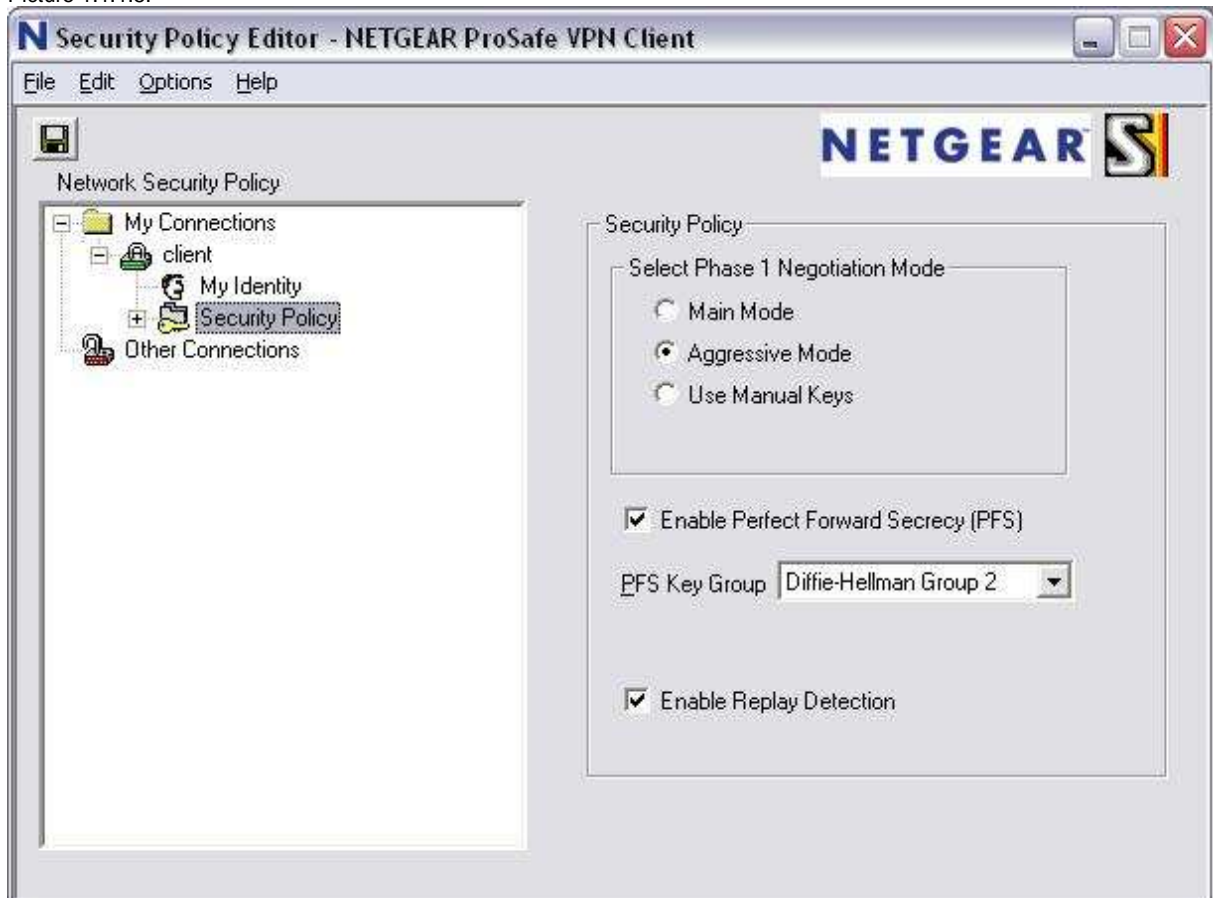
Picture 1.1.1.4:



Picture 1.1.1.5.1:



Picture 1.1.1.5:



## 1.1.2 without ModeConfig

Picture 1.1.2.1:

**Add IKE Policy** Add New VPN Policy

---

**Mode Config Record** help

**Do you want to use Mode Config Record?**

Yes  No

Select Mode Config Record:  view selected

**General** help

Policy Name:

Direction / Type:

Exchange Mode:

**Local** help

Select Local Gateway:  ADSL  Ethernet

Identifier Type:

Identifier:

**Remote** help

Identifier Type:

Identifier:

**IKE SA Parameters** help

Encryption Algorithm:

Authentication Algorithm:

Authentication Method:  Pre-shared key  RSA-Signature

Pre-shared key:  (Key Length 8 - 49 Char)

Diffie-Hellman (DH) Group:

SA-Lifetime (sec):

**Extended Authentication** help

**XAUTH Configuration**

None  Edge Device  IPSec Host

Authentication Type:

Username:

Password:

Picture 1.1.2.2:

**Add VPN Policy**

**General** help

Policy Name:

Policy Type:

Select Local Gateway:  ADSL  WAN Ethernet

Remote Endpoint:  IP Address:   
 FQDN:

Enable NetBIOS?  
 Enable RollOver?

**Traffic Selection** help

Local IP:  Remote IP:

Start IP Address:  Start IP Address:

End IP Address:  End IP Address:

Subnet Mask:  Subnet Mask:

**Manual Policy Parameters** help

SPI-Incoming:  (Max: 3-8 Chars) SPI-Outgoing:  (Max: 3-8 Chars)

Encryption Algorithm:  Integrity Algorithm:

Key-In:  Key-In:

Key-Out:  (DES-8 Char & 3DES-24 Char) Key-Out:  (MD5-16 Char & SHA-1-20 Char)

**Auto Policy Parameters** help

SA Lifetime:

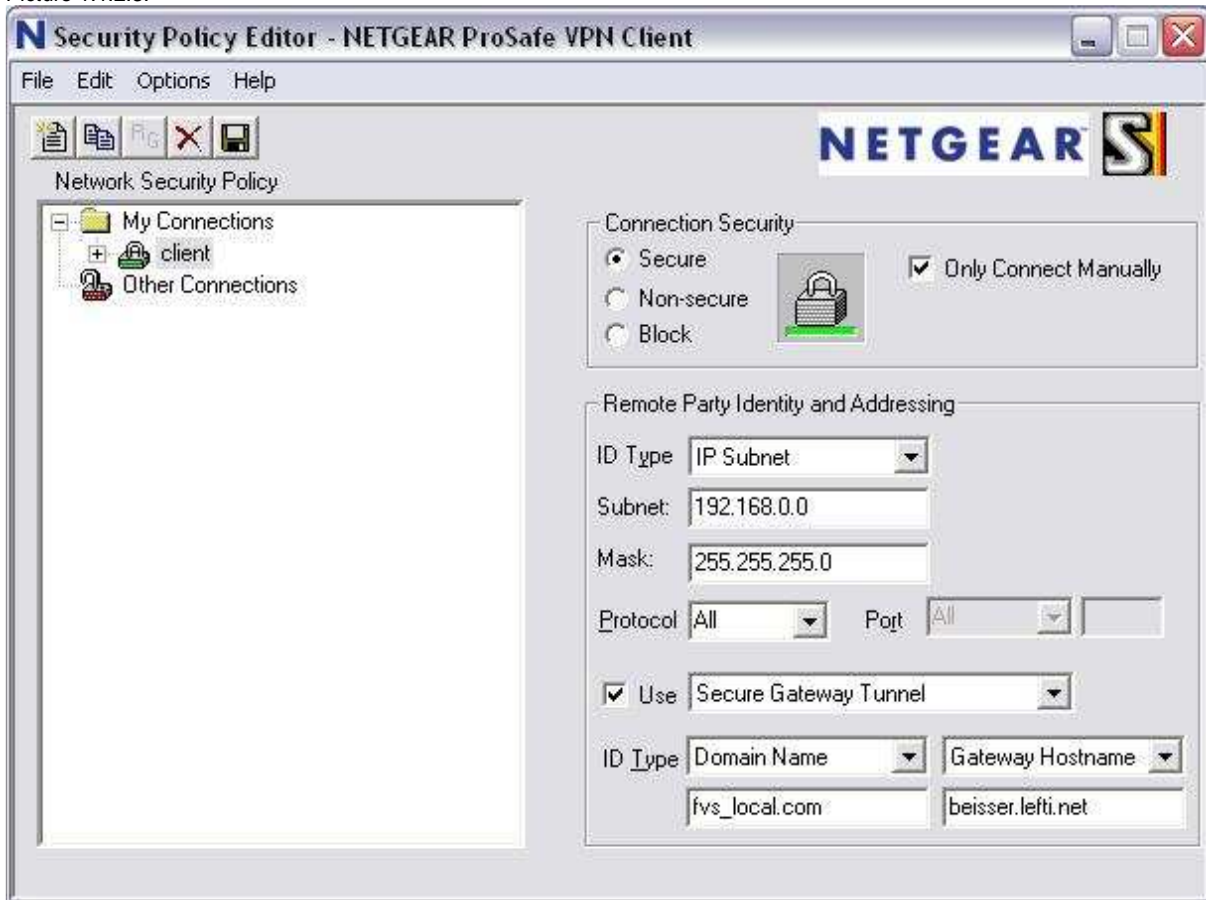
Encryption Algorithm:  Integrity Algorithm:

PFS Key Group:

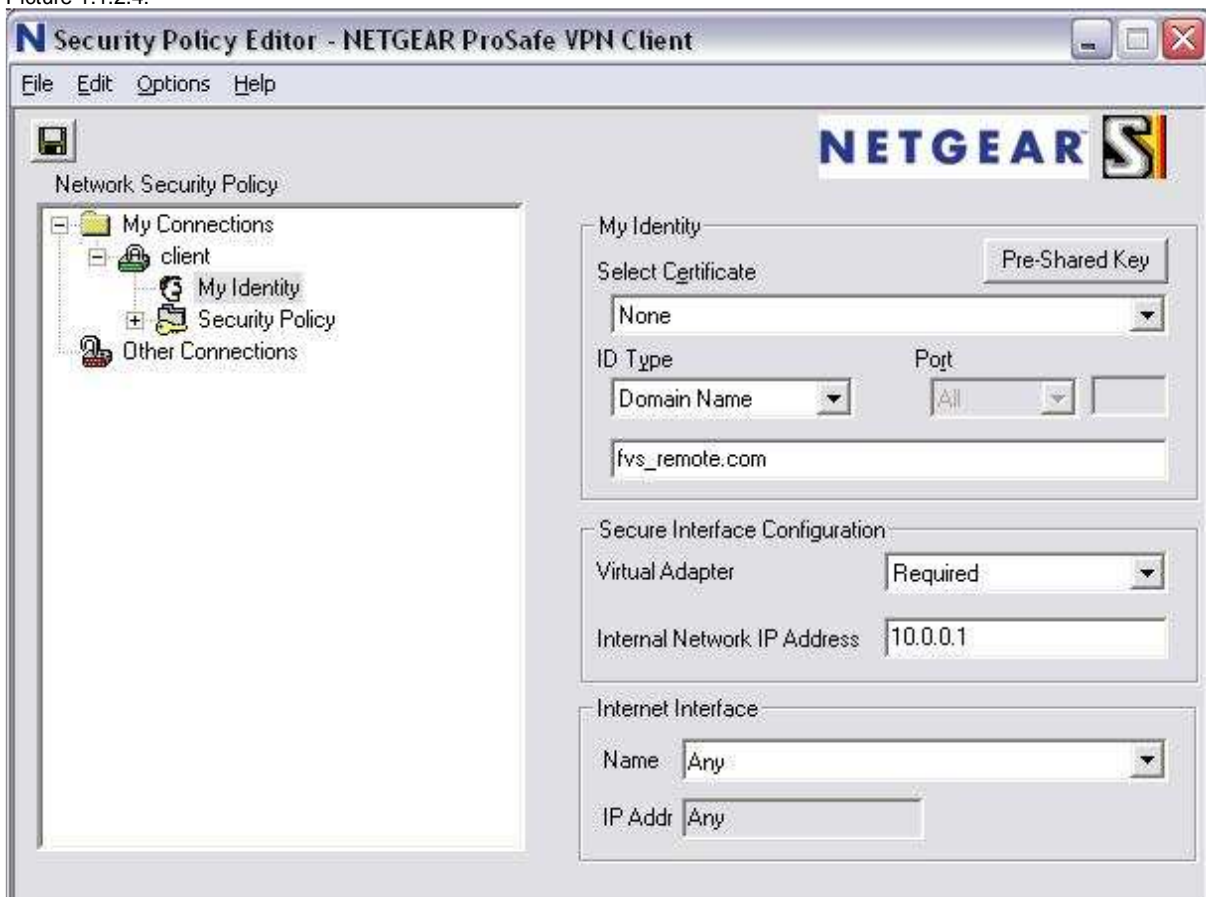
Select IKE Policy:

Netbios kann nicht aktiviert werden, da sonst keine "Single-IP" mehr angegeben werden kann.

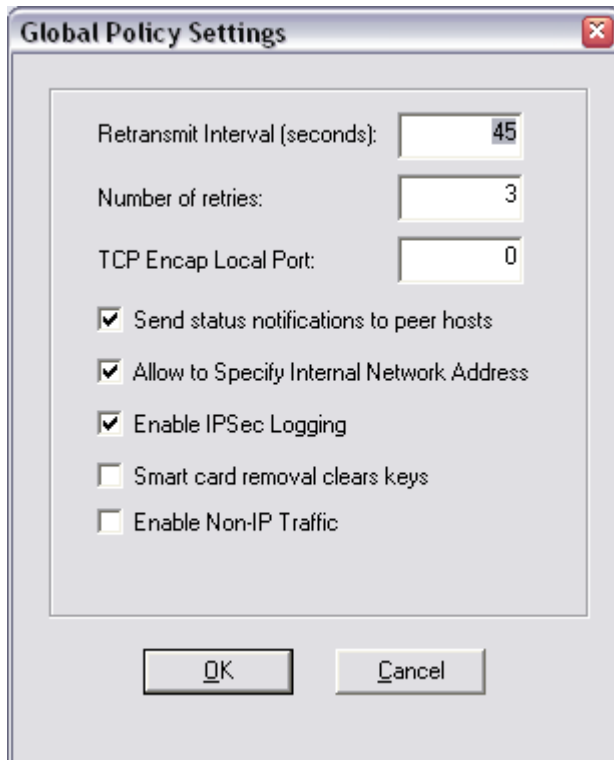
Picture 1.1.2.3:



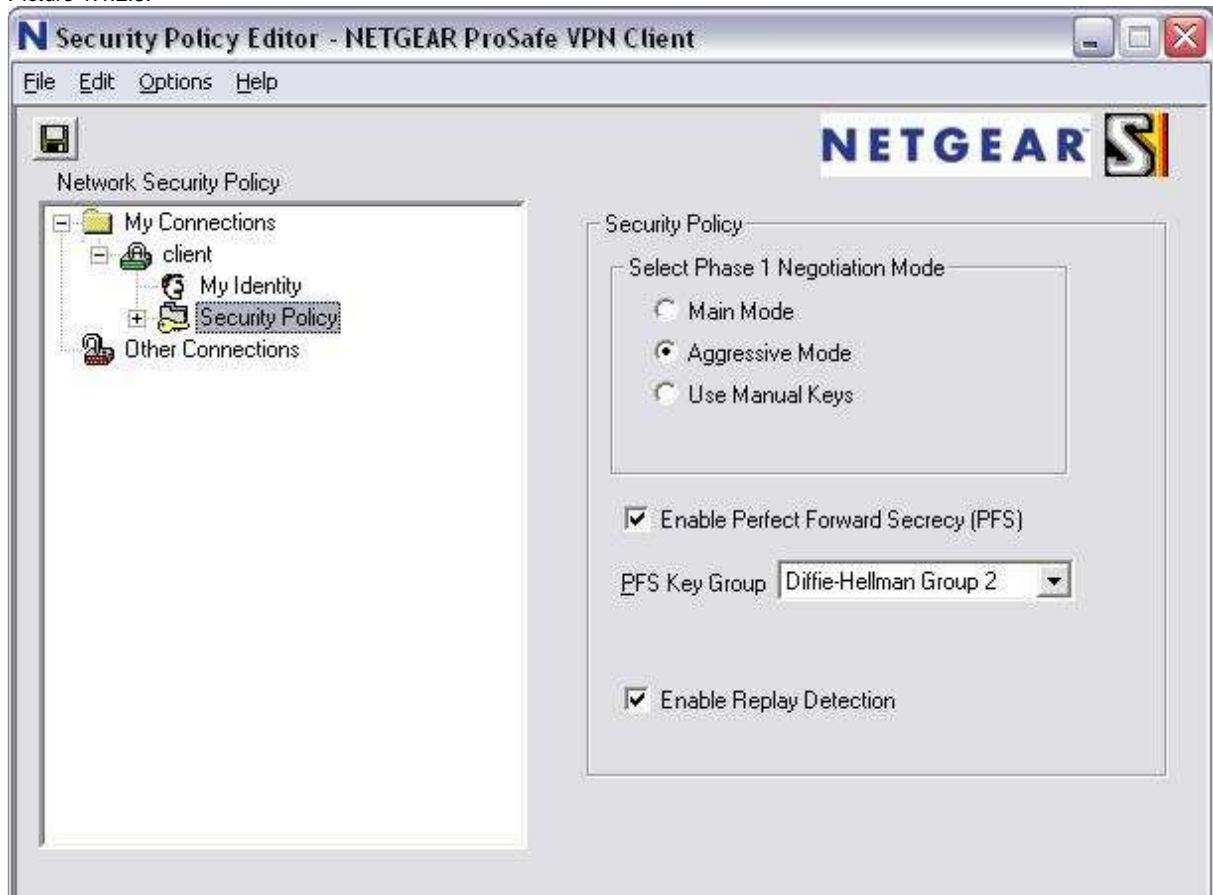
Picture 1.1.2.4:



GGf muss man unter Options -> Global Policy Settings die Option „Allow to Specify internal Network Address“ aktivieren wie im folgenden Screenshot zu sehen:



Picture 1.1.2.5:



## 1.2 Client to old Routermodels (FVS318v3 as example)

Picture 1.2.1:

### IKE Policy Configuration

#### General

Policy Name	<input type="text" value="client"/>
Direction/Type	<input type="text" value="Responder"/>
Exchange Mode	<input type="text" value="Aggressive Mode"/>

#### Local

Local Identity Type	<input type="text" value="Fully Qualified Domain Name"/>
Local Identity Data	<input type="text" value="example.dyndns.org"/>

#### Remote

Remote Identity Type	<input type="text" value="Fully Qualified User Name"/>
Remote Identity Data	<input type="text" value="client@"/>

#### IKE SA Parameters

Encryption Algorithm	<input type="text" value="3DES"/>
Authentication Algorithm	<input type="text" value="SHA-1"/>
Authentication Method	<input checked="" type="radio"/> Pre-shared Key <input type="text" value="*****"/> <input type="radio"/> RSA Signature (requires Certificate)
Diffie-Hellman (DH) Group	<input type="text" value="Group 2 (1024 Bit)"/>
SA Life Time	<input type="text" value="28800"/> (secs)

Picture 1.2.2:

## VPN - Auto Policy

### General

Policy Name:

IKE policy:

IKE Keep Alive

Remote VPN Endpoint: Address Type:   
Address Data:

Ping IP Address:  .  .  .

SA Life Time:  (Seconds)  
 (Kbytes)

IPsec PFS: PFS Key Group:

### Traffic Selector

Local IP:   
Start IP address:  .  .  .   
Finish IP address:  .  .  .   
Subnet Mask:  .  .  .

Remote IP:   
Start IP address:  .  .  .   
Finish IP address:  .  .  .   
Subnet Mask:  .  .  .

### AH Configuration

Enable Authentication: Authentication Algorithm:

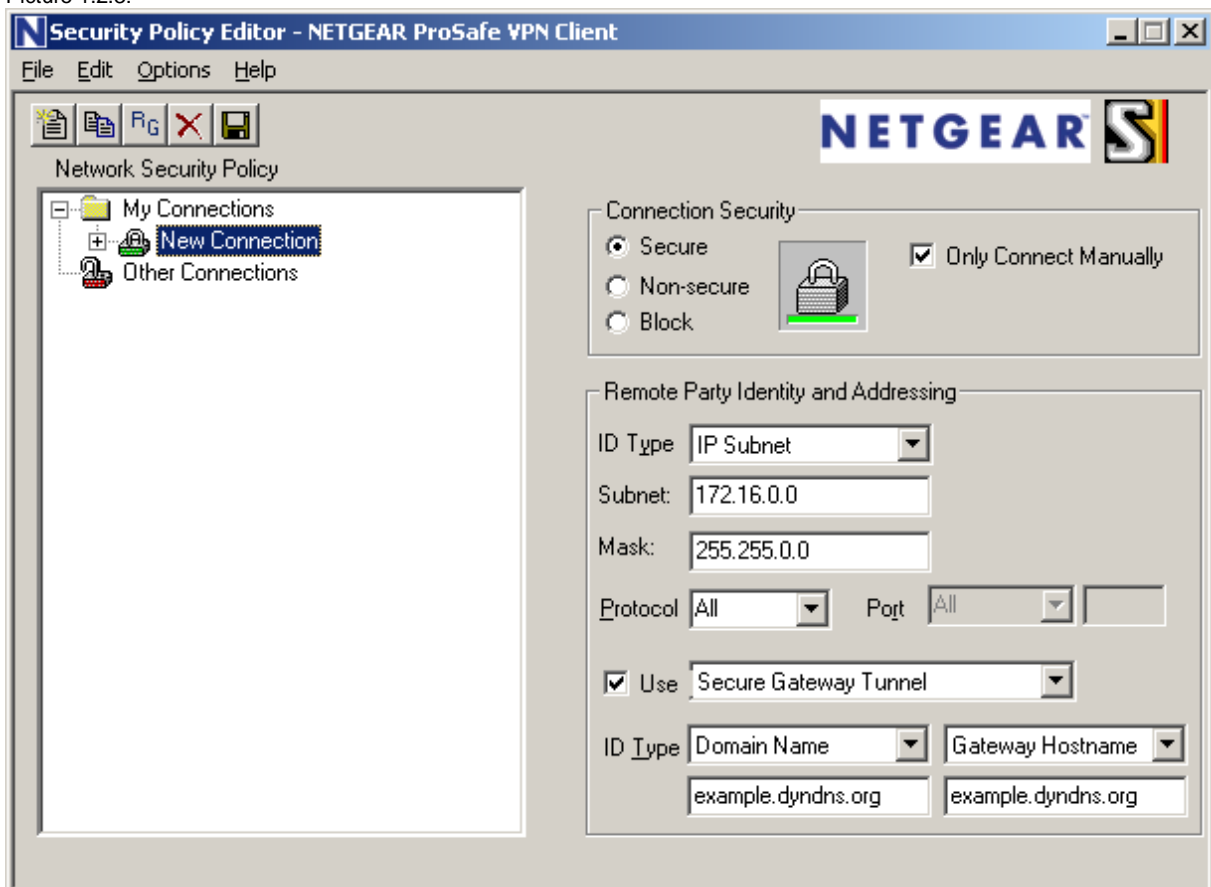
### ESP Configuration

Enable Encryption: Encryption Algorithm:

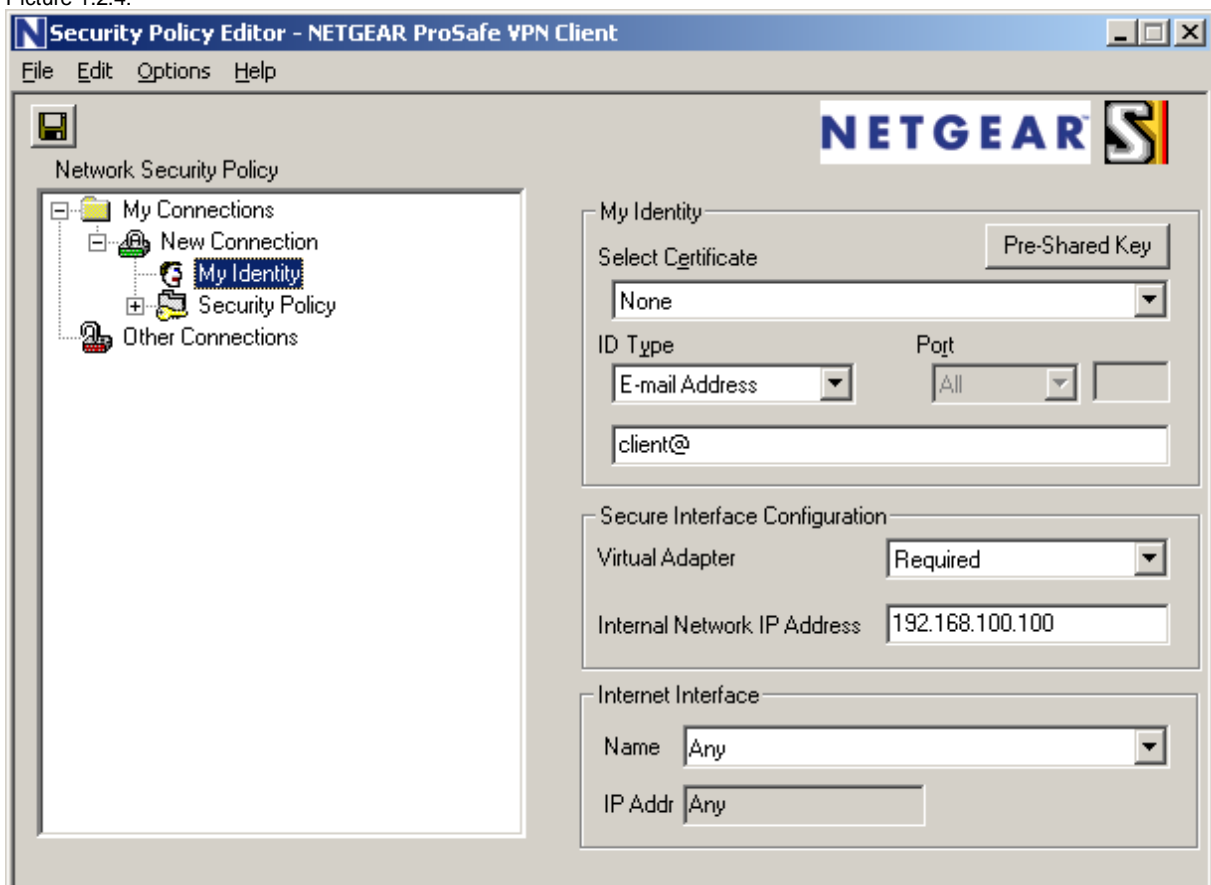
Enable Authentication: Authentication Algorithm:

NETBIOS Enable

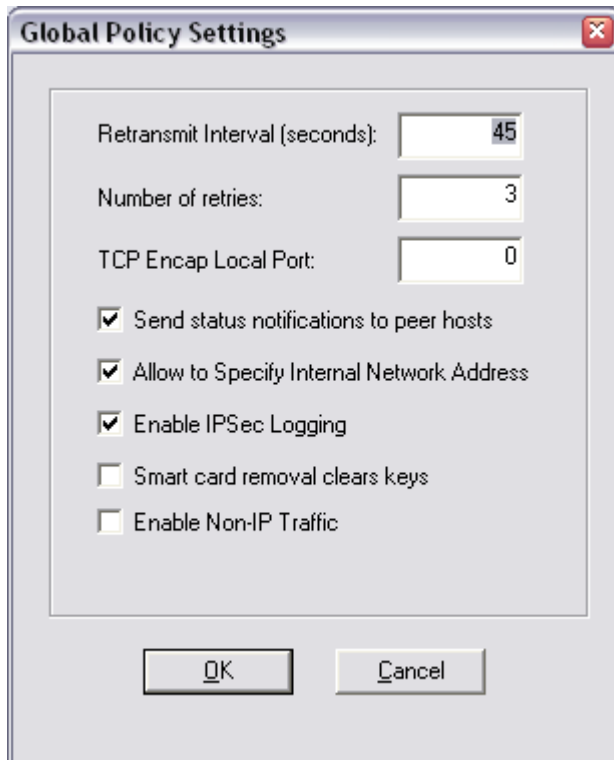
Picture 1.2.3:



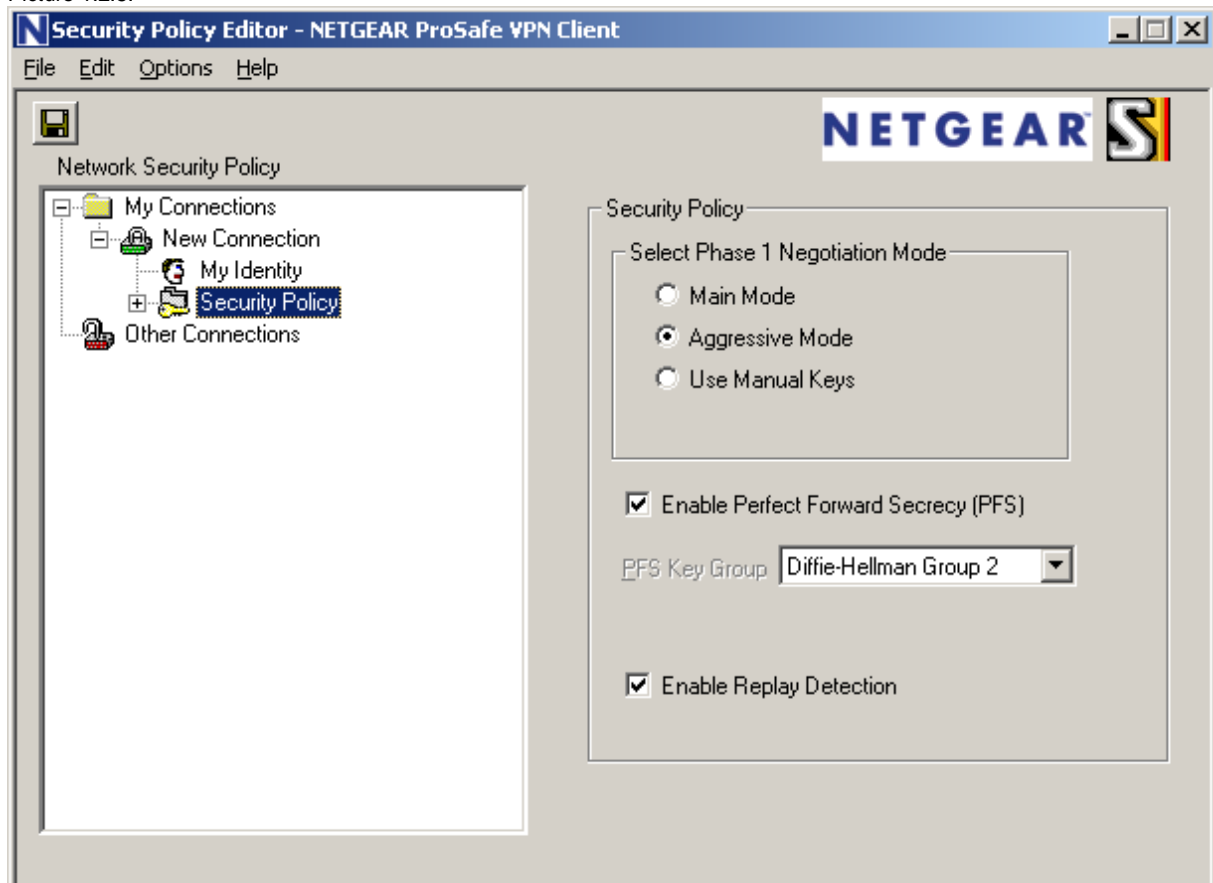
Picture 1.2.4:



GGf muss man unter Options -> Global Policy Settings die Option „Allow to Specify internal Network Address“ aktivieren wie im folgenden Screenshot zu sehen:



Picture 1.2.5:



### 1.3 Client to DG834/B/G/GB

Picture 1.3.1:  
**VPN - automatische Policy**

---

**Allgemeines**

Policy-Name:

Entfernter VPN-Endpunkt: Adresstyp:  Adresdaten:

NETBIOS aktivieren  
 IKE Keep Alive

Ping an IP-Adresse:  .  .  .

---

**Lokales LAN**

IP-Adresse:

Einzelne/Anfangsadresse:  .  .  .

Endadresse:  .  .  .

Subnetzmaske:  .  .  .

---

**Entferntes LAN**

IP-Adresse:

Einzelne/Anfangs-IP-Adresse:  .  .  .

End-IP-Adresse:  .  .  .

Subnetzmaske:  .  .  .

---

**IKE**

Richtung:

Austauschmodus:

Diffie-Hellman-Gruppe (DH):

Lokaler Identitätstyp:

Daten:

Entfernter Identitätstyp:

Daten:

---

**Parameter**

Verschlüsselungsalgorithmus:

Authentifizierungsalgorithmus:

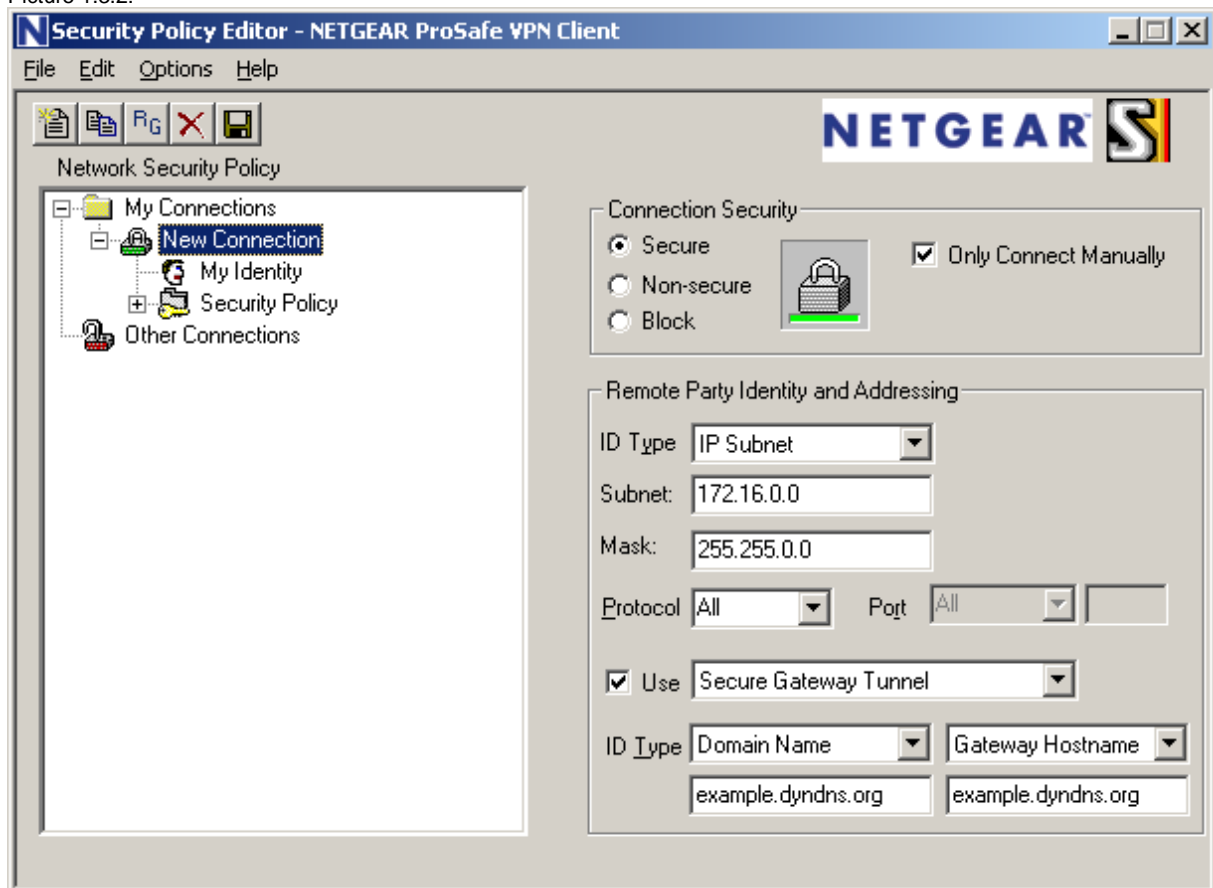
Pre-Shared Key:

SA-Lebenszeit:  (Sekunden)

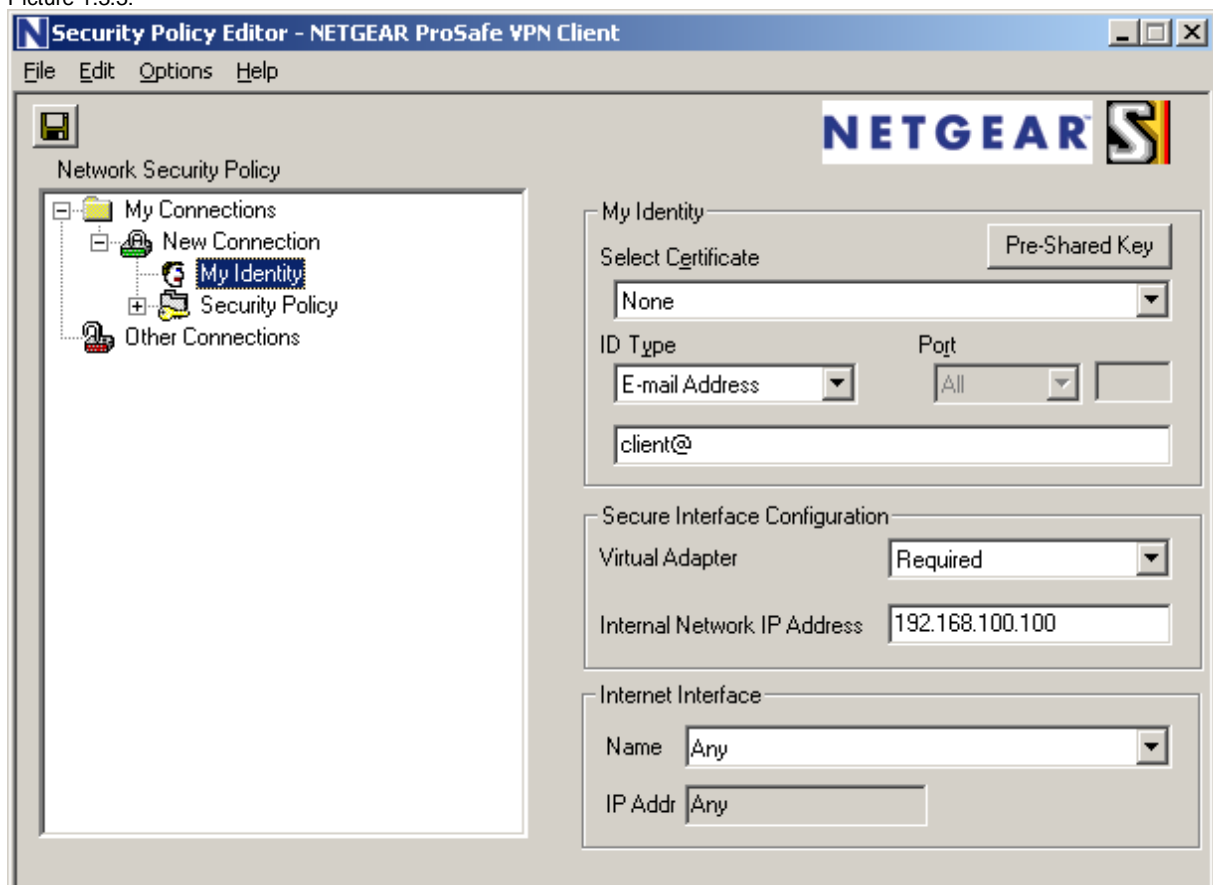
PFS (Perfect Forward Security) aktivieren

---

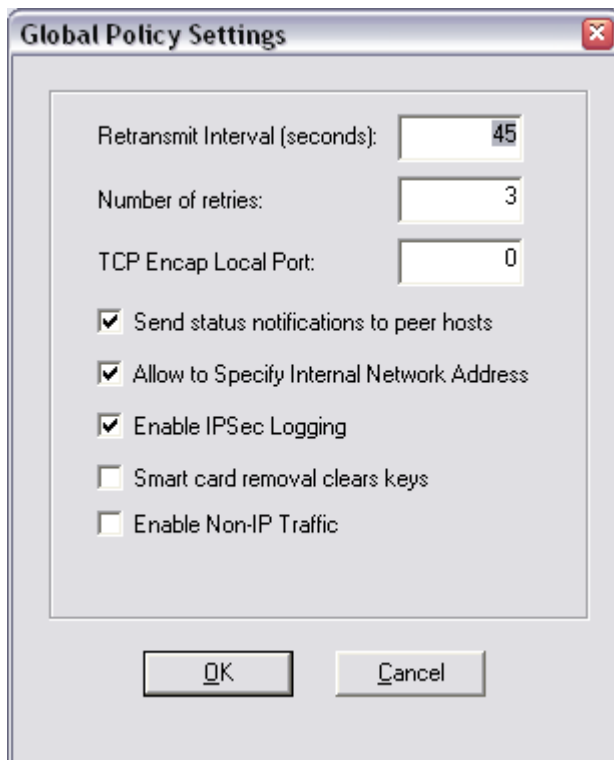
Picture 1.3.2:



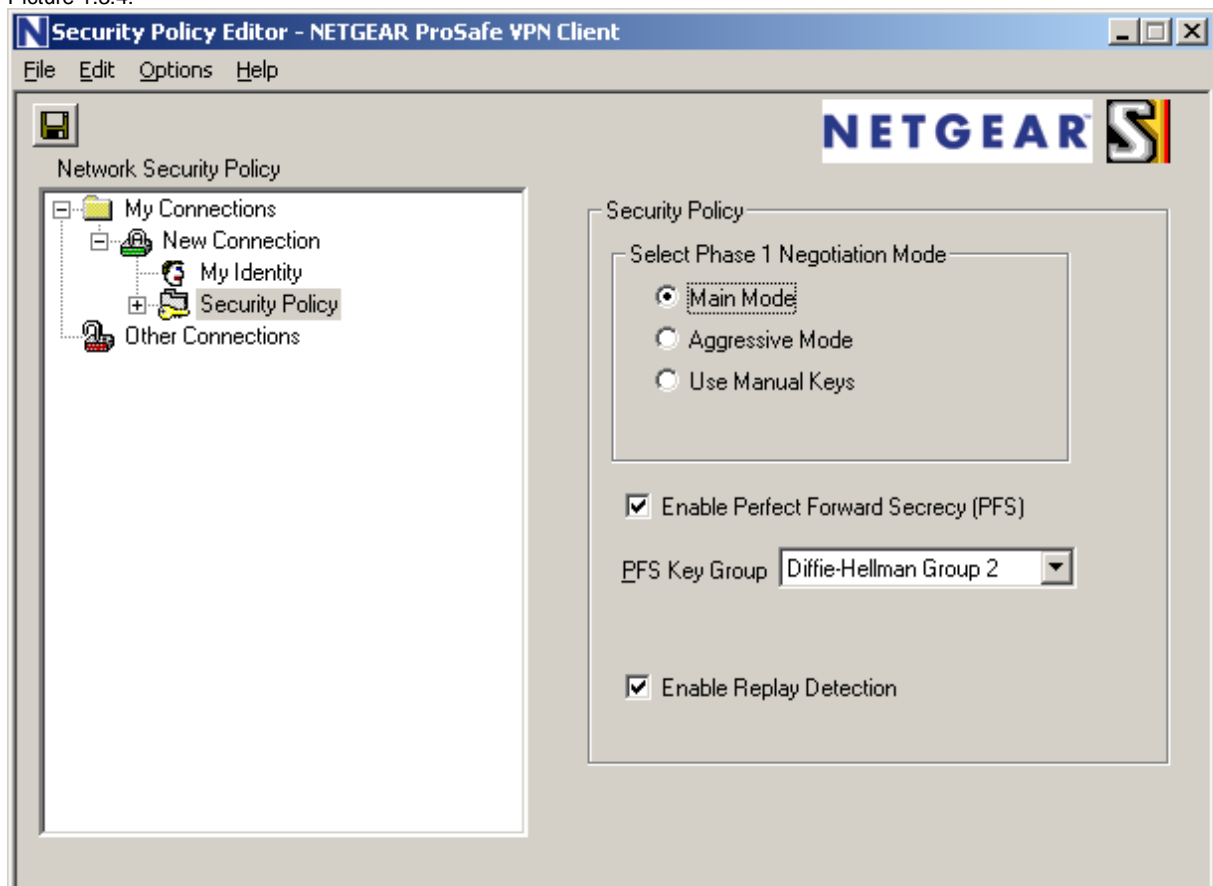
Picture 1.3.3:



GGf muss man unter Options -> Global Policy Settings die Option „Allow to Specify internal Network Address“ aktivieren wie im folgenden Screenshot zu sehen:



Picture 1.3.4:



## 2. Router to Router VPN

### 2.1 FVX538/FVS338/DGFV338 to FVX538/FVS338/DGFV338

#### 2.1.1 Side A (DGFV338)

Picture 2.1.1.1:

**Edit IKE Policy** Add New VPN Policy

Operation succeeded.

<b>Mode Config Record</b> <span>help</span> <b>Do you want to use Mode Config Record?</b> <input type="radio"/> Yes <input checked="" type="radio"/> No Select Mode Config Record: <input type="text" value=""/> <input type="button" value="view selected"/>	<b>General</b> <span>help</span> Policy Name: <input type="text" value="toDNS"/> Direction / Type: <input type="text" value="Both"/> Exchange Mode: <input type="text" value="Main"/>
<b>Local</b> <span>help</span> Select Local Gateway: <input checked="" type="radio"/> ADSL <input type="radio"/> Ethernet Identifier Type: <input type="text" value="Local Wan IP"/> Identifier: <input type="text" value="62.245.151.156"/>	<b>Remote</b> <span>help</span> Identifier Type: <input type="text" value="Remote Wan IP"/> Identifier: <input type="text" value="195.125.145.231"/>
<b>IKE SA Parameters</b> <span>help</span> Encryption Algorithm: <input type="text" value="3DES"/> Authentication Algorithm: <input type="text" value="SHA-1"/> Authentication Method: <input checked="" type="radio"/> Pre-shared key <input type="radio"/> RSA-Signature Pre-shared key: <input type="text" value="12345678"/> (Key Length: 8 - 49 Char) Diffie-Hellman (DH) Group: <input type="text" value="Group 2 (1024 bit)"/> SA-Lifetime (sec): <input type="text" value="28800"/>	
<b>Extended Authentication</b> <span>help</span> <b>XAUTH Configuration</b> <input checked="" type="radio"/> None <input type="radio"/> Edge Device <input type="radio"/> IPSec Host Authentication Type: <input type="text" value="User Database"/> Username: <input type="text"/> Password: <input type="text"/>	

Picture 2.1.1.2:

**Edit VPN Policy**

Operation succeeded.

**General** help

Policy Name:

Policy Type:

Select Local Gateway:  ADSL  WAN Ethernet

Remote Endpoint:  IP Address:   
 FQDN:

Enable NetBIOS?  
 Enable RollOver?

**Traffic Selection** help

This field is not editable, because netbios is selected.

Local IP:

Remote IP:

Start IP Address:

Start IP Address:

End IP Address:

End IP Address:

Subnet Mask:

Subnet Mask:

**Manual Policy Parameters** help

SPI-Incoming:  (Max: 3-8 Chars)

SPI-Outgoing:  (Max: 3-8 Chars)

Encryption Algorithm:

Integrity Algorithm:

Key-In:

Key-In:

Key-Out:  (DES-8 Char & 3DES-24 Char)

Key-Out:  (MD5-16 Char & SHA-1-20 Char)

**Auto Policy Parameters** help

SA Lifetime:

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group:

Select IKE Policy:

## 2.1.2 Side B (FVX538)

Picture 2.1.2.1:

Add New VPN Policy

Operation succeeded.

**Mode Config Record** ? help

**Do you want to use Mode Config Record?**

Yes
  No

Select Mode Config Record:

[view selected](#)

**General** ? help

Policy Name:

Direction / Type:

Exchange Mode:

**Local** ? help

Select Local Gateway:  WAN1  WAN2

Identifier Type:

Identifier:

**Remote** ? help

Identifier Type:

Identifier:

**IKE SA Parameters** ? help

Encryption Algorithm:

Authentication Algorithm:

Authentication Method:  Pre-shared key  RSA-Signature

Pre-shared key:  (Key Length 8 - 49 Char)

Diffie-Hellman (DH) Group:

SA-Lifetime (sec):

**Extended Authentication** ? help

**XAUTH Configuration**

None  
 Edge Device  
 IPSec Host

Authentication Type:

Username:

Password:

Apply Reset

Picture 2.1.2.2:

Operation succeeded.

General
? help

Policy Name:

Policy Type:

Select Local Gateway:  WAN1  WAN2

Remote Endpoint:  IP Address:   
 FQDN:

Enable NetBIOS?  
 Enable RollOver?

Traffic Selection
? help

This field is not editable, because netbios is selected.

Local IP:  Remote IP:

Start IP Address:  Start IP Address:

End IP Address:  End IP Address:

Subnet Mask:  Subnet Mask:

Manual Policy Parameters
? help

SPI-Incoming:  (Hex, 3-8 Chars) SPI-Outgoing:  (Hex, 3-8 Chars)

Encryption Algorithm:  Integrity Algorithm:

Key-In:  Key-In:

Key-Out:  Key-Out:

(DES-8 Char & 3DES-24 Char) (MD5-16 Char & SHA-1-32 Char)

Auto Policy Parameters
? help

SA Lifetime:

Encryption Algorithm:  Integrity Algorithm:

PFS Key Group:

Select IKE Policy:

## 2.2 FVX538/FVS338/DGFV338 to older models (FVS318v3 used here)

### 2.2.1 Side A (DGFV338)

Picture 2.2.1.1:

Operation succeeded.

**Edit IKE Policy** Add New VPN Policy

**Mode Config Record** help

Do you want to use Mode Config Record?  
 Yes  No  
Select Mode Config Record:

**General** help

Policy Name:   
Direction / Type:   
Exchange Mode:

**Local** help

Select Local Gateway:  ADSL  Ethernet  
Identifier Type:   
Identifier:

**Remote** help

Identifier Type:   
Identifier:

**IKE SA Parameters** help

Encryption Algorithm:   
Authentication Algorithm:   
Authentication Method:  Pre-shared key  RSA-Signature  
Pre-shared key:  (Key Length 8 - 63 Char)  
Diffie-Hellman (DH) Group:   
SA-Lifetime (sec):

**Extended Authentication** help

**XAUTH Configuration**

None  
 Edge Device  
 IPSec Host

Authentication Type:   
Username:   
Password:

Picture 2.2.1.2:

**Edit VPN Policy**

Operation succeeded.

**General** help

Policy Name:

Policy Type:

Select Local Gateway:  ADSL  WAN Ethernet

Remote Endpoint:  IP Address:   
 FQDN:

Enable NetBIOS?  
 Enable RollOver?

**Traffic Selection** help

This field is not editable, because netbios is selected.

Local IP:  Remote IP:

Start IP Address:  Start IP Address:

End IP Address:  End IP Address:

Subnet Mask:  Subnet Mask:

**Manual Policy Parameters** help

SPI-Incoming:  (Max: 3-8 Chars) SPI-Outgoing:  (Max: 3-8 Chars)

Encryption Algorithm:  Integrity Algorithm:

Key-In:  Key-In:

Key-Out:  (DES-8 Char & 3DES-24 Char) Key-Out:  (AES-16 Char & SHA-1-20 Char)

**Auto Policy Parameters** help

SA Lifetime:

Encryption Algorithm:  Integrity Algorithm:

PFS Key Group:

Select IKE Policy:

## 2.2.2 Side B (FVS318v3)

Picture 2.2.2.1:

### IKE Policy Configuration

#### General

Policy Name	<input type="text" value="toALI"/>
Direction/Type	<input type="text" value="Both Directions"/>
Exchange Mode	<input type="text" value="Main Mode"/>

#### Local

Local Identity Type	<input type="text" value="WAN IP Address"/>
Local Identity Data	<input type="text" value="195.125.145.232"/>

#### Remote

Remote Identity Type	<input type="text" value="Remote WAN IP"/>
Remote Identity Data	<input type="text" value="0.0.0.0"/>

#### IKE SA Parameters

Encryption Algorithm	<input type="text" value="3DES"/>
Authentication Algorithm	<input type="text" value="SHA-1"/>
Authentication Method	<input checked="" type="radio"/> Pre-shared Key <input type="text" value="*****"/> <input type="radio"/> RSA Signature (requires Certificate)
Diffie-Hellman (DH) Group	<input type="text" value="Group 2 (1024 Bit)"/>
SA Life Time	<input type="text" value="28800"/> (secs)

Picture 2.2.2.2:

## VPN - Auto Policy

### General

Policy Name	<input type="text" value="toALI"/>
IKE policy	<input type="text" value="toALI"/>
<input type="checkbox"/> IKE Keep Alive	Ping IP Address: <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Remote VPN Endpoint	Address Type: <input type="text" value="Fully Qualified Domain Name"/>
	Address Data: <input type="text" value="beisser.lefti.net"/>
SA Life Time	<input type="text" value="28800"/> (Seconds)
	<input type="text" value="100000"/> (Kbytes)
<input checked="" type="checkbox"/> IPSec PFS	PFS Key Group: <input type="text" value="Group 2 (1024 Bit)"/>

### Traffic Selector

Local IP	<input type="text" value="Subnet address"/>
	Start IP address: <input type="text" value="172"/> . <input type="text" value="16"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
	Finish IP address: <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
	Subnet Mask: <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Remote IP	<input type="text" value="Subnet address"/>
	Start IP address: <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
	Finish IP address: <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
	Subnet Mask: <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>

### AH Configuration

<input type="checkbox"/> Enable Authentication	Authentication Algorithm: <input type="text" value="SHA-1"/>
--	--

### ESP Configuration

<input checked="" type="checkbox"/> Enable Encryption	Encryption Algorithm: <input type="text" value="3DES"/>
<input checked="" type="checkbox"/> Enable Authentication	Authentication Algorithm: <input type="text" value="SHA-1"/>

<input checked="" type="checkbox"/> NETBIOS Enable
--

## 2.3 FVX538/FVS338/DGFV338 to DG834/B/G/GB

### 2.3.1 Side A (DGFV338)

Picture 2.3.1.1:

Operation succeeded.

Edit IKE Policy
Add New VPN Policy

<p><b>Mode Config Record</b> <span style="float: right;">? help</span></p> <p><b>Do you want to use Mode Config Record?</b></p> <p><input type="radio"/> Yes <input checked="" type="radio"/> No</p> <p>Select Mode Config Record: <input type="text" value=""/></p> <p style="text-align: right;"><input type="button" value="view selected"/></p>	<p><b>General</b> <span style="float: right;">? help</span></p> <p>Policy Name: <input type="text" value="toDNS"/></p> <p>Direction / Type: <input type="text" value="Both"/></p> <p>Exchange Mode: <input type="text" value="Main"/></p>
<p><b>Local</b> <span style="float: right;">? help</span></p> <p>Select Local Gateway: <input checked="" type="radio"/> ADSL <input type="radio"/> Ethernet</p> <p>Identifier Type: <input type="text" value="Local Wan IP"/></p> <p>Identifier: <input type="text" value="62.245.151.156"/></p>	<p><b>Remote</b> <span style="float: right;">? help</span></p> <p>Identifier Type: <input type="text" value="Remote Wan IP"/></p> <p>Identifier: <input type="text" value="195.125.145.231"/></p>
<p><b>IKE SA Parameters</b> <span style="float: right;">? help</span></p> <p>Encryption Algorithm: <input type="text" value="3DES"/></p> <p>Authentication Algorithm: <input type="text" value="SHA-1"/></p> <p>Authentication Method: <input checked="" type="radio"/> Pre-shared key <input type="radio"/> RSA-Signature</p> <p>Pre-shared key: <input type="text" value="12345678"/> <small>(Key Length 8 - 49 Char)</small></p> <p>Diffie-Hellman (DH) Group: <input type="text" value="Group 2 (1024 bit)"/></p> <p>SA-Lifetime (sec): <input type="text" value="28800"/></p>	
<p><b>Extended Authentication</b> <span style="float: right;">? help</span></p> <p><b>XAUTH Configuration</b></p> <p><input checked="" type="radio"/> None  <input type="radio"/> Edge Device  <input type="radio"/> IPSec Host</p> <p>Authentication Type: <input type="text" value="User Database"/></p> <p>Username: <input type="text" value=""/></p> <p>Password: <input type="text" value=""/></p>	

Picture 2.3.1.2:

**Edit VPN Policy**

Operation succeeded.

**General** help

Policy Name:

Policy Type:

Select Local Gateway:  ADSL  WAN Ethernet

Remote Endpoint:  IP Address:   
 FQDN:

Enable NetBIOS?  
 Enable RollOver?

**Traffic Selection** help

This field is not editable, because netbios is selected.

Local IP:

Remote IP:

Start IP Address:

Start IP Address:

End IP Address:

End IP Address:

Subnet Mask:

Subnet Mask:

**Manual Policy Parameters** help

SPI-Incoming:  (Max: 3-8 Chars)

SPI-Outgoing:  (Max: 3-8 Chars)

Encryption Algorithm:

Integrity Algorithm:

Key-In:

Key-In:

Key-Out:  (DES-8 Char & 3DES-24 Char)

Key-Out:  (MD5-16 Char & SHA-1-20 Char)

**Auto Policy Parameters** help

SA Lifetime:

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group:

Select IKE Policy:

## 2.3.2 Side B (DG834Bv1)

Picture 2.3.2.1:

### VPN - Auto Policy

General	
Policy Name	toALI
Remote VPN Endpoint	Address Type: Fully Qualified Domain Name Address Data: beisser.lefti.net
<input checked="" type="checkbox"/> NetBIOS Enable	
<input type="checkbox"/> IKE Keep Alive	Ping IP Address: . . . .
Local LAN	
IP Address	Subnet address: . . . .
	Single/Start address: 172 . 16 . 0 . 0
	Finish address: . . . .
	Subnet Mask: 255 . 255 . 0 . 0
Remote LAN	
IP Address	Subnet address: . . . .
	Single/Start IP address: 192 . 168 . 0 . 0
	Finish IP address: . . . .
	Subnet Mask: 255 . 255 . 255 . 0
IKE	
Direction	Initiator and Responder
Exchange Mode	Main Mode
Diffie-Hellman (DH) Group	Group 2 (1024 Bit)
Local Identity Type	WAN IP Address
Data	n/a
Remote Identity Type	IP Address
Data	n/a
Parameters	
Encryption Algorithm	3DES
Authentication Algorithm	SHA-1
Pre-shared Key	12345678
SA Life Time	28800 (Seconds)
<input checked="" type="checkbox"/> Enable PFS (Perfect Forward Security)	