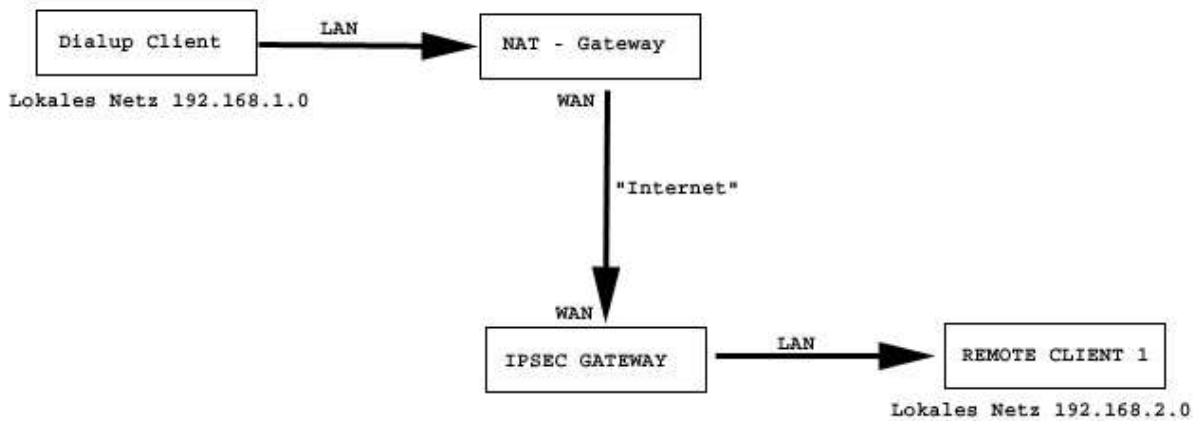
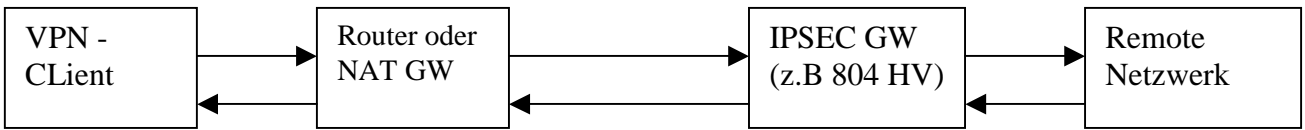


D-Link VPN-IPSEC Test Aufbau



Konfigurationsbeispiel für einen 804-HV:

Konfiguration der IPSEC Einstellungen für das Gateway:

D-Link
Building Networks for People

DI-804HV
Broadband VPN Router

Home | Advanced | Tools | Status | Help

VPN Settings

Item	Setting
VPN	<input checked="" type="checkbox"/> Enable ← 2
NetBIOS broadcast	<input checked="" type="checkbox"/> Enable
Max. number of tunnels	6 ← 3

ID	Tunnel Name	Method
1		IKE [More]
2		IKE [More]
3		IKE [More]
4		IKE [More]
5		IKE [More]

Previous page | Next page

Dynamic VPN Settings... | L2TP Server Setting... | PPTP Server Setting... | View VPN Status...

4 →

- Wählen Sie unter „Home“ VPN aus (Punkt 1)
- Aktivieren Sie das VPN Feature (Punkt 2)
- Wählen Sie die Anzahl der gleichzeitigen VPN Tunnel – z. B „10“ (Punkt 3)
- Bestätigen Sie die Änderungen mit dem Apply Button

Konfiguration eines Dialup-Tunnels:

D-Link
Building Networks for People

DI-804HV
Broadband VPN Router

Home Advanced Tools Status Help

VPN Settings

Item	Setting
VPN	<input checked="" type="checkbox"/> Enable
NetBIOS broadcast	<input checked="" type="checkbox"/> Enable
Max. number of tunnels	6

ID	Tunnel Name	Method
1		IKE More
2		IKE More
3		IKE More
4		IKE More
5		IKE More

Previous page Next page

Dynamic VPN Settings... L2TP Server Setting... PPTP Server Setting... View VPN Status...

Apply Cancel Help

- Klicken Sie auf „Dynamic VPN Settings“

D-Link
Building Networks for People

DI-804HV
Broadband VPN Router

Home Advanced Tools Status Help

VPN Settings - Dynamic VPN Tunnel

Item	Setting
Tunnel Name	dialup
Dynamic VPN	<input checked="" type="checkbox"/> Enable
Local Subnet	192.168.1.0
Local Netmask	255.255.255.0
Preshare Key	*****
IKE Proposal index	Select IKE Proposal...
IPSec Proposal index	Select IPSec Proposal...

Back Apply Cancel Help

- Geben Sie dem Tunnel einen beliebigen Namen (Punkt 1)
Der Name wird verwendet um mehrere Tunnel zu unterscheiden
- Aktivieren Sie die Dialup-Tunnel (Punkt 2)
- Tragen Sie Ihr lokales Subnetz ein. Sofern wir der Zeichnung folgen wollen sollte hier „192.168.2.0“ eingetragen werden. Diese Information ist für das Gateway wichtig, da es später zwischen dem lokalen und Remote-Netzwerk vermitteln muss.



Bei D-Link IPSec Gateways wird zwischen diesen beiden Netzen immer unter Verwendung von NAT vermittelt. Sofern Sie also später einen Clienten verwenden, der die Zuweisung von virtuellen Ips ermöglicht, sollten Sie diese Eigenschaft unbedingt bedenken.

- Als nächsten tragen Sie eine Class C (255.255.255.0) Netzmaske ein (Punkt 4)
- Definieren Sie einen gemeinsamen Schlüssel, der später bei der Konfiguration der Clients bekannt sein muss. (Punkt 5)
- Bestätigen Sie diese Eingaben mit dem Apply Button (Schritt 6)

IKE Proposal Definition:

Das Bild zeigt die Web-Oberfläche eines D-Link DI-804HV Broadband VPN Routers. Die Seite ist in 'VPN Settings - Dynamic VPN Tunnel' unterteilt. Links befindet sich eine Navigationsleiste mit den Optionen Wizard, WAN, LAN, DHCP und VPN. Die Hauptoberfläche zeigt die Konfigurationsoptionen für den Tunnel:

Item	Setting
Tunnel Name	dialup
Dynamic VPN	<input checked="" type="checkbox"/> Enable
Local Subnet	192.168.1.0
Local Netmask	255.255.255.0
Preshare Key	*****
IKE Proposal index	Select IKE Proposal...
IPSec Proposal index	Select IPSec Proposal...

Ein schwarzer Pfeil weist auf den 'Select IKE Proposal...' Button hin. Unten rechts sind die Navigationsbuttons Back, Apply, Cancel und Help zu sehen.

D-Link
Building Networks for People

DI-804HV
Broadband VPN Router

Home **Advanced** **Tools** **Status** **Help**

VPN Settings - Dynamic VPN Tunnel - Set IKE Proposal

IKE Proposal index:

ID	Proposal Name	DH Group	Encrypt algorithm	Auth algorithm	Life time	Life Time Unit
1	<input type="text" value="1"/>	<input type="text" value="Group 2"/>	<input type="text" value="DES"/>	<input type="text" value="MD5"/>	<input type="text" value="28800"/>	<input type="text" value="Sec."/>
2	<input type="text"/>	<input type="text" value="Group 1"/>	<input type="text" value="3DES"/>	<input type="text" value="SHA1"/>	<input type="text" value="0"/>	<input type="text" value="Sec."/>
3	<input type="text"/>	<input type="text" value="Group 1"/>	<input type="text" value="3DES"/>	<input type="text" value="SHA1"/>	<input type="text" value="0"/>	<input type="text" value="Sec."/>
4	<input type="text"/>	<input type="text" value="Group 1"/>	<input type="text" value="3DES"/>	<input type="text" value="SHA1"/>	<input type="text" value="0"/>	<input type="text" value="Sec."/>
5	<input type="text"/>	<input type="text" value="Group 1"/>	<input type="text" value="3DES"/>	<input type="text" value="SHA1"/>	<input type="text" value="0"/>	<input type="text" value="Sec."/>
6	<input type="text"/>	<input type="text" value="Group 1"/>	<input type="text" value="3DES"/>	<input type="text" value="SHA1"/>	<input type="text" value="0"/>	<input type="text" value="Sec."/>
7	<input type="text"/>	<input type="text" value="Group 1"/>	<input type="text" value="3DES"/>	<input type="text" value="SHA1"/>	<input type="text" value="0"/>	<input type="text" value="Sec."/>
8	<input type="text"/>	<input type="text" value="Group 1"/>	<input type="text" value="3DES"/>	<input type="text" value="SHA1"/>	<input type="text" value="0"/>	<input type="text" value="Sec."/>
9	<input type="text"/>	<input type="text" value="Group 1"/>	<input type="text" value="3DES"/>	<input type="text" value="SHA1"/>	<input type="text" value="0"/>	<input type="text" value="Sec."/>
10	<input type="text"/>	<input type="text" value="Group 1"/>	<input type="text" value="3DES"/>	<input type="text" value="SHA1"/>	<input type="text" value="0"/>	<input type="text" value="Sec."/>

Proposal ID: Proposal index

Erklärungen:

Auf dieser Seite sehen Sie 10 Zeilen mit Konfigurationsparametern. Jede einzelne Zeile ermöglicht eine Verbindung, wenn der Client die gleichen Parameter verwendet. Mehrere Zeilen müssen Sie also nur dann verwenden, wenn Sie den Clients zum Beispiel unterschiedliche Verschlüsselungen anbieten möchten. Tragen Sie bitte auf Ihrer Seite die oben dargestellten Werte ein. Ich empfehle aber die Verwendung von 3DES oder AES sofern Ihr Client diese Verfahren unterstützt. Die oben gezeigte Konfiguration ist so gewählt, dass diese in Kombination mit fast jedem Client funktioniert, aber kein Sicherheitsoptimum darstellt. Eine sichere Empfehlung wäre Group 5, 3DES oder AES zur Verschlüsselung und SHA1 als Authentifizierungs-Algorithmus.

Nachdem Sie Einstellungen angepasst haben, wählen Sie unten die Proposal ID 1 aus der Drop-Down Liste aus und klicken auf „Add to“.

Jetzt sollte eine „1“ im IKE Proposal Index erscheinen.

Bestätigen Sie alle Eingaben mit „apply“.

IPSEC Proposal Definition:

D-Link
Building Networks for People

DI-804HV
Broadband VPN Router

Home Advanced Tools Status Help

VPN Settings - Dynamic VPN Tunnel

Item	Setting
Tunnel Name	dialup
Dynamic VPN	<input checked="" type="checkbox"/> Enable
Local Subnet	192.168.1.0
Local Netmask	255.255.255.0
Preshare Key	*****
IKE Proposal index	Select IKE Proposal...
IPSec Proposal index	Select IPSec Proposal...

Back Apply Cancel Help

Klicken Sie auf den Button "Select IPSec Proposal"

D-Link
Building Networks for People

DI-804HV
Broadband VPN Router

Home Advanced Tools Status Help

VPN Settings - Dynamic VPN Tunnel - Set IPSEC Proposal

IPSec Proposal index: - Empty -

Hier sollte anschließend eine "2" erscheinen

Tragen Sie diese Werte ein

ID	Proposal Name	DH Group	Encr. protocol	Encrpt. algorithm	Auth. algorithm	Lifetime	Lifetime Unit
1	2	Group 2	ESP	DES	MD5	3600	Sec.
2		None	ESP	3DES	None	0	Sec.
3		None	ESP	3DES	None	0	Sec.
4		None	ESP	3DES	None	0	Sec.
5		None	ESP	3DES	None	0	Sec.
6		None	ESP	3DES	None	0	Sec.
7		None	ESP	3DES	None	0	Sec.
8		None	ESP	3DES	None	0	Sec.
9		None	ESP	3DES	None	0	Sec.
10		None	ESP	3DES	None	0	Sec.

Proposal ID: 1 Add to Proposal index

Hier wurde , wie schon für die IKE Proposals beschrieben, eine möglichst kompatible Konfiguration verwendet. Benutzen Sie auch hier 3DES oder AES, sofern die Clients diese Algorithmen unterstützen.

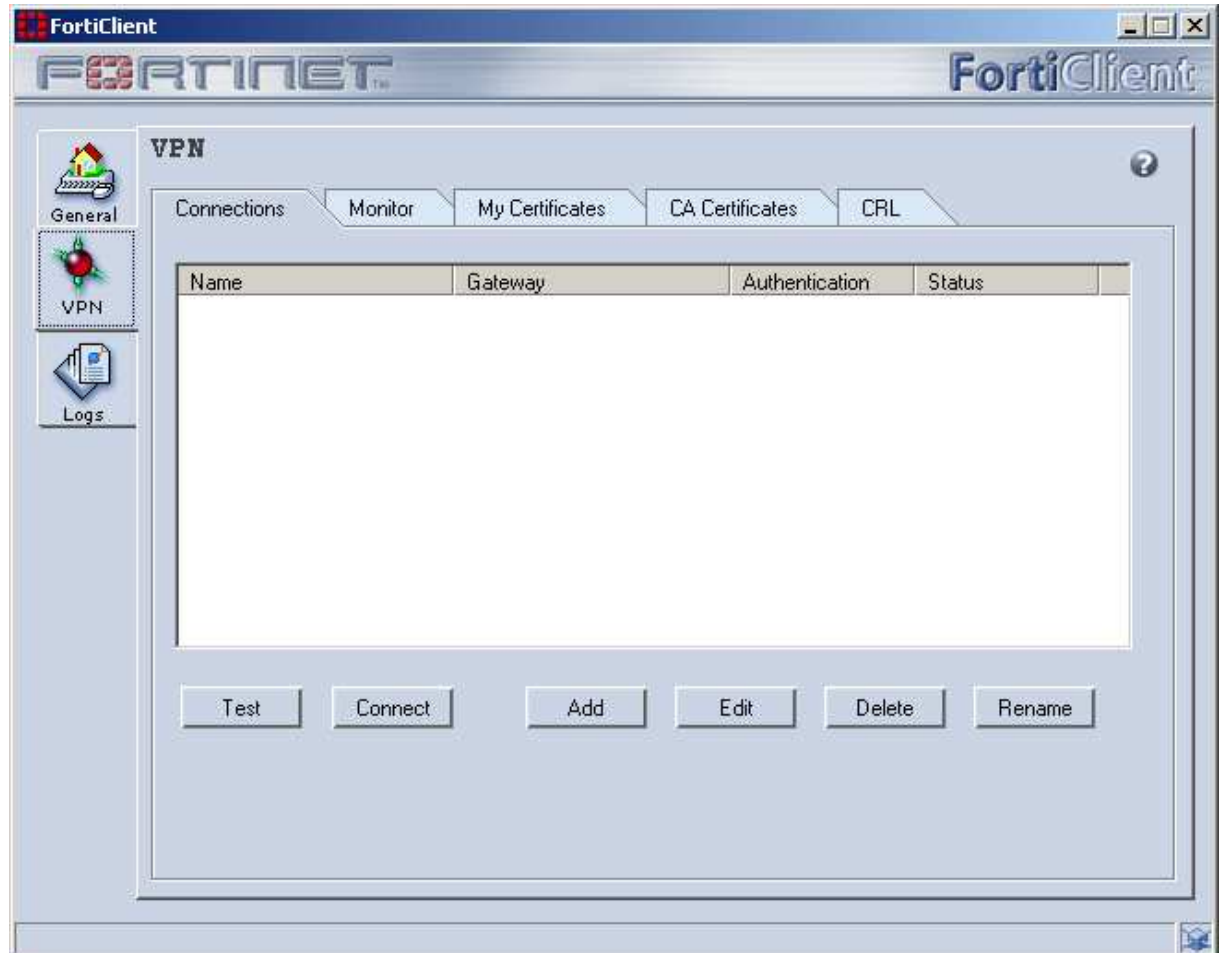
Zunächst übernehmen Sie bitte die Einstellungen aus der oben gezeigten Darstellung. Anschließend wählen Sie die Proposal ID „1“ aus und drücken auf den Button „Add to“. In dem IPSec Proposal Index sollte nun eine „2“ erscheinen. Bestätigen Sie alle Einstellungen mit dem Apply Button.

Die IPSec Gateway Konfiguration ist damit abgeschlossen.

Außerdem sollten Sie überprüfen ob Ihre PPPOE Einstellungen richtig eingegeben wurden, und ob das Gateway eine Verbindung zum Internet aufgebaut hat. In diesem Zusammenhang sollten Sie sich die IP notieren oder aber Dyndns konfigurieren.

Beispiel-Konfiguration für einen IPSEC Client (Forticlient)

- Wichtig: Verwenden Sie auf Ihrem OS immer nur einen IPSEC Client
- Öffnen Sie nach der Installation den FortiClient und klicken Sie auf „VPN“
- Anschließend erstellen Sie eine neue VPN Verbindung indem Sie auf den Button „Add“ klicken

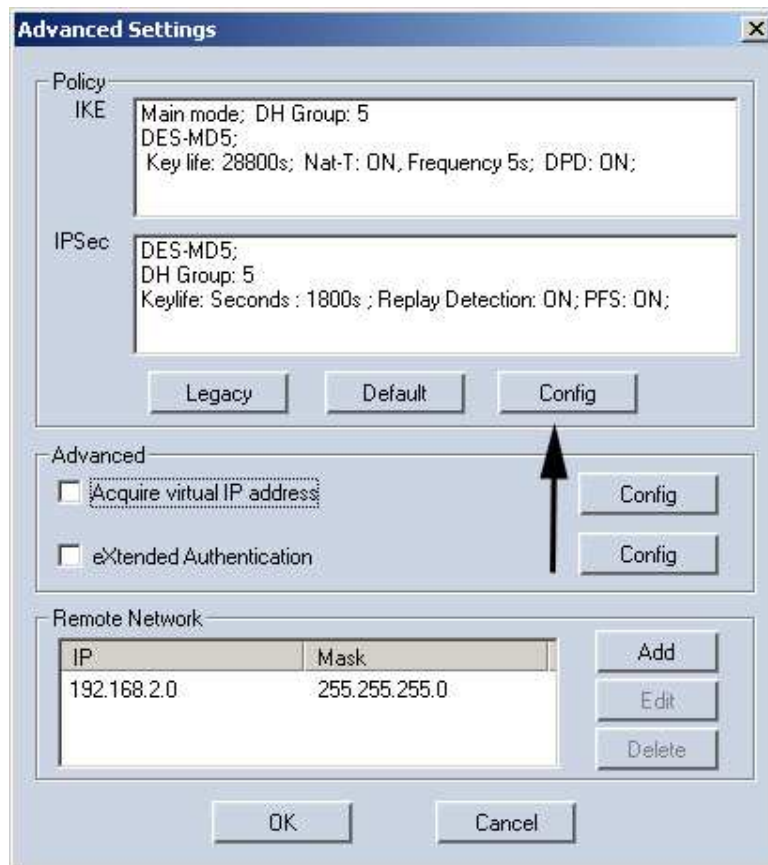


- Geben Sie der Verbindung einen beliebigen Namen. Dieser dient nur der Identifikation.
- Als Remote Gateway IP geben Sie bitte die WAN oder Internet IP des 804HV ein, oder verwenden Sie bei anderen Clients die DynDNS Adresse.
- Das Remote Netzwerk muss auch dem Client bekannt sein, da auch dieser zwischen Remote und lokalem Netzwerk vermitteln muss. In unserem Beispiel habe wir ein 192.168.2.0 C-Netz verwendet. Geben Sie hier unbedingt ein Netz und keine einzelne IP ein.
- Als „Authentication Method“ wählen Sie Preshared Key aus und geben anschließend den Key, den Sie bei der 804Hv Konfiguration definiert haben ein.
- Als nächstes klicken Sie auf „Advanced“ um die IKE und IPSEC Proposals zu konfigurieren.
-

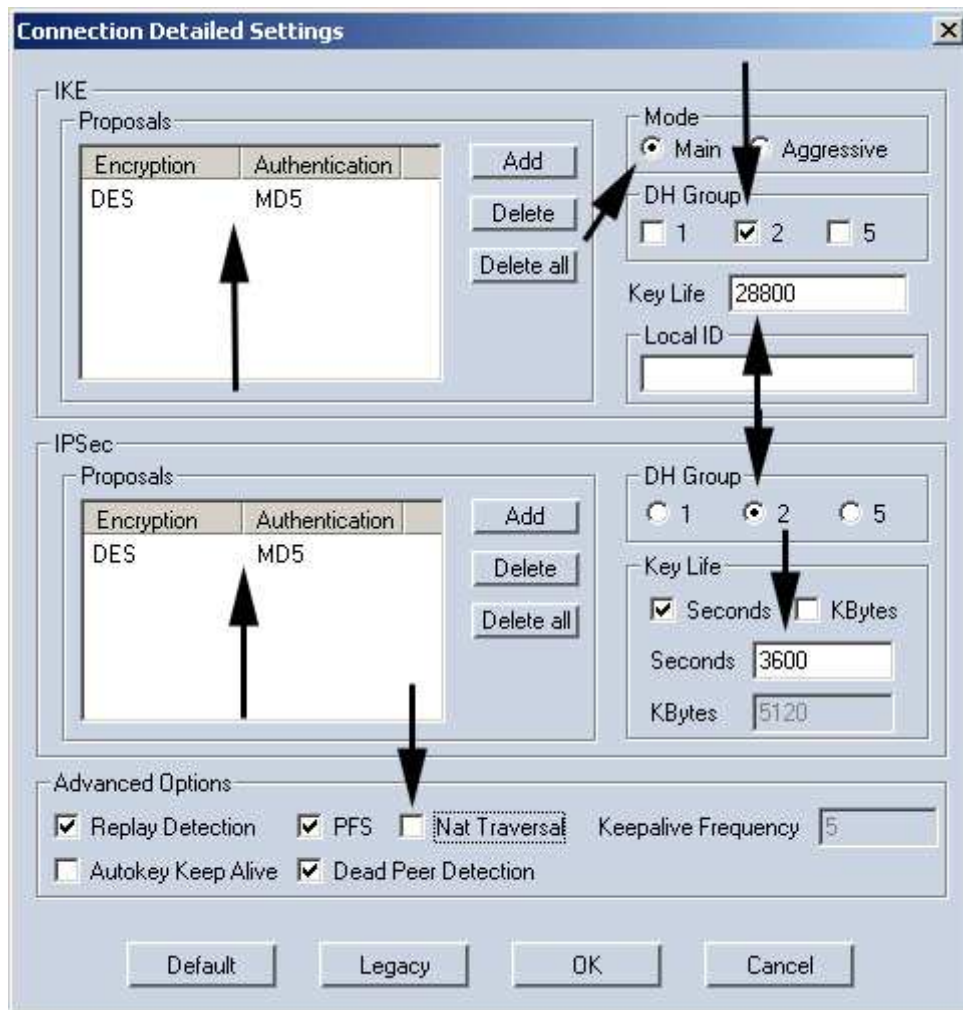
The screenshot shows a 'New Connection' dialog box with the following fields and values:

Connection Name	804 HV Dial UP
Remote Gateway	217 . 167 . 80 . 98
Remote Network	192 . 168 . 2 . 0
	/ 255 . 255 . 255 . 0
Authentication Method	Preshared Key
Preshared Key	*****

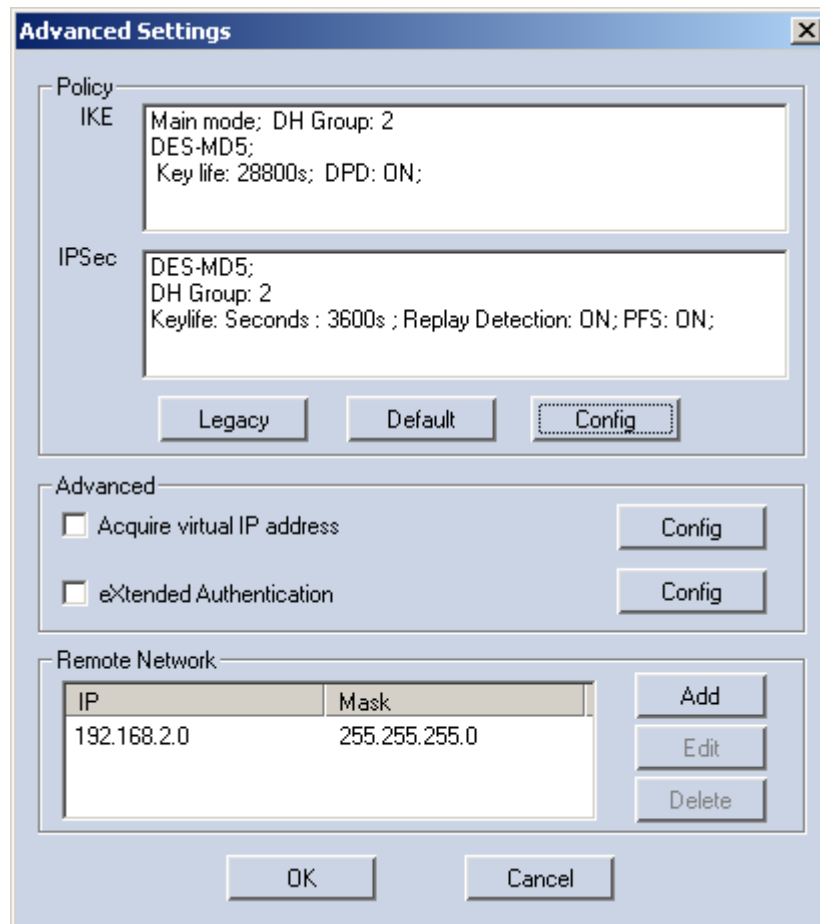
Buttons: Advanced, OK, Cancel



- Klicken Sie auf Config um die IPsec und IKE Einstellungen zu verändern.

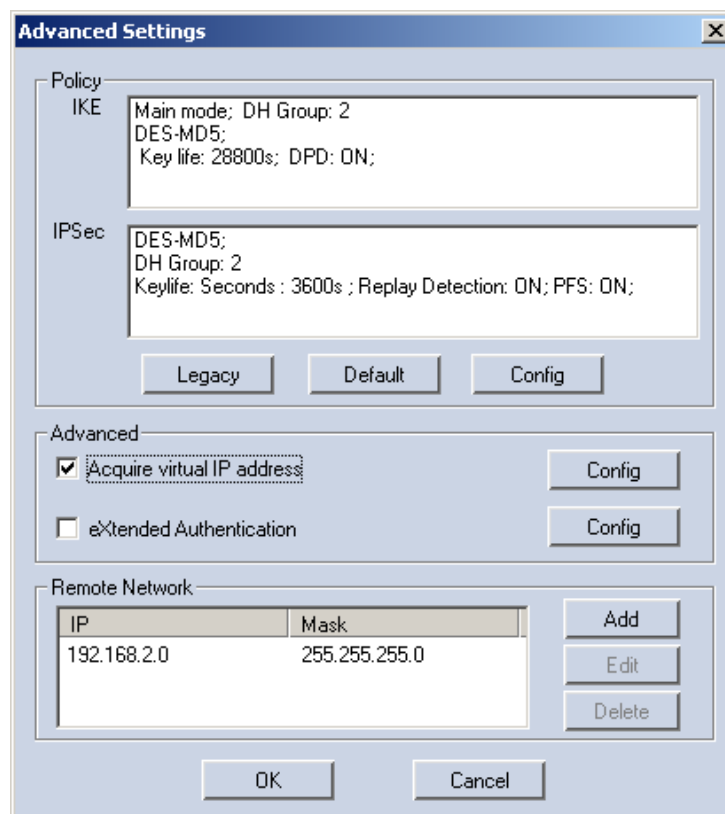


- Stellen Sie alle Parameter, wie oben dargestellt ein. Sofern Sie sich für 3DES oder AES entschieden haben müssen Sie diese Parameter natürlich ändern.
- NAT-Traversal sollten Sie ausschalten, das es zu Konflikten kommen kann wenn dieses Feature verwendet wird. Grundsätzlich setzt man NAT-T nur ein, wenn das Ziel Gateway hinter einem NAT-Gateway betrieben wird.
- Außerdem sollten Sie immer den „Main-Mode“ verwenden.
- Die Dead Peer Detection ist nicht unbedingt notwendig, sorgt aber für einen erneuten Verbindungsaufbau, wenn der Tunnel zusammenbricht.
- Replay Detection: Bei einer Replayattacke werden aufgezeichnete Pakete einer vorher stattgefundenen legalen Verbindung mit dem anzugreifenden System später selektiv von dem Angreifer zum System geschickt (Replay), um bestimmte Reaktionen des Systems hervorzurufen (beispielsweise um eine Authentifizierung zu erreichen). Replayattacken werden für gewöhnlich durch die Vergabe von Sequenznummern in den Paketen oder durch Timestamps verhindert.
- Anschließend schließen Sie den Dialog mit dem „OK“ Button.

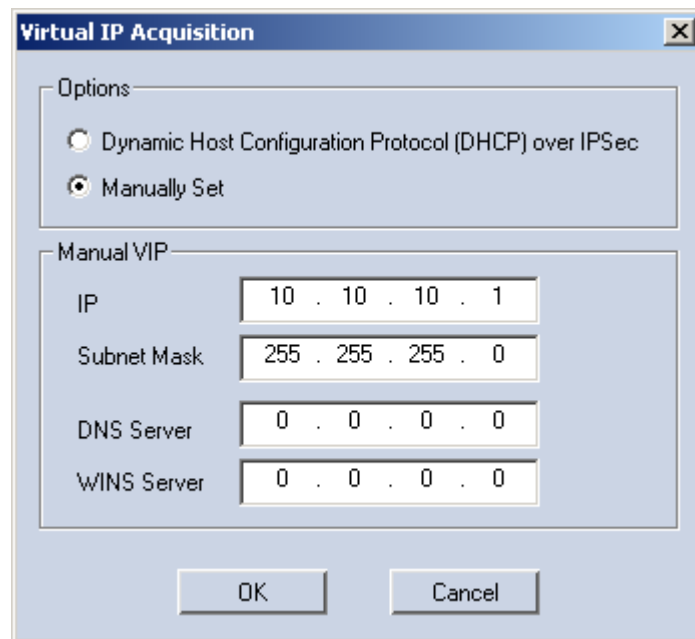


- Schließen Sie auch diesen Dialog, sofern Sie keine virtuelle IP verwenden möchten.

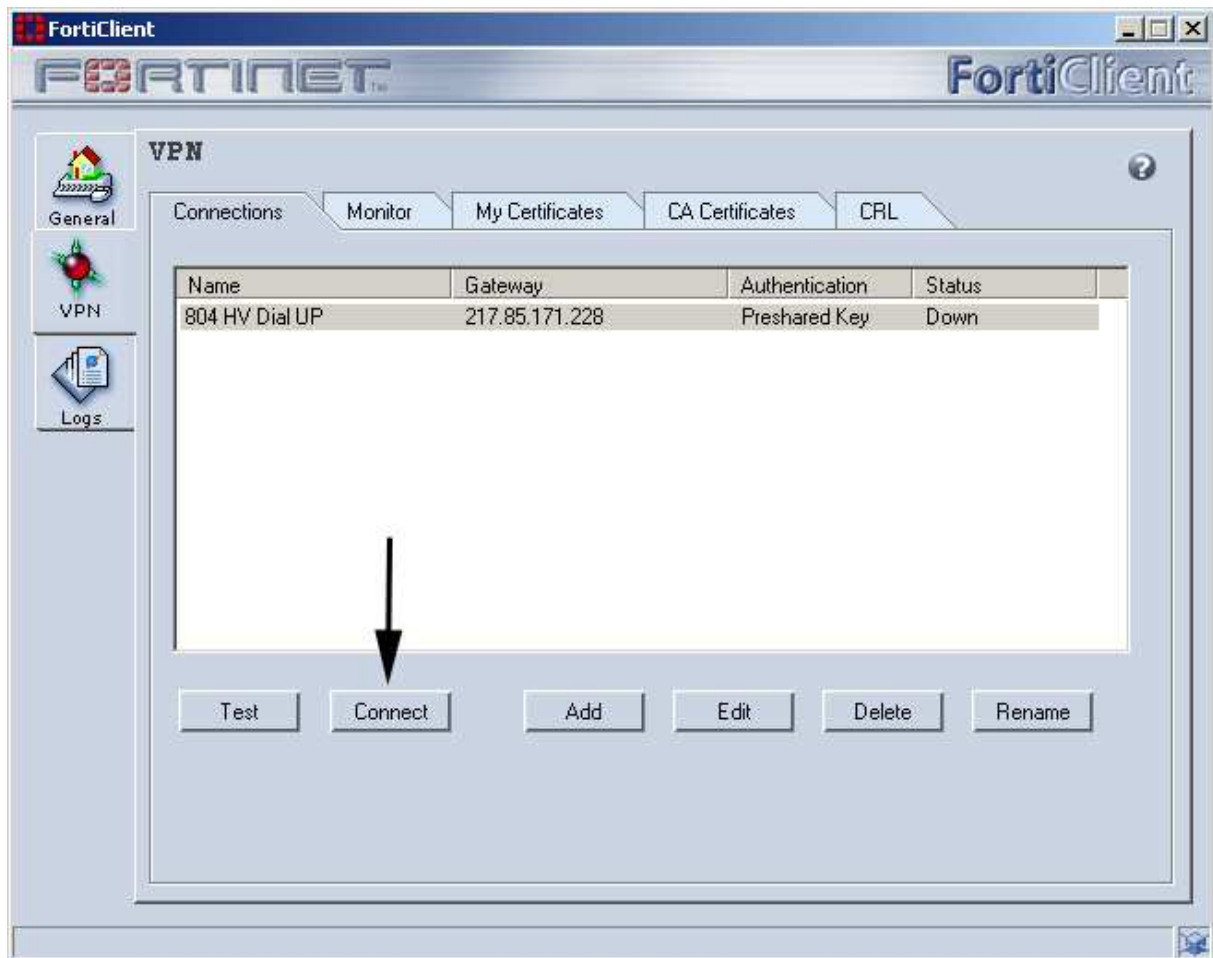
Konfiguration einer virtuellen IP Adresse:



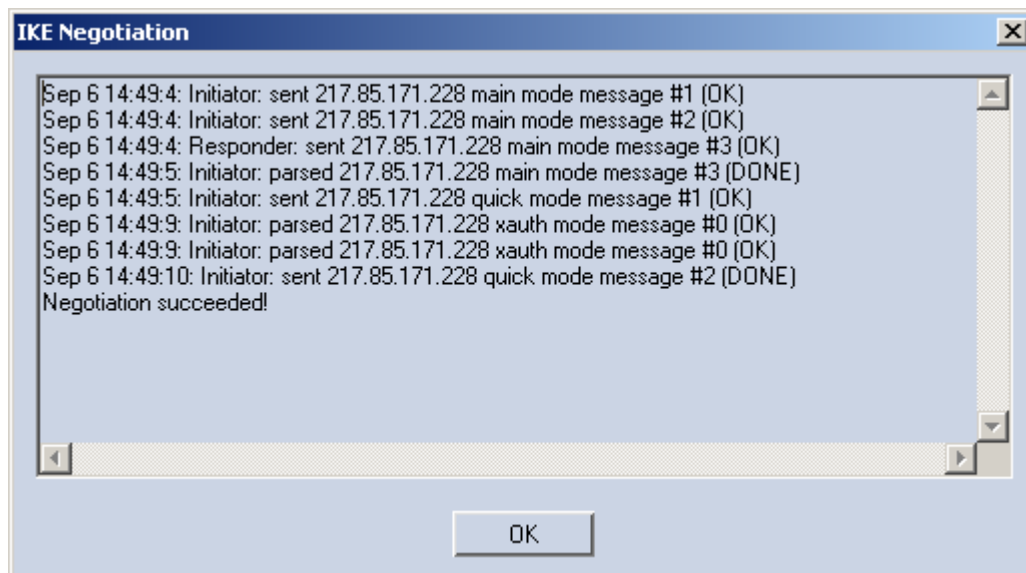
- Setzen Sie den „Acquire IP Address“ Haken und klicken Sie auf den dazugehörigen Config Button



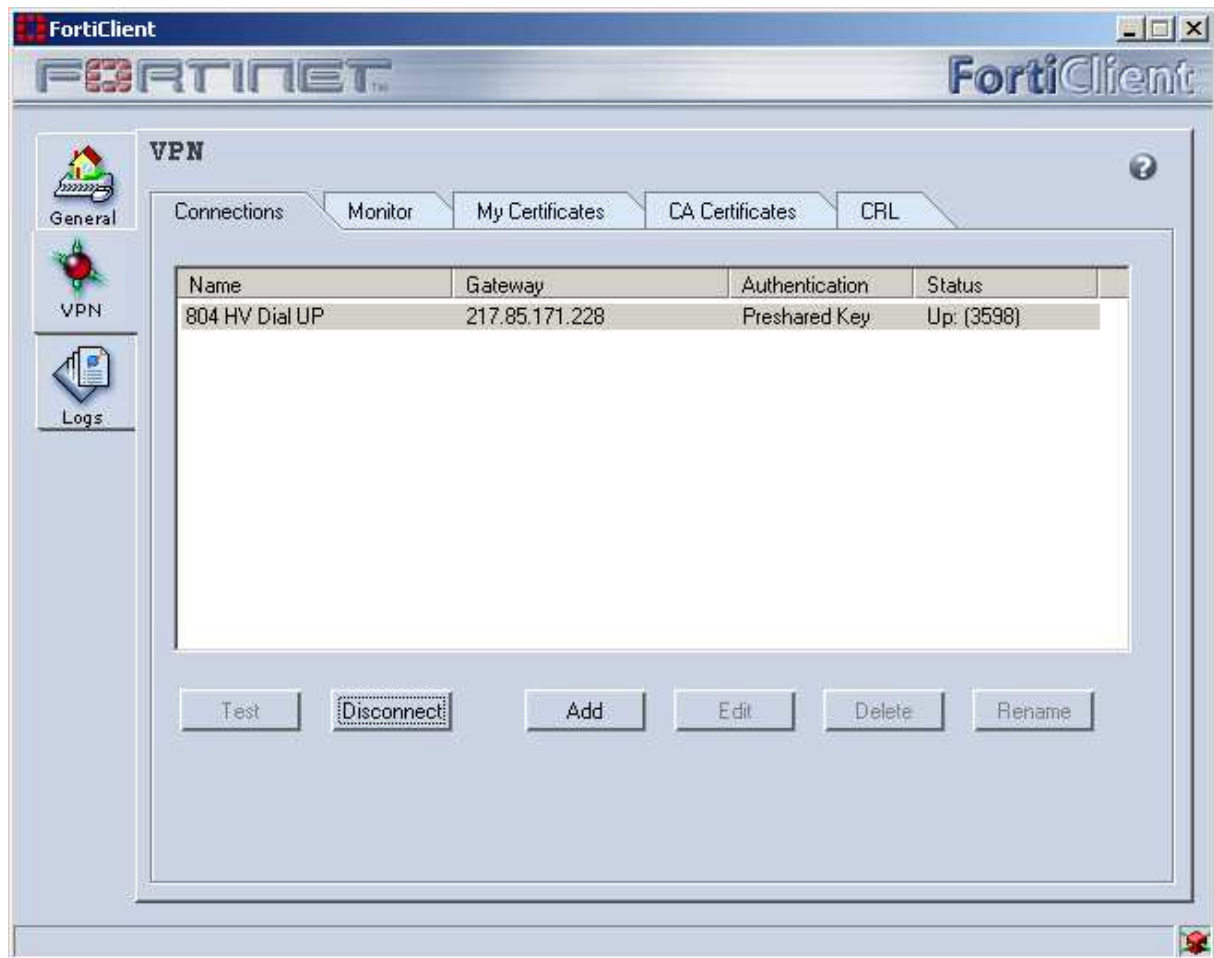
- Sofern Sie kein virtuelle IP verwenden , kann ein Client aus dem Remote Netzwerk Ihren Rechner unter der IP Adresse aus Ihrem lokalen Netzwerk erreichen.
- Wie schon beschrieben dürfen Sie hier auf keinen Fall eine IP aus dem Remote Netzwerk verwenden, da D-Link Geräte zwangsweise NAT verwenden um die Netzwerke zu verbinden. Diese Art der Übersetzung wird als IN oder Outbound NAT bezeichnet. Wenn Sie sich nun meine Beispielkonfiguration ansehen werden Sie feststellen, dass ich ein Netz frei gewählt habe. Die Kommunikation ist aber wegen der NAT Übersetzung möglich. Grundsätzlich empfehle ich die Verwendung von virtuellen Ips nicht. DHCP über IPsec ist leider nur möglich wenn ein IPsec Gateway die Deaktivierung von In-/Outbound NAT zulässt.
- Schließen Sie alle Dialoge mit dem „OK“ Button.



- Klicken Sie auf Connect um die Verbindung zu testen.



- Diese Status Screen sollte auch bei Ihnen erscheinen. Die beiden xauth Zeilen fehlen bei Ihnen, da es sich um ein erweitertes Feature zur User Authentifizierung handelt.
- Sofern die letzte Zeile „Negotiation succeeded“ erscheint haben Sie Ihre Verbindung erfolgreich konfiguriert.



- Sie sehen unter „Status“, dass der Client von 3600 abwärts zählt. Diese Zahl entspricht der IPsec Lifetime. Sofern diese Zeit abgelaufen ist, wird ein Schlüsselwechsel initiiert.
- Sie können jetzt einen Ping-Test durchführen. Die VPN Konfiguration ist damit abgeschlossen.