

Interoperability Guide

Setting up a VPN tunnel between
mGuard and NETGEAR FVS338



mGuard smart



mGuard PCI



mGuard blade



mGuard industrial



mGuard delta

© Innominate Security Technologies AG

July 2006

“Innominate” and “mGuard” are registered trademarks of the Innominate Security Technologies AG. All other brand names or product names are trade names, service marks, trademarks, or registered trade marks of their respective owners.

mGuard technology is protected by the German patents #10138865 and #10305413. Further national and international patent applications are pending.

No part of this documentation may be reproduced or transmitted in any form, by any means without prior written permission of the publisher.

All information contained in this documentation is subject to change without previous notice.

Innominate offers no warranty for these documents. This also applies without limitation for the implicit assurance of scalability and suitability for specific purposes.

In addition, Innominate is neither liable for errors in this documentation nor for damage, accidental or otherwise, caused in connection with delivery, output or use of these documents.

This documentation may not be photocopied, duplicated or translated into another language, either in part or in whole, without the previous written permission of Innominate Security Technologies AG.

Innominate Document Number: 571009-202


TABLE OF CONTENTS

1	Introduction	4
1.1	<i>mGuard in Router mode (Router, PPPoE, PPTP).....</i>	<i>4</i>
1.2	<i>mGuard in Stealth mode.....</i>	<i>5</i>
2	Limitations in using Preshared Secret Keys (PSK)	6
3	Certificates.....	6
3.1	<i>Step 1: Tool XCA - Create and export the CA.....</i>	<i>6</i>
3.2	<i>Step 2: FVS338 - Import of the CA.....</i>	<i>7</i>
3.3	<i>Step 3: FVS338 - Create and export the host certificate request.....</i>	<i>7</i>
3.4	<i>Step 4: Tool XCA – Import the certificate request, sign it with the CA and certificate export.....</i>	<i>8</i>
3.5	<i>Step 5: FVS338 - Import of the signed certificate.....</i>	<i>8</i>
3.6	<i>Step 6: Tool XCA - Create and export the certificate for the mGuard.....</i>	<i>9</i>
4	Configuring the FVS338	10
4.1	<i>IKE Policies.....</i>	<i>10</i>
4.1.1	<i>IKE Policy with PSK</i>	<i>10</i>
4.1.2	<i>IKE Policy with certificates</i>	<i>11</i>
4.2	<i>VPN Policies.....</i>	<i>12</i>
5	Configuring the mGuard.....	13
5.1	<i>Import of the mGuard machine certificate.....</i>	<i>13</i>
5.2	<i>Activating DynDNS monitoring.....</i>	<i>13</i>
5.3	<i>Configuring the VPN connection.....</i>	<i>13</i>
5.3.1	<i>General settings.....</i>	<i>14</i>
5.3.2	<i>Authentication.....</i>	<i>15</i>
5.3.2.1	<i>Certificates.....</i>	<i>15</i>
5.3.2.2	<i>PSK.....</i>	<i>15</i>
5.3.3	<i>Firewall.....</i>	<i>16</i>
5.3.4	<i>IKE Options</i>	<i>17</i>
5.4	<i>mGuard in Stealth mode.....</i>	<i>18</i>
6	Troubleshooting.....	19
6.1	<i>ISAKMP couldn't be established.....</i>	<i>19</i>
6.2	<i>IPsec couldn't be established.....</i>	<i>19</i>

1 Introduction

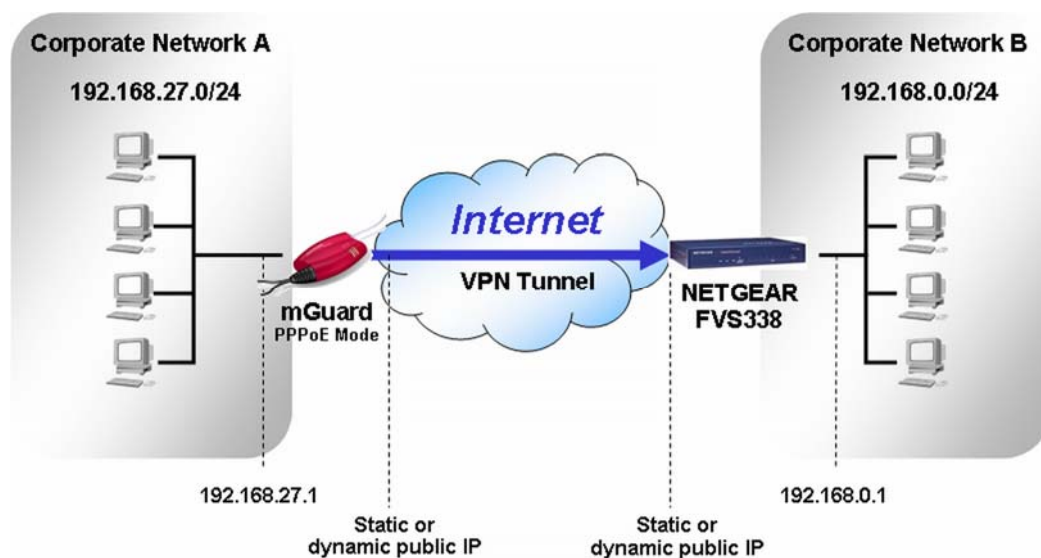
This document describes the required steps to configure a VPN tunnel between the mGuard and the NETGEAR FVS338, in the following called FVS338. We have used a NETGEAR FVS338 v1.6.47 and an mGuard v4.0.0 for this interoperability test.

The VPN tunnel will be initiated by the mGuard. This document describes the usage of the authentication methods PSK (Preshared Secret Key) and PKI with X.509 certificates.

 **Note:** Configuring a VPN using PKI and certificates is considered more secure than using pre-shared secrets.

The following diagram illustrates the machines and addresses involved in the connection. The examples used in this document are taken from this setup.

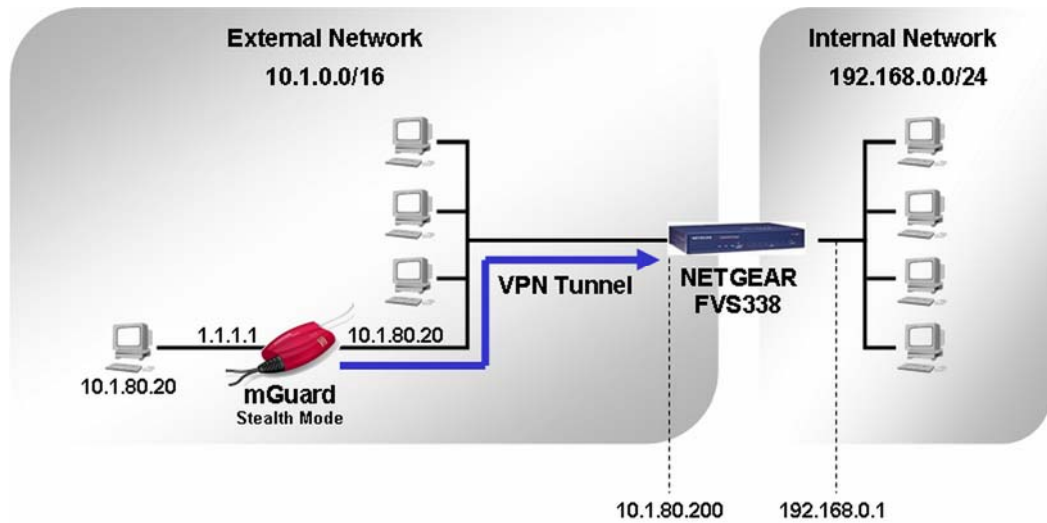
1.1 mGuard in Router mode (Router, PPPoE, PPTP)



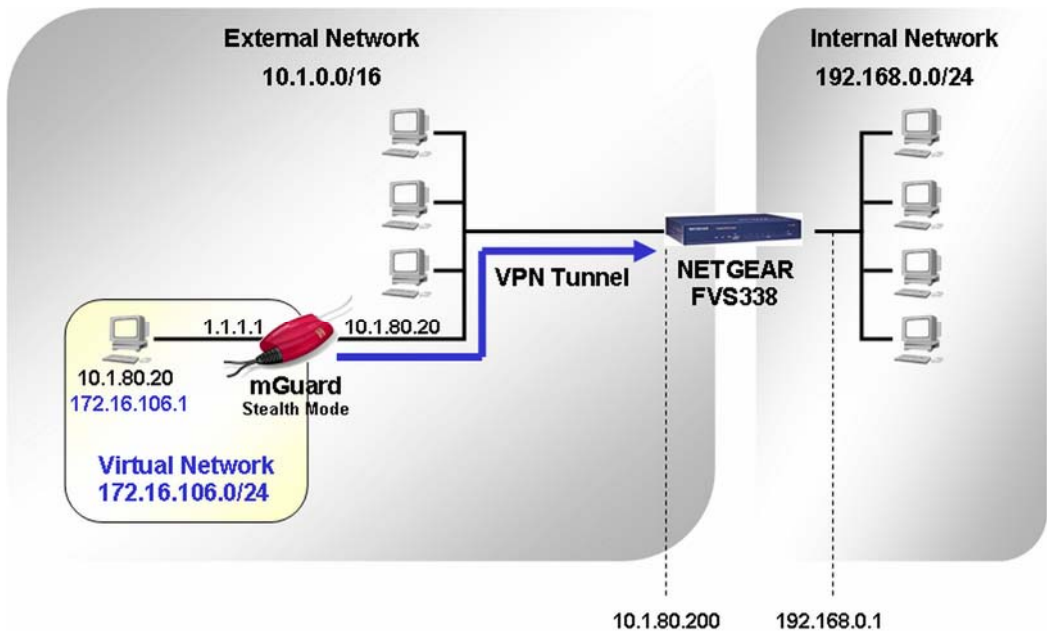
We have selected for this setup 3DES as encryption and MD5 as hash algorithm for *ISAKMP Policy* and *IPsec Policy*. For this setup the parameters for the VPN tunnel are as follows:

	mGuard	FVS338
Remote VPN gateway	IP address of the FVS338 or its DynDNS name	IP address of the mGuard or its DynDNS name
Local VPN subnet	192.168.27.0/24	192.168.0.0/24
Remote VPN subnet	192.168.0.0/24	192.168.27.0/24
IKE Policy, Encryption/Hash	3DES/MD5	3DES/MD5
IPsec Policy, Encryption/Hash	3DES/MD5	3DES/MD5

1.2 mGuard in Stealth mode



The mGuard is operated in *Stealth* mode to protect a single entity, e.g. server, workstation, etc. In contrast to the *Router* modes an internal network does not exist. In this case we need to use a virtual transfer network as local VPN subnet which must not overlap with existing network IPs. In our example we have used as virtual transfer network 172.16.106.0/24. You also need to define a virtual IP on the mGuard which will be used by the client in *Stealth* mode (e.g. 172.16.106.1). This virtual IP address is used to access the client behind the mGuard through the VPN tunnel from the internal network.




2 Limitations in using Preshared Secret Keys (PSK)

- If the mGuard has a dynamic public IP address and PSK shall be used, the mGuard must register its IP address under a fixed name in a DynDNS service and the VPN settings on the FVS338 must refer to this name.
- Using PSK is not possible if the connection will be established across one or more gateways that have *Network Address Translation* (NAT) activated. In this case *Aggressive Mode* would be required which is not supported by the mGuard in the current version. X.509 certificates need to be used in this case.

3 Certificates

There are several tools available for creating and managing certificates, as for example OpenSSL and XCA. We have used the tool XCA v0.5.1. You can download this tool from <http://www.hohnstaedt.de/xca.html>. The documentation is located at <http://xca.sourceforge.net/>.

 **Note:** If you do not specify a directory when exporting a certificate with XCA then the export is located in the XCA installation directory.

The following certificates are required for setting up the connection, all of them signed by the same CA:

- **CA as PEM export:** Needs to be imported on the FVS338.
- **FVS338 host certificate as PEM export:** Needs to be imported on the *FVS338* and on the mGuard as connection certificate.
- **mGuard certificate as PKCS#12 export:** Needs to be imported on the mGuard as machine certificate.

Perform the following steps for creating the required certificates:

- Step 1: Tool XCA - Create and export the CA
- Step 2: FVS338 - Import of the CA
- Step 3: FVS338 - Create and export a certificate request
- Step 4: Tool XCA – Import the certificate request, sign it with the CA and certificate export
- Step 5: FVS338 - Import of the signed certificate
- Step 6: Tool XCA - Create and export the certificate for the mGuard

3.1 Step 1: Tool XCA - Create and export the CA

Create the CA

- Start the program **XCA**.
- Switch to the **Certificates** tab, click **New Certificate** and then **Next**.
- Select the option **Create a self signed certificate with the serial**, select **CA Template** and click **Next**.
- A **new key** needs to be created. Enter a descriptive name for the key (e.g. CA) and click **Create**.
- Use the entry fields from **Internal Name** to **E-Mail Address** for entering the identifying parameters. Click **Next**.
- Enter into the field **Time Range** the lifetime of the CA, click **Apply** and then **Next**.
- Now you only need to confirm the appearing input masks by selecting **Next** until the certificate has been created.

Export of the CA as PEM

- Select the CA and click **Export**.
- Chose **PEM** as **Export Format** and click **OK**.

In our example we have named the file *CA.crt*.

3.2 Step 2: FVS338 - Import of the CA

- From the menu, select **VPN -> CAs**.
 - Click **Add**.
 - Click **Browse** and select the CA you've created and exported in the previous step, in our example *CA.crt*.
 - Click **Upload**.
- ⇒ The imported CA is displayed.



3.3 Step 3: FVS338 - Create and export the host certificate request

- From the menu, select **VPN -> Certificates**.
- Click **Generate Request**.



- Enter a descriptive **Name** for the certificate.
 - Enter the **Subject** of the certificate. This subject corresponds to the common name of the ASN.1 distinguished name of the certificate, in our example */CN=Netgear*.
 - Click **Next**.
- ⇒ The certificate is displayed.



- Copy and paste the contents of the certificate request, including the BEGIN CERTIFICATE and END CERTIFICATE lines and save it e.g. as *Netgear_req.pem*.
- Click **Back**.

3.4 Step 4: Tool XCA – Import the certificate request, sign it with the CA and certificate export

Import of the certificate request

- Switch to the **Certificate signing requests** tab.
- Click **Import** and import the certificate request of the FVS338 you have created in the previous step, in our example *Netgear_req.pem*.

Sign the certificate request with the CA

- Highlight the imported certificate and select **Sign** from the menu.
- Click **Next**.
- Enable **Use this certificate for signing** and select the CA you have created in step 1. Click **Next**.
- Enter into the field **Time Range** the lifetime of the certificate, click **Apply** and then **Next**.
- Now you only need to confirm the appearing input masks by selecting **Next** until the certificate has been signed.
- Switch to the **Certificates** tab. The imported and signed certificate of the FVS338 appears beneath the CA.

Export of the signed FVS338 certificate

- Highlight the signed FVS338 certificate which is located beneath the CA and click **Export**.
- Chose **PEM** as **Export Format**.
- Click **OK**.

In our example we have named the file *Netgear.crt*. This certificate needs to be imported on the FVS338 as *Own Certificate* and on the mGuard as connection certificate (menu *IPSec VPN -> Connections*).

3.5 Step 5: FVS338 - Import of the signed certificate

- From the menu, select **VPN -> Certificates**.

The screenshot shows a web interface titled "Certificates". It is divided into two main sections: "Active Self Certificates" and "Self Certificate Requests".

Active Self Certificates: This section contains a table with columns: Name, Subject Name, Serial Number, Issuer Name, and Expiry Time. Below the table is a "Delete" button.

Self Certificate Requests: This section contains a table with columns: Name and Status. There is one entry with the name "Netgear" and the status "Waiting for Certificate upload". Below the table are "Delete" and "Upload Certificate" buttons.

At the bottom of the interface is a "Generate Request" button.

- Mark in the section **Self Certificate Request** the certificate request and click **Upload Certificate**.
 - Click **Browse**, select the signed certificate you have exported in the previous step, in our example *Netgear.crt*, and click **Upload**.
- ⇒ The uploaded certificate is displayed.

3.6 Step 6: Tool XCA - Create and export the certificate for the mGuard

Create the certificate for the mGuard

- Switch to the **Certificates** tab, select the CA and click **New Certificate**.
- Click **Next**.
- Ensure that **Use this certificate for signing** is enabled and that the CA is selected in the dropdown box.
- Set **Template for the new certificate** to **Client Template** and click **Next**.
- Enter a **Name** for the **New Key** and click **Create**.
- Use the entry fields from **Internal Name** to **E-Mail Address** for entering the identifying parameters.

 **Note:** Entering the ASN.1 DN of the certificate is limited to 64 characters on the FVS338.

- Click **Next**.
- Enter into the field **Time Range** the lifetime of the certificate, click **Apply** and then **Next**.
- Now you only need to confirm the appearing input masks by selecting **Next** until the certificate has been created.

Export of the mGuard certificate as PKCS#12

- Highlight the mGuard certificate which is located beneath the CA and click **Export**.
- Set **Export Format** to **PKCS#12** and click **OK**.
- You'll be prompted to enter a password which protects the certificate against unauthorized usage.

In our example we have named the file *mGuard.p12*. This certificate needs to be imported on the mGuard as machine certificate (menu *IPsec VPN -> Global*, tab *Machine Certificate*).

4 Configuring the FVS338

4.1 IKE Policies

4.1.1 IKE Policy with PSK

When configuring the IKE policy using PSK you need to distinguish whether the mGuard has a static or a dynamic public IP address. If the mGuard has a dynamic public IP address it needs to register the current IP address under a fixed name in a DynDNS service and you must refer to the DynDNS name when configuring the *VPN Policy*.

- From the menu, select **VPN -> IKE Policies**.
- Click **Add**.

- Enter a descriptive **Policy Name**.
- When using PSK you need to set **Direction/Type** to **Both Directions**. *Responder* or *Initiator* is not supported by the FVS338 when using PSK and Main Mode. The mGuard does not support the *Aggressive Mode*.
- Set **Exchange Mode** to **Main Mode**.
- Set **Local Identity Type** to **WAN IP Address**. If the mGuard has a static public IP address, set **Remote Identity Type** to **Remote WAN IP**. Otherwise, if the mGuard has a dynamic public IP address, set **Remote Identity Type** to **Fully Qualified User Name** and enter the user name into **Remote Identity Data**:

- Select the desired **Encryption** and **Authentication Algorithm**, in our example we have used 3DES and MD5.
 - Select **Pre-Shared Key** as **Authentication Method** and enter the shared secret.
 - Set **Diffie-Hellman (DH) Group** to **Group 2 (1024 Bit)**.
 - Click **Apply**.
- ⇒ The policy is displayed in the IKE policy table.

4.1.2 IKE Policy with certificates

- From the menu, select **VPN -> IKE Policies**.
- Click **Add**.

The screenshot shows the 'IKE Policy Configuration' web interface. It is divided into several sections: 'General', 'Local', 'Remote', 'IKE SA Parameters', and 'X AUTHENTICATION'.
- **General:** Policy Name is 'mGuard', Direction/Type is 'Both Directions', and Exchange Mode is 'Main Mode'.
- **Local:** Local Identity Type is 'DER ASN1 DN' and Local Identity Data is '/CN=Netgear'.
- **Remote:** Remote Host Configuration Record is 'None', Remote Identity Type is 'DER ASN1 DN', and Remote Identity Data is '/CN=mGuard/C=de/L=Berlin'.
- **IKE SA Parameters:** Encryption Algorithm is '3DES', Authentication Algorithm is 'MD5', and Authentication Method is 'RSA Signature (requires Certificate)'.
- **Diffie-Hellman (DH) Group:** Set to 'Group 2 (1024 Bit)'.
- **SA Life Time:** Set to '3600 (secs)'.
- **X AUTHENTICATION:** Set to 'None'.
At the bottom, there are 'Back', 'Apply', and 'Cancel' buttons.

- Enter a descriptive **Policy Name**.
 - Set **Direction/Type** either to **Both Directions**, **Responder** or **Initiator**, depending on whether the FVS338 should initiate the connection or wait for the connect request.
 - Set **Exchange Mode** to **Main Mode**. The mGuard does not support the *Aggressive Mode*.
 - Set **Local Identity Type** to **DER ASN1 DN** and enter the distinguished name of the FVS338 certificate, in our example /CN=Netgear.
 - Set **Remote Identity Type** to **DER ASN1 DN** and enter the distinguished name of the mGuard certificate, in our example /CN=mGuard/C=de/L=Berlin/ST=Germany.
 - Select the desired **Encryption** and **Authentication Algorithm**, in our example we have used 3DES and MD5.
 - Select **RSA Signature** as **Authentication Method**.
 - Set **Diffie-Hellman (DH) Group** to **Group 2 (1024 Bit)**.
 - Click **Apply**.
- ⇒ The policy is displayed in the IKE policy table.

4.2 VPN Policies

- From the menu, select **VPN -> VPN Policies**.
- Click **Add Auto Policy**.

- Enter a descriptive **Policy Name**.
 - Select the **IKE policy** you've created in the previous chapter.
 - **Remote VPN Endpoint:**
 - If the mGuard has a static public IP address, set **Address Type** to **IP Address** and enter the public IP address of the mGuard into **Address Data**.
 - If the mGuard has a dynamic public IP address, set **Address Type** to **Fully Qualified Domain Name** and enter the DynDNS name of the mGuard into **Address Data**. Alternatively you can set **Address Type** to **IP Address** and enter 255.255.255.255 into **Address Data** if certificates are used as authentication method.
 - If *Perfect Forward Secrecy* (PFS) shall be used, enable **IPSec PFS** and select **Group 2 (1024 Bit)**. If you enable PFS, this also needs to be done when configuring the VPN connection on the mGuard.
 - **Traffic Selector:** Set **Local IP** and **Remote IP** to **Subnet address**. Enter for the **Local IP** the internal network IP of the FVS338, in our example 192.168.0.0/255.255.255.0 and for the **Remote IP** the internal network IP of the mGuard, in our example 192.168.27.0/255.255.255.0.
 - Enable **Encryption** and **Authentication** in the section **ESP Configuration** and specify the **Encryption** and **Authentication Algorithm** that shall be used, in our example 3DES and MD5.
 - Click **Apply**.
- ⇒ The policy is displayed in the VPN policy table.

5 Configuring the mGuard


Configuring the VPN connection on the mGuard requires the following steps:

- If certificates are used as authentication method: Import of the mGuard machine certificate.
- Enable DynDNS monitoring if the remote VPN gateway has a dynamic public IP address and registers it under a fixed name in a DynDNS service.
- Configuration of the VPN connection.

5.1 Import of the mGuard machine certificate

This step is only required when using certificates as authentication method.

- From the menu, select **IPsec VPN -> Global**, tab **Machine Certificate**.
- Click **Browse** and select the mGuard's machine certificate, in our example *mGuard.p12*.
- Enter the **Password** which protects the certificate against unauthorized usage.
- Click **Import**.
- Finally click **Apply**.

 **Note:** If you don't click **Apply** the certificate won't be stored on the device.

5.2 Activating DynDNS monitoring

You need to activate DynDNS monitoring, if you specify a DynDNS name as remote VPN gateway. If you don't activate this option, the mGuard won't notice when the IP address of the remote gateway has changes.

- From the menu, select **IPsec VPN -> Global**, tab **DynDNS Monitoring**.
- Set **Watch hostnames of remote VPN Gateways** to **Yes**.
- Click **Apply**.

5.3 Configuring the VPN connection

- From the menu, select **IPsec VPN -> Connections**.
- Click **New**, enter a descriptive name for the connection and click **Edit**.

5.3.1 General settings

The screenshot shows the configuration page for an IPsec VPN connection on a Netgear device. The page is titled "IPsec VPN » Connections » Netgear" and has four tabs: "General", "Authentication", "Firewall", and "IKE Options". The "General" tab is selected. The page is divided into two main sections: "Options" and "Tunnel Settings".

Options

A descriptive name for the connection	Netgear
Enabled	Yes
Address of the remote site's VPN gateway (either an IP address, a hostname, or %any)	netgear.dyndns.org
Connection startup (Will be ignored in Stealth Mode.)	Initiate

Tunnel Settings

Connection type	Tunnel (Net <-> Net)
Local network	192.168.27.0/24
Remote network	192.168.0.0/24
The virtual IP which will be used by the client in Stealth mode	192.168.1.1
Enable 1-to-1 NAT to a different internal network in router mode	No
Internal network for 1-to-1 NAT	192.168.2.1

An "Apply" button is located at the bottom right of the configuration area.

- Enter as **Address of the remote site's VPN gateway** either the DynDNS name of the remote VPN gateway or its static public IP address.
- The mGuard should initiate the VPN tunnel. Therefore set **Connection startup** to **Initiate**.
- Set **Connection type** to **Tunnel (Net <-> Net)** for a VPN tunnel connection.
- Enter as **Local Network** the internal network IP of the mGuard, in our example 192.168.27.0/24.
- Enter as **Remote Network** the internal network IP of the FVS338, in our example 192.168.0.0/24.
- The other options are not required for this setup.
- Switch to the tab **Authentication**.

5.3.2 Authentication

5.3.2.1 Certificates

The screenshot shows the 'Authentication' tab in the IPsec VPN configuration for Netgear. The 'Authentication method' is set to 'X.509 Certificate'. Below this, the certificate details are shown in a text area:

```

subject=
CN=Netgear
issuer=
CN=CA
C=de
L=Berlin
ST=Germany
O=Innominate
OU=Support
emailAddress=support@innominate.com
MD5 Fingerprint=6E:92:9B:24:5F:1B:A8:70:02:79:34:13:33:51:12:56
SHA1 Fingerprint=89:6B:74:E0:E0:62:96:BC:CA:84:25:66:EB:E0:34:25:5B:19:24:7D
notBefore=Jun  6 11:23:10 2006 GMT
notAfter=Jun  6 11:23:10 2007 GMT
    
```

The 'Filename (*.cer)' field is empty, with a 'Durchsuchen...' button next to it. Below the filename field is an 'Import' button. The 'VPN Identifier' section has two fields: 'Remote' and 'Local VPN Identifier'. Both have a 'Valid values are:' list below them:

- the certificates distinguished name (same as no entry)
- @fvs338@innominate.com

For the 'Local VPN Identifier' field, the valid values are:

- the certificates distinguished name (same as no entry)
- @mGuard@innominate.com

An 'Apply' button is located at the bottom right of the configuration area.

- Set **Authentication Method** to **X.509 Certificate**.
- Click **Browse** and select the PEM export of the FVS338 host certificate, in our example *Netgear.crt*.
- Click **Import**.
- Switch to the tab **Firewall**.

5.3.2.2 PSK

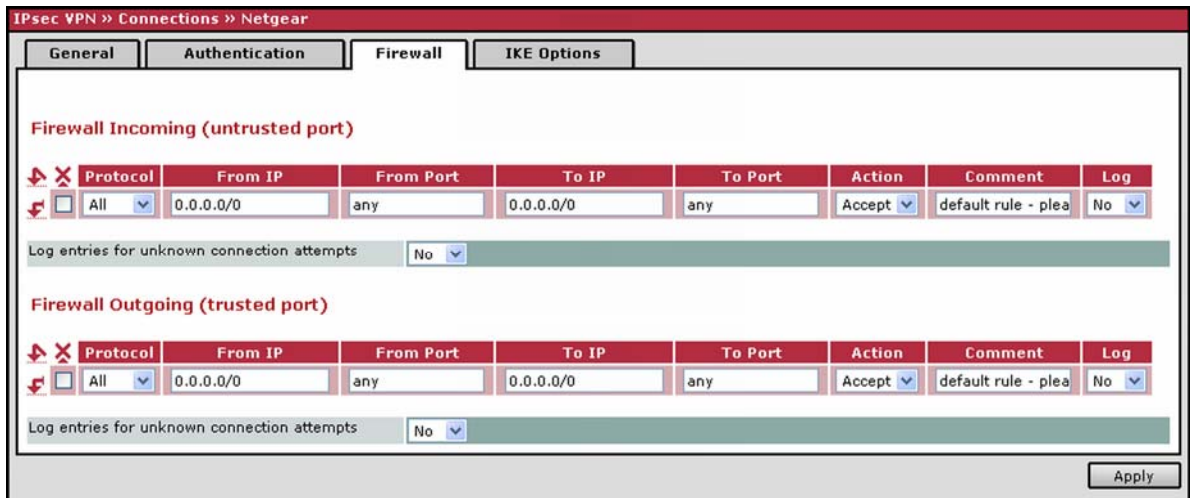
The screenshot shows the 'Authentication' tab in the IPsec VPN configuration for NETGEAR. The 'Authentication method' is set to 'Pre-Shared Secret (PSK)'. Below this, the 'Pre-Shared Secret Key (PSK)' field contains the value 'shared_secret'. The 'VPN Identifier' section has two fields: 'Remote' and 'Local VPN Identifier', both of which are currently empty.

An 'Apply' button is located at the bottom right of the configuration area.

- Set **Authentication Method** to **Pre-Shared Secret**.
- Enter the **Pre-Shared Secret Key**.
- You need to enter the **Local VPN Identifier** of the mGuard if it has a public dynamic IP address. In our example we have used *support@innominate.com* (please refer to chapter 4.1.1 *IKE Policy with PSK*).
- Switch to the tab **Firewall**.

5.3.3 Firewall

The VPN firewall allows restricting the access through the VPN tunnel. You may configure the VPN firewall if desired. In the screenshot below all incoming and outgoing connections will be passed through the VPN tunnel.



- Switch to the tab **IKE Options**.

5.3.4 IKE Options

IPsec VPN » Connections » Netgear

General Authentication Firewall **IKE Options**

ISAKMP SA (Key Exchange)

Encryption Algorithm: 3DES

Hash Algorithm: MD5

IPsec SA (Data Exchange)

Encryption Algorithm: 3DES

Hash Algorithm: MD5

Perfect Forward Secrecy (PFS)
(The remote site must have the same entry. Activation is recommended due to security reasons.)

Yes

Lifetimes

ISAKMP SA Lifetime (seconds): 3600

IPsec SA Lifetime (seconds): 28800

Rekeymargin (seconds): 540

Rekeyfuzz (percent): 100

Keying tries (0 means unlimited tries): 0

Rekey: No

Dead Peer Detection

Action: Hold (Default)

Delay: 30

Timeout: 120

Apply

- Select the **Encryption** and **Hash Algorithm** that shall be used for the **ISAKMP SA**. Those values must correspond to the *IKE policy* settings on the FVS338.
- Select the **Encryption** and **Hash Algorithm** that shall be used for the **IPsec SA**. Those values must correspond to the *VPN policy* settings on the FVS338.
- Enable **Perfect Forward Secrecy** if PFS has also been activated on the FVS338 in the *VPN Policy*.
- Click **Apply**.

5.4 mGuard in Stealth mode

As already mentioned in the *Introduction* of this document, we need to use a virtual transfer network as local VPN subnet if the mGuard is operated in *Stealth* mode. The configuration of the VPN connection on the mGuard is the same as described previously, except for the **Tunnel Settings**:

The screenshot shows the configuration page for an IPsec VPN connection named 'Netgear'. The 'Tunnel Settings' section is expanded, showing the following configuration:

Options	
A descriptive name for the connection	Netgear
Enabled	No
Address of the remote site's VPN gateway (either an IP address, a hostname, or %any)	netgear.dyndns.org
Connection startup (Will be ignored in Stealth Mode.)	Initiate

Tunnel Settings	
Connection type	Tunnel (Net <-> Net)
Local network	172.16.106.0/24
Remote network	192.168.0.0/24
The virtual IP which will be used by the client in Stealth mode	172.16.106.1
Enable 1-to-1 NAT to a different internal network in router mode	No
Internal network for 1-to-1 NAT	192.168.2.1

- Specify as **Local network** the virtual transfer network, in our example 172.16.106.0/24.
- Specify as **Remote network** the internal network IP of the FVS338.
- Enter as **virtual IP which will be used by the client in Stealth mode** the virtual IP of the client, in our example 172.16.106.1. This IP address must belong to the virtual transfer network and is used for accessing the client through the VPN tunnel from the internal network of the FVS338.

6 Troubleshooting

You can retrieve information about the status of the VPN connection from the menus **IPsec VPN -> IPsec Status** and **Logging -> Browse local logs** (option *IPsec VPN*).

Establishing a VPN tunnel connection consists of two phases: phase 1 (ISAKMP SA, key exchange) and phase 2 (IPsec SA, data exchange). In case of a successful connection the status of **ISAKMP** and **IPsec** should be *established* (menu **IPsec VPN -> IPsec Status**).

IPsec VPN » IPsec Status					
Connection Name	Connection			ISAKMP State	IPsec State
Netgear	Gateway	10.1.80.20	85.216.65.161	STATE_MAIN_I4 (ISAKMP SA established) Lifetime:2634s	STATE_QUICK_I2 (sent QI2, IPsec SA established) Lifetime:28229s
	Traffic	192.168.27.0/24	192.168.0.0/24		
	ID	CN=mGuard, C=de, L=Berlin, ST=Germany	CN=Netgear		

6.1 ISAKMP couldn't be established

If establishing the ISAKMP SA has failed this could be caused by the following reasons:

- Check if *User Password* is enabled (menu *User Authentication -> Local Users*) on the mGuard. If this is the case the VPN connection can only be established after entering the corresponding password. The login screen appears on the web browser when trying to access any webpage through http.
- Mismatched pre-shared keys or certificates.
- The mGuard is configured to use PFS but PFS is not enabled on the FVS338.
- Mismatched ISAKMP policy parameters.

6.2 IPsec couldn't be established

If the ISAKMP SA could be established but not the IPsec SA, this could be caused by the following reasons:

- Mismatched IPsec policy parameters.
- Mismatch in the specified VPN subnets.