

Interoperability Guide

Setting up a VPN connection between
mGuard and Check Point NGX (R60)



***mGuard
smart***



***mGuard
PCI***



***mGuard
blade***



***mGuard
industrial***

© Innominate Security Technologies AG

November 2005

"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 patent #10138865. 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: 571009-164


TABLE OF CONTENTS

1	Introduction.....	4
1.1	<i>mGuard in Router modes (Router/PPPoE/PPTP).....</i>	4
1.2	<i>mGuard in Stealth mode.....</i>	5
2	Limitations	6
3	Certificates.....	6
3.1	<i>Create and export the CA with XCA.....</i>	6
3.2	<i>Import the CA on the Check Point.....</i>	7
3.3	<i>Create an export a certificate request on the Check Point.....</i>	8
3.4	<i>Sign the Check Point certificate request with the CA.....</i>	9
3.5	<i>Export of the signed Check Point certificate.....</i>	9
3.6	<i>Import of the certificate on the Check Point.....</i>	9
3.7	<i>Create the mGuard certificate and export it as PKCS#12.....</i>	10
4	Configuring the Check Point NGX.....	11
4.1	<i>Interfaces.....</i>	11
4.2	<i>Global properties.....</i>	12
4.3	<i>Create a new policy package.....</i>	13
4.4	<i>Configure network object for the internal networks.....</i>	14
4.4.1	<i>Check Point</i>	14
4.4.2	<i>mGuard.....</i>	14
4.5	<i>VPN configuration on the Check Point network object.....</i>	15
4.6	<i>Configure the interoperable device (mGuard).....</i>	17
4.6.1	<i>Configuration of the interfaces.....</i>	17
4.6.2	<i>VPN configuration.....</i>	19
4.7	<i>Configure the policy rule.....</i>	20
5	Configuring the mGuard.....	21
5.1	<i>mGuard in Router mode (Router/PPPoE/PPTP).....</i>	21
5.1.1	<i>Menu: VPN -> Connections</i>	21
5.1.2	<i>Menu: VPN -> Machine Certificate</i>	23
5.2	<i>mGuard in Stealth mode.....</i>	23
6	Troubleshooting	24
6.1	<i>ISAKMP couldn't be established.....</i>	24
6.2	<i>IPsec couldn't be established.....</i>	24

1 Introduction

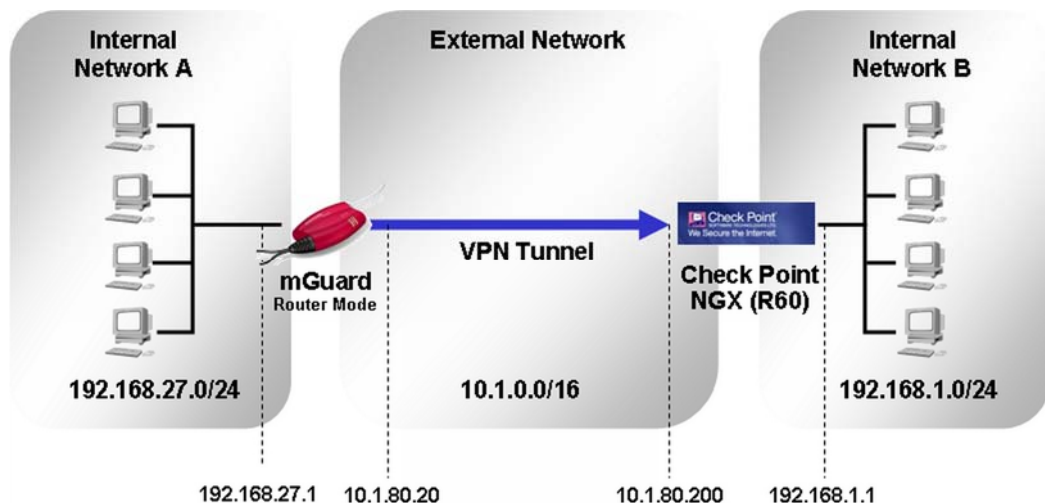
This document describes the required steps to configure a VPN tunnel between the mGuard and the Check Point NGX (R60). We have used a Check Point NGX R60 (Build 244) and an mGuard v3.0.1 for this interoperability test.

The VPN tunnel will be initiated by the mGuard. This document describes the usage of the authentication methods PSK (Pre-shared Secret Key) and 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. Note that we are in a virtual environment and therefore all used IP addresses are from the private address space. The examples used in this document are taken from this setup.

1.1 mGuard in Router modes (Router/PPPoE/PPTP)

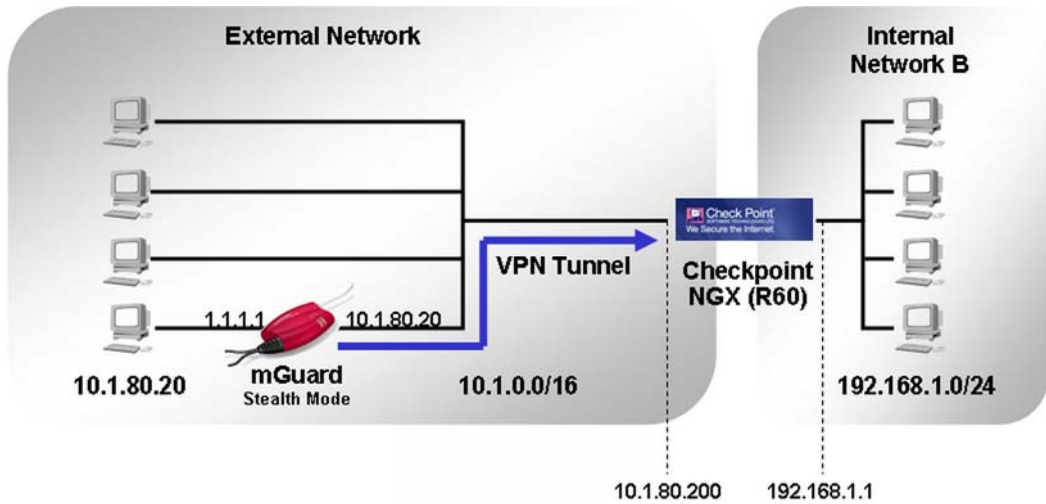


Scenario used for the setup of the VPN tunnel between mGuard (Router mode) and Check Point NGX

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:

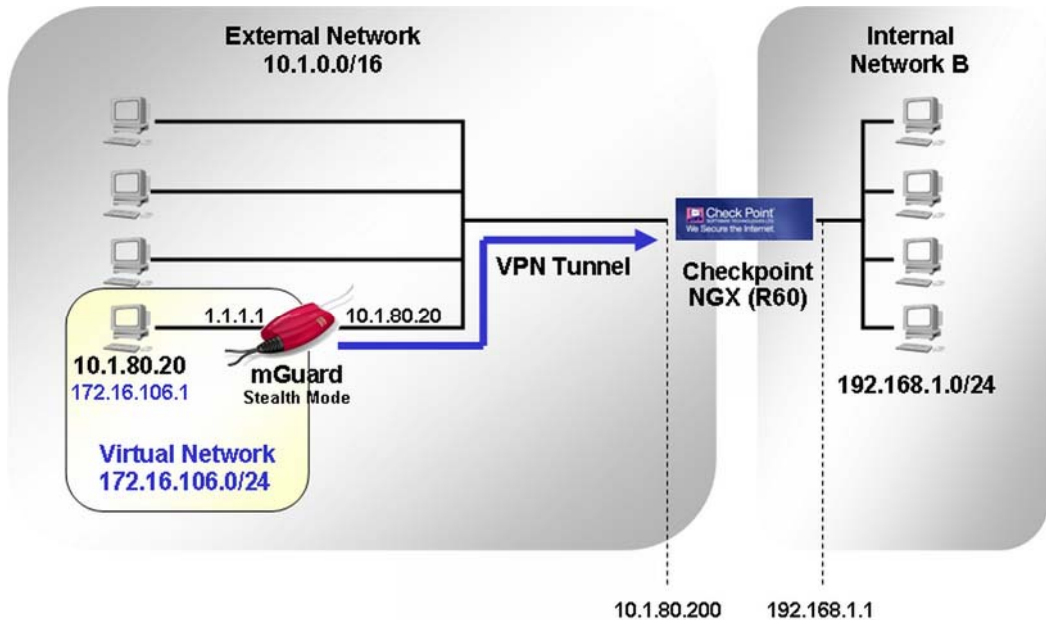
	mGuard	Check Point NGX
Remote VPN gateway	10.1.80.200	10.1.80.20 or dynamic
Local VPN subnet	192.168.27.0/255.255.255.0	192.168.1.0/255.255.255.0
Remote VPN subnet	192.168.1.0/255.255.255.0	192.168.27.0/255.255.255.0
IKE Policy, Encryption/Hash	3DES/MD5	3DES/MD5
IPsec Policy, Encryption/Hash	3DES/MD5	3DES/MD5

1.2 mGuard in Stealth mode



Scenario used for the setup of the VPN tunnel between mGuard (Stealth mode) and Check Point NGX

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 internal network B.




Scenario used for the setup of the VPN tunnel between mGuard (Stealth mode) and Check Point NGX

2 Limitations

- Using pre-shared keys (PSK) is not possible if the mGuard has either a dynamic public IP address or if the connection will be established across one or more gateways that have *Network Address Translation* (NAT) activated. In those cases *Aggressive Mode* would be required which is not supported by the mGuard in the current version. You should use certificates instead of PSK. Apart of this the Check Point NGX requires to use certificates if the external interface's IP address of the remote peer is assigned dynamically by the ISP.
- Dead Peer Detection (DPD) is not supported by the Check Point NGX.

3 Certificates

The Check Point already has a CA which is called *internal_ca*. We can't use this CA because it is not possible to create a new certificate for the mGuard signed by this CA and it is also not possible to export the private key of this CA. Therefore we need to use a separate tool for creating a new CA and the required 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 Check Point always uses an IP address as VPN identifier. As far as we could see during the interoperability test it is not possible to configure the Check Point to use a FQDN or a distinguished name as VPN identifier. This needs to be considered when creating the Check Point certificate because the IP address must be present as *subject alternative name* in the certificate.

The following certificates are required:

- The **CA** as PEM export. The CA needs to be imported on the Check Point and is also used for signing the mGuard and the Check Point certificates.
- The **Check Point certificate** (signed by the CA) as PEM export. This certificate needs to be imported on the Check Point as host certificate and on the mGuard as connection certificate.
- The **mGuard certificate** (signed by the CA) as PKCS#12 export. This certificate needs to be imported on the mGuard as machine certificate.

3.1 Create and export the CA with XCA

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_Key) 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.

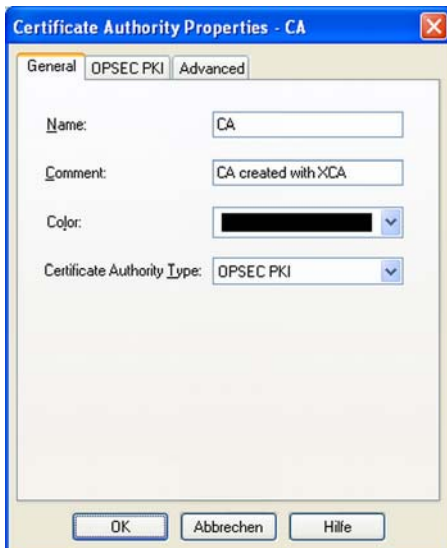
Export of the CA as PEM

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

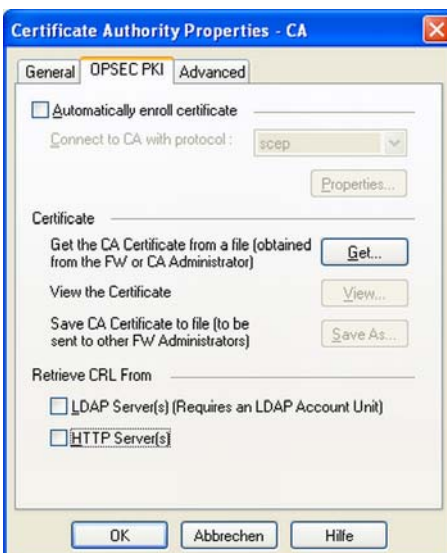
In our example we have named the file *CA.crt*.

3.2 Import the CA on the Check Point

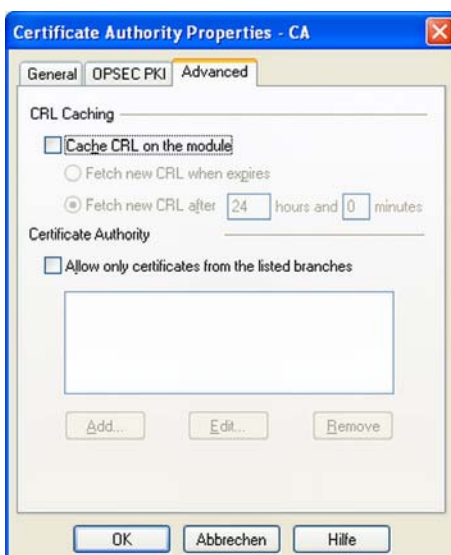
- From the menu, select **Manage -> Servers and OPSEC Applications....**
- Click **New** and select **CA -> Trusted...** from the menu.



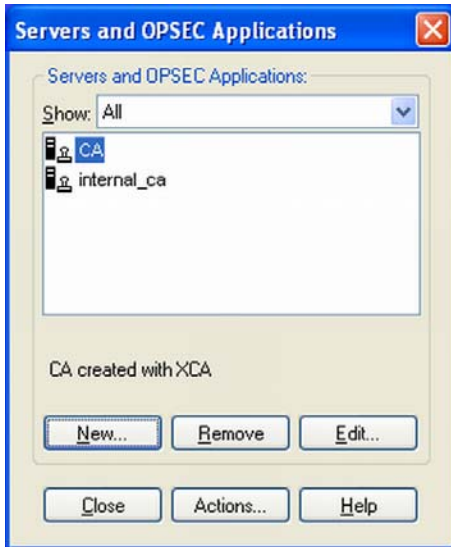
- Enter a descriptive **Name** and set **Certificate Authority Type** to **OPSEC PKI**.
- Switch to the tab **OPSEC PKI**.



- Disable the options in the **Retrieve CRL From** section (we don't use the CRL in this interoperability test).
- Click **Get**.
- Load the CA you have created in the previous chapter (in our example *CA.crt*). You'll be prompted to accept the Certificate Authority certificate.
- Switch to the tab **Advanced**.



- Disable **CRL caching** (we don't use the CRL in this interoperability test).
- Click **OK**.



- The imported CA is displayed.
- Click **Close**.

3.3 Create an export a certificate request on the Check Point

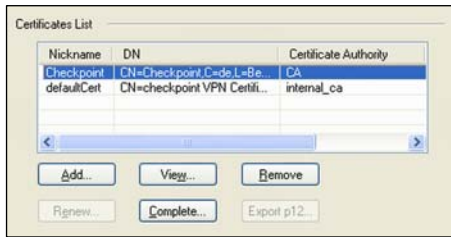
- From the menu, select **Manage -> Network Objects...**
- Select the Check Point network object and click **Edit**.
- Ensure in the **General Properties** page that the *Check Point Product VPN* is enabled.
- Switch to the **VPN** page and click **Add** in *Certificate List*.



- Enter a name for the certificate.
- Select as certificate authority the CA you've imported in the previous step.
- Click **Generate**.



- Enter the distinguished name (DN) of the certificate (in our example we have used CN=Checkpoint, C=de, L=Berlin, ST=Germany, O=Innominate, OU=Support, Email=support@innominate.com).
- Click **OK**.



- The certificate request is displayed in the *Certificate List*. To export the request, highlight the request and click **View**.



- Click **Save To File...** and save the certificate request to the local system. In our example we have named the file *Checkpoint.req*.

3.4 Sign the Check Point certificate request with the CA

- In XCA, switch to the **Certificate signing requests** tab.
- Click **Import** and import the certificate request of the Check Point you have created in the previous step (in our example *Checkpoint.req*).
- Make a right click at the imported certificate request and select **Sign**.
- Click **Next**.
- Enable **Use this certificate for signing** and select the CA you've created in step 1. Click **Next**.
- Enter into the field **Time Range** the lifetime of the certificate, click **Apply**.
- Enter into the field **subject alternative name** the external IP of the Check Point, using the format IP:<IP Address>. In our example we have entered *IP:10.1.80.200*. Click **Next**.
- Now you only need to confirm the appearing input masks by selecting **Next** until the certificate has been signed.
- Switch to the tab **Certificates**. The signed certificate of the Check Point is located beneath the CA.

3.5 Export of the signed Check Point certificate

- Switch to the tab **Certificates**.
- Select the signed certificate of the Check Point which is located beneath the CA and click **Export**.
- Chose **PEM** as **Export Format** and click **OK**.

In our example we have named the certificate *Checkpoint.crt*.

This export needs to be imported on the Check Point and on the mGuard as connection certificate.

3.6 Import of the certificate on the Check Point

- From the menu, select **Manage -> Network Objects....**
- Select the Check Point network object and click **Edit**.
- Switch to the **VPN** page, highlight the Check Point certificate request in the *Certificates List*, click **Complete** and load the signed Check Point certificate. You'll be prompted to accept the certificate.

3.7 Create the mGuard certificate and export it as PKCS#12

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 selected and that the CA is selected in the drop-down box.
- Set **Template for the new certificate** to **Client Template** and click **Next**.
- Enter a **Name** for the **New Key** if prompted 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 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 *VPN* -> *Machine certificate*).

4 Configuring the Check Point NGX

We have used the Check Point *Smart Dashboard* for configuring the device.

4.1 Interfaces

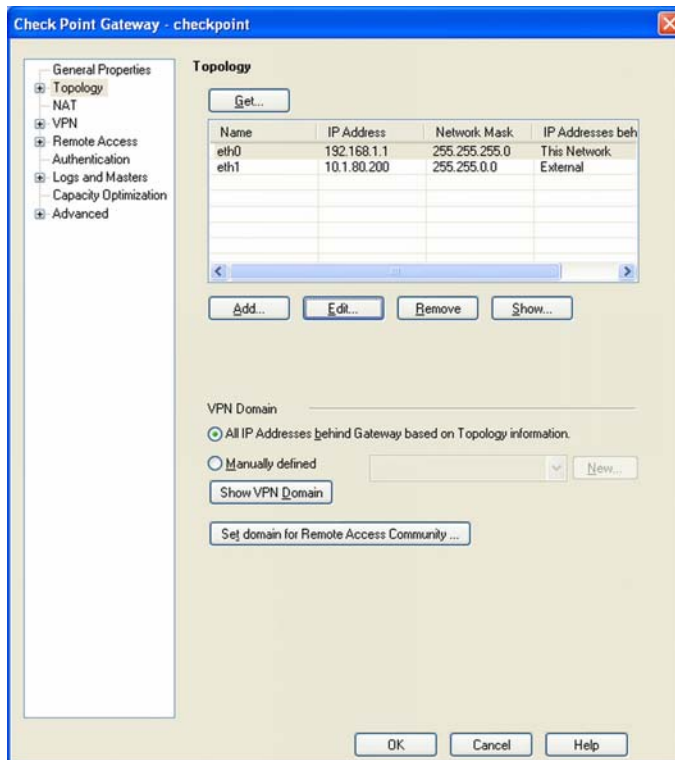
The interfaces were configured as follows:



Name	Type	IP Address	Netmask	Status	Details
eth0	Ethernet	192.168.1.1	255.255.255.0	up	
eth1	Ethernet	10.1.80.200	255.255.0.0	up	

eth0 is the internal interface, *eth1* the external. This also needs to be specified in the network object definition of the Check Point. To do this:

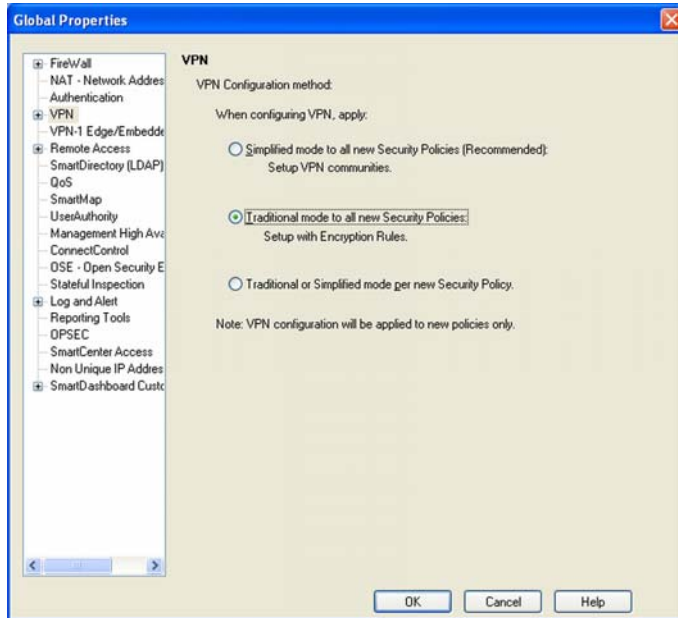
- From the menu, select **Manage -> Network Objects....**
- Select the Check Point network object and click **Edit**.
- Switch to the **Topology** page.



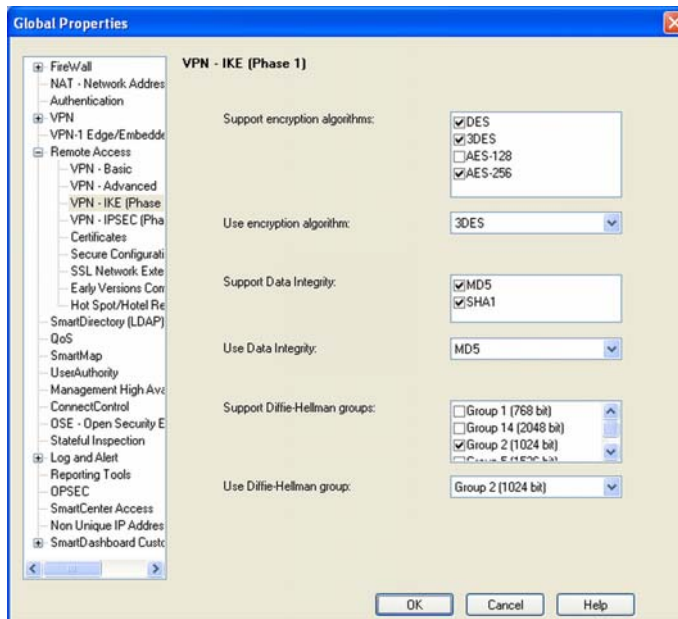
- Select the first interface, click **Edit** and specify in the tab *Topology*, if this is the external or internal interface.
- Repeat the previous step for the second interface.
- Click **OK**.

4.2 Global properties

- From the menu, select **Policy -> Global Properties**.
- Switch to the **VPN** page.

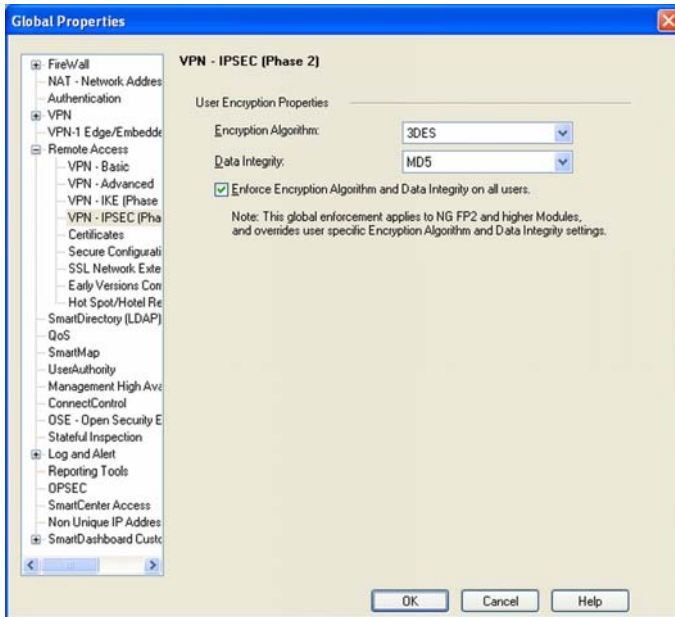


- Enable **Traditional mode to all new Security Policies**.
- Switch to the **Remote Access -> VPN – IKE (Phase 1)** page.

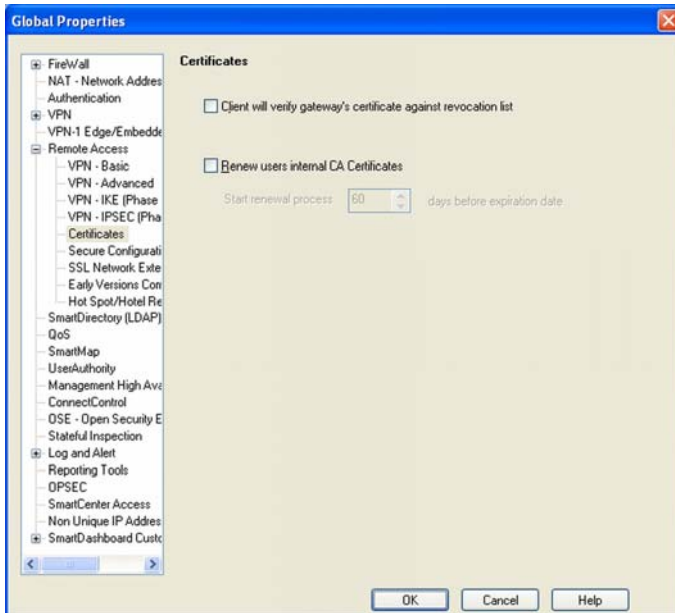


- Enable in the section **Support encryption algorithms** the encryption algorithms that will be supported with remote hosts. In our example we want to use 3DES. Therefore 3DES must be enabled.
- Choose in the section **Use encryption algorithms** the encryption algorithm that will have the highest priority of the selected algorithms. If given a choice of more than one encryption algorithm to use, the algorithm selected in this field will be used.
- Select in the section **Support Data Integrity** the hash algorithms that will be supported with remote hosts to ensure data integrity. In our example we want to use MD5. Therefore MD5 must be enabled.

- Choose in the section **Use Data Integrity** which hash algorithm will be given the highest priority if more than one choice is offered.
- Verify that **Group 2(1024 bit)** is enabled in the section **Support Diffie-Hellman groups** and select this group in the section **Use Diffie-Hellman group**.
- Switch to the **Remote Access -> VPN – IPSEC (Phase 2)** page.



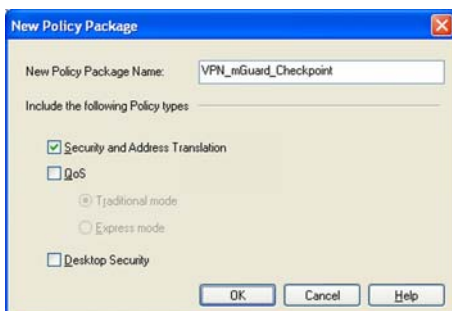
- Specify the **Encryption Algorithm** and **Data Integrity** (hash algorithm) which shall be used for the IPsec security association (SA) negotiation, in our example 3DES and MD5.
- Switch to the **Remote Access -> Certificates** page.



- We don't want to verify the certificates against the certificate revocation list (CRL) in this interoperability test. Therefore we have disabled this option.

4.3 Create a new policy package

- From the menu, select **File -> New**.

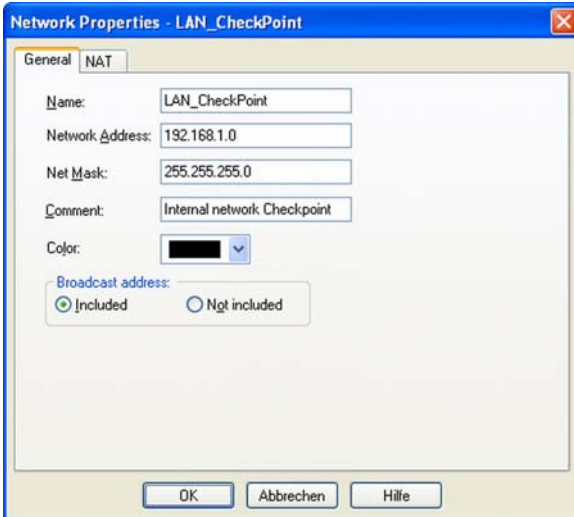


- Enter a descriptive name for the policy package.
- Enable **Security and Address Translation**.
- Click **OK**.

4.4 Configure network object for the internal networks

4.4.1 Check Point

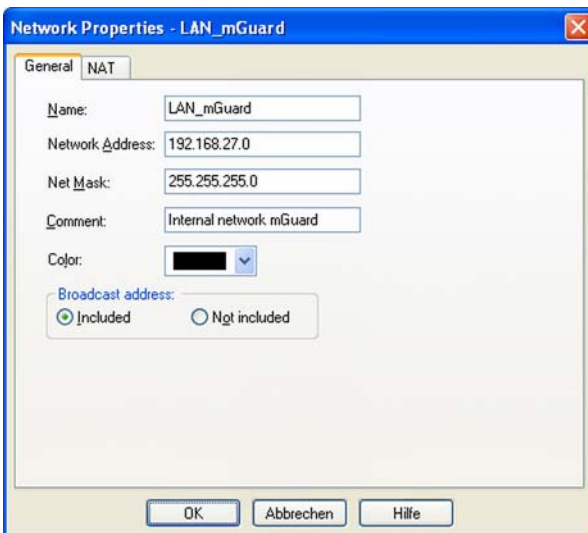
- From the menu, select **Manage -> Network Objects....**
- Click **New** and select **Network** from the menu.



- Enter a descriptive **Name** for the network object.
- Enter into the field **Network Address** the network IP of the internal network of the Check Point, in our example 192.168.1.0.
- Enter into the field **Net Mask** the corresponding subnet mask, in our example 255.255.255.0.
- Click **OK**.

4.4.2 mGuard

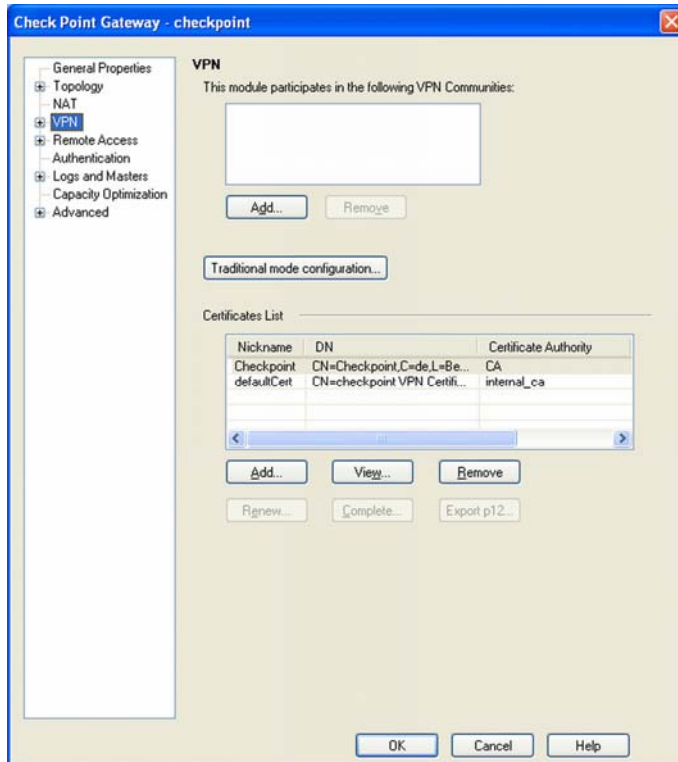
- From the menu, select **Manage -> Network Objects....**
- Click **New** and select **Network** from the menu.



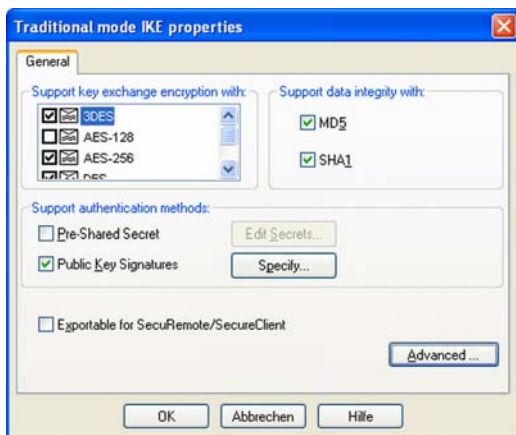
- Enter a descriptive **Name** for the network object.
- Enter into the field **Network Address** the network IP of the internal network of the mGuard, in our example 192.168.27.0.
- Enter into the field **Net Mask** the corresponding subnet mask, in our example 255.255.255.0.
- Click **OK**.

4.5 VPN configuration on the Check Point network object

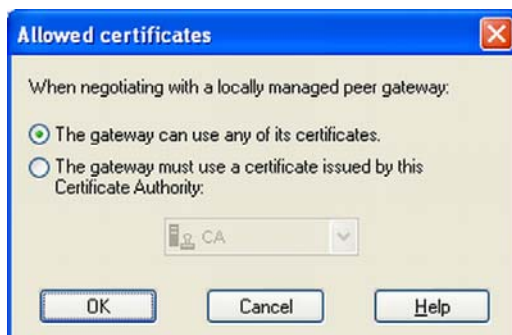
- From the menu, select **Manage -> Network Objects...**
- Select the Check Point network object and click **Edit**.



- Switch to the **VPN** page and click **Traditional mode configuration**.



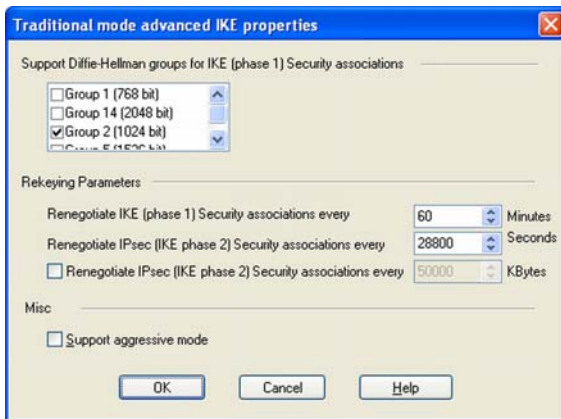
- Specify the supported **encryption** method used for key exchange.
- Specify the supported **data integrity** method used in the IKE negotiation.
- Select either **Public Key Signature** for using certificates or **Pre-Shared Secret** for using PSK as authentication method. If you use **Pre-Shared Secret** then you don't need to click **Edit Secret** for specifying the shared secret. This will be done later when configuring the network object for the mGuard.
- When using certificates, click **Specify**.



- Enable the option **The gateway can use any of its certificates**. This is important if there are already configured VPN connections on the device which use certificates signed by the *internal_ca*. Note that the mGuard will use the Check Point certificate signed by the CA which was previously imported.
- Click **OK**.

VPN between mGuard and Check Point NGX (R60)

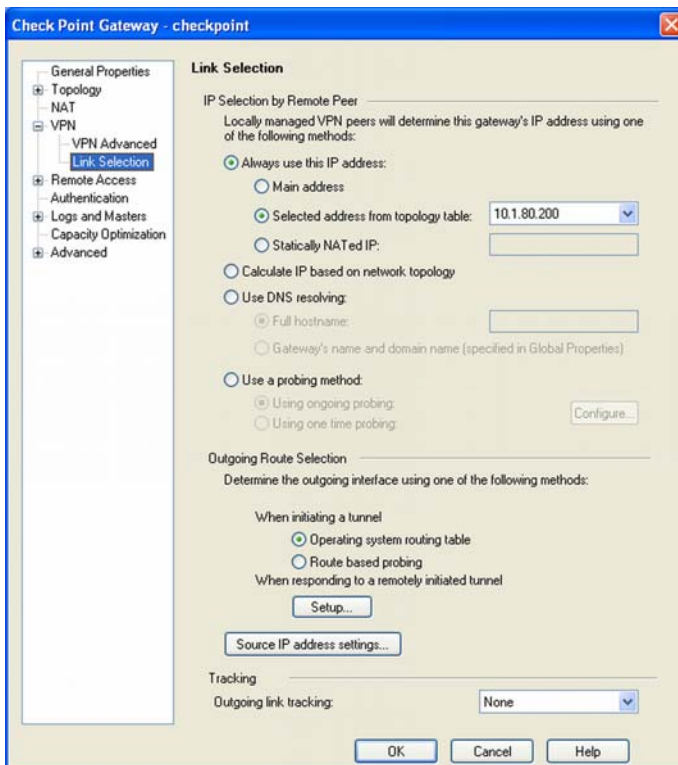
- Click **Advanced** in the *Traditional mode IKE properties* window.



- Specify the **Diffie-Hellman group** for the IKE SA, in our example **Group 2 (1024 bit)**.
 - Adjust the lifetimes of the ISAKMP SA (=IKE phase 1) and IPsec SA to the settings on the mGuard. The default settings on the mGuard are 3600 seconds for the ISAKMP SA and 28800 seconds for the IPsec SA.
 - Click **OK**.
- ⇒ The *Traditional mode advanced IKE properties* window is closed.
- Click **OK** for closing the *Traditional mode IKE properties* window.

As already mentioned before, the Check Point uses an IP address as VPN identifier. The IP address that will be used needs to be defined in the *Link Selection*.

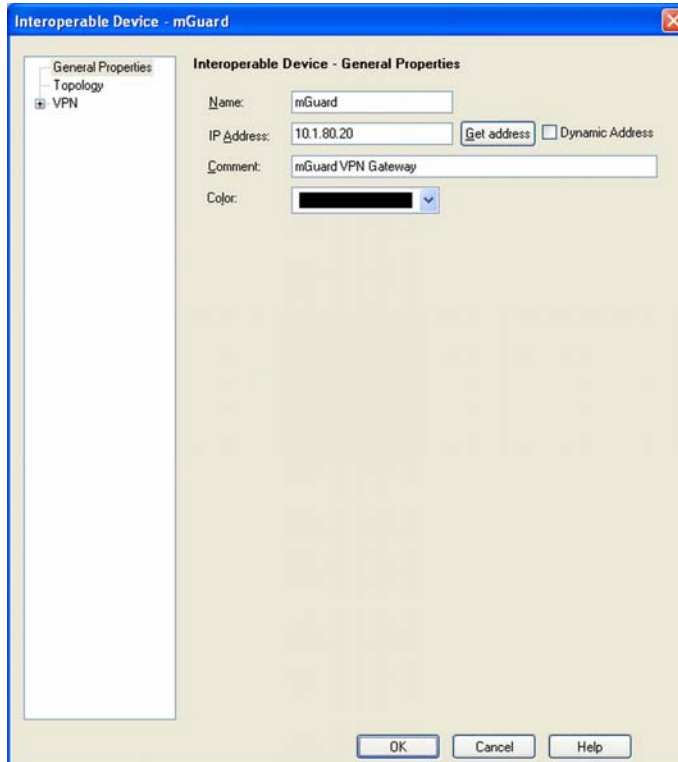
- Switch to the **VPN -> Line Selection** page.



- Enable **Always use this IP address**.
- Enable **Selected address from topology table** and select the IP address of the external interface.
- Click **OK**.

4.6 Configure the interoperable device (mGuard)

- From the menu, select **Manage -> Network Objects...**
- Click **New** and select **Interoperable Device...** from the menu.



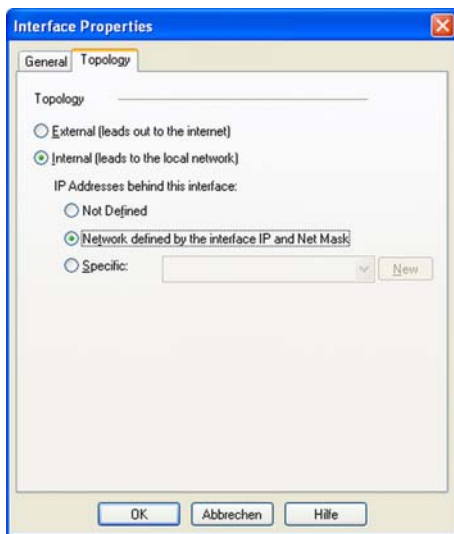
- Enter a descriptive **Name** for the device.
- If the mGuard has a static public IP address, enter it into the field **IP address**. Otherwise select **Dynamic Address**.

4.6.1 Configuration of the interfaces

- Switch to the **Topology** page and click **Add**.



- Enter a descriptive **Name** for the internal interface.
- Enter the **IP Address** and the corresponding **Net Mask** of the internal interface of the mGuard, in our example 192.168.27.1/255.255.255.0.
- Switch to the **Topology** tab.



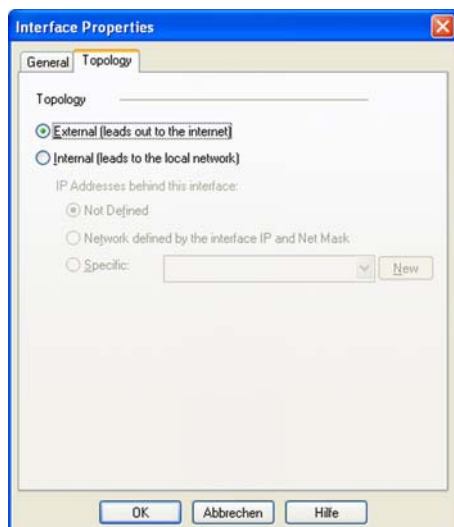
- Select **Internal** and **Network defined by the interface IP and Net Mask**.
- Click **OK**.

The previous steps need to be repeated for configuring the external interface:

- In the **Topology** page click **Add**.



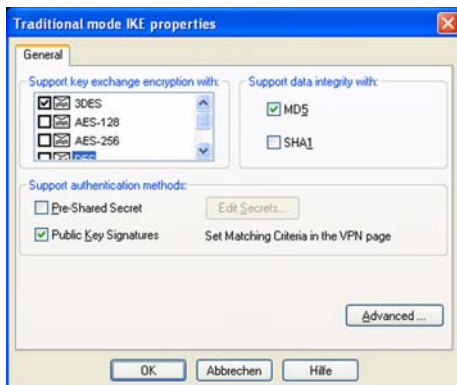
- Enter a descriptive **Name** for the external interface.
- If the mGuard has a static public IP address, enter the **IP Address** and the corresponding **Net Mask** of the external interface, in our example 10.1.80.20/255.255.0.0.
- If you have specified in the **General Properties** page, that the mGuard has a dynamic address, the option **Dynamic IP** is displayed. Select this option if the mGuard has a dynamically assigned IP address.
- Switch to the **Topology** tab.



- Enable **External** and click **OK**.

4.6.2 VPN configuration

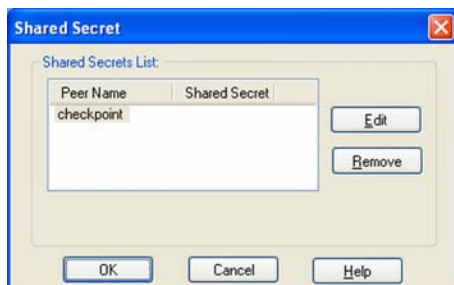
- Switch to the **VPN** page and click **Traditional mode configuration**.



- Specify the supported **encryption** method used for key exchange, in our example 3DES.
- Specify the supported **data integrity** method used in the IKE negotiation, in our example MD5.
- Select either **Public Key Signature** for using certificates or **Pre-Shared Secret** for using PSK as authentication method.

The following two steps are only required when using PSK:

- Click **Edit Secret**.

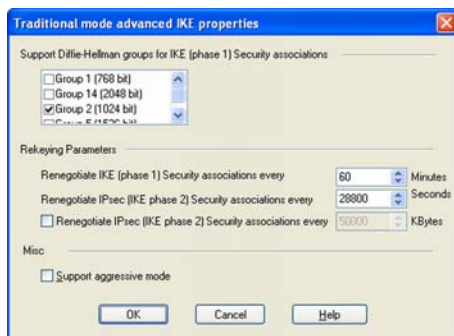


- Highlight the Check Point object.
- Click **Edit**.



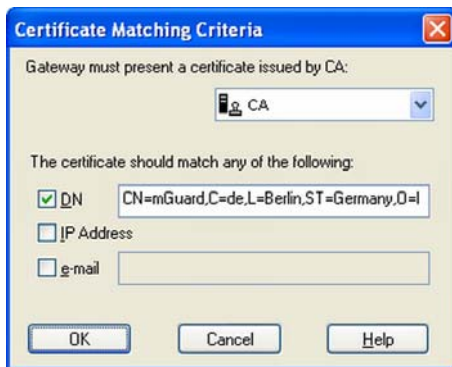
- Enter the shared secret.
- Click **Set**.
- Click **OK**.

- Click **Advanced** in the *Traditional mode IKE properties* window.



- Specify the **Diffie-Hellman group** for the IKE SA, in our example **Group 2 (1024 bit)**.
- Adjust the lifetimes of the ISAKMP SA (=IKE phase 1) and IPsec SA to the settings on the mGuard. The default settings on the mGuard are 3600 seconds for the ISAKMP SA and 28800 seconds for the IPsec SA.
- Click **OK**.
- ⇒ The *Traditional mode advanced IKE properties* window will be closed.
- Click **OK** for closing the *Traditional mode IKE properties* window.

This step is only required when using certificates:



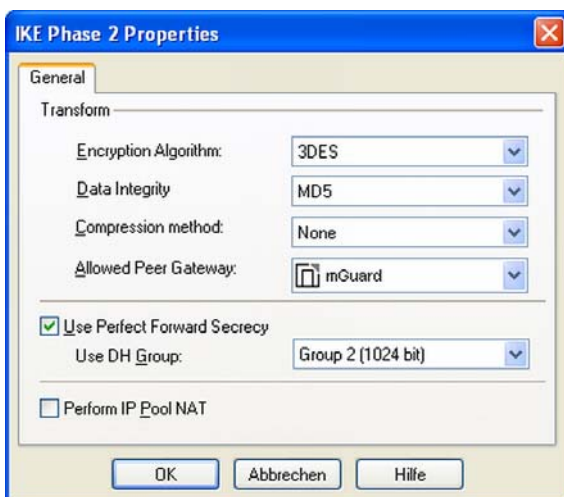
- In the **VPN** page click **Matching Criteria**.
- Select the CA you have created with XCA and uploaded to the Check Point in chapter *Import the CA on the Check Point*.
- Enable **DN** and enter the distinguished name (DN) of the mGuard certificate, in our example CN=mGuard, C=de, L=Berlin, ST=Germany, O=Innominate, OU=Support, Email=support@innominate.com.
- Click **OK**.

4.7 Configure the policy rule

- From the menu, select **Rules -> Add Rules -> Top**.

NO.	NAME	SOURCE	DESTINATION	SERVICE	ACTION
1	VPN mGuard Checkpoint	mGuard LAN_mGuard	checkpoint LAN_CheckPoint	* Any	Encrypt

- Make a right click at the **NAME** entry, click **Edit** and enter a descriptive name for the policy rule.
- Make a right click at the **SOURCE** entry, use the option **Add** to add the network objects of the mGuard and of the mGuard LAN.
- Make a right click at the **DESTINATION** entry, use the option **Add** to add the network objects of the Check Point and of the Check Point LAN.
- Make a right click at the **ACTION** entry and select **Encrypt**.
- Make a double click at **Encrypt**, verify that **IKE** is selected and click **Edit**.



- Specify the encryption and hash algorithms for IKE Phase 2. Those values must correspond to the settings on the mGuard (menu *VPN -> Connections, More IKE Options, ISsec SA (Data Exchange)*).
- Select as **Allowed Peer Gateway** the network object of the mGuard.
- If required, enable **Use Perfect Forward Secrecy** and specify **Group 2**. If you enable PFS on the Check Point then you also need to enable this option on the mGuard (menu *VPN -> Connections, More IKE Options*).
- Click **OK**.

Finally you need to install the policy:

- From the menu, select **Policy -> Install** and confirm the appearing screens.

5 Configuring the mGuard

5.1 mGuard in Router mode (Router/PPPoE/PPTP)

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

- Configuration of the VPN connection through the menu **VPN -> Connections**.
- If certificates are used as authentication method: Import of the mGuard machine certificate through the menu **VPN -> Machine certificate**.

5.1.1 Menu: VPN -> Connections

- Select **VPN -> Connections** from the menu and click **New**.
- Enter a descriptive name for the connection (e.g. Check Point) and click **Edit**.

VPN > Connections > Connection Check Point

A descriptive name for the connection	Check Point
Enabled	Yes
Address of the remote site's VPN gateway (either an IP address, a hostname, or %any)	10.1.80.200
Authentication method	X.509 Certificate <input type="button" value="Configure"/>
Connection type	Tunnel (Net <-> Net)
Connection startup (Will be ignored in Stealth Mode.)	Start connection to... ...remote VPN gateway
More IKE Options	<input type="button" value="Configure"/>

Tunnel Settings

Local network address	192.168.27.0
The appropriate local netmask	255.255.255.0
The virtual IP which will be used by the client in Stealth mode	192.168.1.1
Remote network address	192.168.1.0
The appropriate remote netmask	255.255.255.0

Firewall Incoming (untrusted port)

Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log
<input type="checkbox"/> All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	default rule - please	No
Log entries for unknown connection attempts							No

Firewall Outgoing (trusted port)

Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log
<input type="checkbox"/> All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	default rule - please	No
Log entries for unknown connection attempts							No

- Enter as **Address of the remote site's VPN gateway** the external IP address of the Check Point (in our example *10.1.80.200*).
- Set **Authentication Method** either to **Pre-Shared Secret** or to **X.509 Certificate**, depending on the authentication method you want to use. Click **Configure**. If you use *Pre-shared Keys* then enter the shared secret. Otherwise you need to import the Check Point host certificate (in our example *Checkpoint.crt*).
- Set **Connection type** to **Tunnel (Net <-> Net)** for a VPN tunnel connection.

VPN between mGuard and Check Point NGX (R60)

- The mGuard should initiate the connection. Therefore set **Connection Startup** to **Start connection to**
- **Tunnel settings:**
 - **Local network and netmask:** These parameters specify the VPN subnet (internal network) of the mGuard (in our example *192.168.27.0/255.255.255.0*).
 - **The virtual IP which will be used by the client in stealth mode:** This entry is only required if the mGuard is operated in *Stealth* mode and will be explained in the next chapter.
 - **Remote network and netmask:** These parameters specify the VPN subnet (internal network) of the Check Point (in our example *192.168.1.0/255.255.255.0*).
- Click **Configure** in the line *More IKE Options*.

The screenshot shows the configuration page for 'More IKE Options' under 'VPN > Connections > Connection Check Point'. The page is divided into several sections:

- ISAKMP SA (Key Exchange):** Encryption Algorithm is set to 3DES-168, and Hash Algorithm is set to MD5.
- IPsec SA (Data Exchange):** Encryption Algorithm is set to 3DES-168, Hash Algorithm is set to MD5, and Perfect Forward Secrecy (PFS) is set to Yes.
- Lifetimes:** ISAKMP SA Lifetime (seconds) is 3600, IPsec SA Lifetime (seconds) is 28800, Rekeymargin (seconds) is 540, Rekeyfuzz (percent) is 100, Keying tries (0 means unlimited tries) is 0, and Rekey is set to Yes.
- Dead Peer Detection:** Action is set to Hold (Default), Delay is 30, and Timeout is 120.

A 'Back' button is located at the bottom of the form.

- **ISAKMP SA (Key Exchange):** The settings for **Encryption** and **Hash Algorithm** must be supported by the Check Point (*Check Point network object -> Remote Access -> VPN – IKE (Phase 1)*).
- **IPsec SA (Data exchange):** The settings for **Encryption** and **Hash Algorithm** must correspond to the settings on the Check Point.
- The **ISAKMP SA Lifetime** and **IPsec SA Lifetime** should correspond to the setting on the Check Point.
- Click **Back**.
- Click **OK**.

VPN between mGuard and Check Point NGX (R60)

If you use certificates then you also need to enter the VPN identifier (external IP address) used by the Check Point:

Remote ID Mode	Automatic (Default) ▼
Remote ID	10.1.80.200

- Enable the extended configuration web interface of the mGuard. To do this:
 - Add the user defined language *xt-ra* to the web browser.
 - Move this language to the top of the language selection list.
 - Set the language selection on the mGuard to *Automatic* (menu *Access -> Language*).
 - Refresh the screen.
- Select **VPN -> Connections** from the menu and edit the connection.
- Enter into the field **Remote ID** the external IP address of the Check Point.

5.1.2 Menu: VPN -> Machine Certificate

This step is only required if you use certificates. You need to import the PKCS#12 export of the mGuard certificate.

- Select **VPN -> Machine Certificate** from the menu.
- Click **Browse** and specify the mGuard machine certificate, in our example *mGuard.p12*.
- Enter into the field **password** the password which protects the certificate against unauthorized usage.
- Click **Import**.
- Click **OK** when the upload is finished!

5.2 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**:

Tunnel Settings	
Local network address	172.16.106.0
The appropriate local netmask	255.255.255.0
The virtual IP which will be used by the client in Stealth mode	172.16.106.1
Remote network address	192.168.1.0
The appropriate remote netmask	255.255.255.0

- Specify as **Local network address** the network IP of the virtual transfer network.
- Specify as **appropriate local netmask** the subnet mask of the virtual network.
- 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 be part of the virtual transfer network and is used for accessing the client through the VPN tunnel from the internal network of the Check Point.

Note that you also need to change the definition of the internal network of the mGuard on the Check Point correspondingly.

6 Troubleshooting

You can retrieve information about the status of the VPN connection from the menus **VPN -> IPsec Status** and **VPN -> VPN Logs**.

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

VPN > IPsec Status					
Connection Name	Connection		ISAKMP State	IPsec State	
Check Point	Gateway	10.1.80.20	10.1.80.200	STATE_MAIN_I4 (ISAKMP SA established) Lifetime: 1731s	
	Traffic	192.168.27.0/24	192.168.1.0/24		STATE_QUICK_I2 (sent GI2, IPsec SA established) Lifetime: 26993s
	ID	CN=mGuard, C=de, L=Berlin, ST=Germany, O=Innominate, OU=Support, E=support@innominate.com			
<input type="button" value="Update"/>					

6.1 ISAKMP couldn't be established

If the ISAKMP SA couldn't be established then this could be caused by the following reasons:

- mGuard in *Stealth* mode: Check if there is a desktop firewall (e.g. WinXP Firewall) or a VPN Client with integrated firewall (e.g. Checkpoint VPN Client) running on the client. The firewall must allow ICMP echo requests. The mGuard sends an ICMP echo request to the client for obtaining the MAC address of the default gateway before sending the request to the remote VPN gateway.
- Check if *User Password* is enabled (menu *Access -> Passwords*). 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 Check Point.
- Mismatched ISAKMP policy parameters.

6.2 IPsec couldn't be established

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

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