

Interoperability Guide

Setting up a VPN tunnel between
mGuard and Bintec VPN Access 25



mGuard smart



mGuard PCI



mGuard blade



mGuard industrial



mGuard delta


TABLE OF CONTENTS

1	Introduction	3
1.1	<i>mGuard in router modes (Router/PPPoE/PPTP)</i>	3
1.2	<i>mGuard in Stealth mode.....</i>	4
2	Limitations in using Pre-Shared Secret Keys (PSK)	5
3	Certificates.....	5
3.1	<i>VPN25, prior to version 7.2.1.....</i>	5
3.1.1	Step 1: Tool XCA - Create and export the CA	5
3.1.2	Step 2: VPN25 - Import of the CA	6
3.1.3	Step 3: VPN25 - Create an RSA key	6
3.1.4	Step 4: VPN25 - Request a certificate for the VPN25.....	7
3.1.5	Step 5: Tool XCA - Sign the certificate request with the CA	7
3.1.6	Step 6: VPN25 - Import of the signed certificate.....	8
3.1.7	Step 7: Tool XCA - Create and export the certificate for the mGuard.....	8
3.2	<i>VPN25, version 7.2.1.....</i>	9
3.2.1	Create the required certificates with the Tool XCA.....	9
3.2.2	Import of the CA on the VPN25	9
3.2.3	Import of the VPN25 host certificate (PKCS#12)	9
4	Configuring the VPN25	10
4.1	<i>Interfaces.....</i>	10
4.2	<i>Pre IPsec Rules.....</i>	10
4.3	<i>Remote peer configuration.....</i>	11
4.3.1	Peer address and peer ID/Pre Shared Key	11
4.3.2	IKE/IPsec proposal and lifetimes.....	12
4.3.3	VPN subnets.....	13
5	Configuring the mGuard.....	14
5.1	<i>mGuard in Router mode (Router/PPPoE/PPTP).....</i>	14
5.1.1	Menu: VPN -> Connections.....	14
5.1.2	Menu: VPN -> Machine Certificate.....	15
5.2	<i>mGuard in Stealth mode.....</i>	16
6	Troubleshooting	17
6.1	<i>ISAKMP couldn't be established.....</i>	17
6.2	<i>IPsec couldn't be established.....</i>	17

1 Introduction

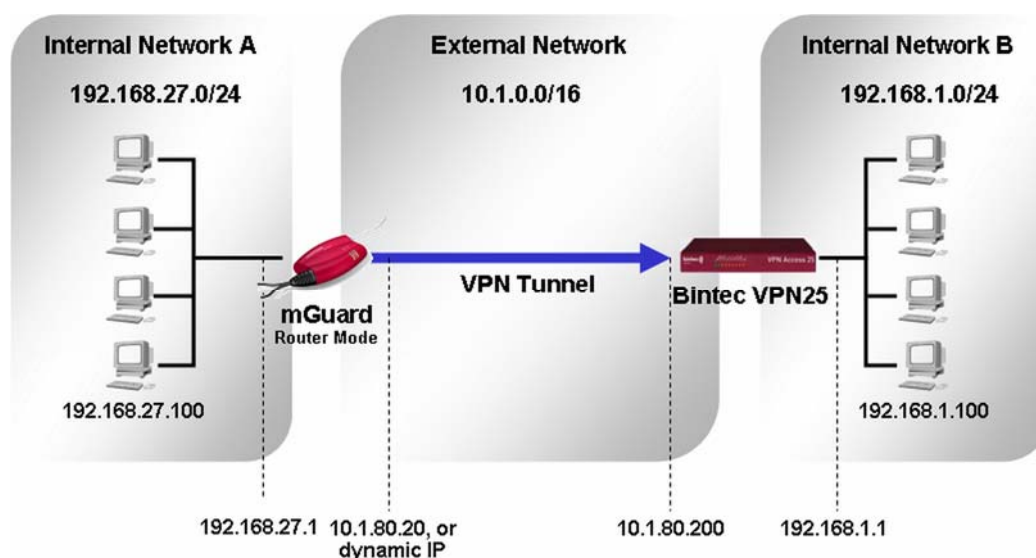
This document describes the required steps to configure a VPN tunnel between the mGuard and the Bintec VPN Access 25. We have used a Bintec VPN Access 25 v7.2.1 and an mGuard v3.1.1 for this interoperability test.

The VPN tunnel will be initiated by the mGuard. This document describes the usage of the authentication methods PSK (Pre-shared Secret Key) and 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. 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)



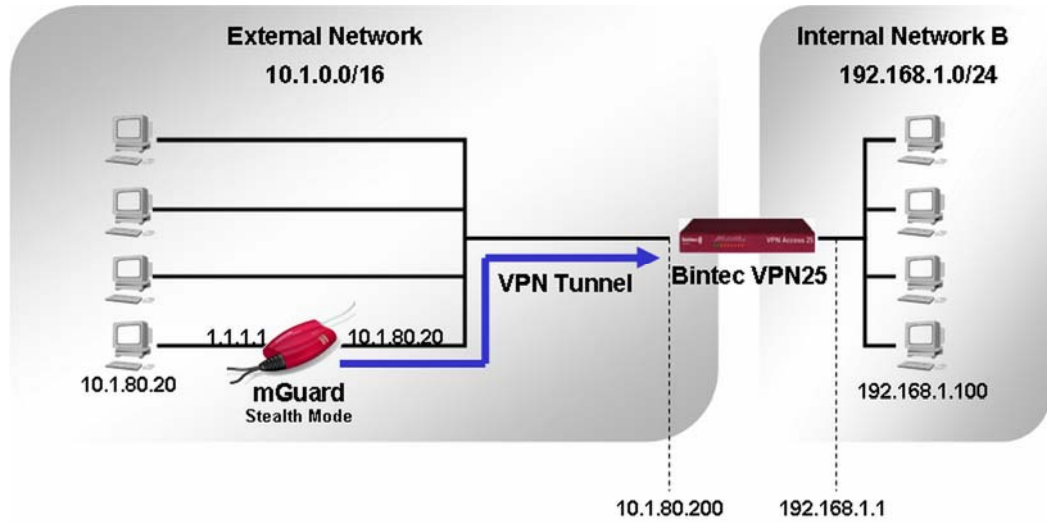
Scenario used for the setup of the VPN tunnel between mGuard (Router mode) and VPN25

 **Note:** If the mGuard has a dynamic public IP address, the mGuard needs to register its IP address under a fixed name in a DynDNS service and the VPN settings on the VPN25 must refer to this name.

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:

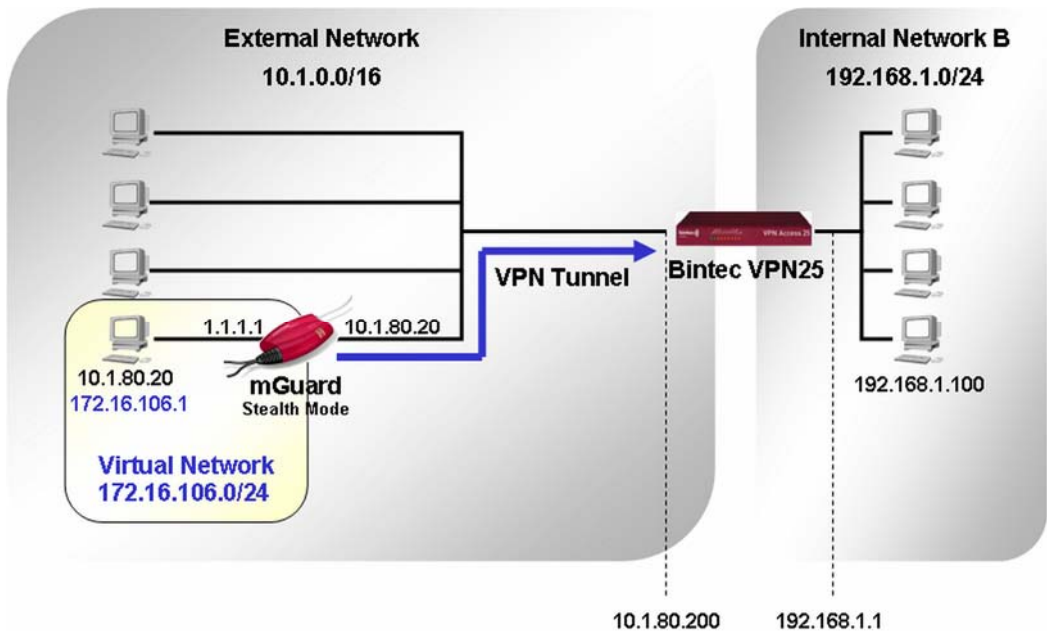
	mGuard	VPN25
Remote VPN gateway	10.1.80.200	10.1.80.20 or DynDNS name of the remote peer
Local VPN subnet	192.168.27.0/24	192.168.1.0/24
Remote VPN subnet	192.168.1.0/24	192.168.27.0/24
IKE Policy, Encryption/Hash	3DES/MD5	3DES/MD5
IPsec Policy, Encryption/Hash	3DES/MD5	3DES/MD5

1.2 mGuard in Stealth mode



Scenario used for the setup of the VPN tunnel between mGuard (Stealth mode) and VPN25

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 VPN25

2 Limitations in using Pre-Shared 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 VPN25 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.

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.

Starting with VPN25 version 7.2.1 is it possible to import the host certificate directly as PKCS#12 through the IPSEC wizard.

3.1 VPN25, prior to version 7.2.1

The following certificates are required:

- The **CA** as PEM export. The CA needs to be imported on the VPN25 and is also used for signing the mGuard and VPN25 certificates.
- The **VPN25 certificate** (signed by the CA) as PEM export. This certificate needs to be imported on the VPN25 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.

The following steps are required for creating the certificates:

- Step 1: Tool XCA - Create and export the CA
- Step 2: VPN25 - Import of the CA
- Step 3: VPN25 - Create an RSA key
- Step 4: VPN25 - Request a certificate for the VPN25
- Step 5: Tool XCA - Sign the certificate request with the CA
- Step 6: VPN25 - Import of the signed certificate
- Step 7: Tool XCA - Create and export the certificate for the mGuard

3.1.1 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_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*.

3.1.2 Step 2: VPN25 - Import of the CA

- From the menu, select **Advanced Configuration -> IPSEC -> Certificate and Key Management -> Certificate Authority Certificates**.
- Click **Download**.

VPN Access 25 HTML setup
vpn25
[IPSEC][CERTMGMT][CAS][GETCERT]: IPsec Configuration - Get Certificate

Import a Certificate/CRL using: TFTP

Type of certificate: Certificate Authority

Server: 192.168.1.100

Name: CA.crt auto

START EXIT

- Set **Import a Certificate/CRL using** to **TFTP**. The other possibility is to import the certificate with copy and paste.
- Enter into the field **Server** the IP address of the TFTP server.
- Enter into the field **Name** the filename of the CA export, in our example *CA.crt*.
- Click **Start**.

- Review the retrieved certificate and click **Import** and then **Exit**.
- ⇒ The imported CA is displayed in the list.
- Click **Exit**.

3.1.3 Step 3: VPN25 - Create an RSA key

You only need to perform this step if an RSA key doesn't exist.

- From the menu, select **Advanced Configuration -> IPSEC -> Certificate and Key Management -> Key Management**.
- Click **Create**.
- Enter a **Description** for the RSA key and click **Create**.
- ⇒ The message should appear that the key generation finished successfully.
- Click **Exit**.
- ⇒ The created key is displayed in the list.
- Click **Exit**.

3.1.4 Step 4: VPN25 - Request a certificate for the VPN25

- From the menu, select **Advanced Configuration -> IPSEC -> Certificate and Key Management -> Key Management**.
- Click **Request Cert**.

The screenshot shows the 'VPN Access 25 HTML setup' window with the following configuration:

- Key to enroll:** 1 (Bintec_RSA)
- Method:** Upload
- Subject Name:** CN=bintec, C=de, L=berlin, ST=germany, O=innominate, OU=supp
- Subject Alternative Names (optional):** All three entries are set to NONE.
- Signing algorithm to use:** md5WithRSAEncryption
- Server:** 192.168.1.100
- Filename:** BintecReq.crt (Format: base64)

- Select as **Key to enroll** the RSA key you have created in the previous step.
- Set **Method** to **Upload**.
- Enter the **Subject Name** of the certificate. In our example we have used *CN=bintec, C=de, L=Berlin, ST=Germany, O=Innominate, OU=Support, MAILTO=support@innominate.com*.
- Set all **Subject Alternative Names** to **None** (we don't use them in this interoperability test).
- Enter into the field **Server** the IP address of the TFTP server.

- Enter into the field **Filename** the filename of the certificate request, in our example *BintecReq.crt*.
 - Click **Start**.
- ⇒ The message should appear that the enrolment finished successfully.
- Click **Exit**.

3.1.5 Step 5: Tool XCA - Sign the certificate request with the CA

Import of the certificate request

- Switch to the **Certificate signing requests** tab.
- Click **Import** and import the certificate request of the VPN25 you have created in the previous step, in our example *BintecReq.crt*.

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 VPN25 appears beneath the CA.

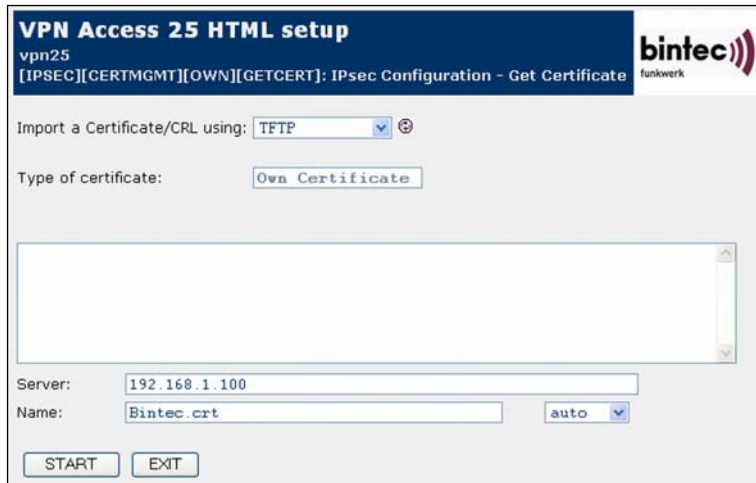
Export of the signed VPN25 certificate

- Highlight the signed VPN25 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 *Bintec.crt*. This certificate needs to be imported on the VPN25 as *Own Certificate* and on the mGuard as connection certificate (menu *VPN -> Connections*).

3.1.6 Step 6: VPN25 - Import of the signed certificate

- From the menu, select **Advanced Configuration -> IPSEC -> Certificate and Key Management -> Own Certificates**.
- Click **Download**.



- Set **Import a Certificate/CRL using** to **TFTP**. The other possibility is to import the certificate with copy and paste.
- Enter into the field **Server** the IP address of the TFTP server.
- Enter into the field **Name** the filename of the VPN25 certificate, in our example *Bintec.crt*.
- Click **Start**.

- Review the retrieved certificate and click **Import** and then **Exit**.
⇒ The imported certificate is displayed in the list.
- Click **Exit**.

3.1.7 Step 7: 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 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** 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*).

3.2 VPN25, version 7.2.1

The following certificates are required:

- The **CA** as PEM export. The CA needs to be imported on the VPN25 and is also used for signing the mGuard and VPN25 certificates.
- The **VPN25 certificate** (signed by the CA) as PEM and PKCS#12 export. The PKCS#12 export needs to be imported on the VPN25 as *Own Certificate*, the PEM 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.

3.2.1 Create the required certificates with the Tool XCA

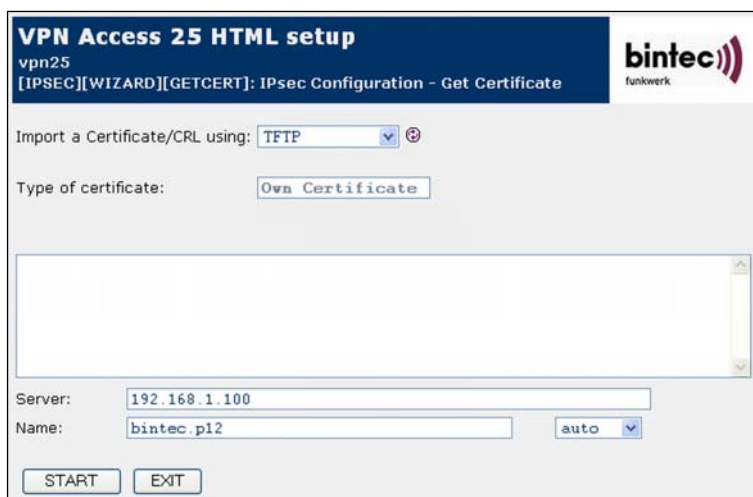
- Create and export the **CA** as described in chapter *Step 1: Tool XCA - Create and export the CA*. The CA needs to be uploaded on the VPN25.
- Create the **mGuard certificate** and export it as PKCS#12 as described in chapter *Step 7: Tool XCA - Create and export the certificate for the mGuard*. This export needs to be uploaded on the mGuard as machine certificate.
- Create the **VPN25 certificate** and export it as PKCS#12 and PEM as described in chapter *Step 7: Tool XCA - Create and export the certificate for the mGuard*. The PKCS#12 export needs to be uploaded on the VPN25 as *Own Certificate*. The PEM export needs to be uploaded on the mGuard as connection certificate.

3.2.2 Import of the CA on the VPN25

- Import the CA on the VPN25 as described in chapter *Step 2: VPN25 - Import of the CA*.

3.2.3 Import of the VPN25 host certificate (PKCS#12)

- From the menu, select **Advanced Configuration -> IPSEC**.
- Do you want to use the wizard? **Yes**
- Select the option **start wizard** and click **Go**.
- Set **Default IPSEC Authentication Method** to **RSA Signature** and click **Go**.
- Set **Request own certificate** to **skip** and click **Go**.
- Set **Import new own certificate** to **start** and click **Go**.



- Set **Import a Certificate/CRL using** to **TFTP**. The other possibility is to import the certificate with copy and paste.
- Enter into the field **Server** the IP address of the TFTP server.
- Enter into the field **Name** the filename of the VPN25 certificate, in our example *Bintec.p12*.
- Click **Start**.

- You need to enter the password which protects the PKCS#12 export against unauthorized usage three times (outer envelope, internal safe, shrouded key).
- Review the retrieved certificate and click **Import** and then **Exit**.

4 Configuring the VPN25

4.1 Interfaces

The interfaces were configured as follows (menu **Advanced Settings -> Ethernet Unit 1 / Ethernet Unit 2**).

VPN Access 25 HTML setup
vpn25
[SLOT 0 UNIT 1 ETH]: Configure Ethernet Interface

IP-Configuration: Manual
 local IP-Number: 192.168.1.1
 local Netmask: 255.255.255.0
 Second Local IP-Number:
 Second Local Netmask:
 Encapsulation: Ethernet II
 Mode: Auto
 MAC Address:
 Bridging: disabled

[Advanced Settings >](#)
[Virtual Interfaces >](#)

SAVE CANCEL

Ethernet Unit 1 (internal interface)

VPN Access 25 HTML setup
vpn25
[SLOT 0 UNIT 2 ETH]: Configure Ethernet Interface

IP-Configuration: Manual
 local IP-Number: 10.1.80.200
 local Netmask: 255.255.0.0
 Second Local IP-Number:
 Second Local Netmask:
 Encapsulation: Ethernet II
 Mode: Auto
 MAC Address:
 Bridging: disabled

[Advanced Settings >](#)
[Virtual Interfaces >](#)

SAVE CANCEL

Ethernet Unit 2 (external interface)

4.2 Pre IPsec Rules

At minimum one rule must be defined which allows UDP traffic on port 500 for establishing the IPsec tunnel. This rule should already be created by the *IPsec Wizard*. If it does not exist, you need to configure it manually.

- Menu: **Advanced Configuration -> IPSEC -> Pre IPsec Rules.**

VPN Access 25 HTML setup
vpn25
[IPSEC][PRE IPSEC TRAFFIC]: IPsec Configuration - Configure Traffic List

Highlight an entry and type 'i' to insert new entry below.
 'u'/'d' to move up/down, 'a' to select as active traffic list

Local Address	M/R	Port	Proto	Remote Address	M/R	Port	A	Proposal
*0.0.0.0	M0	500	udp	0.0.0.0	M0	500	PA	

Notes: Double-click an item to select/edit it / Single-click an item to use the keyboard accelerator(s)

APPEND DELETE EXIT

4.3 Remote peer configuration

4.3.1 Peer address and peer ID/Pre Shared Key

- From the menu, select **Advanced Configuration -> IPSEC -> Configure Peers**.
- Click **Append**.

VPN Access 25 HTML setup
vpn25
[IPSEC][PEERS][ADD]: Configure Peer

Description:

Admin Status:

Peer Address:

Peer IDs:

Pre Shared Key:

Confirm input:


[IPsec Callback >](#)
[Peer specific Settings >](#)

Virtual Interface:

[Traffic List Settings >](#)

- Enter a **Description** for the remote peer.
- Enter into the field **Peer Address** the IP address of the remote peer or its DynDNS name if it has a dynamic public IP address.
- When using certificates, enter the distinguished name of the remote entities certificate into the field **Peer IDs**. In our example we have used <MAILTO=support@innominate.com, OU=Support, O=Innominate, ST=Germany, L=Berlin, C=de, CN=mGuard>.
- When using PSK, enter the shared secret into the fields **Pre Shared Key** and **Confirm input**.

- Click **Peer specific Settings**.

 **Note:** The single parameters of the certificates distinguished name must be entered in a special order. You can obtain it by connecting through the serial port or telnet to the console of the VPN25 and executing the command **subjectname**. The subject name of the remote sites certificate is displayed after the first connection attempt.

4.3.2 IKE/IPsec proposal and lifetimes

- Click **edit** in the line **IKE (Phase 1) Profile** and click **Add**.
- At first we want to create the ISAKMP (IKE) SA and IPsec SA lifetimes before configuring the IKE profile. Click **Edit Lifetimes** and **Add**.
 - Set **Lifetime Restriction Based On to Time**.
 - Enter **3600** seconds. This value corresponds to the default value for the ISAKMP SA lifetime on the mGuard.
 - Click **Save**.
 - Click **Add** again and repeat the previous steps, entering a time of **28800** seconds. This value corresponds to the default value for the IPsec SA lifetime on the mGuard.
 - Click **Exit**.

- Enter a **Description** for the policy.
- Select as **Proposal** the desired encryption and hash algorithm for the key exchange. In our example we want to use 3DES and MD5.
- Set the **Lifetime** to 3600 seconds.
- Select **2 (1024 bit MODP)** as (Diffie-Hellman) **Group**.
- Set **Authentication Method** either to **RSA Signatures** or **Pre Shared Keys** depending on the used authentication method (certificates or PSK).
- Set **Mode** to **id-protect**.
- If certificates are used, select the VPN25 host certificate as **Local Certificate**.
- Enable NAT-Traversal if the VPN tunnel will be established across one or more gateway that have *Network Address Translation* (NAT) activated.
- Click **Save**.

- The new IKE profile is displayed in the list. Click **Exit**.
- Click **edit** in the line **IPsec (Phase 2) Profile** and then **Add**.

- Enter a **Description** for the policy.
- Select as **Proposal** the desired encryption and hash algorithm for the data exchange. In our example we want to use 3DES and MD5.
- Set the **Lifetime** to 28800 seconds.
- If *Perfect Forward Secrecy* shall be used, set **PFS** to **group 2 (1024 bit MODP)**. Note that in this case PFS also needs to be enabled on the mGuard.
- Click **Save**.

- The new IPsec profile is displayed in the list. Click **Exit**.

- Select as **IKE (Phase 1) Profile** the IKE profile you have created.
- Select as **IPsec (Phase 2) Profile** the IPsec profile you have created.
- Click **Save**.

4.3.3 VPN subnets

- Click **Traffic List Settings** and then **Append**.

- Enter a **Description** for the traffic list.
- Enter as **Local** network the network IP of the internal network of the VPN25, in our example 192.168.1.0/24.
- Enter as **Remote** network the network IP of the internal network of the mGuard, in our example 192.168.27.0/24.
- Set **Action** to **protect**.
- Specify as **Profile** the IPsec profile you've created before.
- Click **Save**.

- The new traffic settings are displayed in the list. Click **Save**.
- Complete saving the settings for the configured peer.
- Finally ensure that IPsec is enabled (menu *Advanced Configuration* -> *IPSEC*) on the VPN25.

5 Configuring the mGuard

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 mGuard in Router mode (Router/PPPoE/PPTP)

5.1.1 Menu: VPN -> Connections

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

VPN > Connections > Connection Bintec

A descriptive name for the connection	Bintec																
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	192.168.27.0/24																
Remote network	192.168.1.0/24																
The virtual IP which will be used by the client in Stealth mode	192.168.1.1																
Firewall Incoming (untrusted port)																	
<input type="checkbox"/> <input type="checkbox"/>	<table border="1"> <thead> <tr> <th>Protocol</th> <th>From IP</th> <th>From Port</th> <th>To IP</th> <th>To Port</th> <th>Action</th> <th>Comment</th> <th>Log</th> </tr> </thead> <tbody> <tr> <td>All</td> <td>0.0.0.0/0</td> <td>any</td> <td>0.0.0.0/0</td> <td>any</td> <td>Accept</td> <td>default rule - please</td> <td>No</td> </tr> </tbody> </table>	Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log	All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	default rule - please	No
Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log										
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)																	
<input type="checkbox"/> <input type="checkbox"/>	<table border="1"> <thead> <tr> <th>Protocol</th> <th>From IP</th> <th>From Port</th> <th>To IP</th> <th>To Port</th> <th>Action</th> <th>Comment</th> <th>Log</th> </tr> </thead> <tbody> <tr> <td>All</td> <td>0.0.0.0/0</td> <td>any</td> <td>0.0.0.0/0</td> <td>any</td> <td>Accept</td> <td>default rule - please</td> <td>No</td> </tr> </tbody> </table>	Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log	All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	default rule - please	No
Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log										
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										
<input type="button" value="All Connections"/> <input type="button" value="OK"/>																	

- Enter as **Address of the remote site's VPN gateway** the external IP address of the VPN25, 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*, enter the shared secret. Otherwise you need to import the VPN25 host certificate, in our example *Bintec.crt*.
- Set **Connection type** to **Tunnel (Net <-> Net)** for a VPN tunnel connection.
- The mGuard should initiate the connection. Therefore set **Connection Startup** to **Start connection to**
- **Tunnel settings:**
 - **Local network:** This parameter specifies the VPN subnet (internal network) of the mGuard, in our example *192.168.27.0/24*.
 - **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:** This parameter specifies the VPN subnet (internal network) of the VPN25, in our example *192.168.1.0/24*.

- Click **Configure** in the line *More IKE Options*.

VPN > Connections > Connection Check Point > More IKE Options

ISAKMP SA (Key Exchange)	
Encryption Algorithm	3DES-168
Hash Algorithm	MD5
IPsec SA (Data Exchange)	
Encryption Algorithm	3DES-168
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	Yes
Dead Peer Detection	
Action	Hold (Default)
Delay	30
Timeout	120
<input type="button" value="Back"/>	

- **ISAKMP SA (Key Exchange)**: The settings for **Encryption** and **Hash Algorithm** must correspond to the settings on the VPN25 (*IKE (Phase 1) Profile*).
- **IPsec SA (Data exchange)**: The settings for **Encryption** and **Hash Algorithm** must correspond to the settings on the VPN25 (*IPsec (Phase 2) Profile*).
- The **ISAKMP SA Lifetime** and **IPsec SA Lifetime** should correspond to the setting on the VPN25.
- If you have enabled **Perfect Forward Secrecy** on the VPN25 (*IPsec (Phase 2) Profile*) then you also need to enable it on the mGuard.
- Click **Back**.
- We have kept the default firewall settings.
- Click **OK**.

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	172.16.106.0/24
Remote network	192.168.1.0/24
The virtual IP which will be used by the client in Stealth mode	172.16.106.1

- Specify as **Local network** the network IP of the virtual transfer network.
- Specify as **Remote network** the network IP of the internal network of the VPN25.
- 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 VPN25.

You also need to change the tunnel settings of the remote network on the VPN25 accordingly.

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, 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 **VPN -> IPsec Status**).

VPN > IPsec Status					
Connection Name	Connection		ISAKMP State	IPsec State	
Bintec	Gateway	10.1.80.20	10.1.80.200	STATE_MAIN_I4 (ISAKMP SA established) Lifetime: 2683s	
	Traffic	192.168.27.0/24	192.168.1.0/24		STATE_QUICK_I2 (sent QI2, IPsec SA established) Lifetime: 27863s
	ID	CN=mGuard, C=de, L=Berlin, ST=Germany, O=Innominat, OU=Support, E=support@innominate.com, O=innominate, ST=germany, L=berlin, C=de, CN=bintec			
<input type="button" value="Update"/>					

6.1 ISAKMP couldn't be established

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

- 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 VPN25.
- Mismatched ISAKMP policy parameters.
- mGuard VPN Log error message **AUTHENTICATION_FAILED**:
 - Verify that the time and date settings on the VPN25 are correct. Otherwise the certificate would be invalid.
 - The distinguished name of the mGuard certificate needs to be entered on the VPN25 (peer configuration) in a special order. For obtaining the correct entry:
 - Login to the VPN25 console through telnet or through the serial port.
 - Enter the command: **subjectname**
 - The distinguished names of the configured certificates are displayed. The subject name of the remote sites certificate is displayed after the first connection attempt.

```
vpn25:> subjectname
inx SubjectName(ro)
0 "MAILTO=support@innominate.com, OU=Support, O=Innominat, ST=Germany, L=Berlin, C=de, CN=CA"
1 "CN=bintec, C=de, L=berlin, ST=germany, O=innominate, OU=support, MAILTO=support@innominate.com"
2 "MAILTO=support@innominate.com, OU=Support, O=Innominat, ST=Germany, L=Berlin, C=de, CN=mGuard"
```

In our example we need to use as *Peer ID* on the VPN25: <MAILTO=support@innominate.com, OU=Support, O=Innominat, ST=Germany, L=Berlin, C=de, CN=mGuard>

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.