

# Interoperability Guide

## Configuring IPsec Tunnel Mode VPN between mGuard and Astaro V7



*mGuard smart*



*mGuard centerport*



*mGuard blade*



*mGuard industrial RS*



*mGuard PCI*



*mGuard delta*

Innominate Security Technologies AG  
Rudower Chaussee 13  
12489 Berlin, Germany

Phone: +49 (0)30-921028 0  
Fax: +49 (0)30-921028 020  
contact@innominate.com  
<http://www.innominate.com>

## TABLE OF CONTENTS

<b>1</b>	<b>Disclaimer.....</b>	<b>3</b>
<b>2</b>	<b>Introduction .....</b>	<b>4</b>
2.1	<i>mGuard in Router Mode.....</i>	<i>4</i>
2.2	<i>mGuard in Single Stealth (autodetect/static) Mode.....</i>	<i>5</i>
2.3	<i>mGuard in Multi Stealth (multiple clients) Mode.....</i>	<i>5</i>
<b>3</b>	<b>Configuring the ASG .....</b>	<b>6</b>
3.1	<i>X.509 Certificates.....</i>	<i>6</i>
3.1.1	<i>ASG Certificate.....</i>	<i>6</i>
3.1.2	<i>mGuard Certificate .....</i>	<i>7</i>
3.2	<i>Remote Network.....</i>	<i>9</i>
3.3	<i>IPSec Policy.....</i>	<i>10</i>
3.4	<i>Remote Gateway.....</i>	<i>11</i>
3.4.1	<i>Using PSK .....</i>	<i>11</i>
3.4.2	<i>Using Certificates.....</i>	<i>12</i>
3.5	<i>IPSec Connection.....</i>	<i>13</i>
3.6	<i>Firewall Rules.....</i>	<i>14</i>
<b>4</b>	<b>Configuring the mGuard.....</b>	<b>15</b>
4.1	<i>Import of the Machine Certificate.....</i>	<i>15</i>
4.2	<i>VPN Connection.....</i>	<i>16</i>
4.2.1	<i>General Settings .....</i>	<i>16</i>
4.2.2	<i>Authentication.....</i>	<i>17</i>
4.2.2.1	<i>Using PSK.....</i>	<i>17</i>
4.2.2.2	<i>Using Certificates .....</i>	<i>18</i>
4.2.3	<i>Firewall.....</i>	<i>19</i>
4.2.4	<i>IKE Options .....</i>	<i>20</i>
<b>5</b>	<b>Troubleshooting.....</b>	<b>21</b>
5.1	<i>ISAKMP SA could not be established.....</i>	<i>21</i>
5.2	<i>ISAKMP SA established but not the IPsec SA.....</i>	<i>21</i>
5.3	<i>Tunnel established but Peers of the Remote Network not reachable.....</i>	<i>21</i>

## **1 Disclaimer**

© Innominate Security Technologies AG

December 2009

“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.

## 2 Introduction

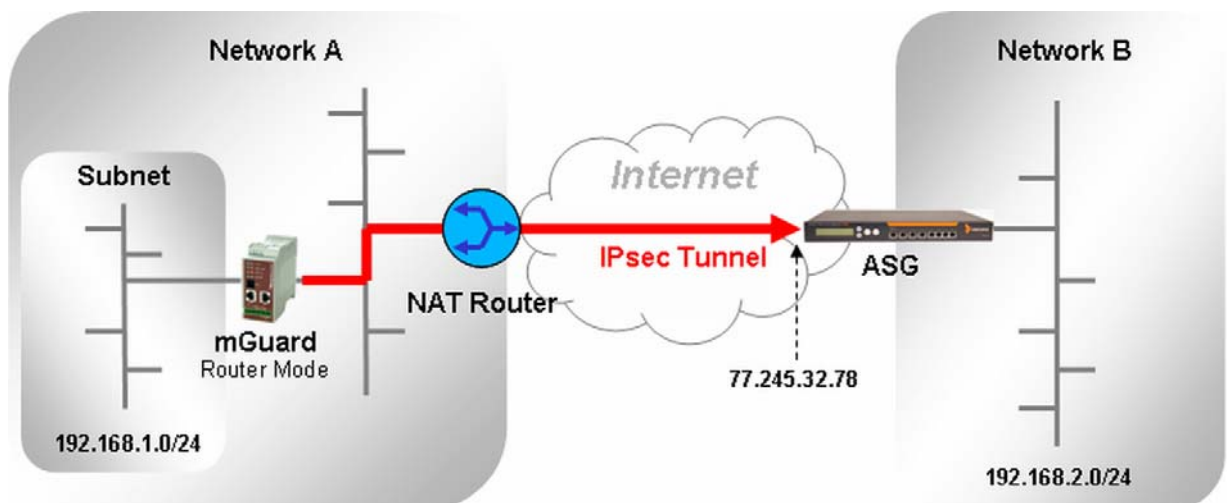
This document describes the required steps to configure an IPsec tunnel mode VPN between the mGuard and an Astaro Security Gateway (in the following called ASG). We have used mGuard 7.0.1 and Astaro 7.501 for this interoperability guide. This document describes the usage of the authentication methods *Preshared Key* (PSK) and PKI with X.509 certificates.

### Note

- Configuring a VPN connection using PKI and certificates is considered more secure than using PSK.
- PSK can only be used if the mGuard and the ASG are connected directly to the same external network or to the Internet. If the connection will be established across one or more gateways that have *Network Address Translation* (NAT) activated, certificates must be used for authentication.
- When using PSK, both sites must have static public IP addresses. If one site has a dynamic public IP address, it must register its IP address with a fixed name at a DynDNS service. The other site must refer to this name to establish the VPN connection.

### 2.1 mGuard in Router Mode

The following diagram illustrates the machines and addresses involved in the connection. The mGuard acts as *Router* between the networks *Network A* and *Subnet* and initiates the VPN connection to the ASG. The examples used in this document are taken from this setup.

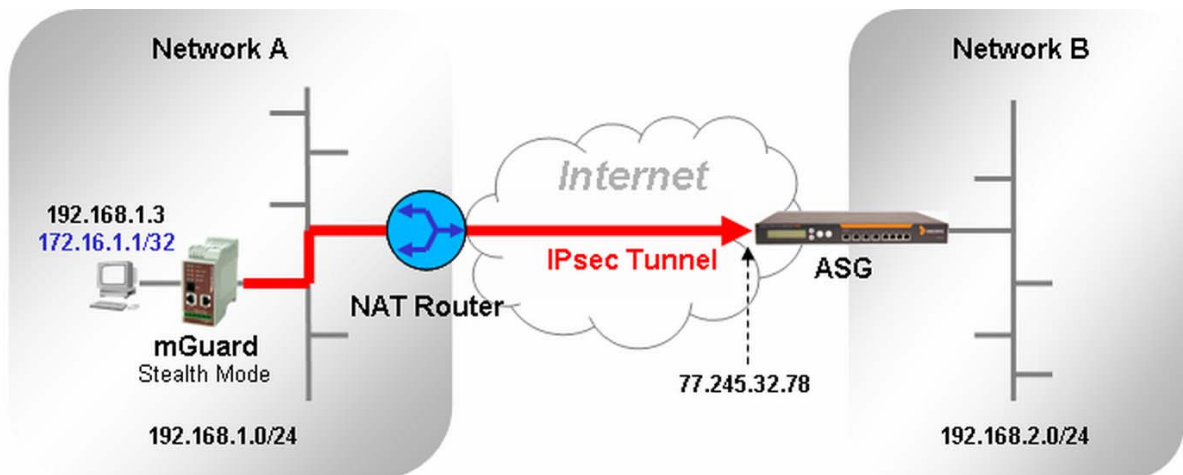


For this setup we have selected AES-256 as encryption and SHA-1 as hash algorithm for the *ISAKMP SA* and for the *IPsec SA*. The parameters for the VPN tunnel configuration are as follows:

VPN parameter	mGuard	ASG
Remote VPN gateway	77.245.32.78	Any IP address
Local VPN network	192.168.1.0/24	192.168.2.0/24
Remote VPN network	192.168.2.0/24	192.168.1.0/24
ISAKMP Policy, Encryption / Hash	AES-256 / SHA-1	AES-256 / SHA-1
IPsec Policy, Encryption / Hash	AES-256 / SHA-1	AES-256 / SHA-1

This setup can also be applied if the mGuard is the gateway to the *Internet*. If the *Internet Service Provider* (ISP) provides an Ethernet line, the mGuard is operated in *Router* mode. If the mGuard connects to the *Internet* through a DSL modem, the mGuard is operated in *PPPoE* mode.

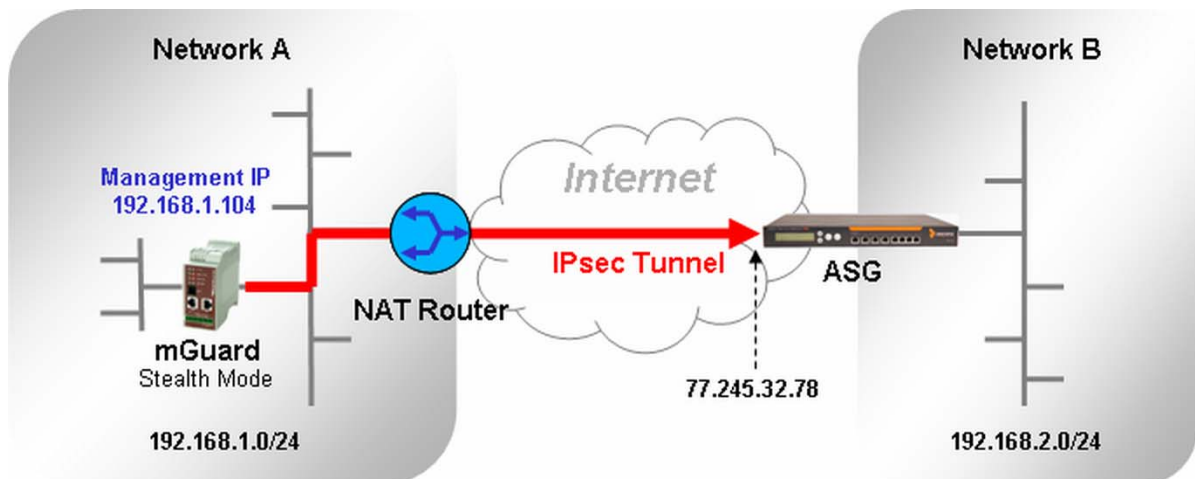
## 2.2 mGuard in Single Stealth (autodetect/static) Mode



If the mGuard is operated in *Single Stealth* (autodetect/static) mode for protecting one single machine only, the following two cases need to be distinguished:

- 1) If the client has a static IP address, this IP address of the client is used for settings up the VPN tunnel (*Local network* = 192.168.1.3/32, *Virtual IP* = 192.168.1.3, *Remote network* = 192.168.2.0/24).
- 2) If the client receives his IP settings from a DHCP server with a slight chance that the IP address could change, a virtual IP address is used for setting up the VPN tunnel (*Local network* = 172.16.1.1/32, *Virtual IP* = 172.16.1.1, *Remote network* = 192.168.2.0/24). The virtual IP is used for accessing the client from *Network B*. The mGuard will perform a 1:1 NAT from the virtual IP to the real IP address of the client automatically.

## 2.3 mGuard in Multi Stealth (multiple clients) Mode



If the mGuard is operated in *Multi Stealth Mode* to protect more than one machine, a *Management IP* must be assigned to the mGuard. The VPN tunnel needs to be configured between the networks *Network A* (192.168.1.0/24) and *Network B* (192.168.2.0/24).

### 3 Configuring the ASG

#### 3.1 X.509 Certificates

Follow the instructions in this chapter if X.509 certificates shall be used for authentication.

The following certificates are required:

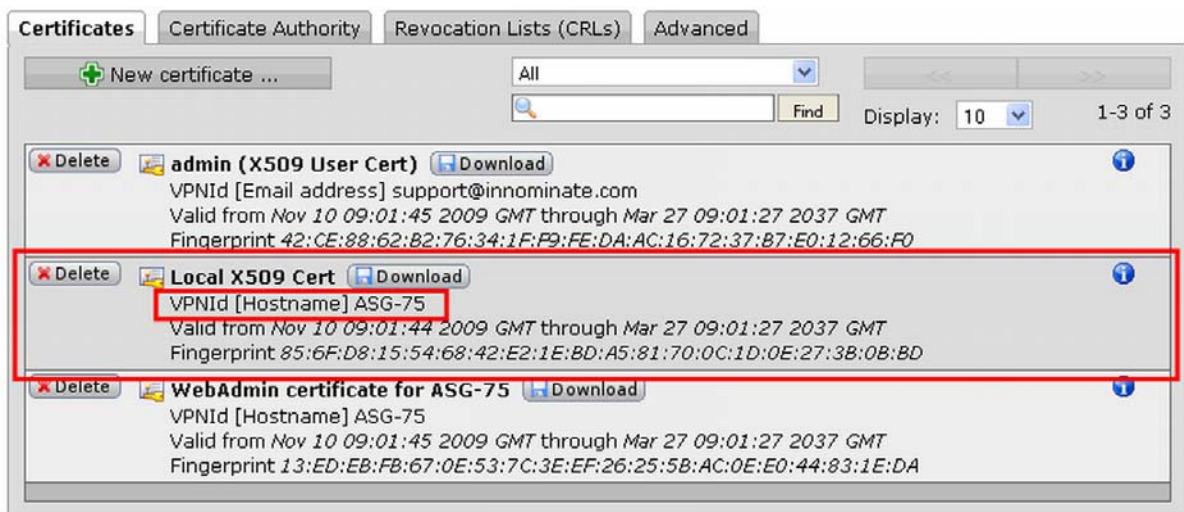
- 1) Each appliance must have its own machine certificate, which contains the private and public key (PKCS#12 export).
- 2) Each appliance requires the certificate (PEM export) of the other appliance for establishing the VPN connection.

##### 3.1.1 ASG Certificate

Usually the ASG already has a machine certificate which was created when getting the ASG into operation the first time. This certificate (PEM export) must be imported on the mGuard when setting up the VPN connection.

Follow these steps to export the ASG certificate:

- Select **Site-to-site VPN >> Certificate Management**, tab **Certificates**.

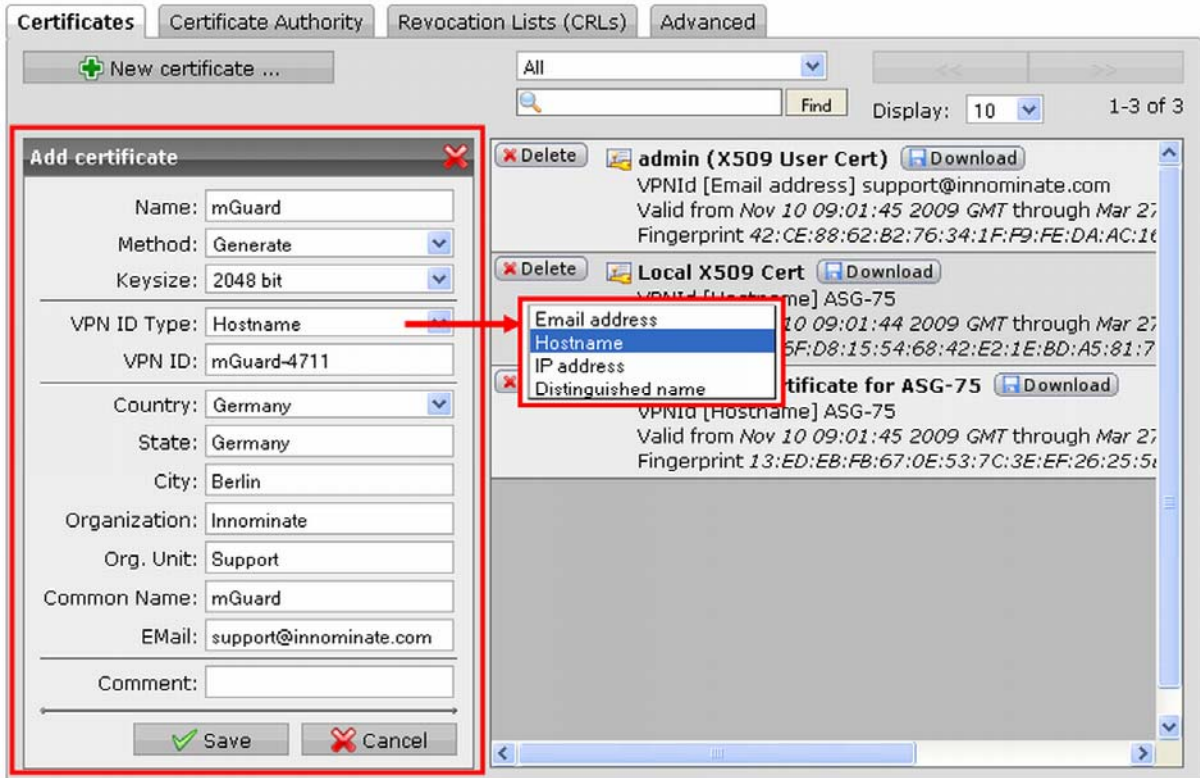


- The certificate of the ASG is displayed as **Local X509 Cert**.
- Click **<Download>**, select **PEM** as export format and save the certificate to the local system (e.g. as *ASG.pem*). This export needs to be imported when configuring the VPN connection on the mGuard.
- **VPNId**: It is important which VPN identifier is used by the ASG (*Hostname, Email Address, IP Address or Distinguished name*). If an other VPN identifier than *Distinguished name* is used, write it down (in the screenshot above: *Hostname = ASG-75*). This VPN identifier needs to be specified on the mGuard when configuring the VPN connection (menu *IPsec VPN >> Connections*, tab *Authentication*, section *VPN Identifier*).

### 3.1.2 mGuard Certificate

Follow these steps to create the mGuard certificate with the ASG:

- Select **Site-to-site VPN >> Certificate Management**, tab **Certificates**.
- Click **<New certificate>**.



#### Site-to-site VPN >> Certificate Management

<b>Name</b>	Enter a descriptive name for the certificate.
<b>Method</b>	Select <i>Generate</i> to create a new certificate.
<b>VPN ID Type</b>	<p>You have to define a unique VPN identifier for the certificate. This identifier is used by VPN gateways to recognize to which configured VPN connection the certificate belongs. By default, the subject of the certificate (e.g. <i>CN=mGuard, O=Innominate, OU=Support, etc.</i>), also called <i>Distinguished Name</i>, is used as VPN identifier.</p> <p>Alternatively you can also use <i>Hostname</i>, <i>Email Address</i> or <i>IP Address</i> as VPN identifier. This alternative VPN identifier will then be added as <i>Subject Alternative Name</i> to the certificate.</p> <p>The <i>Distinguished Name</i> of the certificate can always be used as VPN identifier, even if you have specified here another alternative.</p>
<b>VPN ID</b>	<p>Depending on the selected <i>VPN ID type</i>, enter the appropriate value. Keep in mind that this value must be unique for each certificate.</p> <p>This text box will be hidden when selecting <i>Distinguished Name</i> as <i>VPN ID Type</i>. In this case only the subject of the certificate (values of the text boxes <i>Country</i> to <i>Email</i>) can be used as VPN Identifier.</p>
<b>Country to Email</b>	Enter identifying information about the certificate.

- Click **<Save>**.

## Configuring IPsec Tunnel Mode VPN between mGuard and Astaro V7

⇒ The mGuard certificate is created and displayed in the certificate list.



Now you need to export the mGuard certificate in PKCS#12 format. This export must be imported on the mGuard as machine certificate (menu *Authentication >> Certificates*, tab *Machine Certificates*):

- Click **<Download>**.

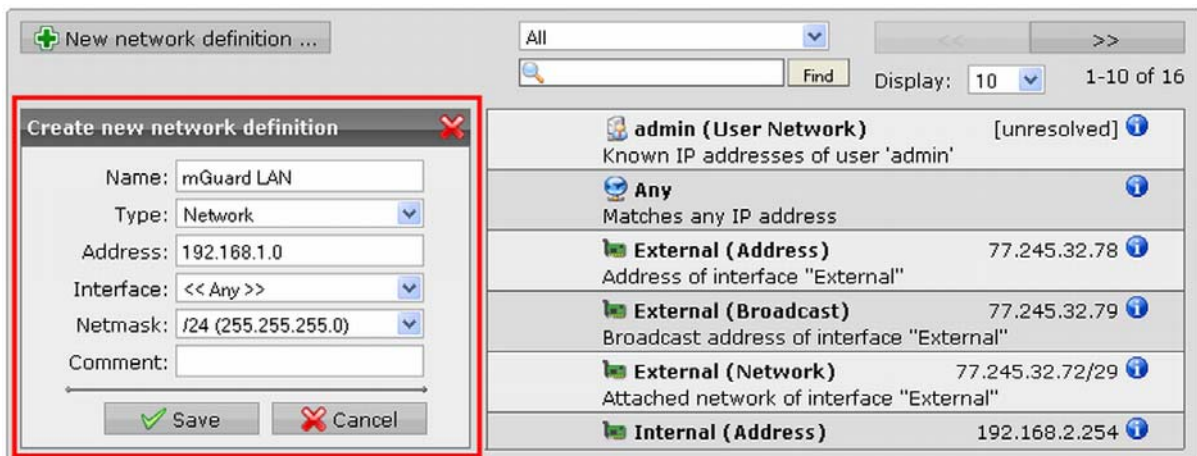


- Select **PKCS#12** as export format.
- Enter the password which protects the export against unauthorized usage.
- Click **<Save>** and specify the filename (e.g. *mGuard.p12*) for storing the export to the local system.

### 3.2 Remote Network

Now we need to create a definition for the internal network of the mGuard, in our example 192.168.1.0/24.

- Select **Definitions >> Networks**.
- Click **<New network definition>**.

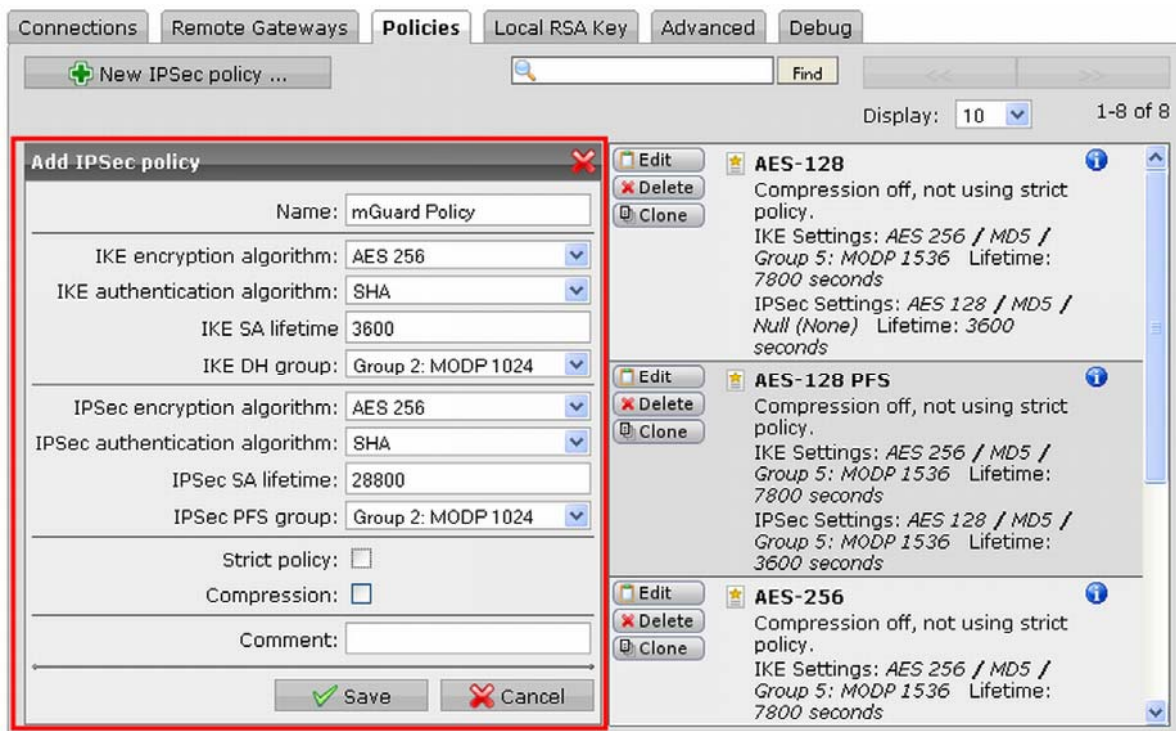


Definitions >> Networks	
<b>Name</b>	Enter a descriptive name for the network definition.
<b>Type</b>	Select <i>Network</i> . If the mGuard is operated in <i>Single Stealth</i> mode, select <i>Host</i> (refer to <a href="#">mGuard in Single Stealth (autodetect/static) Mode</a> ).
<b>Address</b>	Enter the network address of the internal network of the mGuard, in our example 192.168.1.0. If the mGuard is operated in <i>Single Stealth</i> mode, enter the IP address of the client or the used virtual IP address respectively (refer to <a href="#">mGuard in Single Stealth (autodetect/static) Mode</a> ).
<b>Interface</b>	It is not possible to bind this definition to an interface of the ASG in particular. Therefore leave the default value << Any >>.
<b>Netmask</b>	Select the subnet mask of the internal network of the mGuard.

- Click **<Save >**.

### 3.3 IPsec Policy

- Select **Site-to-site VPN >> IPsec**, tab **Policies**.  
At first check if the desired policy is already defined. If it doesn't exist, you need to create a new policy. In our example we want to use *AES-256* and *SHA-1* as encryption and hash algorithm for the IKE/ISAKMP SA and the IPsec SA. The factory default settings for the lifetimes on the mGuard are 3600 seconds for the ISAKMP SA and 28800 seconds for the IPsec SA. In our case we need to create a new policy.
- Click **<New IPsec policy>**.



#### Site-to-site VPN >> IPsec

<b>Name</b>	Enter a descriptive name for the policy.
<b>IKE encryption algorithm</b>	Select the desired encryption algorithm, in our example <i>AES 256</i> .
<b>IKE authentication algorithm</b>	Select the desired hash algorithm, in our example <i>SHA</i> .
<b>IKE SA lifetime</b>	Enter <i>3600</i> . This is the factory default value for the IKE/ISAKMP SA lifetime on the mGuard.
<b>IKE DH group</b>	Select <i>Group 2: MODP 1024</i> .
<b>IPsec encryption algorithm</b>	Select the desired encryption algorithm, in our example <i>AES 256</i> .
<b>IPsec authentication algorithm</b>	Select the desired hash algorithm, in our example <i>SHA</i> .
<b>IPsec SA lifetime</b>	Enter <i>28800</i> . This is the factory default value for the IPsec SA lifetime on the mGuard.
<b>IPsec PFS group</b>	Select <i>Group 2: MODP 1024</i> .

- Click **<Save>**.

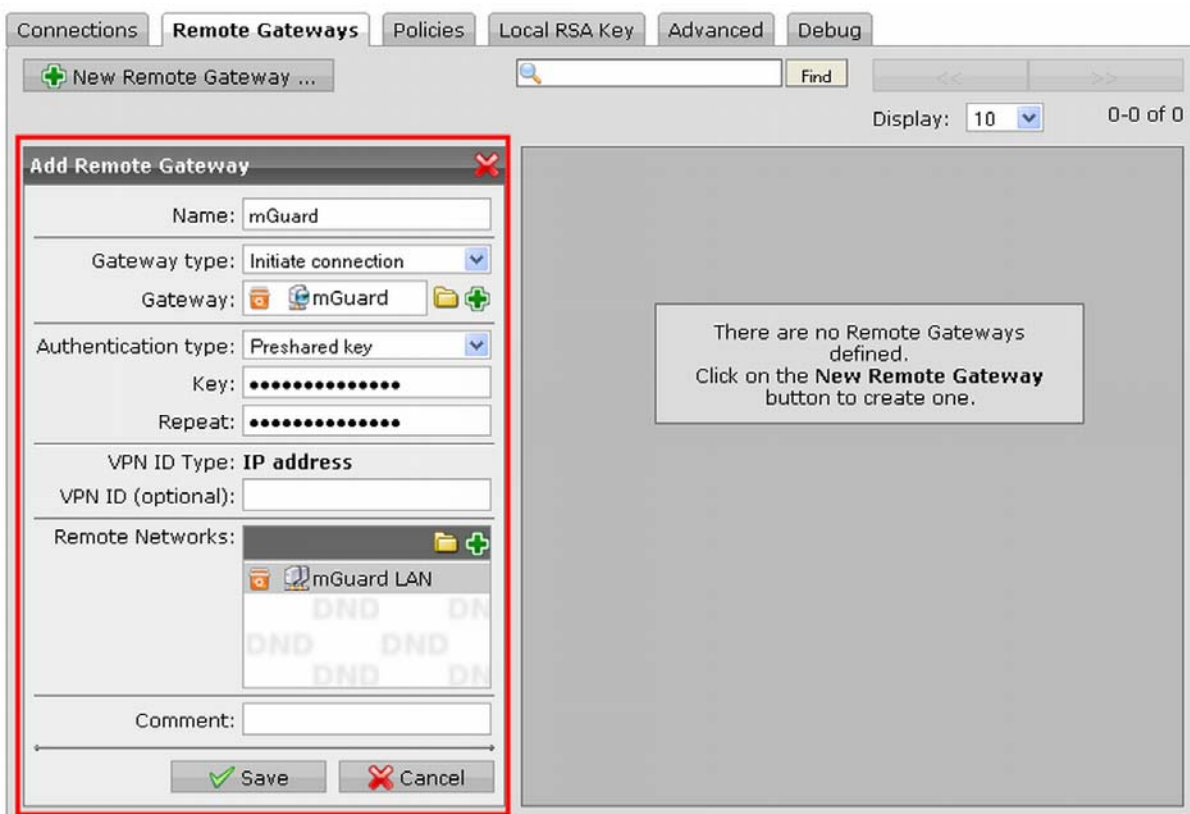
### 3.4 Remote Gateway

#### 3.4.1 Using PSK

**Note**

- Configuring a VPN connection using PKI and certificates is considered more secure than using PSK.
- PSK can only be used if the mGuard and the ASG are connected directly to the same external network or to the Internet. If the connection will be established across one or more gateways that have *Network Address Translation* (NAT) activated, certificates must be used for authentication.
- When using PSK, both sites must have static public IP addresses. If one site has a dynamic public IP address, it must register its IP address with a fixed name at a DynDNS service. The other site must refer to this name to establish the VPN connection.

- Select **Site-to-site VPN >> IPsec**, tab **Remote Gateways**.
- Click **<New Remote Gateway>**.



#### Site-to-site VPN >> IPsec

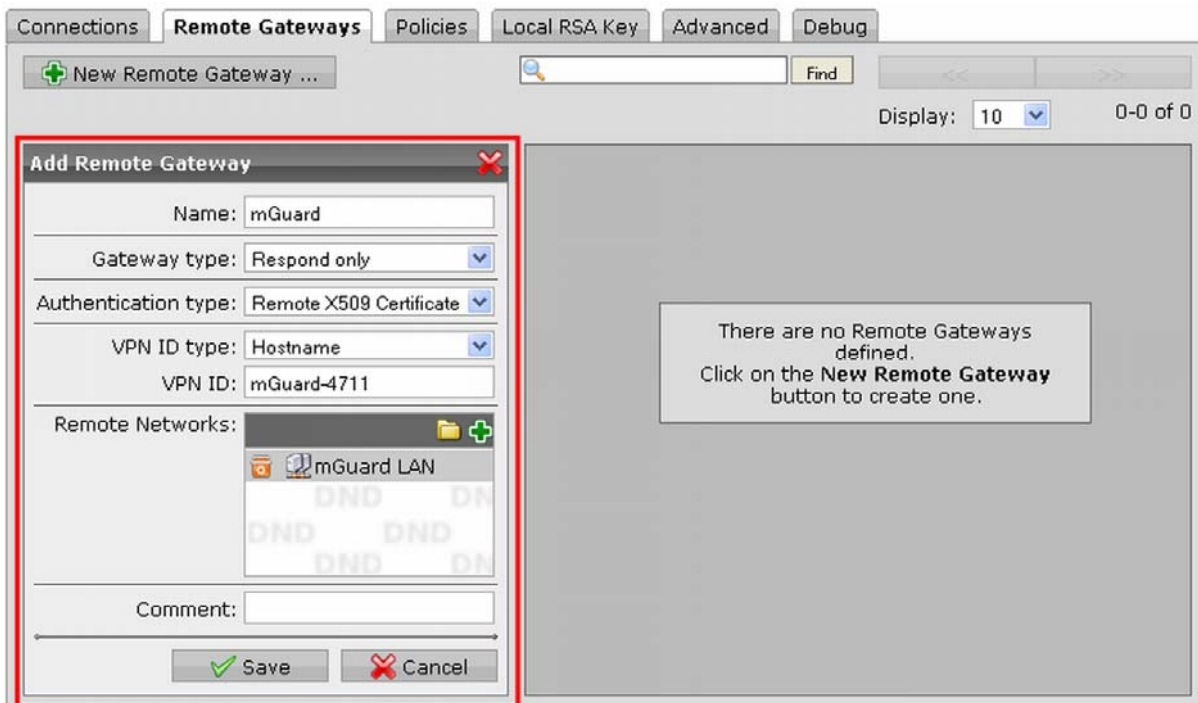
<b>Name</b>	Enter a descriptive name for the remote gateway.
<b>Gateway type</b>	Select <i>Initiate connection</i> .
<b>Gateway</b>	Click the plus icon and create a network definition for the mGuard. This network object could either be of the type <i>Host</i> , if the mGuard has a static IP address, or <i>DNS host</i> , if the mGuard registers its IP address with a fixed name at a DynDNS service.
<b>Authentication type Key / Repeat</b>	Select <i>Preshared key</i> , enter and retype the key which should be used for authentication.
<b>VPN ID type / VPN ID</b>	When using PSK, by default the external/public IP address of the device is used as VPN identifier. There is nothing you need to enter here.
<b>Remote Networks</b>	Specify the remote network definition of the mGuard you have created in chapter <a href="#">Remote Network</a> .

- Click **<Save>**.

### 3.4.2 Using Certificates

Follow these steps if certificates should be used for authentication.

- Select **Site-to-site VPN >> IPsec**, tab **Remote Gateways**.
- Click **<New Remote Gateway>**.

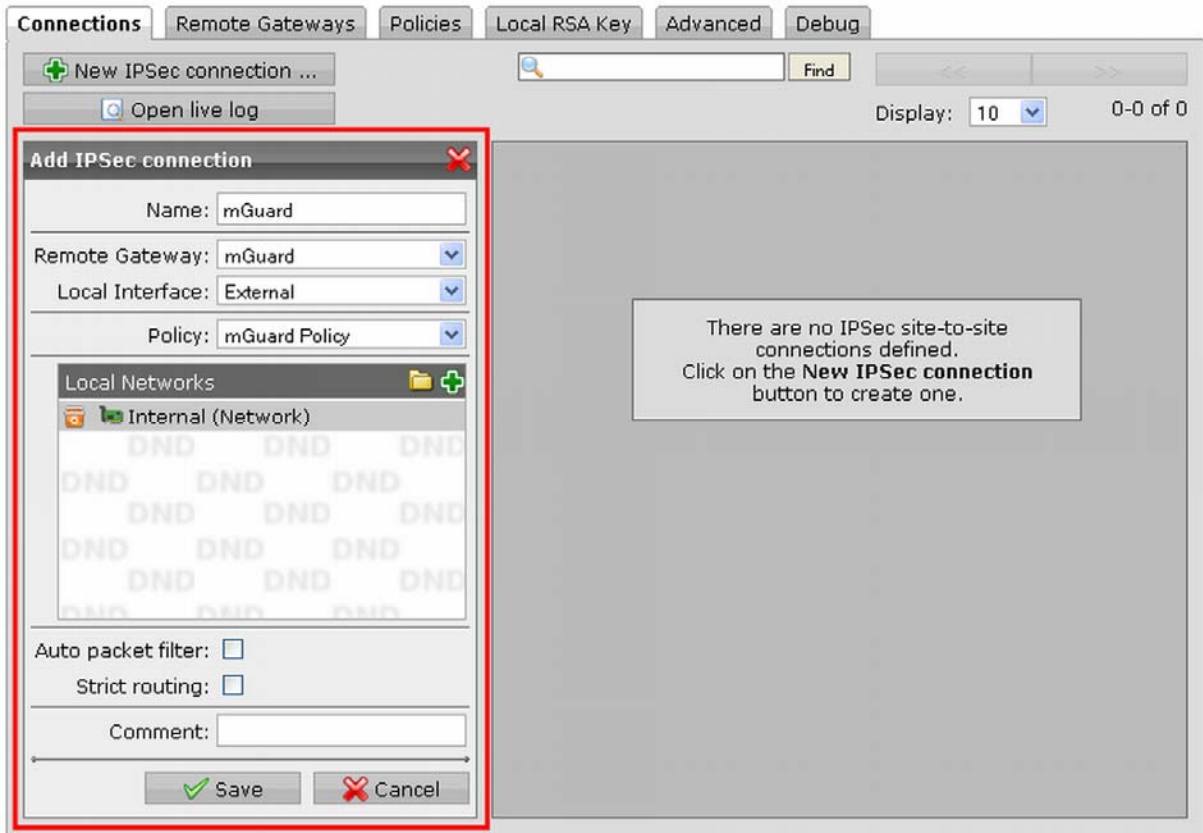


Site-to-site VPN >> IPsec	
<b>Name</b>	Enter a descriptive name for the remote gateway.
<b>Gateway type</b>	Select <i>Respond only</i> because the mGuard initiates the VPN connection and it could also be possible that the remote IP address is unknown or may change, especially if the mGuard is located behind a NAT router with a dynamic public IP address.
<b>Authentication type</b>	Select <i>Remote X509 Certificate</i> .
<b>VPN ID type</b>	Select either <i>Distinguished Name</i> or the <i>VPN ID type</i> you have chosen when creating the mGuard certificate (refer to chapter <a href="#">mGuard Certificate</a> ).
<b>VPN ID</b>	Enter the corresponding VPN identifier. If you have selected <i>Distinguished Name</i> , enter the subject of the certificate (e.g. <i>CN=mGuard, O=Innominate, OU=Support, etc.</i> ), otherwise the <i>VPN ID</i> you have entered when creating the mGuard certificate (refer to chapter <a href="#">mGuard Certificate</a> ).
<b>Remote Networks</b>	Specify the remote network definition of the mGuard you have created in chapter <a href="#">Remote Network</a> .

- Click **<Save>**.

### 3.5 IPsec Connection

- Select **Site-to-site VPN >> IPsec**, tab **Connections**.
- Click **<New IPsec connection >**.



**Site-to-site VPN >> IPsec**

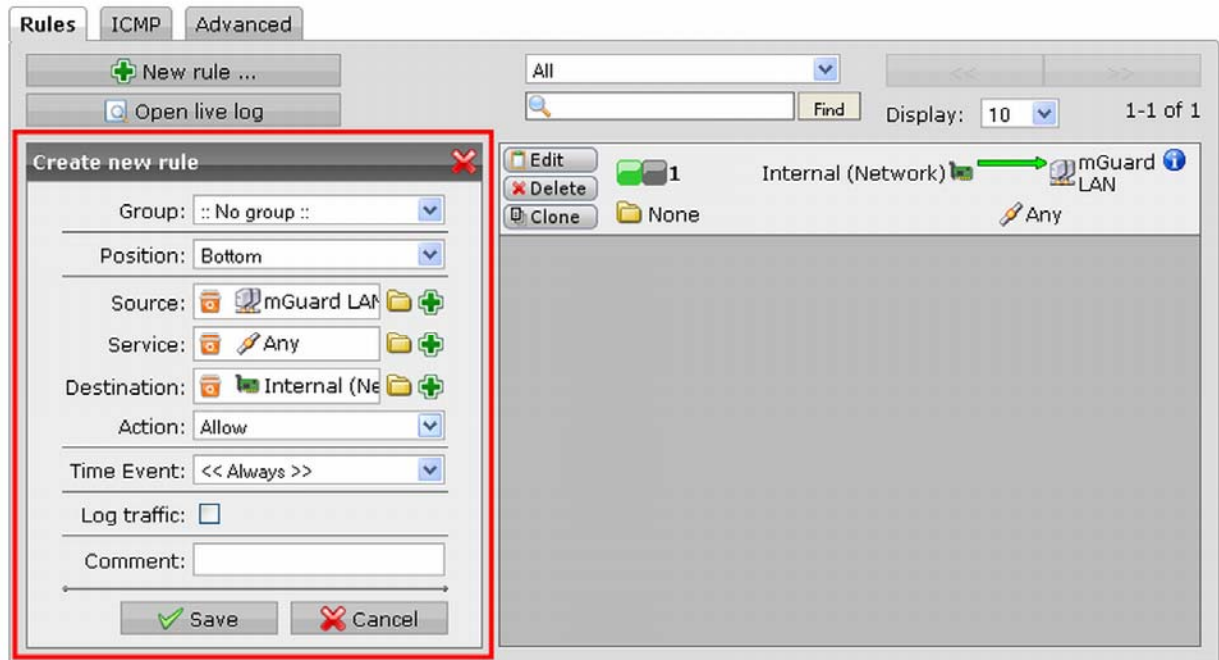
<b>Name</b>	Enter a descriptive name for the connection.
<b>Remote Gateway</b>	Select the remote gateway you have created in the previous chapter.
<b>Local Interface</b>	Select the name of the interface which is used as the local endpoint of the IPsec tunnel.
<b>Policy</b>	Select the policy you have created in chapter <a href="#">IPsec Policy</a> .
<b>Local Networks</b>	Specify the internal network of the ASG.

- Click **<Save>**.

### 3.6 Firewall Rules

Finally you need to define firewall rules for allowing the desired traffic between the two internal networks through the tunnel. In our example we want to allow every kind of traffic from the internal network of the ASG to the internal network of the mGuard and vice versa. Therefore we need to define two rules, one for each direction.

- Select **Network Security >> Packet Filter**, tab **Rules**.
- Click **<New Rule>**.

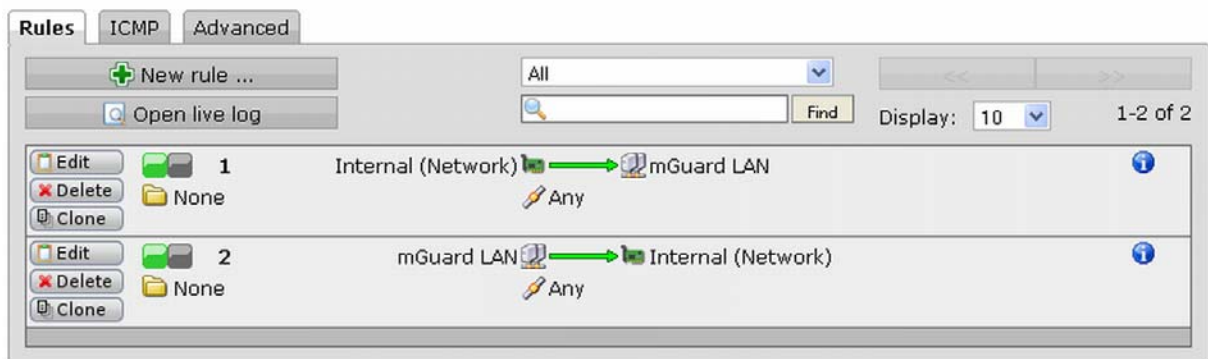


#### Network Security >> Packet Filter

<b>Source</b>	For allowing traffic from the internal network of the mGuard to the internal network of the ASG, select the internal network of the mGuard.
<b>Service</b>	We want to allow every kind of traffic. Therefore we select <i>Any</i> service.
<b>Destination</b>	For allowing traffic from the internal network of the mGuard to the internal network of the ASG, select the internal network of ASG.
<b>Action</b>	<i>Allow.</i>

- Click **<Save>**.

Repeat the previous steps to allow traffic in the opposite direction. We got the following two rules:



## 4 Configuring the mGuard

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

- If certificates are used for authentication: Import of the mGuard machine certificate through the menu **Authentication >> Certificates**, tab **Machine Certificates**.
- Configuration of the VPN connection through the menu **IPsec VPN >> Connections**.

### 4.1 Import of the Machine Certificate

This step is only required if certificates are used for authentication. You need the export of the mGuard certificate in PKCS#12 format.

- Select **Authentication >> Certificates**, tab **Machine Certificates**.

Certificate	
Subject	emailAddress=support@innominate.com,CN=mGuard,OU=Support,O=Innominate,L=Berlin,ST=Germany,C=de
Subject Alternative Names	• @mGuard-4711
Issuer	emailAddress=support@innominate.com,CN=Innominate VPN CA,O=Innominate,L=Berlin,C=de
Validity	From Nov 12 16:13:47 2009 GMT to Mar 27 09:01:27 2037 GMT
Fingerprint	MD5: A7:83:F1:7C:82:CF:FE:3F:92:7B:82:1B:10:5A:4C:90 SHA1: 62:15:47:12:45:B2:8F:EE:65:4A:A8:0A:92:3C:79:29:A7:53:3D:CA
Shortname	mGuard
Upload PKCS#12	Filename: <input type="text"/> <input type="button" value="Durchsuchen..."/> <input type="button" value="Import"/> Password: <input type="password"/>
Download Certificate	<input type="button" value="Current Certificate File"/>

- Click the down arrow to create a new line.
- Click **<Browse>**.
- Select the PKCS#12 export of the mGuard certificate.
- Enter the **Password** which protects the certificate against unauthorized usage.
- Click **<Import>**.
- Click **<Apply>**.

## 4.2 VPN Connection

- Select **IPsec VPN >> Connections**.
- Click the down arrow to create a new line.
- Enter a descriptive name for the connection and click **<Edit>**.

### 4.2.1 General Settings

General	Authentication	Firewall	IKE Options		
<b>Options</b>					
A descriptive name for the connection	ASG				
Enabled	Yes				
Address of the remote site's VPN gateway (Either an IP address, a hostname, or '%any' for any IP, multiple clients or clients behind a NAT gateway.)	77.245.32.78				
Connection startup	Initiate				
Encapsulate the VPN traffic in TCP	No				
<b>Transport and Tunnel Settings</b>					
<input checked="" type="checkbox"/>	Enabled	Type	Local	Remote	
<input checked="" type="checkbox"/>	Yes	Tunnel	192.168.1.0/24	192.168.2.0/24	More...

IPsec VPN >> Connections		
<b>Options</b>	<b>Address of the remote site's VPN gateway</b>	In our example the mGuard initiates the VPN connection to the ASG. Therefore we need to enter the external IP address of the ASG.  You also must enter the IP address of the ASG or its DynDNS name if the ASG initiates the VPN connection and PSK is used. If certificates are used, you also can enter <i>%any</i> if the IP address of the ASG is unknown or may change.
	<b>Connection startup</b>	In our example the mGuard initiates the VPN connection to the ASG. Therefore we have selected <i>Initiate</i> . Select <i>Wait</i> if the VPN connection is initiated by the ASG.
<b>Transport and Tunnel Settings</b>	<b>Type</b>	Select <i>Tunnel</i> for a VPN tunnel connection between two networks.
	<b>Local</b>	Enter the internal network of the mGuard, in our example <i>192.168.1.0/24</i> .  If the mGuard is operated in <i>Single Stealth</i> mode, enter the IP address of the client or the used virtual IP address respectively (refer to <a href="#">mGuard in Single Stealth (autodetect/static) Mode</a> ).
	<b>Remote</b>	Enter the internal network of the ASG, in our example <i>192.168.2.0/24</i> .
	<b>Virtual IP</b>	This option is only displayed if the mGuard is operated in <i>Single Stealth</i> mode.  Enter the IP address (without a subnet mask) of the client or the used virtual IP address respectively (refer to <a href="#">mGuard in Single Stealth (autodetect/static) Mode</a> ).

### 4.2.2 Authentication

- Switch to the tab **Authentication**.

#### 4.2.2.1 Using PSK

General	Authentication	Firewall	IKE Options
<b>Authentication</b>			
Authentication method		Pre-Shared Secret (PSK) ▼	
Pre-Shared Secret Key (PSK)		complicated_like_5Dy0qoD_and_long	
<b>VPN Identifier</b>			
Local		By default the IP address of the peer is used. Other possible settings are a hostname ("@hostname") or an e-mail address ("name@hostname").	
Remote		By default the IP address of the peer is used. Other possible settings are a hostname ("@hostname") or an e-mail address ("name@hostname").	

IPsec VPN >> Connections		
<b>Authentication</b>	<b>Authentication method</b>	Select <i>Pre-Shared Secret (PSK)</i> .
	<b>Pre-Shared Secret Key (PSK)</b>	Enter the preshared key which must match exactly to the one you have enter in the ASG configuration (refer to <a href="#">Using PSK</a> ).
<b>VPN Identifier</b>	<b>Local / Remote</b>	When using PSK the external/public IP address of the appliance is automatically used as VPN identifier. Nothing needs to be entered here.

4.2.2.2 Using Certificates

General	Authentication	Firewall	IKE Options														
<b>Authentication</b>																	
Authentication method	X.509 Certificate																
Local X.509 Certificate	mGuard																
Remote CA Certificate	No CA certificate, but the Remote Certificate below																
Remote Certificate	<table border="1"> <tr> <td>Subject</td> <td>emailAddress=support@innominate.com,CN=ASG-75,O=Innominate,L=Berlin,C=de</td> </tr> <tr> <td>Subject Alternative Names</td> <td>• @ASG-75</td> </tr> <tr> <td>Issuer</td> <td>emailAddress=support@innominate.com,CN=Innominate VPN CA,O=Innominate,L=Berlin,C=de</td> </tr> <tr> <td>Validity</td> <td>From Nov 10 09:01:44 2009 GMT to Mar 27 09:01:27 2037 GMT</td> </tr> <tr> <td>Fingerprint</td> <td>MDS: 84:27:BF:45:B7:8F:C4:F6:16:61:95:8B:90:10:F0:FD SHA1: 85:6F:D8:15:54:68:42:E2:1E:BD:A5:81:70:0C:1D:0E:27:3B:0B:BD</td> </tr> <tr> <td>Filename (*.pem):</td> <td><input type="text"/> <input type="button" value="Durchsuchen..."/></td> </tr> <tr> <td colspan="2"><input type="button" value="Upload"/></td> </tr> </table>			Subject	emailAddress=support@innominate.com,CN=ASG-75,O=Innominate,L=Berlin,C=de	Subject Alternative Names	• @ASG-75	Issuer	emailAddress=support@innominate.com,CN=Innominate VPN CA,O=Innominate,L=Berlin,C=de	Validity	From Nov 10 09:01:44 2009 GMT to Mar 27 09:01:27 2037 GMT	Fingerprint	MDS: 84:27:BF:45:B7:8F:C4:F6:16:61:95:8B:90:10:F0:FD SHA1: 85:6F:D8:15:54:68:42:E2:1E:BD:A5:81:70:0C:1D:0E:27:3B:0B:BD	Filename (*.pem):	<input type="text"/> <input type="button" value="Durchsuchen..."/>	<input type="button" value="Upload"/>	
Subject	emailAddress=support@innominate.com,CN=ASG-75,O=Innominate,L=Berlin,C=de																
Subject Alternative Names	• @ASG-75																
Issuer	emailAddress=support@innominate.com,CN=Innominate VPN CA,O=Innominate,L=Berlin,C=de																
Validity	From Nov 10 09:01:44 2009 GMT to Mar 27 09:01:27 2037 GMT																
Fingerprint	MDS: 84:27:BF:45:B7:8F:C4:F6:16:61:95:8B:90:10:F0:FD SHA1: 85:6F:D8:15:54:68:42:E2:1E:BD:A5:81:70:0C:1D:0E:27:3B:0B:BD																
Filename (*.pem):	<input type="text"/> <input type="button" value="Durchsuchen..."/>																
<input type="button" value="Upload"/>																	
<b>VPN Identifier</b>																	
Local	<input type="text" value="@mGuard-4711"/> Valid values are: <ul style="list-style-type: none"> <li>• the certificates distinguished name (same as no entry)</li> <li>• @mGuard-4711</li> </ul>																
Remote	<input type="text" value="@ASG-75"/> Valid values are: <ul style="list-style-type: none"> <li>• the certificates distinguished name (same as no entry)</li> </ul>																

IPsec VPN >> Connections		
<b>Authentication</b>	<b>Authentication method</b>	Select <i>X.509 Certificate</i> .
	<b>Local X.509 Certificate</b>	Select the mGuard machine certificate you have imported in chapter <a href="#">Import of the mGuard Machine Certificate</a> by its name.
	<b>Remote CA Certificate</b>	Select <i>No CA certificate, but the Remote Certificate below</i> .
	<b>Remote Certificate</b>	Click <b>&lt;Browse&gt;</b> , select the certificate (PEM export) of the ASG (refer to chapter <a href="#">ASG Certificate</a> ) and click <b>&lt;Upload&gt;</b> . For your convenience available alternative VPN identifiers, which are present in the certificate, are displayed in the row <i>Subject Alternative Names</i> , for example the hostname <i>ASG-75</i> in the screenshot above. Only the displayed <i>Subject Alternative Name</i> can be used as <i>Remote VPN Identifier</i> .
<b>VPN Identifier</b>		The mGuard uses by default the subject of the certificate (e.g. <i>CN=mGuard, O=Innominate, OU=Support</i> ) as VPN identifier. If another VPN identifier should be used, as for example <i>Hostname, IP Address</i> or <i>Email Address</i> , this VPN identifier must be present as <i>Subject Alternative Name</i> in the certificate. If you enter a hostname, it must be preceded by the character '@' (e.g. if the hostname is <i>ASG-75</i> , enter <i>@ASG-75</i> ).
	<b>Local</b>	If you have selected <i>Distinguished Name</i> as <i>VPN ID type</i> when creating the remote gateway on the ASG (refer to chapter <a href="#">Remote Gateway</a> ), leave this field empty. Otherwise enter the corresponding VPN identifier.
	<b>Remote</b>	Enter the VPN identifier as it is displayed for the <i>Local X509 Cert</i> on the ASG (menu <b>Site-to-site VPN &gt;&gt; Certificate Management</b> , tab <b>Certificates</b> ). The VPN identifier used by the ASG is also displayed on the ASG in the menu <b>Site-to-site VPN &gt;&gt; IPsec</b> , tab <b>Local RSA Key</b> .

### 4.2.3 Firewall

- Switch to the tab **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 pass through the VPN tunnel (default settings).

General Authentication **Firewall** IKE Options

**Incoming** Log ID: fw-vpn-in-Nº-17ebf757-11d7-1d75-9a03-000cbe022017

No	Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log
1	All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	default rule - please ac	No

Log entries for unknown connection attempts: No

**Outgoing** Log ID: fw-vpn-out-Nº-17ebf758-11d7-1d75-9a03-000cbe022017

No	Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log
1	All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	default rule - please ac	No

Log entries for unknown connection attempts: No

### 4.2.4 IKE Options

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

General	Authentication	Firewall	IKE Options
<b>ISAKMP SA (Key Exchange)</b>			
Encryption Algorithm	AES-256		
Hash Algorithm	SHA-1		
<b>IPsec SA (Data Exchange)</b>			
Encryption Algorithm	AES-256		
Hash Algorithm	SHA-1		
Perfect Forward Secrecy (PFS) (The remote site must have the same entry. Activation is recommended due to security reasons.)	Yes		
<b>Lifetimes</b>			
ISAKMP SA Lifetime	3600	seconds	
IPsec SA Lifetime	28800	seconds	
Rekeymargin	540	seconds	
Rekeyfuzz	100	%	
Keying tries (0 means unlimited tries)	0		
Rekey	Yes		
<b>Dead Peer Detection</b>			
Delay between requests for a sign of life	30	seconds	
Timeout for absent sign of life after which peer is assumed dead	120	seconds	

IPsec VPN >> Connections		
<b>ISAKMP SA</b>	<b>Encryption Algorithm</b>	Select the desired encryption algorithm, in our example <i>AES-256</i> . This algorithm must match to the one you have selected on the <i>ASG</i> (refer to <a href="#">IPSec Policy</a> , parameter <i>IKE encryption algorithm</i> ).
	<b>Hash Algorithm</b>	Select the desired hash algorithm, in our example <i>SHA-1</i> . This algorithm must match to the one you have selected on the <i>ASG</i> (refer to <a href="#">IPSec Policy</a> , parameter <i>IKE authentication algorithm</i> ).
<b>IPsec SA</b>	<b>Encryption Algorithm</b>	Select the desired encryption algorithm, in our example <i>AES-256</i> . This algorithm must match to the one you have selected on the <i>ASG</i> (refer to <a href="#">IPSec Policy</a> , parameter <i>IPsec encryption algorithm</i> ).
	<b>Hash Algorithm</b>	Select the desired hash algorithm, in our example <i>SHA-1</i> . This algorithm must match to the one you have selected on the <i>ASG</i> (refer to <a href="#">IPSec Policy</a> , parameter <i>IPsec authentication algorithm</i> ).
	<b>Perfect Forward Secrecy (PFS)</b>	Disable this option if you have disabled it on the <i>ASG</i> (refer to <a href="#">IPSec Policy</a> , parameter <i>IPsec PFS Group</i> ).
<b>Lifetimes</b>	<b>ISAKMP SA</b>	Adjust the lifetime accordingly if you have specified other than the mGuard default value on the <i>ASG</i> (refer to <a href="#">IPSec Policy</a> , parameter <i>IKE SA lifetime</i> ).
	<b>IPsec SA</b>	Adjust the lifetime accordingly if you have specified other than the mGuard default value on the <i>ASG</i> (refer to <a href="#">IPSec Policy</a> , parameter <i>IPsec SA lifetime</i> ).

- Click **<Apply>**.

## 5 Troubleshooting

After setting up the VPN connection, check its status in the menu **IPsec VPN >> IPsec Status**. Establishing a VPN connection consists of two phases: Phase I (ISAKMP SA) and phase II (IPsec SA). In case of a successful connection the status of **ISAKMP** and **IPsec** should be *established*.

Connection Name	Connection		ISAKMP State	IPsec State	
ASG (MAI0223580030_1)	<b>Gateway</b>	10.1.0.23	77.245.32.78	STATE_MAIN_I4 (ISAKMP SA established) Lifetime:2632s	STATE_QUICK_I2 (sent QI2, IPsec SA established) Lifetime:27342s
<input type="button" value="Edit"/>	<b>Traffic</b>	192.168.1.0/24	192.168.2.0/24		
<input type="button" value="Restart"/>	<b>ID</b>	@mGuard-4711	@ASG-75		
<input type="button" value="Update"/>					

The row *Gateway* displays the external/public IP addresses of both devices, *Traffic* the networks which are connected through the VPN tunnel and *ID* the specified VPN identifier for the local (mGuard) and the remote (ASG) VPN gateway.

If the VPN connection can not be established, check at first the **IPsec Status** on the mGuard to see how far it gets. Then inspect the VPN logging on the mGuard (**Logging >> Browse Local Logs**, option **IPsec VPN**) and on the ASG (**Site-to-site VPN >> IPsec**, button **<Open live log>**) for the first appearing error message when establishing the VPN connection.

### 5.1 ISAKMP SA could not be established

- **INVALID\_ID\_INFORMATION**: PSK or certificates do not match. If certificates are used for authentication, verify that on both sites the correct VPN identifier is specified (refer to the chapters ASG >> [Using Certificates](#) and mGuard >> [Using Certificates](#)).
- **NO\_POPOSAL\_CHOSEN**: The specified encryption and/or hash algorithm for phase I (IKE/ISAKMP SA) do not match on both sites (refer to the chapters ASG >> [IPSec Policy](#) and mGuard >> [IKE Options](#)).

### 5.2 ISAKMP SA established but not the IPsec SA

- **NO\_POPOSAL\_CHOSEN**: The specified encryption and/or hash algorithm for phase II (IPsec SA) do not match on both sites (refer to the chapters ASG >> [IPSec Policy](#) and mGuard >> [IKE Options](#)).
- The specified networks for the tunnel connection do not match on both sites.

### 5.3 Tunnel established but Peers of the Remote Network not reachable

- Check the configured firewall rules on the ASG (refer to [Firewall Rules](#)) and the VPN firewall rules on the mGuard (refer to [Firewall](#)) if they allow the desired traffic.
- The clients of the internal network of the mGuard must use the internal IP address of the mGuard as default gateway and the clients of the internal network of the ASG must use the internal IP address of the ASG as default gateway. Otherwise replies to packets received through the tunnel will not be sent back into the tunnel. An easy test is to “ping” the internal IP address of the mGuard from the internal network of the ASG through the VPN tunnel (assuming that the firewall rules for the tunnel allow “pings”). If this works but if you can not reach any other client of the internal network of the mGuard, probably those clients do not have the internal IP address of the mGuard specified as default gateway.