

## Interoperability Guide

Setting up a VPN connection between  
mGuard and Astaro V5/V6



***mGuard  
smart***



***mGuard  
PCI***



***mGuard  
blade***



***mGuard  
industrial***

© Innominate Security Technologies AG

August 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: 571009-147

**CONTENTS**

**1 Introduction.....4**

    1.1 *mGuard in Router/PPPoE/PPTP mode..... 4*

    1.2 *mGuard in Stealth mode..... 5*

**2 Limitations ..... 6**

**3 Configuration of the Astaro..... 6**

    3.1 *Network interfaces..... 6*

    3.2 *Creating X.509 certificates..... 6*

        3.2.1 *Create the CA..... 7*

        3.2.2 *Create a certificate for the Astaro..... 8*

        3.2.3 *Create a certificate for the mGuard..... 8*

        3.2.4 *Sign the Astaro and mGuard certificates with the CA..... 9*

        3.2.5 *Export of the certificates..... 10*

        3.2.6 *Define the Astaro certificate as local IPSec X.509 key ..... 10*

    3.3 *Creating Pre-Shared Keys..... 11*

    3.4 *Definition of the remote endpoint and remote subnet..... 12*

        3.4.1 *Definition of the remote endpoint (static IP address) ..... 12*

        3.4.2 *Definition of the remote endpoint (DynDNS)..... 12*

        3.4.3 *Definition of the remote subnet ..... 13*

    3.5 *IPSec Policies..... 14*

    3.6 *Configuring the VPN connection..... 15*

**4 Configuration of the mGuard..... 17**

    4.1 *mGuard in PPPoE/PPTP/Router mode..... 17*

        4.1.1 *Menu: VPN -> Connections ..... 17*

        4.1.2 *Menu: VPN -> Machine Certificate ..... 18*

    4.2 *mGuard in Stealth mode..... 19*

**5 Troubleshooting ..... 20**

    5.1 *ISAKMP couldn't be established..... 20*

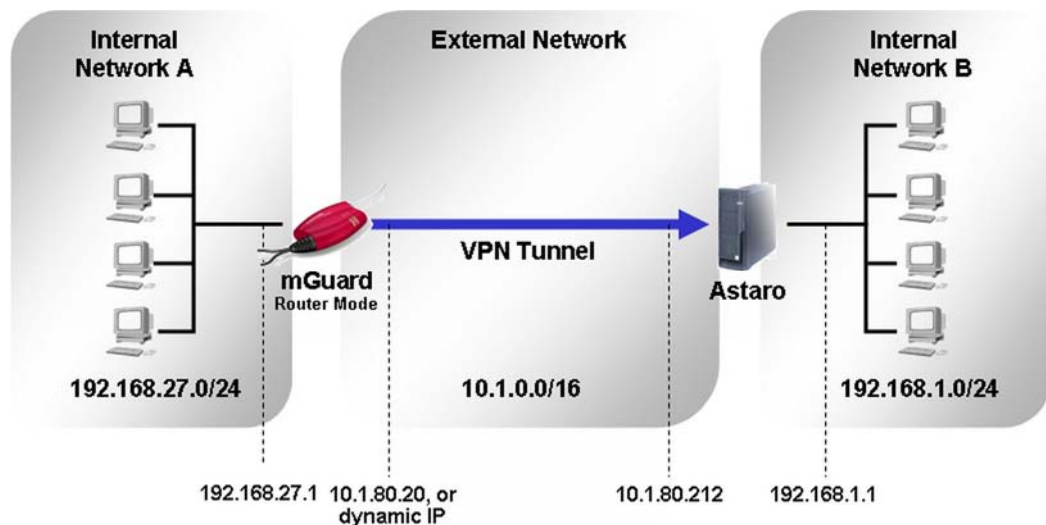
    5.2 *IPsec couldn't be established..... 20*

### 1 Introduction

This document describes the required steps to configure a VPN tunnel between the mGuard and the Astaro V5/V6. We have used an mGuard v2.3.1 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 X.509 certificates.

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/PPPoE/PPTP mode



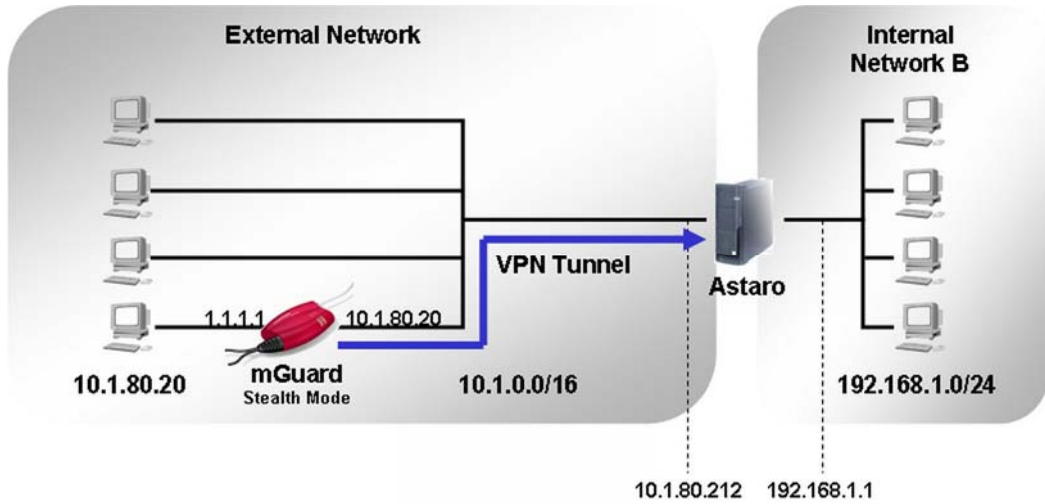
*Scenario used for the setup of the VPN tunnel between mGuard (Router mode) and Astaro*

We have selected for this setup 3DES as encryption algorithm and MD5 as hash algorithm for *IKE Policy* and *IPsec Policy*.

For this setup the parameters for the VPN tunnel are as follows:

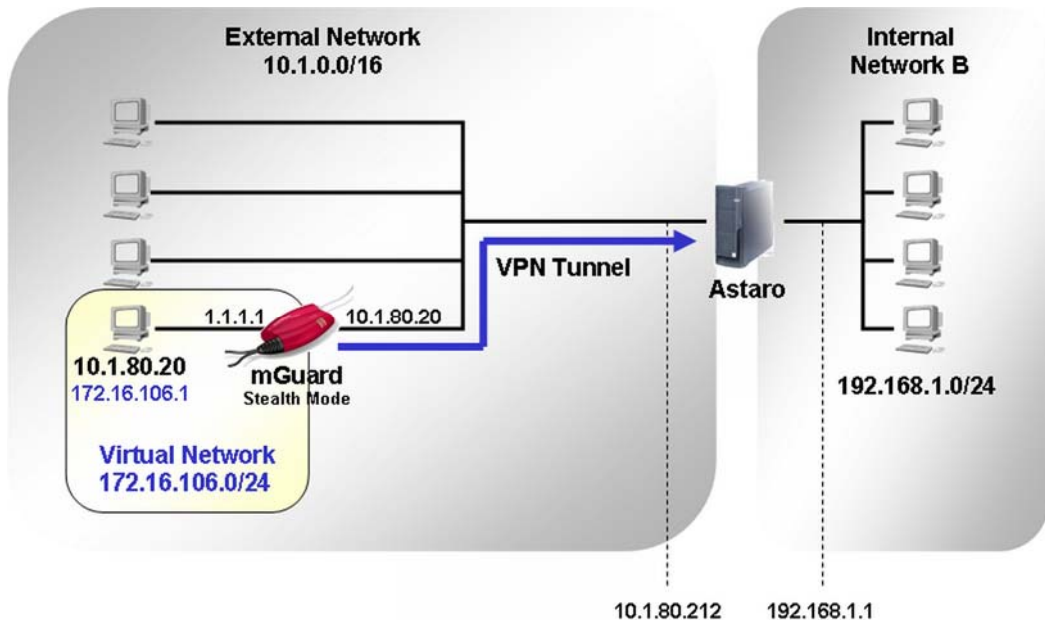
	<i>mGuard</i>	<i>Astaro</i>
<b>Remote VPN gateway</b>	10.1.80.212	10.1.80.20 or dynamic
<b>Local VPN subnet</b>	192.168.27.0/255.255.255.0	192.168.1.0/255.255.255.0
<b>Remote VPN subnet</b>	192.168.1.0/255.255.255.0	192.168.27.0/255.255.255.0
<b>IKE Policy, Encryption/Hash</b>	3DES/MD5	3DES/MD5
<b>IPsec Policy, Encryption/Hash</b>	3DES/MD5	3DES/MD5

1.2 mGuard in Stealth mode



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

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 IP address will be used for accessing 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 Astaro

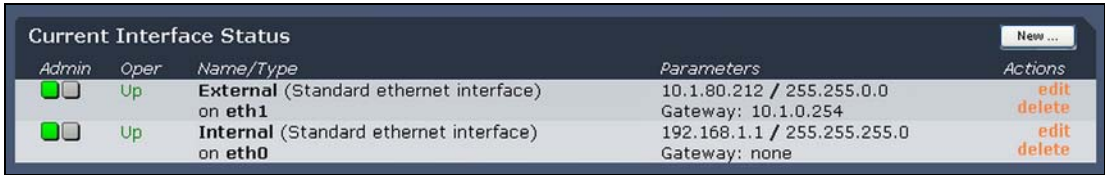
### 2 Limitations

- 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 X.509 certificates instead of PSK or register the mGuard with a fixed name in a DynDNS service and specify this name as remote peer on the Astaro.
- Astaro V5 does not support *Dead Peer Detection* (DPD).

### 3 Configuration of the Astaro

#### 3.1 Network interfaces

In our example the network interfaces were defined as follows (menu *Network -> Interfaces*).



Admin	Oper	Name/Type	Parameters	Actions
<input checked="" type="checkbox"/>	Up	<b>External</b> (Standard ethernet interface) on <b>eth1</b>	10.1.80.212 / 255.255.0.0 Gateway: 10.1.0.254	<a href="#">edit</a> <a href="#">delete</a>
<input checked="" type="checkbox"/>	Up	<b>Internal</b> (Standard ethernet interface) on <b>eth0</b>	192.168.1.1 / 255.255.255.0 Gateway: none	<a href="#">edit</a> <a href="#">delete</a>

#### 3.2 Creating X.509 certificates

Follow the instructions in this chapter if you want to use X.509 certificates as authentication method. You can create the required certificates on the Astaro. The following steps are required:

- Create the CA.
- Create a certificate for the Astaro.
- Create a certificate for the mGuard.
- Sign the Astaro and mGuard certificates with the CA.
- Export of the certificates.
- Define the Astaro certificate as local IPSec X.509 key.

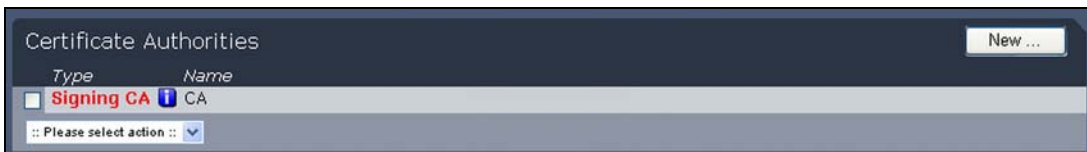
### 3.2.1 Create the CA

- Select **IPSec VPN -> CA Management** from the menu.
- Click **New** in the **Certificates Authority** section.

<input checked="" type="radio"/> Generate	Name:	CA
	Passphrase:	password
	Key Size:	1024 Bits
	Country:	Germany
	State/Region:	de
	City/Locality:	Berlin
	Organization:	Innominate
	Dept./Org.Unit:	Support
	Common Name:	CA
	E-Mail Address:	support@innominate.com

- Select the option **Generate**.
- Enter a descriptive **Name** for the certificate authority.
- Enter a password in the **Passphrase** field.
- Use the drop-down menus and entry fields from **Country** to **E-Mail Address** for entering the identifying parameters.
- Click **Start** for creating the CA.

As result the CA is displayed.



### 3.2.2 Create a certificate for the Astaro

- Select **IPSec VPN -> CA Management** from the menu.
- Click **New** in the **Host CSRs and certificates** section.

The screenshot shows a form titled 'Generate CSR' with the following fields and values:

VPN ID:	X.509 DN
Name:	Astaro
Passphrase:	password
Key Size:	1024 Bits
Country:	Germany
State/Region:	de
City/Locality:	Berlin
Organization:	Innominate
Dept./Org.Unit:	Support
Common Name:	Astaro
E-Mail Address:	support@innominate.com

- Select the option **Generate CSR**.
- Set **VPN ID** to **X.509 DN**.
- Enter a descriptive **Name** for the certificate.
- Enter a password in the **Passphrase** field.
- Use the drop-down menus and entry fields from **Country** to **E-Mail Address** for entering the identifying parameter.
- Click **Start** for creating the certificate.

As result the Astaro certificate is displayed.

Type	Name	VPN ID
<input type="checkbox"/> CSR+KEY	Astaro	X.509 DN from CERT/CSR body

Below the table is a dropdown menu with the text 'Please select action'.

### 3.2.3 Create a certificate for the mGuard

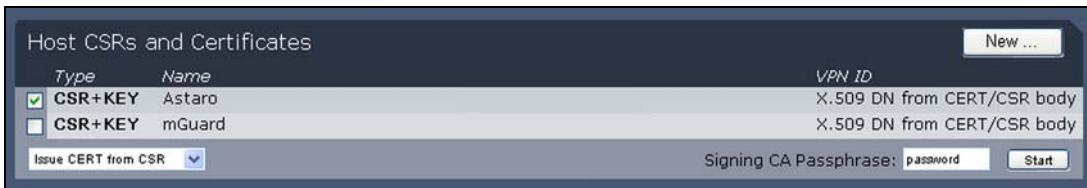
Repeat the previous step for creating the certificate for the mGuard. As result the mGuard certificate is also displayed.

Type	Name	VPN ID
<input type="checkbox"/> CSR+KEY	Astaro	X.509 DN from CERT/CSR body
<input type="checkbox"/> CSR+KEY	mGuard	X.509 DN from CERT/CSR body

Below the table is a dropdown menu with the text 'Please select action'.

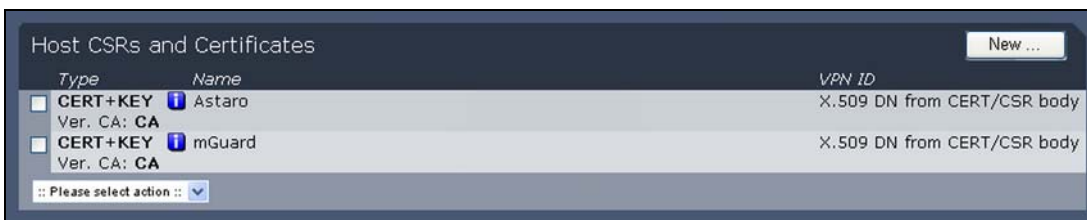
### 3.2.4 Sign the Astaro and mGuard certificates with the CA

- Select **IPSec VPN -> CA Management** from the menu.



- Select the Astaro certificate.
- Select the action **Issue CERT from CSR**.
- Enter as **Signing CA Passphrase** the password you have entered in the *Passphrase* field when creating the CA.
- Click **Start**.

Repeat those steps for signing the mGuard certificate with the CA. As result both certificates are marked with the blue information button.



### 3.2.5 Export of the certificates

The following certificate exports are required:

- Astaro certificate as PEM: This certificate needs to be imported on the mGuard as connection certificate (menu *VPN* -> *Connections*).
- mGuard certificate as PKCS#12: This certificate needs to be imported on the mGuard as machine certificate (menu *VPN* -> *Machine Certificate*).

Export of the Astaro certificate:

- Select **IPSec VPN** -> **CA Management** from the menu.
  - Select the Astaro certificate.
  - Select the action **Download as PEM**.
- ⇒ The *file download* wizard appears which allows storing the certificate to the local system. The certificate is exported as zip file which contains the files *CERTIFICATE\_\*.pem* and *KEY\_\*.pem*. Only the file *CERTIFICATE\_\*.pem* needs to be uploaded on the mGuard as connection certificate.

Export of the mGuard certificate:

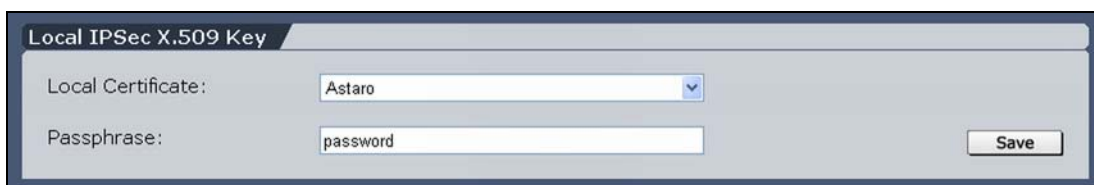
- Select **IPSec VPN** -> **CA Management** from the menu.
- Select the mGuard certificate.
- Select the action **Download as PKCS#12**.



- Enter the **Export Password** which protects the certificate against unauthorized usage.
  - Enter as **Signing CA Passphrase** the password you have entered in the *Passphrase* field when creating the CA.
  - Click **Start**.
- ⇒ The *file download* wizard appears which allows storing the certificate to the local system.

### 3.2.6 Define the Astaro certificate as local IPSec X.509 key

- Select **IPSec VPN** -> **Local Keys** from the menu.



- Select the Astaro certificate as **Local Certificate**.
  - Enter as **Passphrase** the password you have entered in the *Passphrase* field when creating the Astaro certificate.
  - Click **Save**.
- ⇒ As result the Astaro certificate is displayed as active key.

### 3.3 Creating Pre-Shared Keys

Follow the instructions in this chapter if you want to use preshared keys as authentication method.

- Select **IPSec VPN -> Remote Keys** from the menu.



New Remote IPSec Key

Name: PSK\_mGuard\_Astaro

Virtual IP (optional):

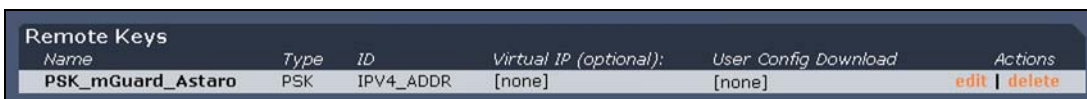
Key Type: PSK

Preshared Key: shared\_secret

VPN Identifier: Remote IP Address Add

- Enter a descriptive **Name** for the remote key.
- Set **Key Type** to **PSK**.
- Enter the **Preshared Key**.
- Click **Add**.

As result the remote key is displayed.



Name	Type	ID	Virtual IP (optional):	User Config Download	Actions
PSK_mGuard_Astaro	PSK	IPV4_ADDR	[none]	[none]	edit   delete

### 3.4 Definition of the remote endpoint and remote subnet

Once the certificates or PSK have been created, you need to create network objects for the remote endpoint and for the remote subnet of the mGuard.

Note the following if the mGuard has a dynamic public IP address:

- If PSK shall be used then the mGuard needs to register its IP address with a fixed name in a DynDNS service (refer to *Limitations*). In this case you need to define the remote endpoint of the mGuard as described in chapter *Definition of the remote endpoint (DynDNS)*.
- If certificates are used you don't need to define a network object for the remote endpoint of the mGuard. In this case you can specify that the mGuard has a dynamic IP address when configuring the IPSec connection on the Astaro.

#### 3.4.1 Definition of the remote endpoint (static IP address)

Perform this step if the mGuard has a static public IP address.

- Select **Definitions -> Networks** from the menu.
- Click **New Definitions**.



The screenshot shows the 'Network Definitions' window with 'Total 9 entries'. The form fields are: Name: mGuard\_IP, Type: Host (dropdown), Address: 10.1.80.20, and Comment: mGuard external IP address. An 'Add Definition' button is at the bottom.

- Enter a descriptive **Name** for the network object.
- Set **Type** to **Host**.
- Enter into the **Address** field the external IP address of the mGuard, in our example 10.1.80.20.
- Click **Add Definition**.

#### 3.4.2 Definition of the remote endpoint (DynDNS)

Perform this step if the mGuard registers its IP address with a fixed name in a DynDNS service.

- Select **Definitions -> Networks** from the menu.
- Click **New Definitions**.

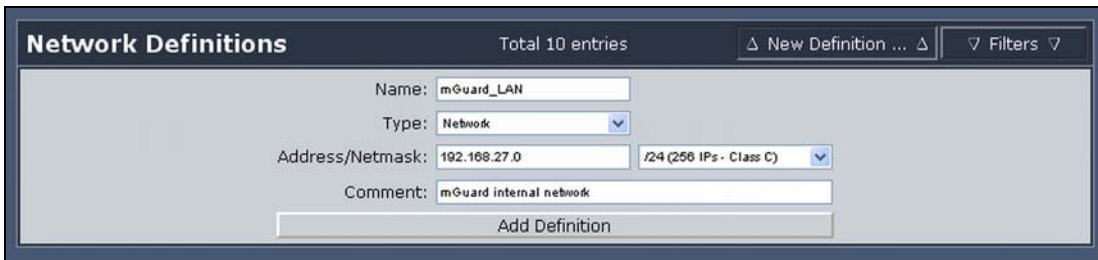


The screenshot shows the 'Network Definitions' window with 'Total 13 entries'. The form fields are: Name: mGuard\_DynDNS, Type: DNS hostname (dropdown), Hostname: mGuard.dyndns.org, and Comment: mGuard DynDNS name. An 'Add Definition' button is at the bottom.

- Enter a descriptive **Name** for the network object.
- Set **Type** to **DNS hostname**.
- Enter in the **Hostname** field the DynDNS name of the mGuard.
- Click **Add Definition**.

### 3.4.3 Definition of the remote subnet

- Select **Definitions** -> **Networks** from the menu.
- Click **New Definitions**.



The screenshot shows a web interface for defining network objects. The title is "Network Definitions" with a subtitle "Total 10 entries". There are two buttons at the top right: "New Definition ..." and "Filters". The form contains the following fields:

- Name:** mGuard\_LAN
- Type:** Network (dropdown menu)
- Address/Netmask:** 192.168.27.0 (text input) and /24 (256 IPs - Class C) (dropdown menu)
- Comment:** mGuard internal network (text input)
- Add Definition** (button)

- Enter a descriptive **Name** for the network object.
- Set **Type** to **Network**.
- Enter in the **Address** field the network IP of the internal network of the mGuard and select the corresponding **Netmask**.
- Click **Add Definition**.

### 3.5 IPSec Policies

Astaro provides a couple of predefined IPSec policies. Select **IPSec VPN -> Policies** from the menu for getting the list of available policies. Nevertheless we have created a new policy for adjusting the ISAKMP SA and the IPSec SA lifetimes to the settings on the mGuard.

- Select **IPSec VPN -> Policies** from the menu.
- Click **New**.

**New IPSec Policy**

Name:

Key Exchange:

---

**ISAKMP (IKE) Settings**

IKE Mode:

Encryption Algorithm:

Authentication Algorithm:

IKE DH Group:

SA Lifetime (secs):

---

**IPSec Settings**

IPSec Mode:

IPSec Protocol:

Encryption Algorithm:

Enforce Algorithms:

Authentication Algorithm:

SA Lifetime (secs):

PFS:

Compression:

- Set **IKE Mode** to **Main Mode**. *Aggressive Mode* is currently not supported by the mGuard.
- The selected **Encryption** and **Authentication Algorithms** for ISAKMP and IPSec must correspond to the settings on the mGuard. In our example we have chosen 3DES and MD5.
- Also the specified **SA lifetimes** must correspond to the settings on the mGuard. The default settings are for the ISAKMP SA lifetime 3600 seconds and for the IPSec SA lifetime 28800 seconds.
- If you enable **PFS** you also need to enable PFS on the mGuard.
- Turn off the **Compression**. IP compression is not supported by the mGuard.
- Click **Add**.

### 3.6 Configuring the VPN connection

- Select **IPSec VPN -> Connections** from the menu.
  - Enter a descriptive **Name** for the connection in the section **New IPSec Connection**.
  - Set **Type** to **Standard**.
- ⇒ After doing this, additional entry fields appear.

**New IPSec Connection**

Name:

Type:

IPSec Policy:

Auto Packet Filter:

Strict Routing:

---

**Endpoint Definition**

Local Endpoint:

Remote Endpoint:

---

**Subnet definition (optional)**

Local Subnet:

Remote Subnet:

---

**Authentication of remote Station(s)**

Key:

- Select the **IPSec Policy** you've created in chapter *IPSec Policies*.
- Specify the external interface of the Astaro as **Local Endpoint**.
- Enter as **Remote Endpoint** one of the following options:
  - If the mGuard has a static public IP address, select the network object you've created in chapter *Definition of the remote endpoint (static IP address)*.
  - If the mGuard registers its dynamic IP address with a fixed name in a DynDNS service, select the network object you've created in chapter *Definition of the remote endpoint (DynDNS)*.
  - Otherwise select >> **Dynamic IP address** <<.
- Specify the internal network of the Astaro as **Local Subnet**.
- Select as **Remote Subnet** the network object you've created in chapter *Definition of the remote subnet* which specifies the internal network of the mGuard.
- Select as **Authentication** either the preshared key you've created in chapter *Creating Pre-Shared Keys* or the mGuard certificate you've created in chapter *Create a certificate for the mGuard*.
- Click **Add**.

As result the VPN connection is displayed. The connection is inactive.

Name	Type	Local <-> Remote Endpoints	Actions
<input type="checkbox"/> <input type="checkbox"/> VPN_mGuard_Astaro	<input type="checkbox"/> Standard	External <-> Any	<input type="button" value="edit"/> <input type="button" value="delete"/>

Click at the gray button right beside the red button for activating the connection.

## VPN between mGuard and Astaro V5/V6

---

IPSec Connections				
	Name	Type	Local <-> Remote Endpoints	Actions
<input checked="" type="checkbox"/>	VPN_mGuard_Astaro	Standard	External <-> Any	<a href="#">edit</a>   <a href="#">delete</a>

## 4 Configuration of the mGuard

### 4.1 mGuard in PPPoE/PPTP/Router mode

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

- Configuration of the VPN connection through the menu **VPN -> Connections**.
- Import of the mGuard machine certificate (if certificates are used as authentication method) through the menu **VPN -> Machine Certificate**.

#### 4.1.1 Menu: VPN -> Connections

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

VPN > Connections > Connection Astaro

A descriptive name for the connection	Astaro														
Enabled	Yes														
Address of the remote site's VPN gateway (either an IP address, a hostname, or %any)	10.1.80.212														
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"/>														
<b>Tunnel Settings</b>															
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														
<b>Firewall Incoming (untrusted port)</b>															
<input type="checkbox"/> <input type="button" value="X"/>	<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>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>No</td> </tr> </tbody> </table>	Protocol	From IP	From Port	To IP	To Port	Action	Log	All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	No
Protocol	From IP	From Port	To IP	To Port	Action	Log									
All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	No									
Log entries for unknown connection attempts						<input type="button" value="No"/>									
<b>Firewall Outgoing (trusted port)</b>															
<input type="checkbox"/> <input type="button" value="X"/>	<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>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>No</td> </tr> </tbody> </table>	Protocol	From IP	From Port	To IP	To Port	Action	Log	All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	No
Protocol	From IP	From Port	To IP	To Port	Action	Log									
All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	No									
Log entries for unknown connection attempts						<input type="button" value="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 Astaro (in our example *10.1.80.212*).
- 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 Astaro certificate (CERTIFICATE\_\*.pem).
- 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 ....**

## VPN between mGuard and Astaro V5/V6

- **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 Astaro (in our example *192.168.1.0/255.255.255.0*).
- Click **Configure** in the row *More IKE Options*.

The screenshot shows the 'More IKE Options' configuration page for 'Connection Astaro'. The page is divided into several sections:

- 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.

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

- The **ISAKMP SA (Key Exchange)**, **IPSec SA (Data exchange)** as well as the **Lifetimes** must correspond to the setting on the Astaro (*IPSec Policy*).
- Click **Back**.
- Click **OK**.

### 4.1.2 Menu: VPN -> Machine Certificate

This step is only required if you use certificates.

- Select **VPN -> Machine Certificate** from the menu.

The screenshot shows the 'Machine Certificate' dialog box. It has a title bar 'VPN > Machine Certificate' and a 'New Certificate' label on the left. The main area contains two input fields: 'PKCS#12 Filename (\*.p12):' with a 'Durchsuchen...' button, and 'Password:'. Below these fields is an 'Import' button. At the bottom of the dialog is an 'OK' button.

- Click **Browse**.
- Specify the PKCS#12 export of the mGuard certificate, in our example *mGuard.p12*.
- Click **Import**.
- When the import of the certificate is finished, click **OK**.

### 4.2 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 behind the mGuard through the VPN tunnel from the internal network of the Astaro.

On the Astaro you need to use the virtual network when configuring the network object for the remote subnet (refer to *Definition of the remote subnet*).

### 5 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
Astaro	Gateway	10.1.80.20		10.1.80.212	
	Traffic	192.168.27.0/24 /		192.168.1.0/24 /	
	ID	C=de, ST=de, L=Berlin, O=Innominat, OU=Support, CN=mGuard, E=support@innominate.com		C=de, ST=de, L=Berlin, O=Innominat, OU=Support, CN=Astaro, E=support@innominate.com	
			STATE_MAIN_I4 (ISAKMP SA established)	STATE_QUICK_I2 (sent QI2, IPsec SA established)	
<input type="button" value="Update"/>					

#### 5.1 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 preshared keys or certificates.
- The mGuard is configured to use PFS but PFS is not enabled on the Astaro.
- Mismatched ISAKMP policy parameters. Compare the *ISAKMP SA (Key exchange)* settings on the mGuard (menu *VPN -> Connection, More IKE Options*) with the *IPsec Policy* settings on the Astaro.

#### 5.2 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. Compare the *IPsec SA (Data exchange)* settings on the mGuard (menu *VPN -> Connection, More IKE Options*) with the *IPsec Policy* settings on the Astaro.
- Mismatched VPN tunnel parameters. Compare the *Tunnel settings* on the mGuard (menu *VPN -> Connection*) with the specified subnets and endpoints (*IPsec VPN connection*) on the Astaro.