

# Interoperability Guide

## Configuring a Site-to-Site VPN between mGuard and Cisco ASA



*mGuard smart*



*mGuard PCI*



*mGuard blade*



*mGuard industrial RS*



*mGuard delta*

Innominate Security Technologies AG  
Albert-Einstein-Str. 14  
12489 Berlin, Germany

Phone: +49 (0)30-6392 3300  
Fax: +49 (0)30-6392 3307  
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 (Router/PPPoE/PPTP)</i>	4
2.2	<i>mGuard in Single-Stealth Mode</i>	5
<b>3</b>	<b>Limitations in using PSK</b>	<b>5</b>
<b>4</b>	<b>X.509 Certificates</b>	<b>6</b>
4.1	<i>Import of the mGuard's Machine Certificate</i>	6
4.2	<i>Import of the CA Certificate on the Cisco ASA</i>	7
4.3	<i>Creating the Identity Certificate on the Cisco ASA</i>	7
<b>5</b>	<b>Configuring the Cisco ASA</b>	<b>9</b>
5.1	<i>IKE Policy</i>	9
5.2	<i>IPsec Transform Set</i>	10
5.3	<i>Access List</i>	11
5.4	<i>Configuring the VPN connection</i>	12
5.4.1	<i>Basic Settings</i>	12
5.4.2	<i>Crypto Map Settings</i>	13
5.4.3	<i>Tunnel Group Settings</i>	14
5.5	<i>Configuring Tunnel Groups</i>	15
5.6	<i>Runtime Settings</i>	16
5.6.1	<i>VPN Configuration with PSK</i>	16
5.6.2	<i>VPN Configuration with Certificates</i>	17
<b>6</b>	<b>Configuring the mGuard</b>	<b>18</b>
6.1	<i>General Settings</i>	18
6.2	<i>Authentication</i>	18
6.2.1	<i>PSK</i>	18
6.2.2	<i>Certificates</i>	19
6.3	<i>Firewall</i>	19
6.4	<i>IKE Options</i>	20
<b>7</b>	<b>Troubleshooting</b>	<b>21</b>
7.1	<i>ISAKMP (IKE) SA couldn't be established</i>	21
7.2	<i>IPsec SA couldn't be established</i>	21
<b>8</b>	<b>Reference</b>	<b>21</b>

## **1 Disclaimer**

© Innominate Security Technologies AG

November 2008

“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.

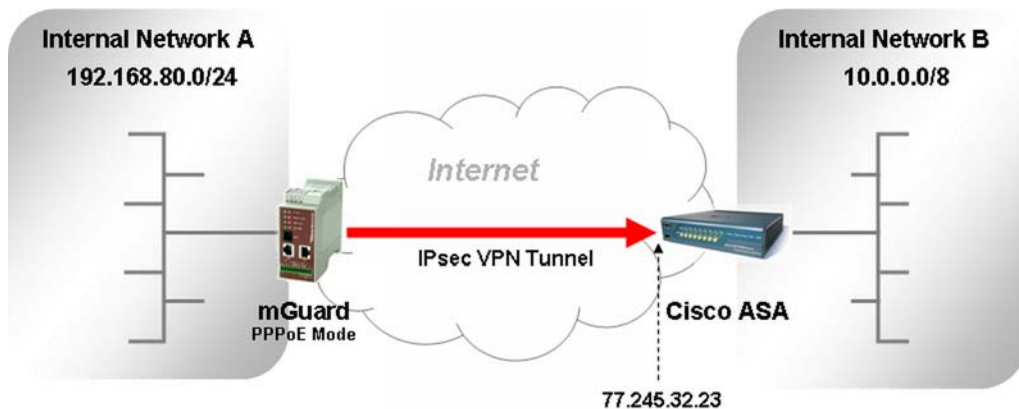
## 2 Introduction

This document describes the required steps to configure a site-to-site VPN between mGuard and Cisco ASA, using X.509 certificates or *Pre-Shared Keys (PSK)* for authentication. We have used Cisco ASA 5510 (ASA version 8.0(3)) and mGuard v5.1.0 and v6.0.1 for this interoperability test. The VPN tunnel will be initiated by the mGuard. We have configured the Cisco ASA through the *Cisco ASDM Launcher 6.0(3)*.

 **Note:** Configuring a VPN using certificates is considered more secure than using *Pre-Shared Keys*.

### 2.1 mGuard in Router Mode (Router/PPPoE/PPTP)

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



Scenario used for the setup of the VPN tunnel between the mGuard and the Cisco ASA

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 configuration are as follows:

Using certificates for authentication:

VPN parameter	mGuard	Cisco ASA
Remote VPN gateway	Static public IP of the Cisco ASA or its DynDNS name	<Dynamic IP>
Local VPN subnet	192.168.80.0/24	10.0.0.0/8
Remote VPN subnet	10.0.0.0/8	192.168.80.0/24
ISAKMP Policy, Encryption / Hash	AES 256 / SHA	AES-256 / SHA-1
IPsec Policy, Encryption / Hash	AES 256 / SHA	AES-256 / SHA-1

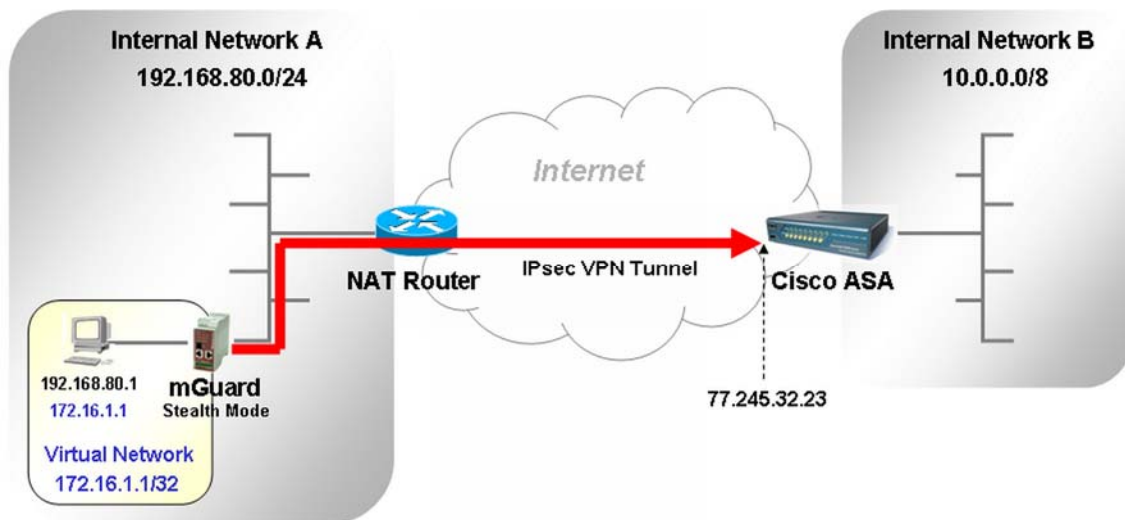
Using PSK for authentication:

VPN parameter	mGuard	Cisco ASA
Remote VPN gateway	Static public IP of the Cisco ASA or its DynDNS name	Static public IP of the mGuard or its DynDNS name
Local VPN subnet	192.168.80.0/24	10.0.0.0/8
Remote VPN subnet	10.0.0.0/8	192.168.80.0/24
ISAKMP Policy, Encryption / Hash	AES 256 / SHA	AES-256 / SHA-1
IPsec Policy, Encryption / Hash	AES 256 / SHA	AES-256 / SHA-1

## 2.2 mGuard in Single-Stealth Mode

If the mGuard is operated in *Single Stealth* mode (autodetect/static) to protect one single client, you need to distinguish between the following cases:

- If the client uses static IP settings and if the IP address of the client does not belong to the remote network, you can use the IP address of the client (192.168.80.1/32) as local network when configuring the VPN tunnel.
- If the IP address of the client belongs to the remote network or if the client receives its IP settings from a DHCP server with a slight chance that the clients IP address may change, use a virtual network (e.g. 172.16.1.1/32) as local network when configuring the VPN tunnel. The virtual IP of the client (172.16.1.1) only needs to be used when accessing the client from the remote network through the VPN tunnel.



## 3 Limitations in using PSK

- 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 certificates must be used for authentication.
- If one site has a dynamic public IP address and if PSK is used for authentication, it must register its IP address under a fixed name in a DynDNS service and the remote VPN gateway must refer to this name.

## 4 X.509 Certificates

When using certificates for authentication, the following certificates are required:

- An **mGuard certificate** signed by a **CA certificate**. You can use freeware tools like for example XCA or OpenSSL for creating the CA and the mGuard certificate or you may request them from a Microsoft CA server. Please refer to the document *How to obtain X.509 certificates* which is available through our homepage (<http://www.innominat.com> -> Downloads -> Application Notes).
  - The CA certificate must be imported on the Cisco ASA (section *Site-to-Site VPN*, menu *Certificate Management* -> *CA Certificates*).
  - The PKCS#12 export of the mGuard certificate must be imported on the mGuard through the menu *Authentication* -> *Certificates*, tab *Machine Certificates*).
- An **identity certificate** to authenticate the VPN access. This certificate will be created on the Cisco ASA (section *Site-to-Site VPN*, menu *Certificate Management* -> *Identity Certificates*) and needs to be imported on the mGuard when configuring the VPN connection (menu *IPsec VPN* -> *Connections*, tab *Authentication*).

**Note:** Creating a self-signed certificate for the mGuard on the Cisco ASA as identity certificate, exporting it as PKCS#12 and using this export on the mGuard as machine certificate will not work. The Cisco ASA authenticates the certificate of the mGuard by the CA certificate which was used for signing the mGuard's certificate. This CA certificate does not exist when creating the mGuard's certificate on the Cisco ASA as self-signed certificate.

### 4.1 Import of the mGuard's Machine Certificate

- From the menu, select **Authentication** -> **Certificates**, tab **Machine Certificates**.
- Click **Browse** and open the PKCS#12 export of the mGuard certificate.
- Enter the **Password** which protects the certificate against unauthorized usage.
- Click **Import** and then **Apply**.

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

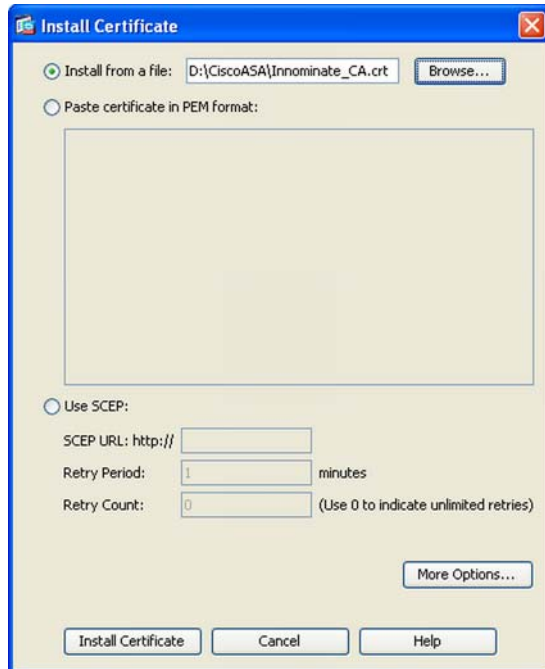
The screenshot shows the 'Authentication » Certificates' section with the 'Machine Certificates' tab selected. The 'Certificate' details are as follows:

Certificate	
Subject	CN=mGuard,OU=Support,O=Innominat
Subject Alternative Names	
Issuer	CN=Innominat CA,OU=Support,O=Innominat
Validity	From Jul 21 13:01:53 2008 GMT to Jul 19 13:01:53 2017 GMT
Fingerprint	MD5: 65:11:E1:86:6B:BD:C3:10:03:72:B4:E7:08:92:13:D3 SHA1: 34:52:F7:4A:89:E9:EB:29:D4:E3:55:00:27:ED:BC:72:4A:8A:E2:3C
Shortname	mGuard
Upload PKCS#12	Filename: <input type="text"/> <input type="button" value="Durchsuchen..."/> <input type="button" value="Import"/>
	Password: <input type="password" value="****"/>
Download Certificate	<input type="button" value="Current Certificate File"/>

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

## 4.2 Import of the CA Certificate on the Cisco ASA

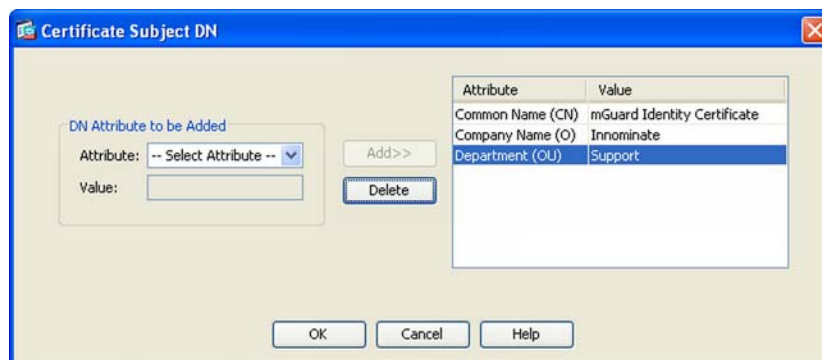
- At first create a PEM export of the CA certificate which was used for signing the mGuard certificate.
- On the Cisco ASA, switch to the section **Site-To-Site VPN**.
- From the menu, select **Certificate Management -> CA Certificates**.
- Click **Add**.



- Select **Install from a file**.
  - Click **Browse** and open the PEM export of the CA certificate.
  - Click **Install Certificate**.
- ⇒ A message should indicate that the CA certificate was imported successfully.
- Of course you may also open the PEM export of the CA certificate with a text editor and use the option **Paste certificate in PEM format** to import the certificate.

## 4.3 Creating the Identity Certificate on the Cisco ASA

- Switch to the section **Site-To-Site VPN**.
- From the menu, select **Certificate Management -> Identity Certificates**.
- Click **Add**.
- Select the option **Add a new identify certificate**.
- Click **Select** in the line *Certificate Subject DN*.



- Select the type of **Attribute** you want to specify (e.g. CN, O, OU, etc.), enter the **Value** and click **Add**. Repeat this step until you have entered all desired attributes.
  - Click **OK**.
  - Back in the *Add Identity Certificate* dialog, select **Generate self-signed certificate**.
  - Click **Advanced**.
  - Ensure that all entries (*FQDN*, *E-mail* and *IP Address*) are empty and click **OK**.
  - Click **Add Certificate**.
- ⇒ A message should indicate that the certificate was enrolled successfully.

To export the identity certificate:

- Highlight the identity certificate in the table.
  - Click **Export**.
  - Choose **PEM Format** as *Certificate Format*.
  - Click **Browse**.
  - Specify the location on your local system where the certificate should be stored and enter the filename (e.g. *CiscoASA.pem*). Click **Export ID certificate file**.
  - Click **Export Certificate**.
- ⇒ A message should indicate that the certificate was exported successfully.

This certificate needs to be imported on the mGuard when configuring the VPN connection (menu *IPsec VPN -> Connections*, tab *Authentication*).

## 5 Configuring the Cisco ASA


- Start the *Cisco ASDM Launcher* and connect to the device.
- From the toolbar, select **Configuration** and switch to the **Site-to-Site VPN** configuration.

### 5.1 IKE Policy

The IKE policy specifies which encryption and hash algorithm should be used for establishing the ISAKMP (IKE) security association (SA) (phase I), its lifetime, the Diffie-Hellmann group which will be used when performing a new Diffie-Hellmann exchange and whether the IKE policy should be used for certificate or PSK authentication.

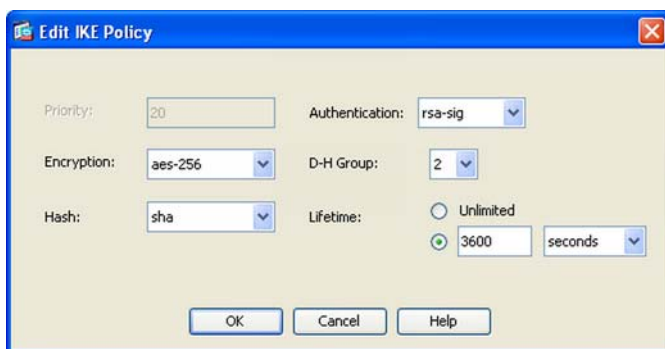
It may be possible that an according IKE policy with the desired parameters is already configured on the device. Please check this first before creating a new policy.

---

 **Note:** The lifetime of the ISAKMP (IKE) SA must exactly match to the one specified on the mGuard (default value = 3600 seconds). Otherwise establishing the VPN connection will fail.

---

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



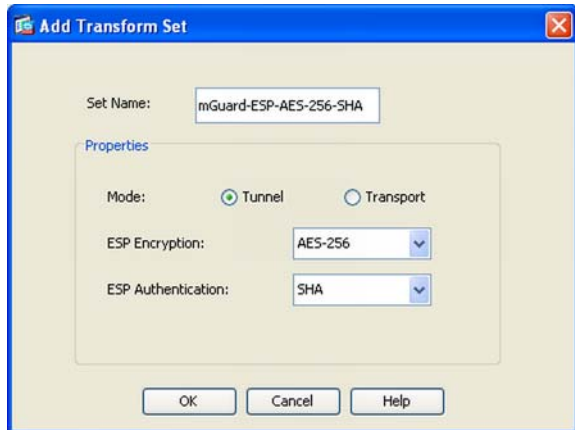
- Enter a **Priority** for the policy.
- Select the desired **Encryption** and **Hash** algorithm, in our example AES-256 and SHA.
- Select as **Authentication** either *pre-share* or *rsa-sig*, depending on whether PSK or certificates are used for authentication.
- Select **DH-Group 2**.
- The specified **Lifetime** must match to the one specified on the mGuard. The default value on the mGuard is *3600* seconds.
- Click **OK**.

## 5.2 IPsec Transform Set

The IPsec transform set specifies which encryption and hash algorithm should be used for establishing the IPsec SA (phase II) and whether the connection is a tunnel (net-to-net) or a transport (host-to-host) connection.

It may be possible that an according set with the desired parameters is already configured on the device. Please check this first before creating a new policy.

- From the menu, select **Advanced -> IPsec Transform Sets**.
- Click **Add**.

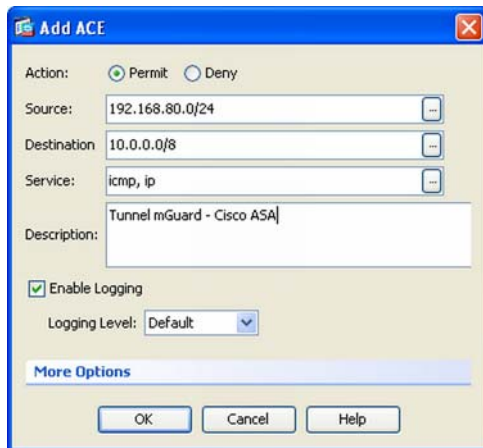


- Enter a descriptive **Name** for the transform set.
- Set **Mode** to **Tunnel**.
- Select the desired encryption and hash algorithm, in our example AES-256 and SHA.
- Click **OK**.
- Click **Apply**.

### 5.3 Access List

The access list controls connections between inside and outside networks. You need to create an access list entry to allow traffic between the internal network of the mGuard and the Cisco.

- From the menu, select **Advanced -> ACL Manager**.
- Click **Add -> Add ACL**.
- Enter a descriptive name for the access list and click **OK**.
- ⇒ The new created access list name is displayed in the list.
- Highlight the new created access list and click **Add -> Add ACE**.

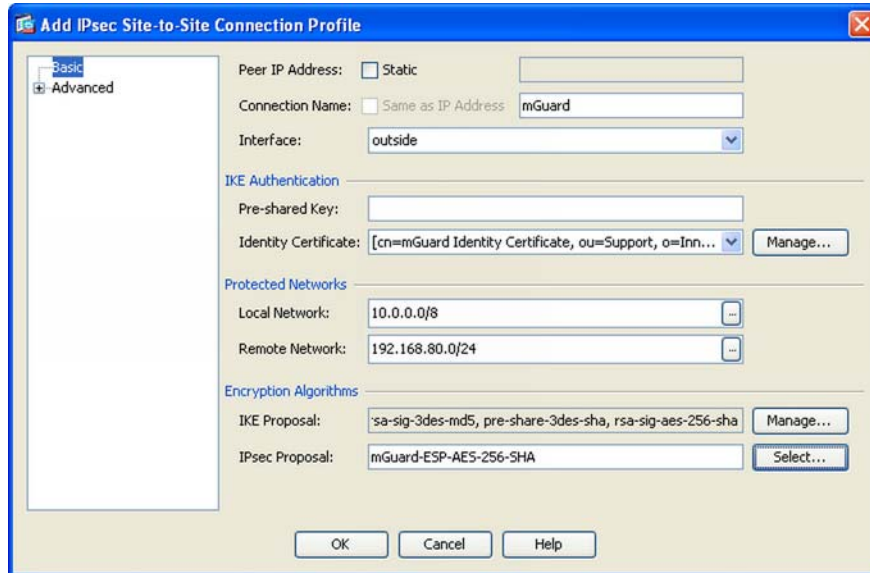


- Select **Permit** as **Action**.
- **Source**: Click the button to the right of this line. The *Browse Source* dialog appears.
  - Select the internal network of the mGuard, in our example 192.168.80.0/24. If this network doesn't exist, click **Add**, create the according network object and click **OK**.
- **Destination**: Click the button to the right of this line. The *Browse Destination* dialog appears.
  - Select the internal network of the Cisco, in our example 10.0.0.0/8. If this network doesn't exist, click **Add**, create the according network object and click **OK**.
- **Service**: Click the button to the right of this line and select the services which should be allowed between both internal networks.
- Click **OK**.
- Click **Apply**.

## 5.4 Configuring the VPN connection

### 5.4.1 Basic Settings

- From the menu, select **Connection Profiles** and click **Add**.



- Peer IP Address:** If the mGuard has a static public IP address or if the mGuard registers its dynamic public IP address under a fixed name in a DynDNS service, check **Static** and enter the mGuard's IP address or DynDNS name. This is absolutely required when using PSK for authentication. Otherwise uncheck the option **Static**.
- Connection name:** Enter a descriptive name for the connection.
- Select the **Interface** which should listen for incoming VPN connections.
- IKE authentication**
  - When using PSK, enter the **Pre-shared Key**.
  - When using certificates, select the **Identity Certificate** you've created in chapter [Creating the Identity Certificate on the Cisco ASA](#).
- Protected Networks**
  - Local Network:** Click the button to the right of this line. The *Browse Local Network* dialog appears.
    - Select the internal network of the Cisco, in our example 10.0.0.0/8. If this network doesn't exist, click **Add**, create the according network object and click **OK**.
  - Remote Network:** Click the button to the right of this line. The *Browse Remote Network* dialog appears.
    - Select the internal network of the mGuard, in our example 192.168.80.0/24. If this network doesn't exist, click **Add**, create the according network object and click **OK**.
- Encryption Algorithms**
  - The **IKE Proposal** should already contain the desired settings (refer to chapter [IKE Policy](#)).
  - IPsec Proposal:** Click **Select** and specify the IPsec proposal you've created in chapter [IPsec Transform Set](#).

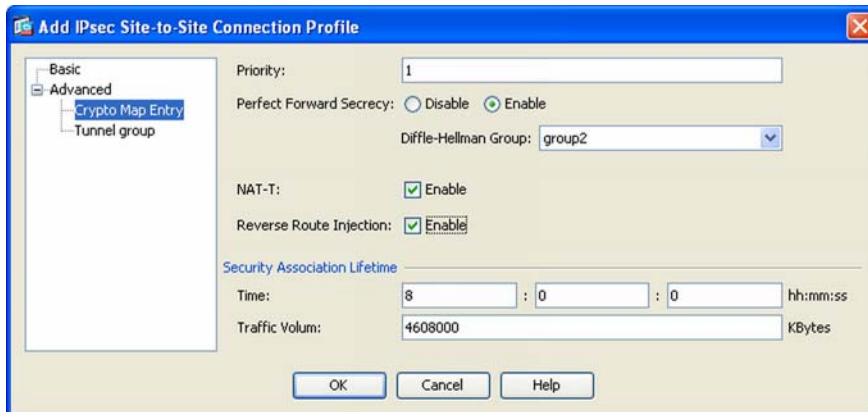
---

**Note:** If you don't check **Static**, you need to create a **Tunnel Group** for this connection later on. The *Tunnel Group* must have the same name as specified in the OU parameter of the certificates subject (refer to chapter [Configuring Tunnel Groups](#)).

---

### 5.4.2 Crypto Map Settings

- Switch to the menu **Advanced -> Crypto Map Entry**.



- Enable **Perfect Forward Secrecy** (PFS). PFS is enabled by default on the mGuard.
- Select **Diffie-Hellman Group 2**.
- Ensure that **NAT-T** and **Reverse Route Injection** are enabled.
- The specified **Lifetime** must match to the one specified on the mGuard. The default value on the mGuard for the IPsec SA lifetime is *28800* seconds (8 hours).

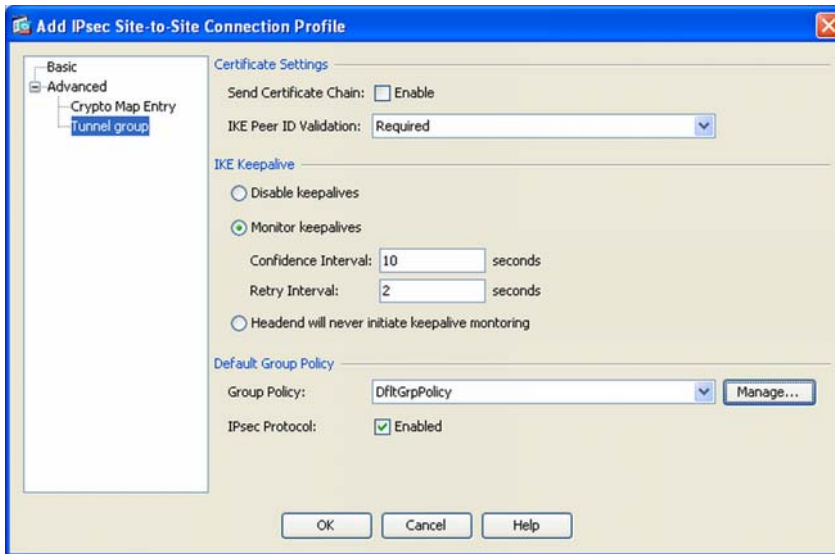
---

**Note:** The lifetime of the IPsec SA must exactly match to the one specified on the mGuard (default value = 28800 seconds). Otherwise establishing the VPN connection will fail.

---

### 5.4.3 Tunnel Group Settings

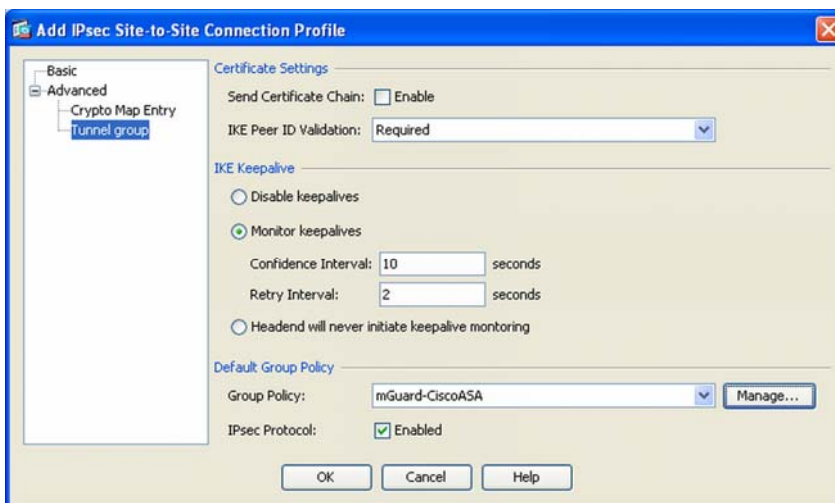
- Switch to the menu **Advanced -> Tunnel Group**.



- In the section *Default Group Policy*, click **Manage**.
- Click **Add** to create a new policy.



- Enter a descriptive **Name** for the policy.
- In the section *Tunneling Protocols*, disable **Inherit** and enable **IPsec**.
- In the section *Filter*, disable **Inherit** and select the access list you've created in chapter [Access List](#).
- Click **OK**.

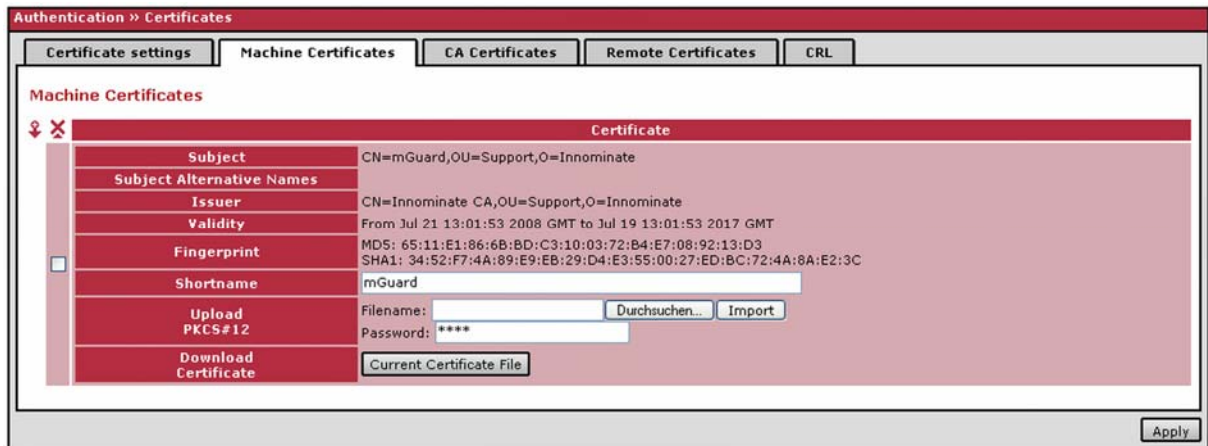


- In the section *Default Group Policy*, ensure that **IPsec Protocol** is enabled.
  - Click **OK**.
- ⇒ The new connection profile is displayed in the list.
- Click **Apply**.

## 5.5 Configuring Tunnel Groups

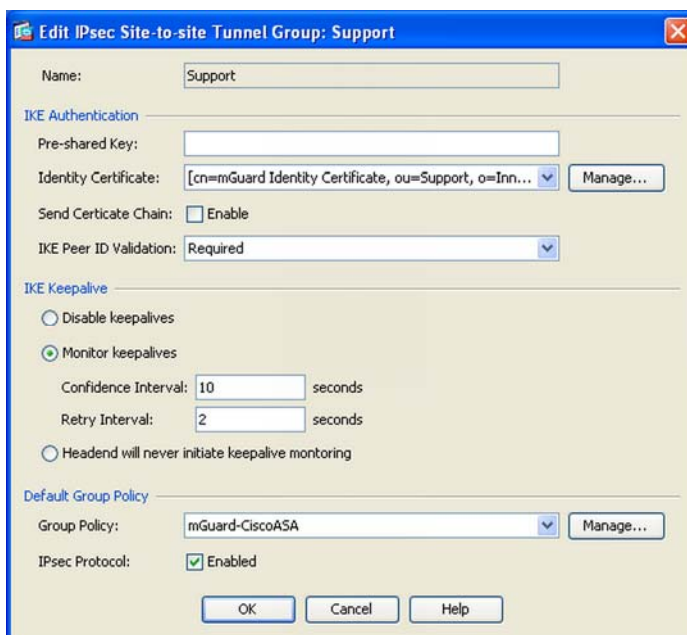
This step is only required when using certificates for authentication and if you did not enter the mGuard's public IP address or DynDNS name when configuring the VPN connection.

At first you need to know the name of the *Organization Unit* (OU) which was entered when creating the mGuard's machine certificate. This parameter is displayed in the web interface of the mGuard after importing the certificate (menu *Authentication -> Certificates*, tab *Machine Certificate*, refer to chapter [Import of the mGuard's Machine Certificate](#)).



In our example we need to create a **Tunnel Group** with the name **Support**.

- From the menu, select **Advances -> Tunnel Groups** and click **Add**.



- Enter the value of the *Organization Unit* as **Name**, in our example *Support*.
- Select the **Identity Certificate** which should be used for this group.
- In the section *Default Group Policy* select the policy you've created when configuring the VPN connection through the menu *Connection Profiles*.
- Ensure that **IPsec Protocol** is enabled.
- Click **OK**.

### 5.6 Runtime Settings

#### 5.6.1 VPN Configuration with PSK

```
ciscoasa# show run
...
object-group protocol DM_INLINE_PROTOCOL_1
  protocol-object ip
  protocol-object icmp

access-list outside_1_cryptomap extended permit object-group DM_INLINE_PROTOCOL_1 10.0.0.0 255.0.0.0
192.168.80.0 255.255.255.0
access-list inside_nat0_outbound extended permit ip 10.0.0.0 255.0.0.0 192.168.80.0 255.255.255.0 inactive

nat (inside) 0 access-list inside_nat0_outbound

crypto ipsec transform-set mGuard-ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto map outside_map 1 match address outside_1_cryptomap
crypto map outside_map 1 set pfs
crypto map outside_map 1 set peer 77.245.32.78
crypto map outside_map 1 set transform-set mGuard-ESP-AES-256-SHA
crypto map outside_map 1 set reverse-route
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 30
  authentication pre-share
  encryption aes-256
  hash sha
  group 2
  lifetime 3600

group-policy mGuard-CiscoASA internal
group-policy mGuard-CiscoASA attributes
  vpn-filter none
  vpn-tunnel-protocol IPSec
tunnel-group 77.245.32.78 type ipsec-l2l
tunnel-group 77.245.32.78 general-attributes
  default-group-policy mGuard-CiscoASA
  tunnel-group 77.245.32.78 ipsec-attributes
  pre-shared-key *
!
...
```

### 5.6.2 VPN Configuration with Certificates

```
ciscoasa# show run
...
object-group protocol DM_INLINE_PROTOCOL_2
 protocol-object ip
 protocol-object icmp

access-list mGuard_cisco_vpn remark Tunnel mGuard - Cisco ASA
access-list mGuard_cisco_vpn extended permit object-group DM_INLINE_PROTOCOL_2 192.168.80.0
255.255.255.0 10.0.0.0 255.0.0.0
access-list outside_cryptomap extended permit ip 10.0.0.0 255.0.0.0 192.168.80.0 255.255.255.0

crypto ipsec transform-set mGuard-ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto dynamic-map mGuard 1 match address outside_cryptomap
crypto dynamic-map mGuard 1 set pfs
crypto dynamic-map mGuard 1 set transform-set mGuard-ESP-AES-256-SHA
crypto dynamic-map mGuard 1 set reverse-route
crypto map outside_map3 1 ipsec-isakmp dynamic mGuard
crypto map outside_map3 interface outside

crypto ca trustpoint ASDM_TrustPoint0
 enrollment terminal
 crl configure
crypto ca trustpoint ASDM_TrustPoint3
 enrollment self
 fqdn none
 subject-name CN=mGuard Identity Certificate,OU=Support,O=Innominate
 no client-types
 crl configure
crypto ca server
 shutdown
crypto ca certificate chain ASDM_TrustPoint0
 certificate ca 01
 30820204 .....
 quit
crypto ca certificate chain ASDM_TrustPoint3
 certificate 31
 3082020e .....
 quit

crypto isakmp enable outside
crypto isakmp enable vpn
crypto isakmp policy 20
 authentication rsa-sig
 encryption aes-256
 hash sha
 group 2
 lifetime 3600

group-policy mGuard-CiscoASA internal
group-policy mGuard-CiscoASA attributes
 vpn-filter value mGuard_cisco_vpn
 vpn-tunnel-protocol IPSec

tunnel-group mGuard type ipsec-l2l
tunnel-group mGuard general-attributes
 default-group-policy mGuard-CiscoASA
tunnel-group mGuard ipsec-attributes
 trust-point ASDM_TrustPoint3
tunnel-group Support type ipsec-l2l
tunnel-group Support general-attributes
 default-group-policy mGuard-CiscoASA
tunnel-group Support ipsec-attributes
 trust-point ASDM_TrustPoint3
!
...
```

## 6 Configuring the mGuard

- From the menu, select **IPsec VPN -> Connections**.
- Click the down arrow for creating a new line.
- Enter a descriptive name for the connection and click **Edit**.

### 6.1 General Settings

IPsec VPN » Connections » VPN to Cisco ASA

General Authentication Firewall IKE Options

**Options**

A descriptive name for the connection: VPN to Cisco ASA

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.): 77.245.32.23

Connection startup: Initiate

**Transport and Tunnel Settings**

Enabled	Type	Local	Remote
<input checked="" type="checkbox"/> Yes	Tunnel	192.168.80.0/24	10.0.0.0/8

Back

- **Address of the remote site's VPN gateway:** Enter the public IP address or the DnyDNS name of the Cisco ASA.
- Set **Connection Startup** to **Initiate**.
- **Transport and Tunnel Settings**
  - Set **Type** to **Tunnel**.
  - Enter as **Local** network the internal network of the mGuard, in our example 192.168.80.0/24.
  - Enter as **Remote** network the internal network of the Cisco ASA, in our example 10.0.0.0/8.

### 6.2 Authentication

- Switch to the tab **Authentication**.

#### 6.2.1 PSK

IPsec VPN » Connections » VPN to Cisco ASA

General Authentication Firewall IKE Options

**Authentication**

Authentication method: Pre-Shared Secret (PSK)

Pre-Shared Secret Key (PSK): complicated\_like\_5Dy0qoD\_and\_long

**VPN Identifier**

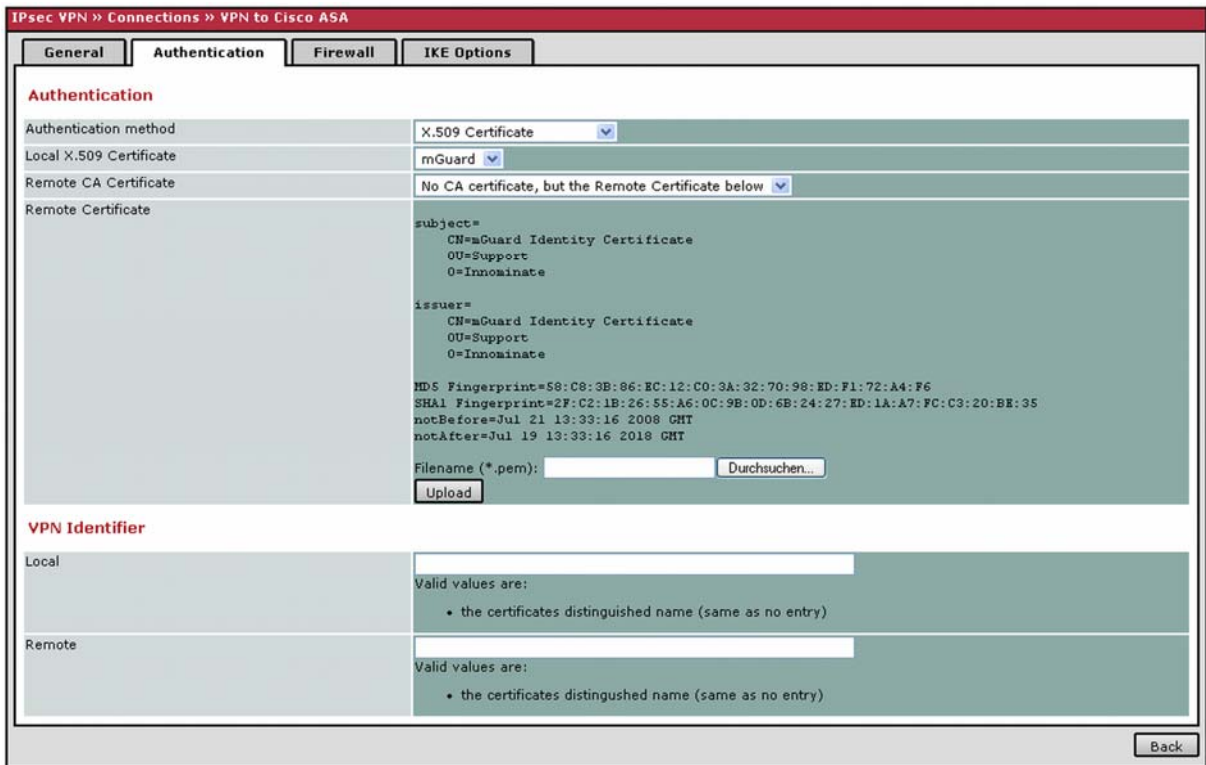
Local:   
By default the IP address of the peer is used. Other possible settings are a hostname ("hostname") or an e-mail address ("name@hostname").

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").

Back

- Set **Authentication method** to **Pre-Shared Secret (PSK)**.
- Enter the Pre-Shared Secret Key.

### 6.2.2 Certificates

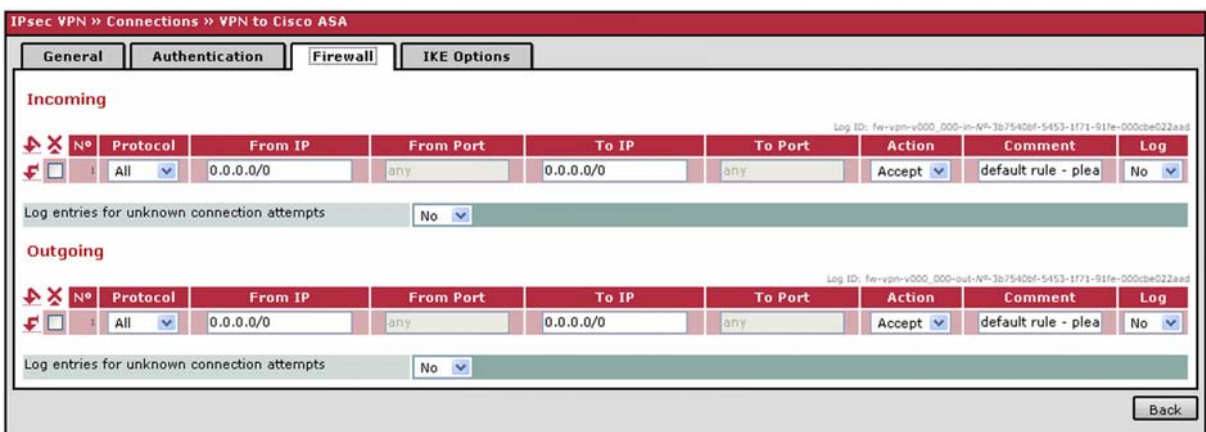


- Set **Authentication method** to **X.509 Certificate**.
- Select as **Local X.509 Certificate** the mGuard's machine certificate you have imported in chapter [Import of the mGuard's Machine Certificate](#).
- Set **Remote CA Certificate** to **No CA certificate, but the Remote Certificate below**.
- Click **Browse** and open the PEM export of the identity certificate you've created on the Cisco ASA (refer to chapter [Creating the Identity Certificate on the Cisco ASA](#)).
- Click **Upload**.

### 6.3 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).



## 6.4 IKE Options

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

The screenshot shows the 'IKE Options' configuration page in the mGuard interface. The page is titled 'IPsec VPN » Connections » VPN to Cisco ASA'. It has four tabs: 'General', 'Authentication', 'Firewall', and 'IKE Options'. The 'IKE Options' tab is selected. The configuration is organized into several sections:

- ISAKMP SA (Key Exchange):**
  - Encryption Algorithm: AES-256
  - Hash Algorithm: SHA-1
- IPsec SA (Data Exchange):**
  - Encryption Algorithm: AES-256
  - Hash Algorithm: SHA-1
  - Perfect Forward Secrecy (PFS): 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: Restart
  - Delay: 30
  - Timeout: 120

A 'Back' button is located at the bottom right of the configuration area.

- **ISAKMP SA (Key Exchange):** Specify desired **Encryption** and **Hash Algorithm** for phase I (IKE), in our example ASE-256 and SHA (refer to [IKE Policies](#)).
- **IPsec SA (Data exchange):** Specify the desired **Encryption** and **Hash Algorithm** for phase II (IPsec), in our example ASE-256 and SHA (refer to [IPsec Transform Sets](#)).
- If you have enabled **Perfect Forward Secrecy (PFS)** on the Cisco ASA you also need to enable this option on the mGuard.
- You need to adjust the lifetimes if you did not configure the Cisco ASA to use the default values of the mGuard.
- Set **DPD Action** to **Restart**. The mGuard should try to reestablish the VPN connection once the dead peer detection (DPD) has encountered the connection as dead.
- Click **Apply**.

## 7 Troubleshooting

You can retrieve information about the status of the VPN connection from the menus **IPsec VPN -> IPsec Status** and **Logging -> Browse local logs**, option **IPsec VPN**. Establishing a VPN connection consists of two phases: Phase I (ISAKMP (IKE) SA) and phase II (IPsec SA). In case of a successful connection the status of **ISAKMP** and **IPsec** is **established** (menu **IPsec VPN -> IPsec Status**).

IPsec VPN » IPsec Status					
Connection Name	Connection			ISAKMP State	IPsec State
VPN to Cisco ASA (v000_001) <input type="button" value="Edit"/> <input type="button" value="Restart"/>	Gateway	77.245.32.78	77.245.32.23	STATE_MAIN_I4 (ISAKMP SA established) Lifetime:2981s	STATE_QUICK_I2 (sent QI2, IPsec SA established) Lifetime:27718s
	Traffic	192.168.80.0/24	10.0.0.0/8		
	ID	O=Innominate, OU=Support, CN=mGuard Identity Certificate			
<input type="button" value="Update"/>					

*IPsec status of a VPN connection using certificates for authentication*

### 7.1 ISAKMP (IKE) SA couldn't be established

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

- Mismatched certificates or PSK.
- If you did not specify the mGuard's IP address or DynDNS name when configuring the connection profile, ensure that a *Tunnel Group* was configured using as name the same name specified in the identity certificate in the parameter *Organization Unit* (OU) (refer to chapter [Configuring Tunnel Groups](#)).
- The mGuard is configured to use PFS but PFS is not enabled on the Cisco device.
- Mismatched phase I (ISAKMP) policy parameters. Compare the *ISAKMP SA (Key exchange)* settings (encryption and hash algorithm) on the mGuard with the settings on the Cisco device (IKE Policy).
- The specified lifetime for the ISAKMP SA do not match on both devices.

### 7.2 IPsec SA couldn't be established

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

- Mismatched IPsec policy parameters. Compare the *IPsec SA (Data exchange)* settings (encryption and hash algorithm) on the mGuard with the settings on the Cisco device.
- The specified lifetime for the IPsec SA do not match on both devices.
- Mismatched VPN subnet parameters. Verify that the same subnets were specified for the local and remote network on both devices accordingly.

## 8 Reference

We like to thank Mr. Martin Mosfeldt from Nworks / Denmark ([www.nworks.dk](http://www.nworks.dk)) for his help and for granting us administrative access to the Cisco ASA appliance. Without his assistance making this interoperability guide wouldn't have been possible.