

# Interoperability Guide

## Configuring IPsec Tunnel Mode VPN between mGuard and Cisco 1812



*mGuard smart*



*mGuard PCI*



*mGuard blade*



*mGuard industrial*



*EAGLE mGuard*



*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>3</b>
2.1	<i>mGuard in Router Mode (Router/PPPoE/PPTP)</i>	4
2.2	<i>mGuard in Stealth Mode</i>	5
<b>3</b>	<b>Limitations in using Preshared Secret Keys (PSK)</b>	<b>5</b>
<b>4</b>	<b>X.509 Certificates</b>	<b>6</b>
4.1	<i>XCA: Create the CA and export it as PEM</i>	7
4.1.1	Create the CA	7
4.1.2	PEM Export of the CA Certificate	8
4.2	<i>Cisco: Create a Certificate Request</i>	9
4.3	<i>XCA: Import the Certificate Request and sign it with the CA</i>	10
4.4	<i>XCA: Export the signed Cisco Certificate as PEM</i>	11
4.5	<i>Cisco: Import of the CA and the Cisco Certificate</i>	12
4.6	<i>XCA: Create the mGuard Certificate export it as PKCS#12</i>	14
4.6.1	Create the mGuard certificate	14
4.6.2	Export of the mGuard Certificate as PKCS#12	15
<b>5</b>	<b>Configuring the Cisco Device</b>	<b>16</b>
5.1	<i>Remote Peer IP Address and Authentication Method</i>	16
5.1.1	Using PSK as Authentication Method	16
5.1.2	Using PKI with X.509 Certificates as Authentication Method	16
5.2	<i>IKE Proposal</i>	17
5.3	<i>IPsec Proposal (Transform Set)</i>	17
5.4	<i>VPN Subnets (Traffic to protect)</i>	18
5.5	<i>Perfect Forward Secrecy (PFS) and IPsec SA Lifetime</i>	18
5.5.1	mGuard with a dynamic public IP Address	18
5.5.2	mGuard with a static public IP Address	19
5.6	<i>VPN Identifier</i>	20
5.7	<i>Check Certificate Revocation List</i>	20
5.8	<i>Configuration Example (Certificates)</i>	21
5.9	<i>Configuration Example (PSK)</i>	22
<b>6</b>	<b>Configuring the mGuard</b>	<b>23</b>
6.1	<i>Import of the mGuard Certificate</i>	23
6.2	<i>Configuring the VPN Tunnel</i>	23
6.2.1	General Settings	23
6.2.2	Authentication	24
6.2.3	Firewall	25
6.2.4	IKE Options	25
<b>7</b>	<b>Troubleshooting</b>	<b>26</b>
7.1	<i>ISAKMP SA couldn't be established</i>	26
7.2	<i>IPsec SA couldn't be established</i>	26

## 1 Disclaimer

© Innominate Security Technologies AG

May 2007

"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 the Cisco 1812. We have used a Cisco 1812 (IOS version: 12.4(6)T5, SDM version: 2.3.1) and an mGuard v4.2.1 for this interoperability test.

The VPN tunnel will be initiated by the mGuard. This document describes the usage of the authentication methods PSK (Preshared Secret Key) and PKI with X.509 certificates.

The Cisco device was configured through the *Security Device Manager* (SDM).

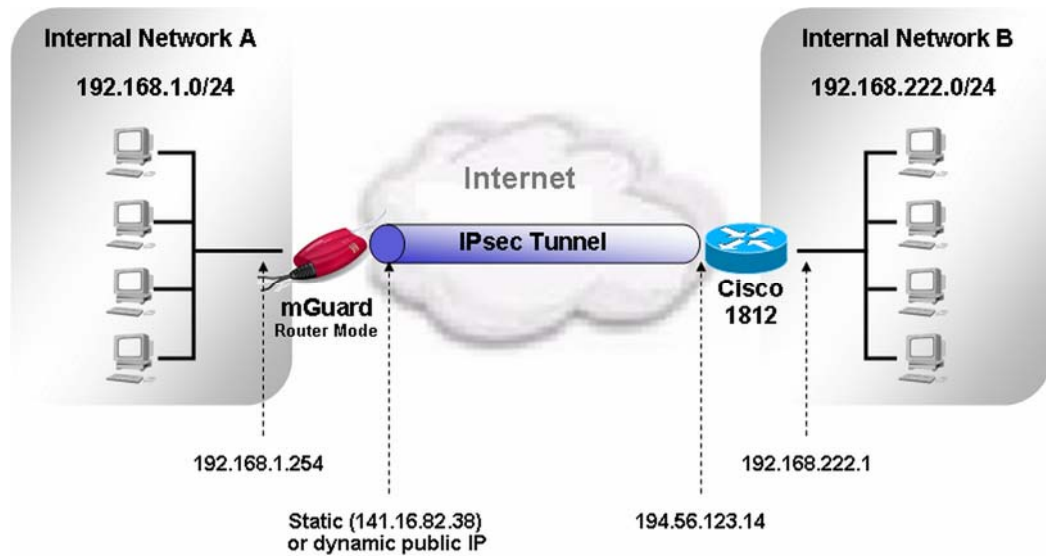
---

 **Note:** Configuring a VPN using PKI and X.509 certificates is considered more secure than using pre-shared secrets.

---

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

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



Scenario used for the setup of the VPN tunnel between mGuard (Router mode) and Cisco 1812

For this setup we have selected 3DES as encryption and MD5 as hash algorithm for the *ISAKMP* and *IPsec* policies. The parameters for the VPN tunnel are as follows:

Using PSK (Preshared Secret Key) as authentication method:

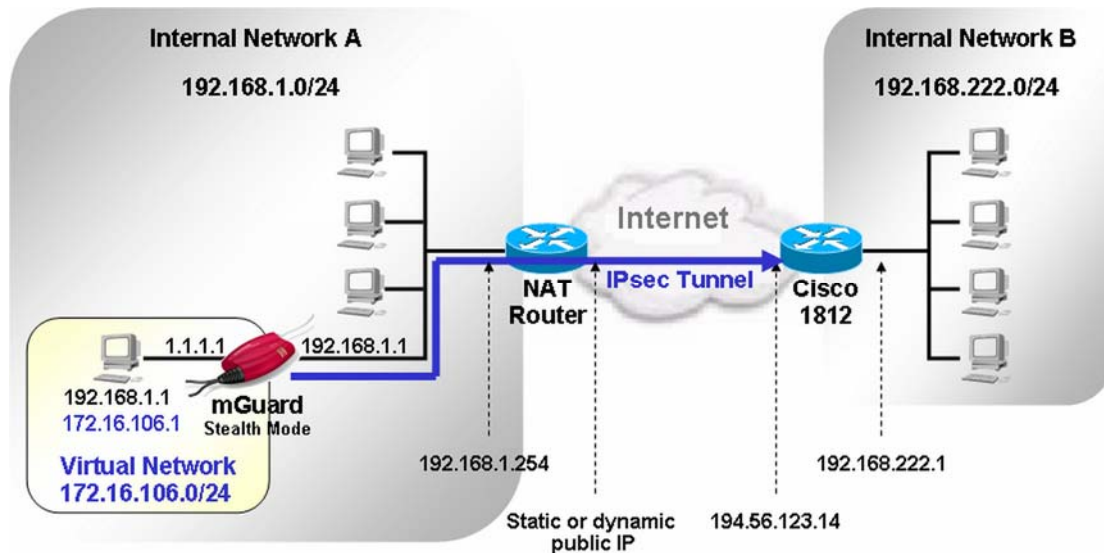
VPN parameter	mGuard	Cisco 1812
Remote VPN gateway	194.56.123.14	141.16.82.38
Local VPN subnet	192.168.1.0/24	192.168.222.0/24
Remote VPN subnet	192.168.222.0/24	192.168.1.0/24
ISAKMP Policy, Encryption / Hash	3DES / MD5	3DES / MD5
IPsec Policy, Encryption / Hash	3DES / MD5	3DES / MD5

Using PKI with X.509 certificates as authentication method:

VPN parameter	mGuard	Cisco 1812
Remote VPN gateway	194.56.123.14	<Dynamic IP>
Local VPN subnet	192.168.1.0/24	192.168.222.0/24
Remote VPN subnet	192.168.222.0/24	192.168.1.0/24
ISAKMP Policy, Encryption / Hash	3DES / MD5	3DES / MD5
IPsec Policy, Encryption / Hash	3DES / MD5	3DES / MD5

## 2.2 mGuard in Stealth Mode

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 a virtual transfer network (e.g. 172.16.106.0/24) or a virtual IP address (e.g. 172.16.106.1/32) needs to be used as local VPN subnet. This virtual network or IP address must not overlap with existing network IPs and needs to be entered on the mGuard as local VPN network and on the Cisco device as remote VPN network. Apart of this you also need to define a virtual IP on the mGuard which will be used by the client in *Stealth* mode (e.g. 172.16.106.1). This virtual IP address is used to access the client behind the mGuard through the VPN tunnel from the Cisco LAN.



Scenario used for the setup of the VPN tunnel between mGuard (Stealth mode) and Cisco 1812

### Note:

- If the IP address of the client does not belong to the Cisco LAN you can specify the client's IP address as local VPN network (e.g. 192.168.1.1/32) and as *virtual IP of the client which will be used in Stealth mode* (e.g. 192.168.1.1) on the mGuard. On the Cisco device this IP address must be entered as remote VPN network.
- PKI with X.509 certificates must be used as authentication method because the connection will be established across one or more gateways that have *Network Address Translation* (NAT) activated. Using PSK is not possible for this setup.

## 3 Limitations in using Preshared Secret Keys (PSK)

- If the mGuard has a dynamic public IP address and PSK shall be used, the mGuard must register its IP address under a fixed name in a DynDNS service and the VPN settings on the Cisco 1812 must refer to this name. Otherwise, if you would specify a dynamic IP address for the remote gateway (*dynamic crypto map*) on the Cisco device, this would require the *Aggressive Mode* which is not supported by the mGuard in the current version.
- 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 PKI with X.509 certificates must be used.

### 4 X.509 Certificates

You may obtain the required certificates by using the *Simple Certificate Enrollment Protocol (SEP)* provided by the Cisco device.

There are several tools available for creating and managing certificates, as for example OpenSSL and XCA. This section explains briefly how to create X.509 certificates with the tool XCA. XCA provides much more functionality than explained in this document. Please refer to the XCA documentation for further information. XCA is available for Linux and Windows. You can download this tool from <http://xca.sourceforge.net>. The screenshots and descriptions in this chapter are related to XCA v0.6.2.

After installing XCA you need to create a database. To do this:

- From the menu, select **File -> New DataBase**.
  - Specify the storage location and filename of the database.
  - Click **Save**.
- ⇒ You'll be prompted to enter a password which protects the database against unauthorized usage.

When restarting XCA you need to connect to the database through the menu **File -> Open DataBase** first.

The following certificates are required:

- **CA as PEM export:** Needs to be imported on the Cisco device.
- **Cisco certificate as PEM export:** Needs to be imported on the Cisco device and on the mGuard as connection certificate.
- **mGuard certificate as PKCS#12 export:** Needs to be imported on the mGuard as machine certificate.

The following steps need to be performed for obtaining the required certificates with the tool XCA:

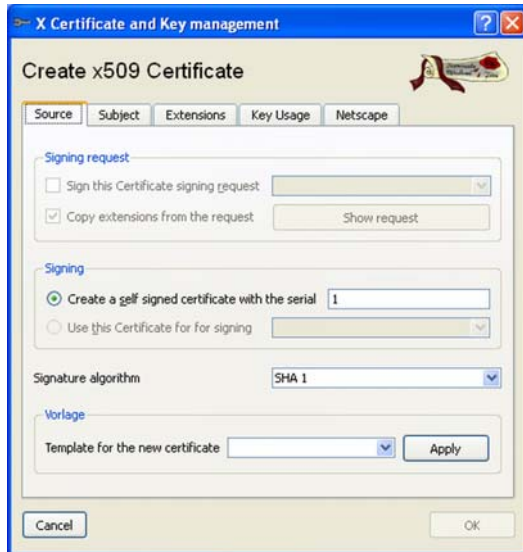
- 1) XCA: Create the CA and export it as PEM
- 2) Cisco: Create a certificate request
- 3) XCA: Import the certificate request and sign it with the CA
- 4) XCA: Export the signed Cisco certificate as PEM
- 5) Cisco: Import of the CA and the Cisco certificate
- 6) XCA: Create the mGuard certificate and export it as PKCS#12

## 4.1 XCA: Create the CA and export it as PEM

A client certificate must be signed by the CA certificate to become a valid certificate, as long as self signed certificates are not used. Therefore you need to create the CA certificate first before creating the client certificates. The CA certificate is a self signed certificate.

### 4.1.1 Create the CA

- Start the program **XCA** and connect to the database.
- Switch to the tab **Certificates**.
- Click **New Certificate**.



- Ensure that **Create a self signed certificate with the serial** is selected.
- You may enter a serial number for the certificate or leave the default value.
- Set **Signature algorithm** to **SHA 1**.
- Switch to the tab **Subject**.



- Use the entry fields from **Internal name** to **E-Mail address** for entering the subject attributes to be included in the CA's certificate. At least an entry for **Common name** is required.
- Click **Generate a new key** for creating the private RSA key for the CA.



- Enter a **Name** for the key, specify the desired **Keysize** and click **Create**.
- Switch to the tab **Extensions**.



- Set **Type** to **Certification Authority**.
  - Enter the lifetime of the CA certificate in the section **Time Range**. For a CA certificate you may want it to last longer than the client certificates so that you do not have to reissue the certificates so often. We have chosen a lifetime of 10 years. Click **Apply**.
  - Click **OK**.
- ⇒ The created CA certificate is displayed in the tab **Certificates**.

### 4.1.2 PEM Export of the CA Certificate

- Switch to the tab **Certificates**.
- Highlight the CA certificate you have created in the previous step.
- Click **Export**.



- Select **PEM** as **Export Format**.
- Specify the desired **Filename** and the location where the export should be stored. In our example we have named the file *CA.crt*.
- Click **OK**.

This CA certificate needs to be imported on the Cisco device later.

## 4.2 Cisco: Create a Certificate Request

- Connect to the Cisco's *Security Device Manager* (SDM).
  - In the toolbar, click **Configure**.
  - From the left frame, select **VPN**.
  - Select **VPN Components -> Public Key Infrastructure -> Certificate Wizards** from the VPN tree.
  - Select **Cut-and-Paste / Import from PC** and click **Launch the selected task**.
- ⇒ You'll be prompted to enter the SSH credentials.
- The *Welcome to the Certificate Wizard* appears. Click **Next**.
  - Select **Begin new enrollment** and click **Next**.

The screenshot shows the 'Cut-and-Paste Certificate Wizard' dialog box with the 'Certificate Authority(CA) Information' step selected. The 'Certificate Authority Details' section has a 'CA Server Nickname' field containing 'CA'. The 'Challenge Password' section has two empty text boxes for 'Challenge Password' and 'Confirm Challenge Password'. A note explains that the challenge password can be used for certificate revocation. Navigation buttons at the bottom include '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

- Enter a **CA Server Nickname**.
- Click **Next**.

The screenshot shows the 'Cut-and-Paste Certificate Wizard' dialog box with the 'Certificate Subject Name Attributes' step selected. It offers three options to include in the certificate request: 'Include router's Fully Qualified Domain Name (FQDN)' (with a text box for 'mgtest.yourdomain.com'), 'Include router's IP address' (with radio buttons for 'IP address' and 'Interface'), and 'Include router's serial number'. A button labeled 'Other Subject Attributes...' is at the bottom right. Navigation buttons at the bottom include '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

- Disable **Include router's Fully Qualified Domain Name (FQDN)**.
- Click **Other Subject Attributes**.

The screenshot shows the 'Other Subject Attributes' dialog box. It prompts the user to enter subject attributes for the router's certificate, with 'Common name (cn)' as the minimum recommended entry. The form contains several text boxes: 'Common Name (cn): Cisco', 'Organization Unit (ou): Support', 'Organization (o): Innominate', 'State (st):', 'Country (c):', and 'E-Mail (e):'. Navigation buttons at the bottom are 'OK', 'Cancel', and 'Help'.

- Use the entry fields from **Common name (cn)** to **E-Mail (e)** for entering the subject attributes to be included in the router's certificate. At least an entry for **Common name** is required.
- Click **OK**.
- Click **Next** in the *Certificate Wizard*.

- Now you have the option to create a new key pair or to use an existing one. In this interoperability test we have used the existing key. Click **Next**.
- Review the displayed summary and click **Next** if the parameters are correct.
- Confirm the *Commands Delivery Status* dialog by clicking **OK**.

⇒ The enrollment request is generated.



- Click **Save** and store the Cisco's certificate request to your local system. In this example we have named the file *CiscoRequest.pem*.
- Click **Finish**.

### 4.3 XCA: Import the Certificate Request and sign it with the CA

Before you can import the certificate request to XCA you need to modify the file. Usually a certificate request starts with the line "-----BEGIN CERTIFICATE REQUEST-----" and ends with the line "-----END CERTIFICATE REQUEST-----". For some reasons the certificate request of the Cisco device does not contain those lines.

Open the certificate request with a text editor, add the missing lines so that the file looks like the example below and save the changed.

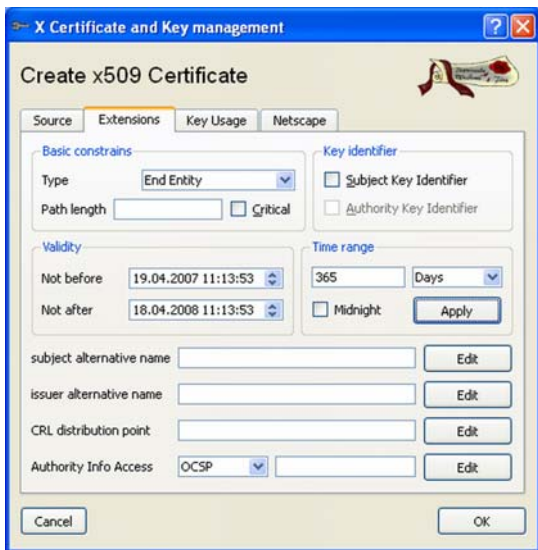
```
-----BEGIN CERTIFICATE REQUEST-----
MIIBEjCBvQIBADA3MQ4wDAYDVQQDEwVDAxNjBzEQMA4GA1UECzMHU3VwcG9y
dDEtMBEGA1UEChMKSW5ub21pbmF0ZTBcMA0GCsQGSib3DQEBAQUAA0sAMEgCQD
Vz+7t/FL1EnBmicDc8+uiR+NhfSfjUTJ+laoz34ayOCHjwUTv76ADk9g9q3Ev3yQhIge
WINLJWdF8Apov6JhAgMBAAGglTafBgkqhkiG9w0BQC4xEjAQMA4GA1UdDwEB/wQE
AwIFoDANBgkqhkiG9w0BAQQFAANBAD5qNCDcw2F3pkdu8KsxbDO9NOwJ/p+gFspO
4fUNb66NNNJCYB7zKxyq9OLE3zY3b014nGgh80KcdocHoJ8jDWB=
-----END CERTIFICATE REQUEST-----
```

*Modified certificate request file*

- In XCA, switch to the tab **Certificate signing requests**.
  - Click **Import**.
  - Select the certificate request and click **Open**.
- ⇒ The imported certificate request is displayed in the tab **Certificate signing requests**.
- Make a right click on the certificate request and select **Sign** from the context menu.



- Ensure that **Use this Certificate for signing** and the corresponding CA are selected.
- Set **Signature algorithm** to **SHA 1**.
- Switch to the tab **Extensions**.



- Set **Type** to **End Entity**.
  - Select the lifetime of the certificates in the section **Time Range** and click **Apply**.
  - Click **OK**.
- ⇒ The signed certificate request is displayed in the tab **Certificates** beneath the CA.

#### 4.4 XCA: Export the signed Cisco Certificate as PEM

- Switch to the tab **Certificates**.
- Highlight the Cisco certificate which is located beneath the CA.
- Click **Export**.

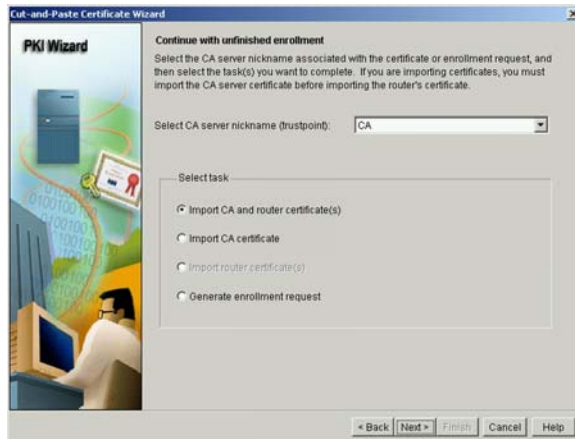


- Select **PEM** as **Export Format**.
- Specify the desired **Filename** and the location where the export should be stored. In our example we have named the file *Cisco.crt*.
- Click **OK**.

This certificate needs to be imported on the Cisco device and on the mGuard as connection certificate.

#### 4.5 Cisco: Import of the CA and the Cisco Certificate

- In the SMD toolbar, click **Configure**.
- From the left frame, select **VPN**.
- Select **VPN Components -> Public Key Infrastructure -> Certificate Wizards** from the VPN tree.
- Select **Cut-and-Paste / Import from PC** and click **Launch the selected task**.
- The *Welcome to the Certificate Wizard* appears. Click **Next**.
- Select **Continue an unfinished enrollment**. Click **Next**.



- Ensure that the correct **CA server nickname** is selected.
- Select **Import CA and router certificate(s)**.
- Click **Next**.



- At first the CA needs to be imported, in our example the file *CA.crt*.
- Click **Browse**.
- Select the CA you have created and exported in chapter [XCA: Create the CA and export it as PEM](#).
- Click **Next**.



- Now the Cisco certificate needs to be imported, in our example the file *Cisco.crt*.
- Click **Browse**.
- Select the Cisco certificate you have exported in chapter [XCA: Export the signed Cisco certificate as PEM](#).
- Click **Next**.

- After the import of the CA server certificate you must verify the CA's server certificate to complete the certificate enrollment process. Click **Yes** if the fingerprint of the CA server certificate is correct.
- Finally the router certificate is imported and the enrollment status is displayed. Click **Finish**.

## Configuring IPsec Tunnel Mode VPN between mGuard and Cisco 1812

To verify the import of the certificates:

- Select **VPN Components -> Public Key Infrastructure -> Router Certificates** from the VPN tree.
- Click **Refresh**.
- Highlight the CA in the upper window.
- Both imported certificates, the CA and the router certificate, should be displayed in the *Certificate Chain* area.

The screenshot shows the Cisco Router and Security Device Manager (SDM) interface. The navigation tree on the left is expanded to **VPN Components > Public Key Infrastructure > Router Certificates**. The main area displays the **Router Certificates** configuration page. It shows a table of trustpoints configured on the router:

Name	Enrollment URL	Enrollment Type
CA	terminal	Cut & Paste
TP-self-signed-418*		Unsupported in SDM

Below this, the **Certificate Chain for trustpoint CA** is displayed, showing a table of certificates:

Type	Usage	Serial Number	Issuer	Status	Expires (Days)	Expiry Date
Certificate	General Purpose	04	cn=CA,ou	Available	364	Apr 18 2007
CA Certificate	General Purpose	01	cn=CA,ou	Available	3649	Apr 16 2007

The interface also includes a **Save Certificates to USB Token** button at the bottom right. The status bar at the bottom indicates "Configuration delivered to router." and the time "15:53:10 PCTime Thu Apr 19 2007".

## 4.6 XCA: Create the mGuard Certificate export it as PKCS#12

### 4.6.1 Create the mGuard certificate

- Switch to the tab **Certificates**.
- Click **New Certificate**.

**X Certificate and Key management**

Create x509 Certificate

Source | Subject | Extensions | Key Usage | Netscape

Signing request

Sign this Certificate signing request Cisco

Copy extensions from the request Show request

Signing

Create a self signed certificate with the serial 1

Use this Certificate for signing CA

Signature algorithm SHA 1

Vorlage

Template for the new certificate Apply

Cancel OK

- Ensure that **Use this certificate for signing** and the correct CA are selected.
- Set **Signature algorithm** to **SHA 1**.
- Switch to the tab **Subject**.

**X Certificate and Key management**

Create x509 Certificate

Source | Subject | Extensions | Key Usage | Netscape

Distinguished name

Internal name mGuard Organisation Innominate

Country code Organ. unit Support

State or Province Common name mGuard

Locality E-Mail address

commonName Add Delete

Type	Content

Private key

mGuard (RSA) Generate a new key

Cancel OK

- Use the entry fields from **Internal name** to **E-Mail address** for entering the subject attributes to be included in the mGuard's certificate. At least an entry for **Common name** is required.
- Click **Generate a new key** for creating the private RSA key for the mGuard certificate.

**New key**

New key

Please give a name to the new key and select the desired keysize

Key properties

Name mGuard

Keysize 1024 bit Keytype RSA

Cancel Create

- Enter a **Name** for the key, specify the desired **Keysize** and click **Create**.
- Switch to the tab **Extensions**.



- Set **Type** to **End Entity**.
  - Enter the lifetime of the certificates in the section **Time Range** and click **Apply**.
  - Click **OK**.
- ⇒ The mGuard certificate is displayed in the tab **Certificates** beneath the CA.

### 4.6.2 Export of the mGuard Certificate as PKCS#12

- Switch to the tab **Certificates**.
- Highlight the mGuard certificate which is located beneath the CA.
- Click **Export**.



- Set **Export Format** to **PKCS#12**.
  - Specify the desired **Filename** and the location where the export should be stored. In this example we have named the file *mGuard.p12*.
  - Click **OK**.
- ⇒ You'll be prompted to enter a password which protects the export against unauthorized usage. Enter the **Password** and click **OK**.

This certificate needs to be imported on the mGuard as machine certificate.

## 5 Configuring the Cisco Device

- Connect to the Cisco's *Security Device Manager* (SDM).
- In the toolbar, click **Configure**.
- From the left frame, select **VPN**.
- Select **Site-to-Site VPN** from the VPN tree.
- Select **Create a Site to Site VPN** and click **Launch the selected task**.
- Select **Step by step wizard** and click **Next**.

### 5.1 Remote Peer IP Address and Authentication Method

#### 5.1.1 Using PSK as Authentication Method

The screenshot shows the 'Site-to-Site VPN Wizard' window. Under 'VPN Connection Information', the interface is set to 'FastEthernet0'. Under 'Peer Identity', the peer type is 'Peer with static IP address' and the IP address is '141.16.82.38'. Under 'Authentication', the 'Pre-shared keys' radio button is selected. The 'pre-shared key' and 'Re-enter Key' fields are filled with asterisks. Navigation buttons at the bottom include '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

- Select the interface for the **VPN connection** to which the VPN connection should be established.
- Select **Peer with static IP address** and enter the IP address.
- Select **Pre-shared keys** and enter the shared secret.
- Click **Next**.

#### 5.1.2 Using PKI with X.509 Certificates as Authentication Method

The screenshot shows the 'Site-to-Site VPN Wizard' window. Under 'VPN Connection Information', the interface is set to 'FastEthernet0'. Under 'Peer Identity', the peer type is 'Peer(s) with dynamic IP address'. Under 'Authentication', the 'Digital Certificates' radio button is selected. The 'pre-shared key' and 'Re-enter Key' fields are empty. Navigation buttons at the bottom include '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

- Select the interface for the **VPN connection** to which the VPN connection should be established.
- Select either **Peer with static IP address** and enter the IP address or **Peer with dynamic IP address**, depending on the kind of the mGuard's public IP address (dynamic or static).
- Select **Digital Certificates**.
- Click **Next**.

## 5.2 IKE Proposal

If the desired IKE proposal doesn't already exist, perform the steps described in this chapter. Otherwise click **Next**.

- Click **Add**.

- Select the desired **Encryption** and **Hash** algorithm, in our example **3DES** and **MD5**.
- If PSK is used, set **Authentication** to **RSA\_SHARE**. Select **RSA\_SIG** if certificates are used.
- Select **group 2** as **D-H Group**.
- The specified **Lifetime** must match the settings on the mGuard. The default ISAKMP SA lifetime on the mGuard is 3600 seconds (1 hour).
- Click **OK**.
- Click **Next** in the *Site-to-Site VPN wizard*.

---

**Note:** The VPN connection won't be established if the specified lifetimes for the *ISAKMP SA* and the *IPsec SA* do not match on both devices.

---

## 5.3 IPsec Proposal (Transform Set)

If the desired transform set doesn't already exist, perform the steps described in this chapter. Otherwise click **Next**.

- Click **Add**.

- Enter a descriptive **Name** for the transform set.
- Select the desired **Encryption** and **Integrity** algorithm, in our example **3DES** and **MD5**.
- Click **OK**.
- Click **Next** in the *Site-to-Site VPN wizard*.

## 5.4 VPN Subnets (Traffic to protect)



- Enter for the **Local Network** the network IP and the subnet mask of the Cisco LAN, in our example 192.168.222.0/24.
- Enter for the **Remote Network** the network IP and the subnet mask of the mGuard LAN, in our example 192.168.1.0/24.
- Click **Next**.

Verify the summary of the configuration and click **Finish** if all the settings are correct.

## 5.5 Perfect Forward Secrecy (PFS) and IPsec SA Lifetime

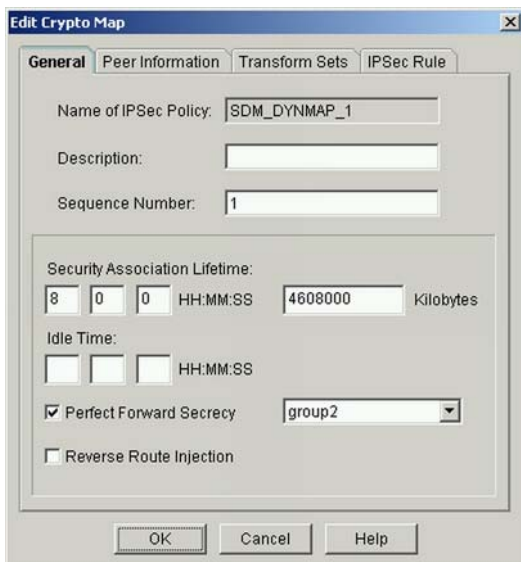
Perform the following steps to enable PFS or to adjust the IPsec SA lifetime.

### 5.5.1 mGuard with a dynamic public IP Address

- Select **VPN Component -> IPsec -> Dynamic Crypto Map Sets** from the VPN tree.
- Highlight the name of the corresponding *Dynamic Crypto Map* and click **Edit**.



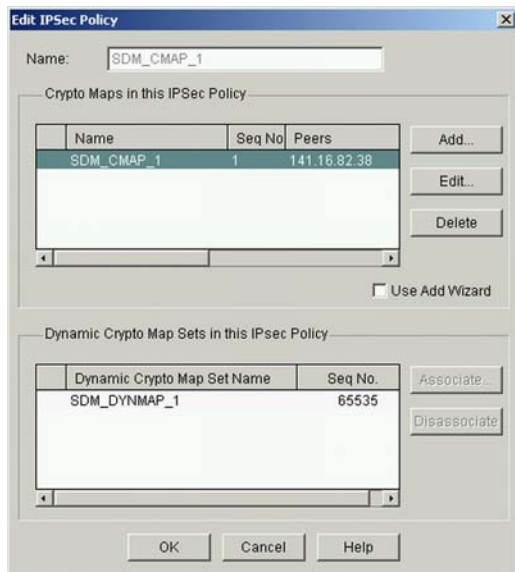
- Highlight the name of the corresponding *Dynamic Crypto Map Set*.
- Click **Edit**.



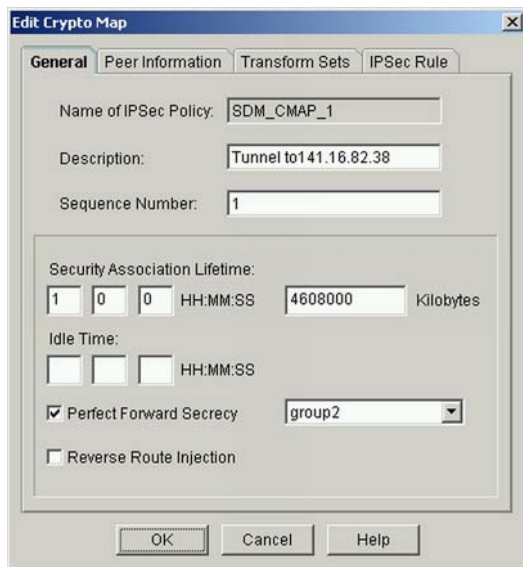
- Enter the desired **Security Association Lifetime**. The default value used by the mGuard is 28800 seconds (8 hours)
- If desired, enable **Perfect Forward Secrecy** and select **group 2**. If you enable PFS, you also need to enable this feature when configuring the mGuard.
- Click **OK**.
- Click **OK** again in the *Edit Dynamic Crypto Map Set* dialog.

### 5.5.2 mGuard with a static public IP Address

- Select **VPN Component -> IPsec -> IPsec Policies (Crypto Map Sets)** from the VPN tree.
- Highlight the name of the corresponding *IPsec Policy* and click **Edit**.



- Highlight the name of the corresponding *Crypto Map*.
- Click **Edit**.



- Enter the desired **Security Association Lifetime**. The default value used by the mGuard is 28800 seconds (8 hours).
- If desired, enable **Perfect Forward Secrecy** and select **group 2**. If you enable PFS, you also need to enable this feature when configuring the mGuard.
- Click **OK**.
- Click **OK** again in the *Edit IPsec Policy* dialog.

## 5.6 VPN Identifier

This step is only required when using PKI with X.509 certificates as authentication method.

The Cisco device uses as default VPN identifier the IP address, the mGuard the ASN.1 distinguished name. If the peers use different VPN identifiers the VPN connection will not be established.

Perform the following steps to set the VPN identifier to ASN.1 distinguished name on the Cisco device:

- Select **VPN Components** from the VPN tree.
- Click **Edit**.
- Set **Identifier (of this router)** to **DISTINGUISHED NAME**.
- Click **OK**.

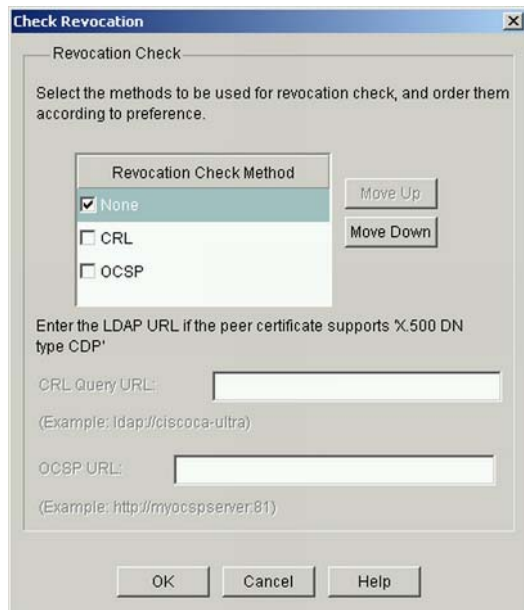
## 5.7 Check Certificate Revocation List

This step is only required when using PKI with X.509 certificates as authentication method.

After importing a new the CA the default setting for this CA is to check the certificates against a *Certificate Revocation List* (CRL). If the CRL is not configured, the VPN connection will not be established.

Perform the following steps to disable the usage of a CRL for the CA:

- Select **VPN Components -> Public Key Infrastructure -> Router Certificates** from the VPN tree.
- Highlight the corresponding CA and click **Check Revocation**.



- Set **Revocation Check Method** to **None**.
- Click **OK**.

## 5.8 Configuration Example (Certificates)

The following lines display the IPsec relevant settings of the running configuration:

```
crypto pki trustpoint CA
enrollment terminal
serial-number none
fqdn none
ip-address none
password
subject-name O=Innominat, OU=Support, CN=Cisco
revocation-check none
rsa keypair TP-self-signed-4181023096.server

crypto pki certificate chain TP-self-signed-4181023096
certificate self-signed 01
 3082024F 308201B8 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
...
 1D88B296 19C52DA3 FB5006B8 E2982630 EA8750
quit
crypto pki certificate chain CA
certificate 04
 308201BA 30820123 A0030201 02020104 300D0609 2A864886 F70D0101 05050030
...
quit
certificate ca 01
 308201EE 30820157 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
...
quit

crypto isakmp policy 2
encr 3des
hash md5
group 2
lifetime 3600
crypto isakmp identity dn

crypto ipsec transform-set mGuard esp-3des esp-md5-hmac

crypto dynamic-map SDM_DYNMAP_1 1
set security-association lifetime seconds 28800
set transform-set mGuard
set pfs group2
match address 103

crypto map SDM_CMAP_1 65535 ipsec-isakmp dynamic SDM_DYNMAP_1

interface FastEthernet0
...
ip address 194.56.123.14 255.255.255.128
ip access-group 102 in
...
crypto map SDM_CMAP_1

interface Vlan1
description $ETH-SW-LAUNCH$$INTF-INFO-FE 2$$ES_LAN$$FW_INSIDE$
ip address 192.168.222.1 255.255.255.0
...
...
access-list 102 permit udp any host 194.56.123.14 eq non500-isakmp
access-list 102 permit udp any host 194.56.123.14 eq isakmp
access-list 102 permit esp any host 194.56.123.14
...
access-list 103 remark SDM_ACL Category=4
access-list 103 remark IPsec Rule
access-list 103 permit ip 192.168.222.0 0.0.0.255 192.168.1.0 0.0.0.255
```

### 5.9 Configuration Example (PSK)

The following lines display the IPsec relevant settings of the running configuration:

```
crypto isakmp policy 2
  encr 3des
  hash md5
  authentication pre-share
  group 2
  lifetime 3600

crypto isakmp key test address 141.16.82.38

crypto ipsec transform-set mGuard esp-3des esp-md5-hmac

crypto map SDM_CMAP_1 1 ipsec-isakmp
  description Tunnel to141.16.82.38
  set peer 141.16.82.38
  set security-association lifetime seconds 28800
  set transform-set mGuard
  set pfs group2
  match address 104

interface FastEthernet0
  description $ES_WAN$$FW_OUTSIDE$
  ip address 194.56.123.14 255.255.255.128
  ip access-group 102 in
  ...
  crypto map SDM_CMAP_1

interface Vlan1
  description $ETH-SW-LAUNCH$$INTF-INFO-FE 2$$ES_LAN$$FW_INSIDE$
  ip address 192.168.222.1 255.255.255.0
  ...
  ...
access-list 102 permit udp host 141.16.82.38 host 194.56.123.14 eq non500-isakmp
access-list 102 permit udp host 141.16.82.38 host 194.56.123.14 eq isakmp
access-list 102 permit esp host 141.16.82.38 host 194.56.123.14
...
access-list 104 remark SDM_ACL Category=4
access-list 104 remark IPsec Rule
access-list 104 permit ip 192.168.222.0 0.0.0.255 192.168.1.0 0.0.0.255
```

## 6 Configuring the mGuard


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

- If X.509 certificates are used as authentication method: Import of the mGuard certificate through the menu **IPsec VPN -> Global**, tab **Machine Certificate**.
- Configuration of the VPN tunnel through the menu **IPsec VPN -> Connections**.

### 6.1 Import of the mGuard Certificate

- From the menu, select **IPsec VPN -> Global**, tab **Machine Certificate**.
- Click **Browse**.
- Select the PKCS#12 export of the mGuard certificate, in our example *mGuard.p12*.
- Enter the **Password** which protects the certificate against unauthorized usage.
- Click **Import**.
- Click **Apply**.

---

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

---

### 6.2 Configuring the VPN Tunnel

- Select **IPsec VPN -> Connections** from the menu and click **New**.
- Enter a descriptive name for the connection and click **Edit**.

#### 6.2.1 General Settings

General	Authentication	Firewall	IKE Options
<b>Options</b>			
A descriptive name for the connection	Cisco		
Enabled	Yes <input type="button" value="v"/>		
Address of the remote site's VPN gateway (either an IP address, a hostname, or %any)	194.56.123.14		
Connection startup (Will be ignored in Stealth Mode.)	Initiate <input type="button" value="v"/>		
<b>Tunnel Settings</b>			
Connection type	Tunnel (Net <-> Net) <input type="button" value="v"/>		
Local network	192.168.1.0/24		
Enable 1-to-1 NAT of the local network to an internal network	No <input type="button" value="v"/>		
Remote network	192.168.222.0/24		
Enable 1-to-1 NAT of the remote network to a different network	No <input type="button" value="v"/>		

- Enter as **Address of the remote site's VPN gateway** the external IP address of the Cisco device, in our example 192.56.123.14.
- The mGuard should initiate the VPN tunnel. Therefore set **Connection startup** to **Initiate**.
- Set **Connection type** to **Tunnel (Net <-> Net)** for an IPsec tunnel mode VPN connection.
- Enter as **Local Network** the internal network IP of the mGuard, in our example 192.168.1.0/24.
- Enter as **Remote Network** the internal network IP of the Cisco device, in our example 192.168.222.0/24.
- The other options are not relevant for this setup.
- Switch to the tab **Authentication**.

## 6.2.2 Authentication

### 6.2.2.1 Using Pre-Shared Secret Keys (PSK)


General	Authentication	Firewall	IKE Options
<b>Authentication</b>			
Authentication method	Pre-Shared Secret (PSK) ▼		
Pre-Shared Secret Key (PSK)	shared_secret		
<b>VPN Identifier</b>			
Remote			
Local VPN Identifier			

- Set **Authentication Method** to **Pre-Shared Secret (PSK)**.
- Enter the **Pre-Shared Secret Key**.
- Switch to the tab **Firewall**.

### 6.2.2.2 Using X.509 certificates

General	Authentication	Firewall	IKE Options
<b>Authentication</b>			
Authentication method	X.509 Certificate ▼		
X.509 Certificate	No Certificate installed		
Filename (*.pem)	D:\Cisco\Cisco.crt <input type="button" value="Durchsuchen..."/>		
	<input type="button" value="Import"/>		
<b>VPN Identifier</b>			
Remote	Valid values are: • the certificates distinguished name (same as no entry)		
Local VPN Identifier	Valid values are: • the certificates distinguished name (same as no entry)		

- Set **Authentication Method** to **X.509 Certificate**.
- Click **Browse**.
- Select the export of the Cisco certificate, in our example *Cisco.crt*, and click **Open**.
- Click **Import**.
- Switch to the tab **Firewall**.

 **Note:** The mGuard uses as default the *ASN.1 Distinguished Name* (DN) of the certificate (e.g. */CN=mGuard/C=de/O=Innominate/OU=Support*) as VPN identifier. If another VPN identifier should be used (e.g. hostname, email address or IP address), you can enter it into the fields *Remote* and/or *Local VPN Identifier* respectively. Using another VPN identifier than the ASN.1 DN requires that the identifier is present in the certificate as *Subject Alternative Name* and that the Cisco device is configured accordingly.

### 6.2.3 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).

The screenshot shows the Firewall configuration page with tabs for General, Authentication, Firewall, and IKE Options. The Firewall tab is active, displaying two rule sections: Incoming and Outgoing. Each section has a table with columns: N°, Protocol, From IP, From Port, To IP, To Port, Action, Comment, and Log. The Incoming rule table has one entry: N° 1, Protocol All, From IP 0.0.0.0/0, From Port any, To IP 0.0.0.0/0, To Port any, Action Accept, Comment default rule - plea, and Log No. Below the table is a checkbox for 'Log entries for unknown connection attempts' set to No. The Outgoing rule table is identical. Below it is also a checkbox for 'Log entries for unknown connection attempts' set to No.

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

### 6.2.4 IKE Options

The screenshot shows the IKE Options configuration page with tabs for General, Authentication, Firewall, and IKE Options. The IKE Options tab is active, displaying configuration for ISAKMP SA (Key Exchange) and IPsec SA (Data Exchange). Under ISAKMP SA, Encryption Algorithm is 3DES and Hash Algorithm is MD5. Under IPsec SA, Encryption Algorithm is 3DES, Hash Algorithm is MD5, and Perfect Forward Secrecy (PFS) is Yes. The Lifetimes section includes: ISAKMP SA Lifetime (seconds) 3600, IPsec SA Lifetime (seconds) 28800, Rekeymargin (seconds) 540, Rekeyfuzz (percent) 100, Keying tries (0 means unlimited tries) 0, and Rekey Yes. The Dead Peer Detection section includes: Action Hold (Default), Delay 30, and Timeout 120.

- **ISAKMP SA (Key Exchange)**: Specify the **Encryption** and **Hash Algorithm** for phase I, in our example 3DES/MD5.
- **IPsec SA (Data exchange)**: Specify the **Encryption** and **Hash Algorithm** for phase II, in our example 3DES/MD5.
- Enable **Perfect Forward Secrecy (PFS)** if this option has also been enabled on the Cisco device (refer to [Perfect Forward Secrecy \(PFS\) and IPsec SA Lifetime](#)).
- Ensure that the lifetimes for the ISAKMP SA and the IPsec SA match the settings on the Cisco device (refer to [IKE Proposal](#) and [Perfect Forward Secrecy \(PFS\) and IPsec SA Lifetime](#)).
- 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 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**).

Connection Name	Connection		ISAKMP State	IPsec State
Cisco	Gateway	141.16.82.38	194.56.123.14	STATE_MAIN_I4 (ISAKMP SA established)
	Traffic	192.168.1.0/24	192.168.222.0/24	
	ID	O=Innominat, OU=Support, CN=mGuard	CN=Cisco, OU=Support, O=Innominat	
				STATE_QUICK_I2 (sent Q12, IPsec SA established)
				Lifetime:27156s

*IPsec status of a VPN connection using X.509 certificates as authentication method*

### 7.1 ISAKMP SA couldn't be established

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

- Mismatched X.509 certificates or PSK.
- When using certificates:
  - CRL is activated on the Cisco device but not configured (refer to [Check Certificate Revocation List](#)).
  - Mismatch of the used VPN identifier (refer to [VPN Identifier](#)).
- The mGuard is configured to use PFS but PFS is not enabled on the Cisco device (refer to [Perfect Forward Secrecy \(PFS\) and IPsec SA Lifetime](#)).
- 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.
- 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.