

Innominate mGuard/mGuard PCI

Interoperability Guide

Setting up a VPN connection between
mGuard v2.x and Intermate TrustGate 5



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
www.innominate.com

© Innominate Security Technologies AG

January 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: 571009-124

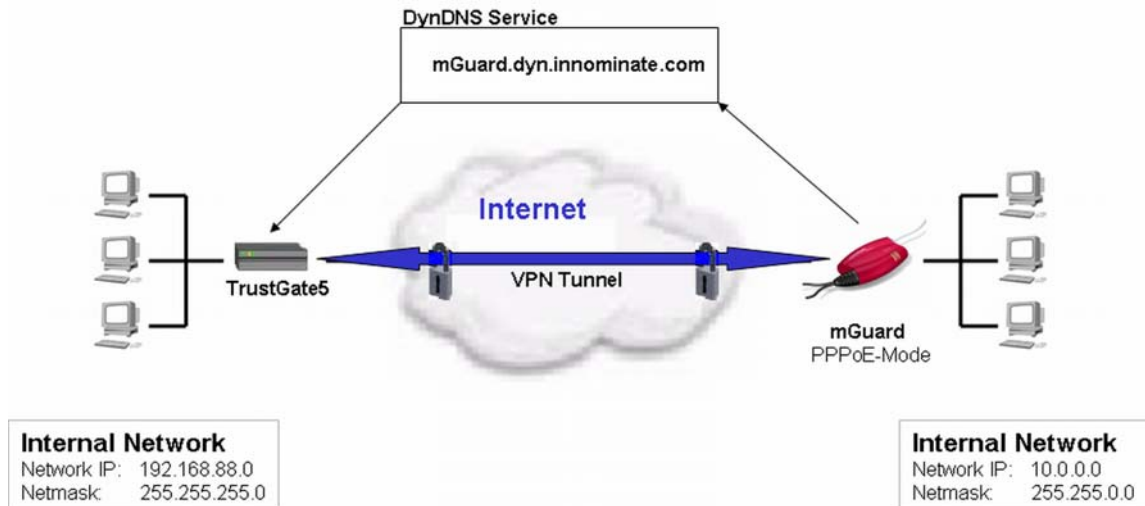
CONTENTS

1	Introduction	4
2	X.509 Certificates	5
2.1	<i>Required certificates</i>	5
2.2	<i>XCA: Create and export the certificates for the mGuard</i>	5
2.2.1	Step 1: Create the Root CA	5
2.2.2	Step 2: Create the mGuard certificate	5
2.2.3	Step 3: Export of the mGuard certificate as PEM and PKCS#12	6
2.3	<i>TrustGate: Create and export the local certificate</i>	6
3	Configuration of the TrustGate	7
3.1	<i>Prerequisites</i>	7
3.2	<i>Configuration of the remote gateway (mGuard)</i>	7
3.3	<i>Configuration of the VPN tunnel</i>	8
4	Configuration of the mGuard	9
4.1	<i>Import of the mGuard machine certificate</i>	9
4.2	<i>Configuration of the VPN tunnel</i>	9
5	Getting status information about the VPN tunnel	10
5.1	<i>mGuard</i>	10
5.2	<i>TrustGate</i>	10
6	Troubleshooting	11
6.1	<i>ISAKMP couldn't be established</i>	11
6.2	<i>IPsec couldn't be established</i>	11

1 Introduction

This document describes the required steps to configure a VPN tunnel between the mGuard v.2.x and the Intermate TrustGate 5 Model 20 (Firmware: V17_3391). The mGuard was configured to operate in *PPPoE-Mode* and registers its IP-address within a DynDNS-Service. The VPN tunnel will be initiated by the TrustGate. 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. 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 TrustGate

Due to this setup we have the following parameters for the VPN-Tunnel:

	mGuard	TrustGate
Remote VPN gateway	%any	mGuard.dyn.innominat.com
Local VPN subnet	10.0.0.0/255.255.0.0	192.168.88.0/255.255.255.0
Remote VPN subnet	192.168.88.0/255.255.255.0	10.0.0.0/255.255.0.0

2 X.509 Certificates

2.1 Required certificates

You need the following certificates for setting up the VPN connection:

- Local certificate of the TrustGate.
 - ⇒ Export as PEM: Import on the mGuard as connection certificate.
- mGuard certificate:
 - ⇒ Export as PEM: Import on the TrustGate as connection certificate.
 - ⇒ Export as PKCS#12: Import on the mGuard as machine certificate.

The local certificate of the TrustGate has to be created on the TrustGate. How to do this is described in chapter "TrustGate: Create and export the local certificate". We used the tool XCA for creating and exporting the certificates for the mGuard. You can download this tool from <http://www.hohnstaedt.de/xca.html>. The documentation is located at <http://xca.sourceforge.net/>.

2.2 XCA: Create and export the certificates for the mGuard

You need to perform the following steps for creating the required certificates for the mGuard with the tool XCA:

- Step 1: Create the Root CA.
- Step 2: Create the mGuard certificate (this certificate will be signed with the Root CA).
- Step 3: Export of the mGuard certificate as PEM and PKCS#12.

2.2.1 Step 1: Create the Root CA

- Start the tool **XCA**.
- Switch to the tab **Certificates**, click at **New Certificate** and then at **Next**.
- Select the option **Create a self signed certificate with the serial**, select **CA Template** and click at **Next**.
- A **new key** needs to be created. Enter a descriptive name for the key (e.g. Fortigate Root CA) and click at **Create**.
- Use the entry fields from **Internal Name** to **E-Mail Address** for entering the identifying parameters. Click at **Next**.
- Enter into the fields **Time Range** the lifetime of the Root-CA, click at **Apply** and then at **Next**.
- Now you only need to confirm the appearing input masks by selecting **Next** until the certificate has been created.

2.2.2 Step 2: Create the mGuard certificate

- Switch to the tab **Certificates**, select the Root-CA and click at **New Certificate**.
- Click at **Next**.
- Ensure that **Use this certificate for signing** is selected and that the Root-CA is selected in the drop-down box.
- Set **Template for the new certificate** to **Client Template** and click at **Next**.
- Enter a **Name** for the **New Key** and click at **Create**.
- Use the entry fields from **Internal Name** to **E-Mail Address** for entering the identifying parameters. Click at **Next**.
- Enter into the fields **Time Range** the lifetime of the certificate, click at **Apply** and then at **Next**.
- Now you only need to confirm the appearing input masks by selecting **Next** until the certificate has been created.

2.2.3 Step 3: Export of the mGuard certificate as PEM and PKCS#12

- Select the mGuard certificate in the tab **Certificates** and click at **Export**.
- Set **Export Format** to **PKCS#12** and click at **OK**.
- You'll be prompted to enter a password which protects the certificate against unauthorized usage.
- ⇒ If you did not specify a directory for saving the certificate then the export is located in the XCA installation directory.
- Select the mGuard certificate in the tab **Certificates** and click at **Export**.
- Set **Export Format** to **PEM** and click at **OK**.
- ⇒ If you did not specify a directory for saving the certificate then the export is located in the XCA installation directory.

2.3 TrustGate: Create and export the local certificate

- Select **Certificates -> Local** from the menu.
- Click at **Create**.

Note: Fields with red border are mandatory, others are optional.

Name:	<input type="text" value="TrustGate5"/>
Organization:	<input type="text" value="Innominate"/>
Organizational Unit:	<input type="text" value="Support"/>
Country (2-letter code):	<input type="text" value="de"/>
State or Province:	<input type="text" value="Germany"/>
Locality:	<input type="text" value="Berlin"/>
Email Address:	<input type="text" value="support@innominati"/>
DNS Name:	<input type="text"/>
IP Address:	<input type="text"/>

- Use the entry fields from **Name** to **E-Mail Address** for entering the identifying parameters.
- Click at **Create**.
- ⇒ The local certificate for the TrustGate will be created.
- Copy the part from “-----BEGIN CERTIFICATE REQUEST-----” until “-----END CERTIFICATE REQUEST-----” (including also those lines), paste them into a text editor and save the file for example as trustgate.pem. This file needs to be imported as connection certificate on the mGuard.

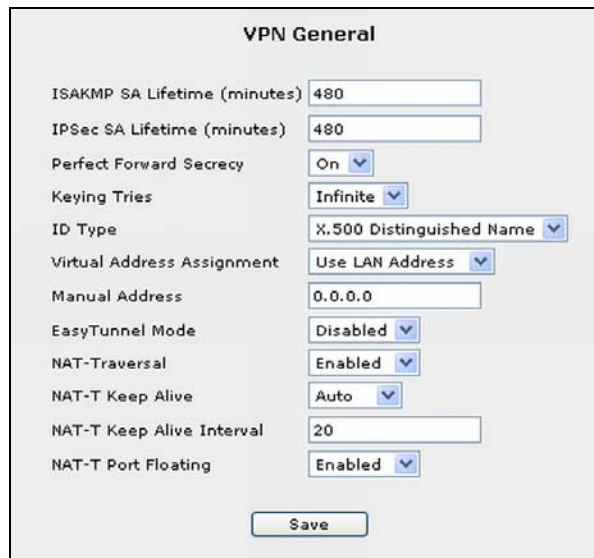
3 Configuration of the TrustGate

3.1 Prerequisites

It is important that you set the VPN identifier to "Distinguished Name". This is suitable if you setup a new system. Please contact support@innominate.com if you want to integrate the mGuard into an existing environment without the possibility to change the used VPN identifier.

Perform the following steps for changing the VPN identifier to "Distinguished Name":

- Select **VPN -> General** from the menu.

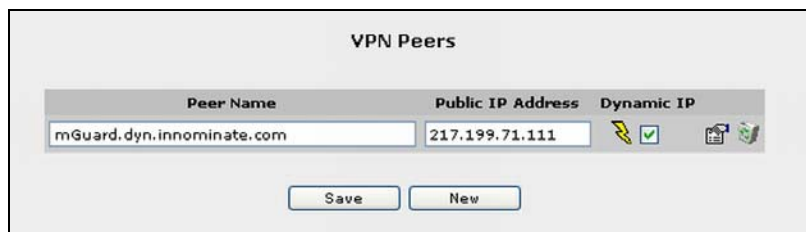


The screenshot shows the 'VPN General' configuration window. The 'ID Type' dropdown menu is set to 'X.500 Distinguished Name'. Other settings include: ISAKMP SA Lifetime (480), IPsec SA Lifetime (480), Perfect Forward Secrecy (On), Keying Tries (Infinite), Virtual Address Assignment (Use LAN Address), Manual Address (0.0.0.0), EasyTunnel Mode (Disabled), NAT-Traversal (Enabled), NAT-T Keep Alive (Auto), NAT-T Keep Alive Interval (20), and NAT-T Port Floating (Enabled). A 'Save' button is at the bottom.

- Set **ID Type** to **X.500 Distinguished Name**.
- Click at **Save**.
- Reboot the TrustGate.

3.2 Configuration of the remote gateway (mGuard)


- Select **VPN -> Peers** from the menu.
- Click at **New**.



The screenshot shows the 'VPN Peers' configuration window. It contains a table with the following data:

Peer Name	Public IP Address	Dynamic IP
mGuard.dyn.innominate.com	217.199.71.111	<input checked="" type="checkbox"/>

Below the table are 'Save' and 'New' buttons. The 'Dynamic IP' column has a lightning bolt icon and a checkmark.

- You can either enter a static IP address into the field **Public IP Address** or enter a DynDNS-Name into the field **Peer Name** and activate the flag **Dynamic IP**. The FortiGate5 will resolve the DynDNS-Name and display its current IP address in the field *Public IP Address* after saving the settings.
- Click at **Save**.
- Click at the icon  for specifying either the Preshared Key or for importing the certificate.


- If you want to use X.509 certificates: Open the PEM export of the mGuard certificate (in our example mGuard.pem) with a text editor, copy the complete certificate including the lines "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" and paste it into the input field **Pre-Loaded Certificate**.
- If you want to use Pre-shared Keys: Set in the section **Pre-Shared Key** the data type to **ASCII** and enter the pre-shared key.
- Click at **Save**.

3.3 Configuration of the VPN tunnel

- Select **VPN -> Tunnels** from the menu.
- Click at **New**.

Peer	Local Network	Local Subnet Mask	Remote Network	Remote Subnet Mask	Compress
new: mGuard.dyn.innominat.com	192.168.88.0	255.255.255.0	10.0.0.0	255.255.0.0	<input type="checkbox"/>

- Select the remote **Peer** to which the VPN tunnel should be established.
- The TrustGate already enters the values for the **Local Network** and the **Local Subnet Mask** with the network IP of the internal network, in our example 192.168.88.0/255.255.255.0.
- Enter into the fields **Remote Network** and **Remote Subnet Mask** the network IP of the internal network of the mGuard, in our example 10.0.0.0/255.255.0.0.
- Click at **Save**.

Now the configuration of the VPN tunnel at the TrustGate is finished. Click at the icon  for establishing the connection from the TrustGate to the mGuard.

4 Configuration of the mGuard

4.1 Import of the mGuard machine certificate

You only need to perform this step if you are using X.509 certificates.

- Select **VPN -> Machine Certificate** from the menu.
- Click at **Browse** and specify the PKCS#12 export of the mGuard certificate, in our example mGuard.p12.
- Enter the **Password** which protects the certificate against unauthorized usage.
- Click at **Import**.
- Click at **OK** when the import of the certificate is finished.

4.2 Configuration of the VPN tunnel

- Select **VPN -> Connections** from the menu.
 - Click at **New**.
 - Enter a descriptive name for the connection (e.g. Intermate) and click at **Edit**.
- ⇒ The following screen appears:

VPN > Connections > Connection Intermate

A descriptive name for the connection	Intermate						
Enabled	Yes <input type="button" value="v"/>						
Address of the remote site's VPN gateway (either an IP address, a hostname, or %any)	%any						
Connection type	Tunnel (Net <-> Net) <input type="button" value="v"/>						
Connection startup	Wait for connection from... <input type="button" value="v"/> ...remote VPN gateway.						
ISAKMP SA (Key Exchange)							
Authentication method	X.509 Certificate <input type="button" value="v"/> <input type="button" value="Configure"/>						
Encryption Algorithm	3DES-168 <input type="button" value="v"/>						
Hash Algorithm	All algorithms <input type="button" value="v"/>						
IPsec SA (Data Exchange)							
Encryption Algorithm	AES-128 <input type="button" value="v"/>						
Hash Algorithm	All algorithms <input type="button" value="v"/>						
Perfect Forward Secrecy (PFS) (The remote site must have the same entry. Activation is recommended due to security reasons.)	Yes <input type="button" value="v"/>						
Tunnel Settings							
Local network address	10.0.0.0						
The appropriate local netmask	255.255.0.0						
The virtual IP which will be used by the client in Stealth mode	192.168.1.1						
Remote network address	192.168.88.0						
The appropriate remote netmask	255.255.255.0						
Firewall Incoming (untrusted port)							
Protocol	From IP	From Port	To IP	To Port	Action	Log	
All <input type="button" value="v"/>	0.0.0.0/0	any	0.0.0.0/0	any	Accept <input type="button" value="v"/>	No <input type="button" value="v"/>	<input type="button" value="Delete"/>
Log entries for unknown connection attempts						No <input type="button" value="v"/>	<input type="button" value="New"/>
Firewall Outgoing (trusted port)							
Protocol	From IP	From Port	To IP	To Port	Action	Log	
All <input type="button" value="v"/>	0.0.0.0/0	any	0.0.0.0/0	any	Accept <input type="button" value="v"/>	No <input type="button" value="v"/>	<input type="button" value="Delete"/>
Log entries for unknown connection attempts						No <input type="button" value="v"/>	<input type="button" value="New"/>
<input type="button" value="All Connections"/> <input type="button" value="OK"/>							

- **Address of the remote site’s VPN gateway:** Enter **%any** if the connection will be initiated by the TrustGate. Otherwise enter the static IP or the DynDNS-name of the TrustGate.
- Set **Connection type** to **Tunnel (Net <-> Net)**.
- Specify with the parameter **Connection Startup** if the connection will be initiated by the mGuard (**Start connection to ...**) or by the TrustGate (**Wait for connection from ...**),
- **Authentication method:**
 - Pre-Shared Keys: Set **Authentication method** to **Pre-shared Secret**. Click at **Configure** and enter the shared secret.
 - X.509 Certificates: Set **Authentication method** to **X.509 Certificate**. Click at **Configure** and import the local certificate of the TrustGate (in our example: trustgate.pem).
- **ISAKMP SA (Key Exchange):** Set the parameters as follows:
 - Encryption Algorithm = 3DES-168
 - Hash Algorithm = All algorithms
- **IPSec SA (Data exchange):** Set the parameters as follows:
 - Encryption Algorithm = AES-168
 - Hash Algorithm = All algorithms
 - Perfect Forward Secrecy = Yes
- **Tunnel settings / local network and netmask:** These parameters specify the internal network of the mGuard, in our example 10.0.0.0/255.255.0.0.
- **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*.
- **Tunnel settings / remote network and netmask:** These parameters specify the internal network of the TrustGate, in our example 192.168.88.0/255.255.0.0.
- **Firewall incoming / outgoing:** Those entries can be used for specifying an incoming and outgoing Firewall specific to the VPN tunnel. Note that this firewall applies to the VPN tunnel only.
- Click at **OK**.

The mGuard will try immediately to establish the VPN connection if:

- The mGuard is operated in *Router/PPPoE-Mode*,
- The VPN connection is enabled,
- The mGuard should initiate the VPN connection.

5 Getting status information about the VPN tunnel

5.1 mGuard

Select **VPN -> IPSec Status** from the menu. **ISAKMP State** and **IPSec State** should be established in case of a successful connection.

VPN > IPSec Status				
Connection Name	Connection		ISAKMP State	IPsec State
Intermate [1]	Gateway	82.144.46.29		80.143.49.177
	Traffic	172.16.106.100/32 /		192.168.88.0/24 /
	ID	CN=mGuard, C=de, L=Berlin, ST=Germany, O=Innominat, OU=Innominat, E=support@innominate.com	CN=TrustGate5, O=Innominat, OU=Support, C=de, ST=Germany, L=Berlin	80.143.49.177 STATE_MAIN_R3 (sent MR3, ISAKMP SA established)

5.2 TrustGate

Select **Status -> Tunnels** from the menu. The status of the tunnel should be "Up" in case of a successful connection.

6 Troubleshooting

Establishing a VPN connection consists of two phases: phase 1 (ISAKMP) and phase 2 (IPSec).

6.1 ISAKMP couldn't be established

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

- Mismatched pre-shared keys or certificates.
- Mismatched or not supported ISAKMP policy parameters. Edit the VPN connection (menu: VPN -> Connections) and compare the parameters of the section "ISAKMP SA (Key exchange)" with the settings on the remote entity. Check if you have specified the same settings on both entities and if the remote entity supports the selected parameters.

6.2 IPsec couldn't be established

If ISAKMP could be established but not the IPSec then this could be caused by the following reasons:

- Mismatched or not supported IPSec policy parameters. Edit the VPN connection (menu: VPN -> Connections) and compare the parameters of the section "IPSec SA (Data exchange)" with the settings on the remote entity. Check if you have specified the same settings on both entities and if the remote entity supports the selected parameters.
- Mismatched tunnel (subnet) parameters.