

Innominate mGuard/mGuard PCI

Interoperability Guide

Setting up a VPN connection between
mGuard v2.x and Netscreen 5GT / 204 / 5400



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

Interop Guide – VPN connection between mGuard and Netsreen

© Innominate Security Technologies AG

March 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: 571009-129

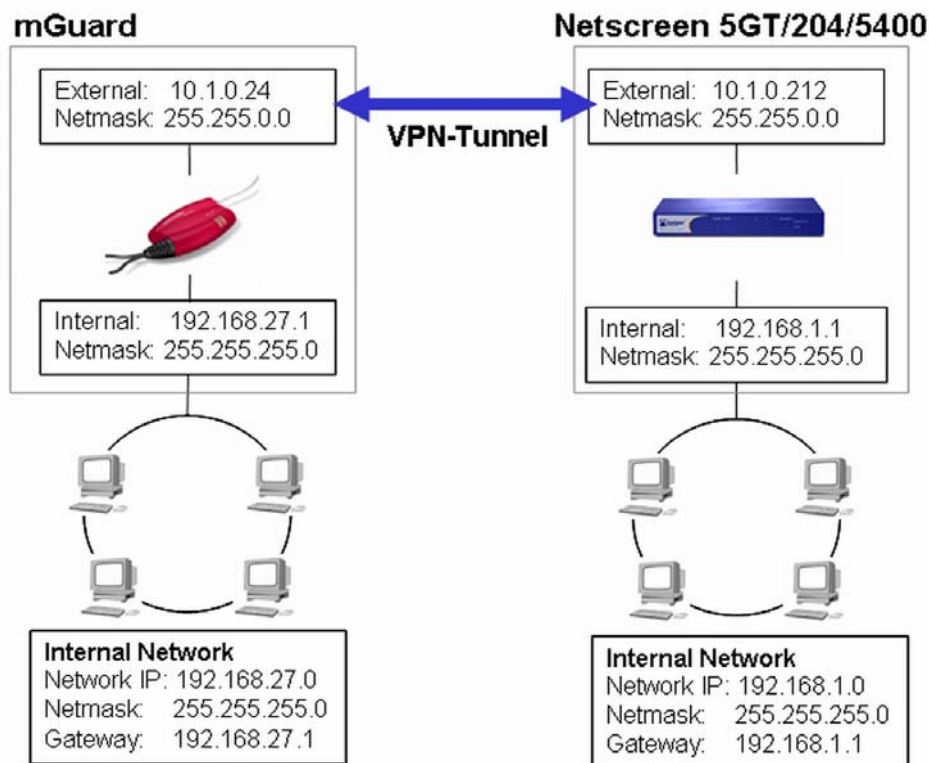
CONTENTS

1	Introduction	4
2	Limitations	5
3	X.509 Certificates	5
3.1	Step 1: Create a certificate request on the Netscreen	6
3.2	Step 2: Create the CA	7
3.3	Step 3: Import the certificate request of the Netscreen and sign it with the CA	7
3.4	Step 4: Create a certificate for the mGuard, signed by the CA	7
3.5	Step 5: Create a Certificate Revocation List (CRL)	8
3.6	Step 6: Export of the certificates	8
3.7	Step 7: Import of the certificates (CA, CRL and local certificate) on the Netscreen	8
4	Configuration of the Netscreen	9
4.1	Import of the certificates (CA, CRL and local certificate)	9
4.2	Internal (trusted) and external (un-trusted) interfaces	9
4.3	Internal networks of the mGuard and of the Netscreen	10
4.3.1	Internal network of the mGuard	10
4.3.2	Internal network of the Netscreen	10
4.4	Remote VPN Gateway	11
4.4.1	Pre-shared Keys (PSK)	11
4.4.2	X.509 certificates	12
4.5	AutoKey IKE (Phase 2 Proposal)	13
4.6	Policy for the VPN connection	14
5	Configuration of the mGuard	15
5.1	Menu: VPN -> Connections	15
5.2	Menu: VPN -> Machine Certificate	16
6	Overview about the performed interoperability tests	17
6.1	PSK, X.509 Certificates, NAT-T	17
6.2	Phase 1 and Phase 2, hash and encryption algorithm	17
6.3	Random tests with different methods	17
7	Troubleshooting	18
7.1	ISAKMP couldn't be established	18
7.2	IPsec couldn't be established	18

1 Introduction

This document describes the procedures required to configure a VPN connection between the mGuard v.2.x and the Netscreen 5GT / 204 / 5400. The mGuard was configured to operate in *Router-Mode*. The VPN tunnel will be initiated by the mGuard. This document describes the usage of the authentication methods PSK (Pre-shared Secret Keys) 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 private. The examples used in this document are taken from this setup. The screenshots were taken from the interoperability test between the mGuard and the Netscreen 5GT because the Web-Interface for the configuration for the Netscreen 204 and the Netscreen 5400 do not differ. Exactly the same setup was used for the interoperability test between the mGuard and the Netscreen 204 / 5400.



Scenario used for the setup of the VPN-tunnel between the mGuard and the Netscreen 5GT/204/5400

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

	mGuard	Netscreen
Remote VPN gateway	10.1.0.212	10.1.0.24 or dynamic (X.509)
Local VPN subnet	192.168.27.0/255.255.255.0	192.168.1.0/255.255.255.0
Remote VPN subnet	192.168.1.0/255.255.255.0	192.168.27.0/255.255.255.0

2 Limitations

If Pre-Shared Secret Key (PSK) is used as authentication method and if the VPN tunnel will be established across one or more gateways that have Network Address Translation (NAT) activated then the remote VPN gateway (mGuard) requires a static IP or must register its dynamic IP with a DynDNS-Service. Otherwise *Aggressive Mode* needs to be used which is not supported by the mGuard due to security reasons.

3 X.509 Certificates

We have used the tool XCA v0.5.1 for creating the required certificates. You can download this tool from <http://www.hohnstaedt.de/xca.html>. The documentation is located at <http://xca.sourceforge.net/>.

Important note: The Netscreen uses its FQDN (Fully Qualified Domain Name) as VPN identifier. This requires that the FQDN of the Netscreen is present in the certificate as subject alternative name. This is the case but the current version of XCA does not copy the extensions when importing the certificate request. Therefore you must add manually the FQDN of the Netscreen as subject alternative when signing the request with the CA. Select *Network -> DNS* from the menu for obtaining the FQDN (Host name + Domain name). In our example the Netscreen has the FQDN *ns5gt.netscreen.com*. Apart of this the Netscreen also expects the presence of the Certificate Revocation List (CRL).

Using certificates for the VPN connection between the mGuard and the Netscreen requires the following steps:

Netscreen:

- Step 1: Create a certificate request on the Netscreen.

XCA:

- Step 2: Create the CA.
- Step 3: Import the certificate request of the Netscreen and sign it with the CA.
- Step 4: Create a certificate for the mGuard, signed by the CA.
- Step 5: Create a Certificate Revocation List (CRL).
- Step 6: Export of the certificates.
 - CA as PEM.
 - Signed certificate request of the Netscreen as PEM.
 - Certificate of the mGuard as PKCS#12.
 - Certificate Revocation List (CRL) as PEM.

Netscreen:

- Step 7: Import of the certificates (CA, CRL and local certificate) on the Netscreen.

3.1 Step 1: Create a certificate request on the Netscreen

- Select **Objects -> Certificates** from the menu.
- Click at **New**.

The screenshot shows a form titled "Certificate Subject Information". It contains several input fields for personal and organizational details. Below these fields is a "Key Pair Information" section with radio buttons for "RSA" (selected) and "DSA", and a dropdown menu for key length set to "1024". At the bottom are "Generate" and "Cancel" buttons.

Name:	NetScreen
Phone:	
Unit/Department:	Support
Organization:	Innominate
County/Locality:	Berlin
State:	Germany
Country:	de
E-mail:	support@innominate.cc
IP Address:	
FQDN:	ns5gt.netscreen.com

Key Pair Information:
 RSA DSA
Create new key pair of 1024 length.

- Use the entry fields from **Name** to **FQDN** for entering the identifying parameters. Click at **Generate**.

The screenshot shows a dialog box titled "Certificate Request". It contains a large text area with a certificate request string. Below the text area are "Save To File" and "Automatically enroll to" options. Under "Automatically enroll to", there are radio buttons for "New CA server settings" (selected) and "Existing CA server settings". The "New CA server settings" section includes input fields for "RA CGI", "CA CGI", "CA IDENT", and "Challenge". There is also an "Advanced Settings..." link. At the bottom are "OK" and "Cancel" buttons.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICQDCCAAkCAQAwgbYxCzAJBgNVBAYTAmR1MR4wDgYDVQQIEwdHZXJtYW55MQ8w
DQYDVQQHEwZCZXJsaU4xZzARBgNVBAoTCk1ubm9taU5hdGUxEDAOBgNVBAsTB1N1
cHBvcnQxGTAXBgNVBANTEDAwNjQwHjIwHDQwHDI3NDUxEDA0BgNVBANTB3JzYS1r
ZXkxHDAABgNVBANTe25zNWd0Lm5ldHNjcmVlb15jb20xEjAQBgNVBANTCUs1dFNj
cmVlbjCBnzANBgkqhkiG9w0BAQEFAAOBjQAUGYkCgYEA4HnD0gkrpScfFy60OPVb
SBEjIAn93wOH4135+kCNAaYOFhPM5rSxEoBDY61R84p1GpKN85eDyQsC0SnsWLI
NXQ32TcniH7053XyJztAifwssF7G99AVj5tMQee7nUGst3Td9pUzjXnljV4eG1OT
F9Ld8255kN0dN6HV6512gCOCawEAAaBJMEcGCSqGSIb3DQEJdjE6HDgwNgYDVROR
BC8wLYITbnM123QubmV0c2NyZWVuLmNvbYUc3VwcG9ydEBpbm5vbWluYXR1LmNv
```

Save To File

E-mail to:

Automatically enroll to

New CA server settings

RA CGI

CA CGI

CA IDENT

Challenge

[Advanced Settings...](#)

Existing CA server settings

- Click at **Save to File** and save the certificate request.
- Click at **Cancel** (the certificate request was already created when selecting <Save to File>).

Issuer	Friendly Name	Type	Serial#	Expired	Status	Configure
-	-	LOCAL	0000000000000000	-	Key Pair	Detail , Remove Submit Request

⇒ The certificate request is displayed in the list. Note that this request still needs to be signed by the CA. We will sign this certificate request with the tool XCA with the CA (Step 3) and import the signed certificate later (Step 7).

3.2 Step 2: Create the 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. Netscreen 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 field **Time Range** the lifetime of the 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.

3.3 Step 3: Import the certificate request of the Netscreen and sign it with the CA

- Switch to the tab **Certificate signing requests**, click at **Import** and import the certificate request of the Netscreen you have created in step 1.
- Make a right click at the imported certificate and select **Sign** from the menu.
- Click at **Next**.
- Enable **Use this certificate for signing** and select the CA you've created in step 2. Click at **Next**.
- Enter into the field **Time Range** the lifetime of the local certificate and click at **Apply**.
- **ATTENTION:** Enter into the field **subject alternative name** the FQDN of the Netscreen, using the syntax *DNS:<FQDN>* (in our example: *DNS:ns5gt.netscreen.com*) and click at **Next**.
- Now you only need to confirm the appearing input masks by selecting **Next** until the certificate has been signed.
- Switch to the tab **Certificates**. The imported and signed certificate of the Netscreen appears beneath the CA.

3.4 Step 4: Create a certificate for the mGuard, signed by the CA

- Switch to the tab **Certificates**, select the CA and click at **New Certificate**.
- Click at **Next**.
- Ensure that **Use this certificate for signing** is selected and that the 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. Write down the entered parameters because you'll need them when configuring the remote gateway on the Netscreen! Click at **Next**.
- Enter into the field **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.

3.5 Step 5: Create a Certificate Revocation List (CRL)

- Switch to the tab **Certificates** and make a right click at the CA.
 - Select **CA -> CRL Days** from the menu, enter the lifetime of the CRL in days and click at **OK**.
 - Make again a right click at the CA and select **CA -> Generate CRL** from the menu.
- ⇒ The generated CRL is displayed in the tab **Revocation lists**.

3.6 Step 6: Export of the certificates

- Switch to the tab **Certificates**.

Export of the CA as PEM

- Select the CA and click at **Export**.
 - Chose **PEM** as **Export Format** 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.

In our example we have named the file "CA.crt".

Export of the signed certificate request of the Netscreen as PEM

- Select the signed certificate request of the Netscreen which is located beneath the CA and click at **Export**.
 - Chose **PEM** as **Export Format** 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.

In our example we have named the file "Netscreen_local.crt".

Export of the mGuard certificate as PKCS#12

- Select the mGuard certificate which is located beneath the CA 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.

In our example we have named the file "mGuard.p12".

Export of the Certificate Revocation List (CRL) as PEM

- Switch to the tab **Revocation lists**.
- Make a right click at the revocation list and select **Export -> PEM** from the menu.

In our example we have named the file "CA.crl".

3.7 Step 7: Import of the certificates (CA, CRL and local certificate) on the Netscreen

Please refer to the next chapter "Import of the certificates (CA, CRL and local certificate)".

4 Configuration of the Netscreen

4.1 Import of the certificates (CA, CRL and local certificate)

Import of the CA

- Select **Objects -> Certificates** from the menu.
- Click at **Browse** and select the PEM-export of the CA (in our example: CA.crt).
- Click at **Load**.

Import of the local certificate

- Select **Objects -> Certificates** from the menu.
- Click at **Browse** and select the PEM-export of signed certificate request (in our example: Netscreen_local.crt).
- Click at **Load**.

Import of the certificate revocation list (CRL)

- Select **Objects -> Certificates** from the menu.
- Set **Load** to **CRL**.
- Click at **Browse** and select the PEM-export of the certificate revocation list (in our example: CA.crl).
- Click at **Load**.

The local certificate is displayed when you set **Show** to **Local**:

Issuer	Friendly Name	Type	Serial#	Expired	Status	Configure
CA	10	LOCAL	00000008	02-17-2006 13:01	Active	Detail, Remove

The CA and the CRL are displayed when you set **Show** to **CA**:

Issuer	Friendly Name	Type	Serial#	Expired	Status	Configure
Secure Server Certification Authority Server Settings	2	CA	02ad667e4e45fe5e576f3c98195eddc0	01- 7-2010 23:59	Active	Detail, Remove
CA Server Settings	8	CA	00000001	02-17-2006 13:01	Active	Detail, Remove
CA	-	CRL	0000000000000000	02-18-2006 15:05	Active	Detail, Remove

4.2 Internal (trusted) and external (un-trusted) interfaces

We have configured the following internal (trusted) and external (un-trusted) interfaces on the Netscreen (menu: **Network -> Interfaces**):

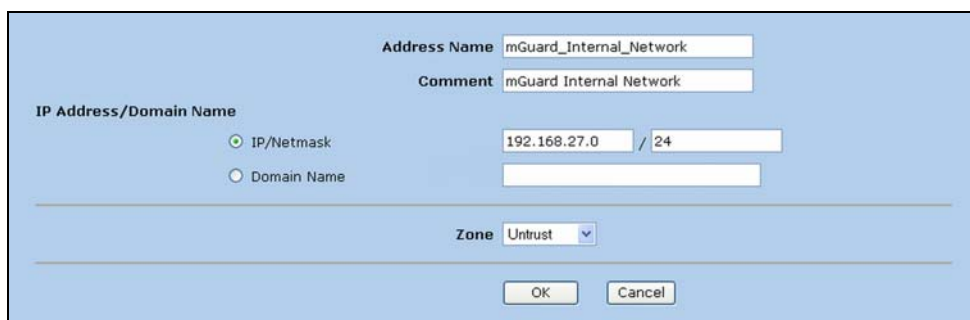
Name	IP/Netmask	Zone	Type	Link	Configure
trust	192.168.1.1/24	Trust	Layer3	up	Edit
untrust	10.1.0.212/16	Untrust	Layer3	up	Edit

4.3 Internal networks of the mGuard and of the Netscreen

Now you need to define the internal networks of the mGuard and of the Netscreen. Those definitions are used later when configuring the VPN tunnel.

4.3.1 Internal network of the mGuard

- Select **Objects -> Addresses -> List** from the menu.
- Select **Untrust** and click at **New**.



The screenshot shows a configuration window for creating a new address object. The fields are filled with the following values:

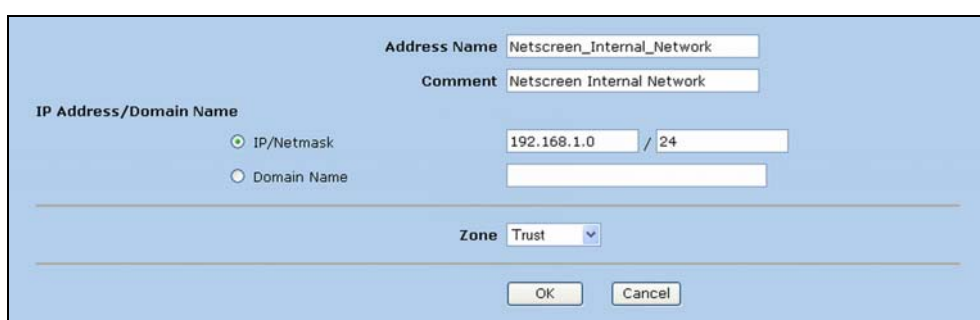
- Address Name:** mGuard_Internal_Network
- Comment:** mGuard Internal Network
- IP Address/Domain Name:** IP/Netmask (selected), 192.168.27.0 / 24
- Zone:** Untrust (selected in the dropdown menu)

Buttons for **OK** and **Cancel** are visible at the bottom.

- Enter as **Address Name** a name for this object and as **Comment** a descriptive comment.
- Enter into the fields **IP/Netmask** the network IP of the internal network of the mGuard, in our example 192.168.27.0/24.
- Ensure that **Untrust** is selected as **Zone**.
- Click at **OK**.

4.3.2 Internal network of the Netscreen

- Select **Objects -> Addresses -> List** from the menu.
- Select **Trust** and click at **New**.



The screenshot shows a configuration window for creating a new address object. The fields are filled with the following values:

- Address Name:** Netscreen_Internal_Network
- Comment:** Netscreen Internal Network
- IP Address/Domain Name:** IP/Netmask (selected), 192.168.1.0 / 24
- Zone:** Trust (selected in the dropdown menu)

Buttons for **OK** and **Cancel** are visible at the bottom.

- Enter as **Address Name** a name for this object and as **Comment** a descriptive comment.
- Enter into the fields **IP/Netmask** the network IP of the internal network of the Netscreen, in our example 192.168.1.0/24.
- Ensure that **Trust** is selected as **Zone**.
- Click at **OK**.

4.4 Remote VPN Gateway

4.4.1 Pre-shared Keys (PSK)

This chapter explains how to configure the remote VPN gateway on the Netscreen when using Pre-shared Keys. If you want to use X.509 certificates, skip this chapter and refer to the next chapter "X.509 certificates".

- Select **VPNs -> AutoKey Advanced -> Gateway** from the menu.
- Click at **New**.

The screenshot shows the 'Remote VPN Gateway' configuration window. The 'Gateway Name' is 'Remote VPN Gateway (PSK)'. The 'Security Level' is set to 'Custom'. Under 'Remote Gateway Type', 'Static IP Address' is selected. The 'IP Address/Hostname' is '10.1.0.24'. 'Peer ID', 'User', and 'Group' are all set to 'None'. The 'Preshared Key' is masked with four dots, and 'Use As Seed' is unchecked. 'Local ID' is an optional field. The 'Outgoing Interface' is 'untrust'. At the bottom are 'OK', 'Cancel', and 'Advanced' buttons.

- Enter as **Gateway Name** a descriptive name for the remote gateway.
- Set **Security Level** to **Custom**.
- Select **Static IP Address** and enter as **IP Address/Hostname** the IP-address of the mGuard, in our example 10.1.0.24.
- Enter as **Preshared Key** the pre-shared secret.
- Click at **Advanced**.

The screenshot shows the 'Security Level' configuration window. 'Predefined' options are 'Standard', 'Compatible', and 'Basic'. 'User Defined' options are 'Custom'. Under 'Phase 1 Proposal', 'pre-g2-3des-md5' is selected. 'Mode (Initiator)' is set to 'Main (ID Protection)'. 'Enable NAT-Traversal' is checked. 'UDP Checksum' is unchecked. 'Keepalive Frequency' is set to '0' seconds. At the bottom are 'Return' and 'Cancel' buttons.

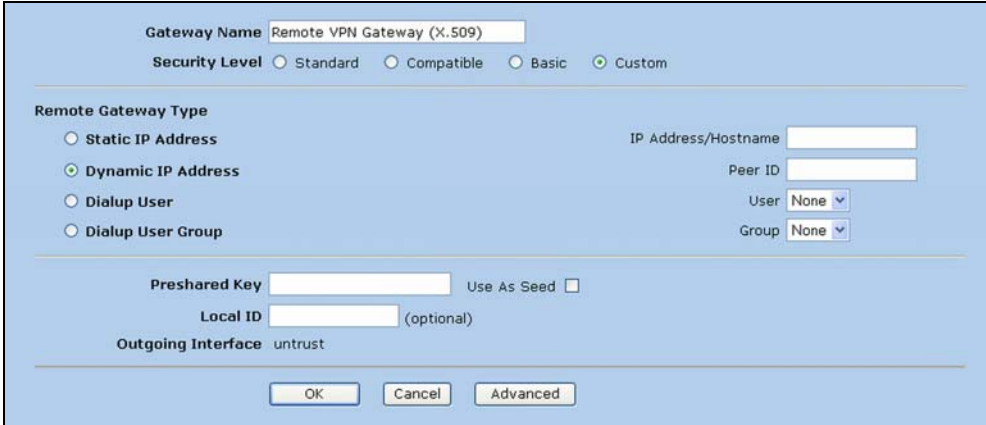
- Set **Security Level** to **User Defined – Custom**.
- Specify the **Phase 1 Proposal**. In our example we have chosen **pre-g2-3des-md5** which means:
 - pre = Authentication method Preshared Key
 - g2 = DH Group 2
 - 3des = Encryption Algorithm 3DES
 - md5 = Hash Algorithm MD5
- Ensure that **Mode** is set to **Main (ID Protection)**.
- Enable **NAT-Traversal** if the VPN tunnel will be established across one or more gateways that have Network Address Translation activated.
- Click at **Return** and then at **OK**.

Interop Guide – VPN connection between mGuard and Netscreen

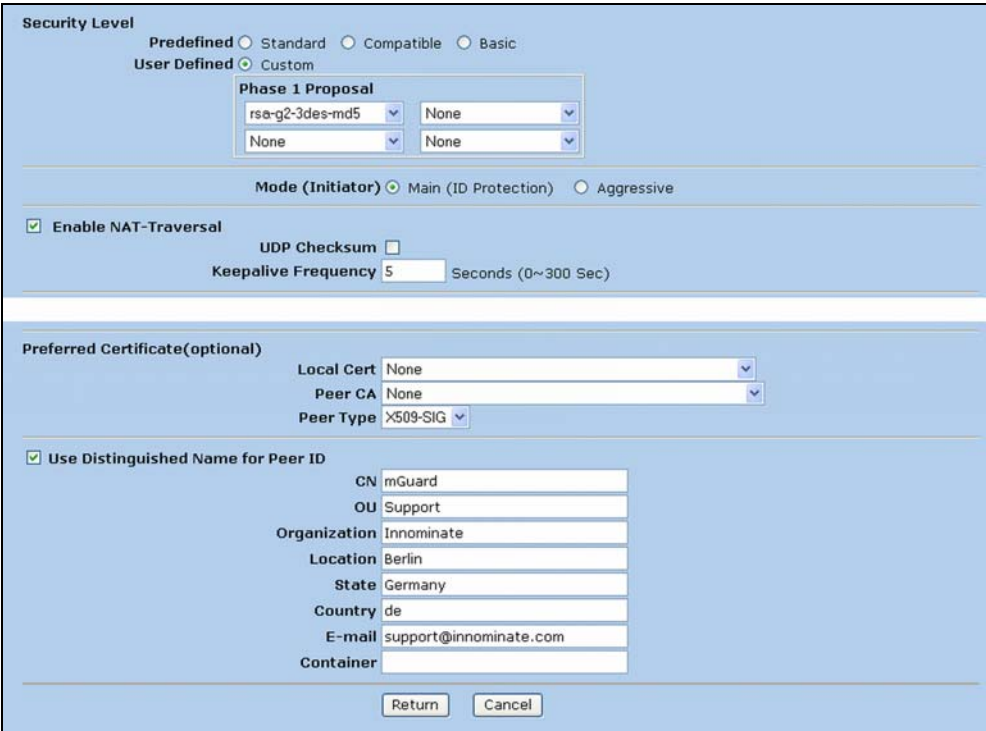
4.4.2 X.509 certificates

This chapter explains how to configure the remote VPN gateway on the Netscreen when using X.509 certificates.

- Select **VPNs -> AutoKey Advanced -> Gateway** from the menu and click at **New**.



- Enter as **Gateway Name** a descriptive name for the remote gateway.
- Set **Security Level** to **Custom**.
- Set **Remote Gateway Type** either to **Static IP Address** and enter the external IP address of the mGuard into the field **IP Address/Hostname** (in our example 10.1.0.24) or select **Dynamic IP Address**.
- Click at **Advanced**.



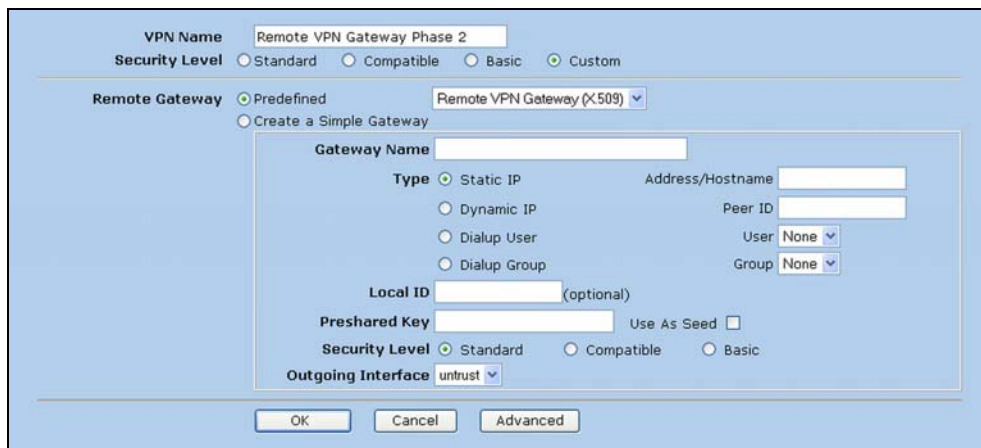
- Specify the **Phase 1 Proposal**. In our example we have chosen **rsa-g2-3des-md5** which means:
 - rsa = Authentication method X.509 certificates
 - g2 = DH Group 2
 - 3des = Encryption Algorithm 3DES
 - md5 = Hash Algorithm MD5

Interop Guide – VPN connection between mGuard and Netscreen

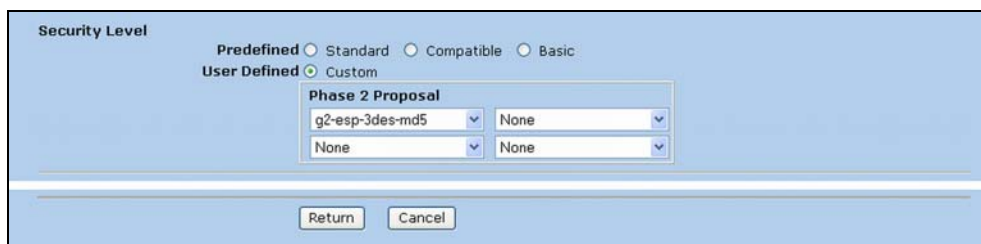
- Ensure that **Mode** is set to **Main (ID Protection)**.
- Enable **NAT-Traversal** if the VPN tunnel will be established across one or more gateways that have Network Address Translation activated.
- Set **Peer Type** to **X.509-SIG**.
- Enable **Use Distinguished Name for Peer ID** and enter the same certificate identifying parameters you've used when creating the certificate for the mGuard (refer to chapter "Step 4: Create a certificate for the mGuard, signed by the CA").
- Click at **Return** and then at **OK**.

4.5 AutoKey IKE (Phase 2 Proposal)

- Select **VPNs -> AutoKey IKE** from the menu.
- Click at **New**.



- Enter a descriptive **VPN Name**.
- Select the remote VPN gateway you've defined in the previous step as **Remote Gateway**.
- Set **Security Level** to **Custom** and click at **Advanced**.



- Specify the **Phase 2 Proposal**. In our example we have chosen **g2-esp-3des-md5** which means:
 - g2 = DH Group 2
 - esp = Encapsulating Security Payload
 - 3des = Encryption Algorithm 3DES
 - md5 = Hash Algorithm MD5
- Click at **Return** and then at **OK**.

4.6 Policy for the VPN connection

- Select **Policies** from the menu.
- Set **From=Untrust, To=Trust** and click at **New**.

The screenshot shows a configuration dialog box for a VPN policy. The fields are as follows:

- Name (optional):** VPN mGuard To Netscreen
- Source Address:** Address Book Entry: mGuard_Internal_Network (Multiple)
- Destination Address:** Address Book Entry: Netscreen_Internal_Network (Multiple)
- Service:** ANY (Multiple)
- Application:** None
- Action:** Tunnel (Deep Inspection)
- Antivirus Objects:** Attached AV Object Names (empty) and Available AV Object Names (scan-mgr)
- Tunnel:** VPN (Remote VPN Gateway Phase 2) (checkbox: Modify matching bidirectional VPN policy)
- L2TP:** None
- Logging:** checked

Buttons at the bottom: OK, Cancel, Advanced

- Enter a descriptive **Name**.
- Select as **Source Address** the address book entry for the internal network of the mGuard you have created in chapter "Internal network of the mGuard".
- Select as **Destination Address** the address book entry for the internal network of the Netscreen you have created in chapter "Internal network of the Netscreen".
- Set **Action** to **Tunnel** and specify as **Tunnel** the VPN-tunnel you have created in the previous step.
- Click at **OK**.

5 Configuration of the mGuard

5.1 Menu: VPN -> Connections

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

The screenshot shows the configuration page for a VPN connection named 'Netscreen'. The interface is organized into several sections:

- General Settings:** Includes fields for 'A descriptive name for the connection' (Netscreen), 'Enabled' (Yes), 'Address of the remote site's VPN gateway' (10.1.0.212), 'Connection type' (Tunnel (Net <-> Net)), and 'Connection startup' (Start connection to...).
- ISAKMP SA (Key Exchange):** Includes 'Authentication method' (X.509 Certificate), 'Encryption Algorithm' (3DES-168), and 'Hash Algorithm' (MD5).
- IPsec SA (Data Exchange):** Includes 'Encryption Algorithm' (3DES-168) and 'Hash Algorithm' (MD5).
- Perfect Forward Secrecy (PFS):** Set to Yes.
- Tunnel Settings:** Includes '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), and 'The appropriate remote netmask' (255.255.255.0).
- Remote ID:** Set to @ns5gt.netscreen.com.
- Firewall Incoming (untrusted port):** A table with columns for Protocol, From IP, From Port, To IP, To Port, Action, and Log. The default entry is All, 0.0.0.0, any, 0.0.0.0, any, Accept, No.
- Firewall Outgoing (trusted port):** A similar table with the same default entry.

At the bottom, there are buttons for 'All Connections' and 'OK'.

- Enter as **Address of the remote site's VPN gateway** the external IP-address of the Netscreen (in our example 10.1.0.212).
- 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**
- **ISAKMP SA (Key Exchange)** parameters:
 - **PSK:** 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 Netscreen (in our example: Netscreen_local.crt).
 - Select as **Encryption Algorithm** and **Hash Algorithm** the same settings you've specified on the Netscreen for the *Phase 1 Proposal*, in our example we have used **3DES-168** and **MD5**.

Interop Guide – VPN connection between mGuard and Netscreen

- **IPSec SA (Data exchange)** parameters: Select as **Encryption Algorithm, Hash Algorithm** and **Perfect Forward Secrecy (PFS)** the same settings you've specified on the Netscreen for the *Phase 2 Proposal*, in our example we have used **3DES-168, MD5** and **PFS** is enabled.
- **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*.
 - **Remote network and netmask:** These parameters specify the VPN-subnet (internal network) of the Netscreen, in our example 192.168.1.0/255.255.255.0.
- When using X.509 Certificates: You need to enter as **Remote ID** the FQDN of the Netscreen, using the syntax *@<FQDN>* (in our example: @ns5gt.netscreen.com). This entry field is only visible if you've added the user defined language *xt-ra* to the Web-Browser settings and if the language selector on the mGuard is set to *Automatic* (menu: *Access -> Language*).
- Click at **OK**.

5.2 Menu: VPN -> Machine Certificate

This step is only required if you use X.509 certificates. You need to import the PKCS#12 export of the mGuard certificate you've created in chapter "Step 4: Create a certificate for the mGuard, signed by the CA" (in our example: *mGuard.p12*).

6 Overview about the performed interoperability tests

6.1 PSK, X.509 Certificates, NAT-T

VPN with	Netscreen 5GT	Netscreen 204	Netscreen 5400
PSK	OK	OK	OK
X.509 Certificates	OK	OK	Not tested
NAT-T / X.509 Certificates	OK	OK	Not tested
Re-keying (standard settings with 12h long-term test)	OK	OK	OK

6.2 Phase 1 and Phase 2, hash and encryption algorithm

Phase 1	DES	3DES	AES	AES128	AES192	AES256	SHA1	MD5
NS 5GT	OK	OK	OK	OK	OK	OK	OK	OK
NS 204	OK	OK	OK	OK	OK	OK	OK	OK
NS 5400	OK	OK	OK	OK	OK	OK	OK	OK

Phase 2	DES	3DES	AES	AES128	AES192	AES256	SHA1	MD5
NS 5GT	OK	OK	OK	OK	OK	OK	OK	OK
NS 204	OK	OK	OK	OK	OK	OK	OK	OK
NS 5400	OK	OK	OK	OK	OK	OK	OK	OK

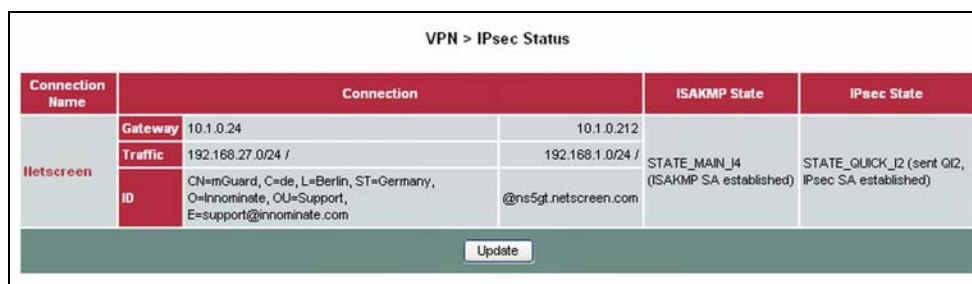
6.3 Random tests with different methods

	Phase 1	Phase 2	X509/ PSK
NS 5GT	3DES – MD5 – DH Group2	3DES – MD5 – PFS	PSK
NS 5GT	3DES – SHA1 – DH Group2	3DES – SHA1 – PFS	PSK
NS 5GT	3DES – MD5 – DH Group2	3DES – MD5 – PFS	X509
NS 5GT	3DES – SHA1 – DH Group2	3DES – SHA1 – PFS	X509
NS 204	AES256 – SHA1 – DH Group 5	AES256 – SHA1 – PFS Group 2	X509
NS 204	DES – MD5 – DH Group 2	AES256 – SHA1 – PFS Group 2	X509
NS 204	AES128 – SHA1 – DH Group 2	AES256 – SHA1 – PFS Group 2	X509
NS 204	3DES – SHA1 – DH Group2	3DES – SHA1 – no PFS	PSK
NS 204	3DES – SHA1 – DH Group2	DES – SHA1 – no PFS	PSK
NS 204	3DES – SHA1 – DH Group2	DES – MD5 no PFS	PSK
NS 204	3DES – SHA1 – DH Group2	3DES – SHA1 – PFS Group 2	PSK
NS 204	3DES – SHA1 – DH Group2	AES128 – SHA1 – PFS Group 2	PSK
NS 204	3DES – SHA1 – DH Group2	AES256 – SHA1 – PFS Group 5	PSK
NS 5400	AES128 – SHA1 - PFS Group2	3DES – SHA1 – no PFS	PSK
NS 5400	AES256 – SHA1 – PFS Group5	AES256 – SHA1 – PFS Group 2	PSK

7 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) and phase 2 (IPSec). In case of a successful connection the status of **ISAKMP** and **IPSec** should be **established** (menu: **VPN -> IPsec Status**).



The screenshot shows a table titled "VPN > IPsec Status" with the following data:

Connection Name	Connection		ISAKMP State	IPsec State
Netscreen	Gateway	10.1.0.24	10.1.0.212	
	Traffic	192.168.27.0/24 /	192.168.1.0/24 /	
	ID	CN=mGuard, C=de, L=Berlin, ST=Germany, O=Innominate, OU=Support, E=support@innominate.com	@ns5gt.netscreen.com	STATE_MAIN_I4 (ISAKMP SA established)
			STATE_QUICK_I2 (sent QI2, IPsec SA established)	

An "Update" button is located at the bottom center of the table.

Menu: *VPN -> IPsec Status*

7.1 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 X.509 certificates.
- Mismatched ISAKMP policy parameters. Compare the "ISAKMP SA (Key exchange)" settings on the mGuard (menu: VPN -> Connection) with the settings for the "Phase 1 Proposal" on the Netscreen (menu: VPNs -> Gateway, edit the gateway definition and click at <Advanced>).

7.2 IPsec couldn't be established

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

- Mismatched IPsec policy parameters. Compare the "IPsec SA (Data exchange)" settings on the mGuard (menu: VPN -> Connection) with the settings for the "Phase 2 Proposal" on the Netscreen (menu: VPNs -> AutoKey IKE, edit the definition and click at <Advanced>).
- Mismatched VPN-tunnel parameters.