

## **Innominate mGuard/mGuard PCI**

### **Interoperability Guide**

Setting up a VPN connection between  
mGuard v2.x and FortiGate-60



**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 FortiGate-60***

---

© Innominate Security Technologies AG

December 2004

“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: 5519-112

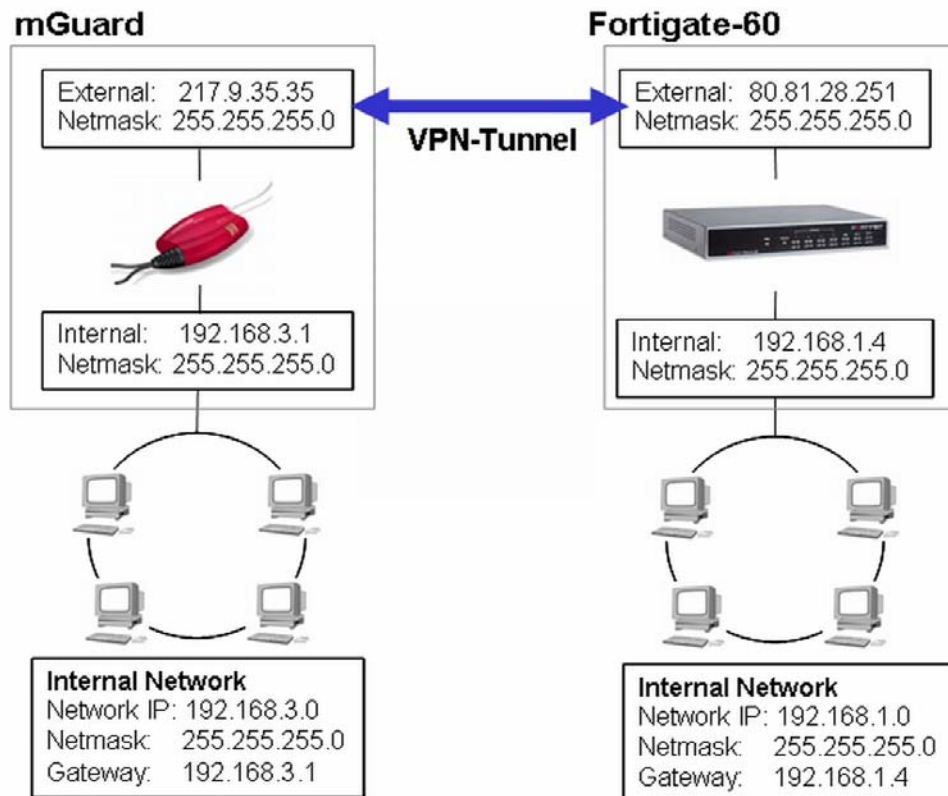
## CONTENTS

<b>1</b>	<b>Introduction</b>	<b>4</b>
1.1	<i>Used SA Encryption Parameters</i>	4
1.2	<i>Limitations</i>	4
<b>2</b>	<b>X.509 Certificates</b>	<b>5</b>
2.1	<i>Required certificates</i>	5
2.2	<i>XCA: Create and export the Root-CA</i>	5
2.3	<i>FortiGate: Import of the Root-CA</i>	6
2.4	<i>FortiGate: Create and export the local certificate</i>	6
2.5	<i>XCA: Import and sign of the local certificate</i>	6
2.6	<i>XCA: Export of the signed local certificate</i>	6
2.7	<i>FortiGate: Import of the signed local certificate</i>	6
2.8	<i>XCA: Create and export a machine certificate for the mGuard</i>	7
2.9	<i>mGuard: Import of the machine certificate</i>	7
<b>3</b>	<b>Configuration of the FortiGate-60 Appliance</b>	<b>8</b>
3.1	<i>Network Interfaces</i>	8
3.2	<i>Configuration of the VPN subnets</i>	8
3.3	<i>VPN configuration with Pre-Shared Key (PSK) and static peer IPs</i>	9
3.3.1	<i>Phase 1 Configuration</i>	9
3.3.2	<i>Phase 2 Configuration</i>	10
3.3.3	<i>Firewall Encryption Policy</i>	10
<b>4</b>	<b>VPN Configuration with X.509 Certificates (PKI) and dynamic IPs (Dialup Connections)</b>	<b>12</b>
4.1	<i>Configure the FortiGate for dialup connections (dynamic IP)</i>	12
4.1.1	<i>Phase 1 Configuration</i>	12
4.1.2	<i>Phase 2 Configuration</i>	12
4.1.3	<i>Firewall Encryption Policy</i>	13
4.2	<i>Dialup Monitor</i>	13
<b>5</b>	<b>Configuration of the mGuard</b>	<b>14</b>
<b>6</b>	<b>Troubleshooting</b>	<b>16</b>
6.1	<i>ISAKMP couldn't be established</i>	16
6.2	<i>IPSec couldn't be established</i>	16

## 1 Introduction

This document describes the procedures required to configure a VPN connection between the mGuard v.2.x and a FortiGate-60 Appliance (Firmware 2.50). 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 PKI with X.509 Certificates.

The following diagram illustrates the machines and addresses involved in the connection. Note that we are in a public environment and therefore you have to use your own public or private IPs. 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 FortiGate*

### 1.1 Used SA Encryption Parameters

The following SA encryption settings were used for this interoperability test:

	<b><i>IKE Phase I (ISAKMP SA)</i></b>	<b><i>IKE PHASE II (IPSEC- A)</i></b>
<b><i>HASH Algorithm</i></b>	SHA1	SHA1
<b><i>Encryption Algorithm</i></b>	3DES	3DES
<b><i>PFS</i></b>	DH Group5 (1680bit)	DH Group2 (1024bit)

### 1.2 Limitations

It is not possible to enter a DynDNS-entry for the remote VPN gateway on the FortiGate (Firmware 2.50). You need to specify either the IP address of the remote VPN gateway or use the Dial-up option which is equivalent to a dynamic IP. Using a DynDNS is supported with the FortiGate Firmware 2.80.

## **2 X.509 Certificates**

### **2.1 Required certificates**

You need the following certificates for the VPN connection:

- Root-CA.
  - ⇒ Import on the FortiGate as "CA Certificate".
- FortiGate-Certificate signed with the Root-CA, exported as PEM.
  - ⇒ Import on the FortiGate as "Local Certificate".
  - ⇒ Import on the mGuard as connection certificate.
- mGuard-Certificate signed with the Root-CA, exported as PKCS#12.
  - ⇒ Import on the mGuard as machine certificate.

Using certificates on the FortiGate requires the following steps:

- Import of the Root-CA (menu: *VPN -> Certificates*, tab "*CA Certificates*", button *Import*).
- Create a local certificate (menu: *VPN -> Certificates*, tab "*Local Certificates*", button *Generate*).
  - ⇒ The displayed status of the certificate is PENDING.
- Export of the local certificate (menu: *VPN -> Certificates*, tab "*Local Certificates*", button *Download*).
- The exported certificate must be signed with the Root-CA by the Certification Authorities.
- Import the signed certificate (menu: *VPN -> Certificates*, tab "*Local Certificates*", button *Import*).
  - ⇒ Now the displayed status of the certificate should be OK.

We used the tool XCA for creating the Root-CA and for signing the exported certificates with the CA. 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 Root-CA**

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.

Export the Root-CA:

- Select the Root-CA in the tab **Certificates** 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.

### **2.3 FortiGate: Import of the Root-CA**

- Select **VPN -> Certificates** from the menu and switch to the tab **CA Certificates**.
- Click at **Import** and upload the export of the Root.CA.

### **2.4 FortiGate: Create and export the local certificate**

Create a local certificate:

- Select **VPN -> Certificates** from the menu, switch to the tab **Local Certificates** and click at **Generate**.
- Enter a descriptive **Certification Name**. (e.g. fortigate).
- Set **ID Type** to **Host IP**.
- Use the entry fields from **Organization Unit** to **e-mail** for entering the identifying parameters.
- Click at **OK**.
  - ⇒ The certificate appears in the list with the status PENDING.

Export the local certificate:

- Select **VPN -> Certificates** from the menu, switch to the tab **Local Certificates**.
- Click at the **Download** icon and save the certificate to the local machine.

### **2.5 XCA: Import and sign of the local certificate**

- Switch to the tab **Certificate signing requests**, click at **Import** and select the local certificate.
- Make a right click at the imported certificate and select **Sign**.
- Click at **Next**.
- Enable **Use this certificate for signing** and select the Root-CA you've created in chapter "XCA: Create and export the Root-CA". Click at **Next**.
- Enter into the fields **Time Range** the lifetime of the local 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 signed.
  - ⇒ Switch to the tab **Certificates**. The imported and signed local certificate appears beneath the Root-CA.

### **2.6 XCA: Export of the signed local certificate**

- Switch to the tab **Certificates**.
- Expand the tree of the Root-CA, select the signed local certificate 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.

### **2.7 FortiGate: Import of the signed local certificate**

- Select **VPN -> Certificates** from the menu, switch to the tab **Local Certificates** and click at **Import**.
- Select the signed certificate and click at **OK**.

### **2.8 XCA: Create and export a machine certificate for the mGuard**

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.

Export of the mGuard certificate:

- 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.

### **2.9 mGuard: Import of the machine certificate**

- Select **VPN -> Machine Certificate** from the menu and import the machine certificate of the mGuard we have created in the previous step.

### 3 Configuration of the FortiGate-60 Appliance

#### 3.1 Network Interfaces

The internal and external (wan1) network interfaces were configured as follows:



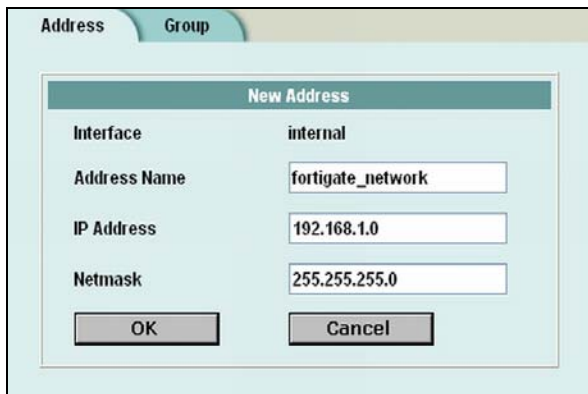
Name	IP	Netmask	Zone	Access	Status	Modify
internal	192.168.1.4	255.255.255.0		HTTPS,PING,TELNET	⬆	
wan1	80.81.28.251	255.255.255.224		HTTPS,PING	⬆	

*Menu: System -> Network -> Interfaces*

#### 3.2 Configuration of the VPN subnets

Now you need to configure the local and remote subnets for the VPN connection. The subnets are already given by the internal networks at the mGuard and at the FortiGate.

- Select **Firewall -> Addresses** from the menu.
- Select the appropriate **Interface**. If you create the VPN subnet for the mGuard, select the external interface (in our example "wan1"). If you create the VPN subnet for the FortiGate, select the internal interface (in our example "internal").
- Click at **New**.



**New Address**

Interface: internal

Address Name: fortigate\_network

IP Address: 192.168.1.0

Netmask: 255.255.255.0

OK Cancel



**New Address**

Interface: wan1

Address Name: mguard\_network

IP Address: 192.168.3.0

Netmask: 255.255.255.0

OK Cancel

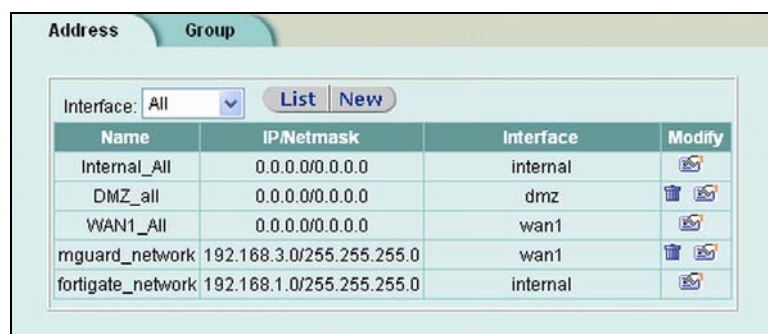
*Menu: Firewall -> Addresses -> New (FortiGate)*

*Menu: Firewall -> Addresses -> New (mGuard)*

- Enter a descriptive **Address Name**.
- Enter the **IP Address** of the VPN subnet. If you create the VPN subnet for the mGuard, enter the network IP of the internal network to which the mGuard is connected. In case of the FortiGate you'd need to enter the network IP of the internal network of the FortiGate.
- Enter the appropriate **Netmask** and click at **OK**.

## Interop Guide – VPN connection between mGuard and FortiGate-60

The VPN subnets for the mGuard and for the FortiGate are displayed in the list. In our example we called them "mguard\_network" and "fortigate\_network".



Name	IP/Netmask	Interface	Modify
Internal_All	0.0.0.0/0.0.0.0	internal	
DMZ_all	0.0.0.0/0.0.0.0	dmz	
WAN1_All	0.0.0.0/0.0.0.0	wan1	
mguard_network	192.168.3.0/255.255.255.0	wan1	
fortigate_network	192.168.1.0/255.255.255.0	internal	

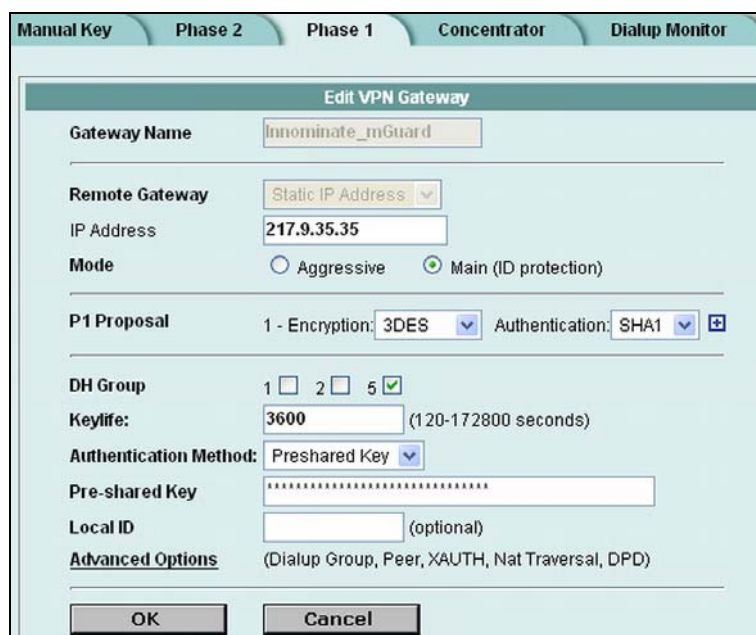
Menu: Firewall -> Addresses

### 3.3 VPN configuration with Pre-Shared Key (PSK) and static peer IPs

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

#### 3.3.1 Phase 1 Configuration

- Switch to the tab **Phase 1**.



Menu: VPN -> IPSec, Phase 1

- Enter into the field **Gateway Name** a descriptive name for the remote VPN gateway.
- Set **Remote Gateway** to **Static IP Address**.
- Enter as **IP Address** the external IP of the remote gateway.
- Set **Mode** to **Main (ID protection)**. The mGuard does not support *Aggressive Mode* due to security reason.
- **P1 Proposal**: We've chosen 3DES and SHA1 for this interoperability test.
- **DH Group**: We've chosen DH Group 5 for this interoperability test.
- **Authentication Method**: Select whether you want to use **Preshared Key** or **RSA Signature** (Certificates). In this case we need to select **Preshared Key**.
- **Pre-shared Key**: If you've selected **Preshared Key** as authentication method then you need to enter the pre-shared key into this field. Note that you have to use the same key on both VPN peers.

### 3.3.2 Phase 2 Configuration

- Switch to the tab **Phase 2**.

The screenshot shows the 'Edit VPN Tunnel' configuration window with the following settings:

- Tunnel Name:** vpn\_mguard
- Remote Gateway:** Innominate\_mGuard
- P2 Proposal:** 1- Encryption: 3DES, Authentication: SHA1
- Enable replay detection
- Enable perfect forward secrecy(PFS).
- DH Group:** 5 (selected)
- Keylife:** 28800 (Seconds), 4608000 (KBytes)
- Autokey Keep Alive:**  Enable
- Concentrator:** None
- Quick Mode Identities:**  Use selectors from policy,  Use wildcard selectors

Menu: VPN -> IPsec, Phase 2

- Enter a descriptive **Tunnel Name**.
- Select as **Remote Gateway** the gateway name you've created in the previous step (refer to "Phase 1 Configuration").
- P2 Proposal:** We've chosen 3DES, SHA1 and DH Group 5 for this interoperability test.
- Set **Quick Mode Identities** to **Use selectors from policy** for using a policy-based VPN. The configuration of the policy-based VPN is explained in the next chapter.

### 3.3.3 Firewall Encryption Policy

- Select **Firewall -> Policy** from the menu.

		Policy	
		From	
To		internal	wan1
internal			<a href="#">Edit</a>
wan1		<a href="#">Edit</a>	

Menu: Firewall -> Policy

- Click at **Edit** in the matrix field "**From Internal**" – "**To wan1**".

Now you need to specify the policy for the VPN connection.

Policy

Edit Policy internal -> wan1

Source: fortigate\_network

Destination: mguard\_network

Schedule: Always

Service: ANY

Action: ENCRYPT

VPN Tunnel: vpn\_mguard

Allow inbound  Inbound NAT

Allow outbound  Outbound NAT

Traffic Shaping

Guaranteed Bandwidth: 0 (KBytes/s)

Maximum Bandwidth: 0 (KBytes/s)

Traffic Priority: High

Anti-Virus & Web filter

Content Profile: Strict

Log Traffic

Comments: maximum 63 characters

OK Cancel

Menu: Firewall -> Policy, Edit policy

- Select as **Source** the VPN subnet of the FortiGate we have created in chapter "Configuration of the VPN subnets".
- Select as **Destination** the VPN subnet of the mGuard we have created in chapter "Configuration of the VPN subnets".
- You need to set **Action** to **ENCRYPT** for a VPN connection.
- Select as **VPN Tunnel** the VPN tunnel you have created in chapter "Phase 2 Configuration".
- Click at **OK**.

The new created policy appears in the list:

8	11	fortigate_network	mguard_network	Always	ANY	ENCRYPT	<input checked="" type="checkbox"/>				
---	----	-------------------	----------------	--------	-----	---------	-------------------------------------	--	--	--	--

Now the configuration of the VPN tunnel on the FortiGate is finished.

### 4 VPN Configuration with X.509 Certificates (PKI) and dynamic IPs (Dialup Connections)

This chapter describes how to setup a VPN connection between the mGuard and the FortiGate, using X.509 certificates as the authentication method. Using certificates allows using a dynamic IP for the remote site (mGuard). This kind of setup is called "Dialup connection" on the FortiGate.

#### 4.1 Configure the FortiGate for dialup connections (dynamic IP)

##### 4.1.1 Phase 1 Configuration

- Select **VPN** → **IPSec** from the menu.
- Switch to the tab **Phase 1**.

The screenshot shows the 'Edit VPN Gateway' configuration window in the FortiGate GUI, with the 'Phase 1' tab selected. The configuration is as follows:

- Gateway Name:** mguard\_cert
- Remote Gateway:** Dialup User
- Mode:**  Aggressive,  Main (ID protection)
- P1 Proposal:** 1 - Encryption: 3DES, Authentication: SHA1
- DH Group:** 1  2  5
- Keylife:** 3600 (120-172800 seconds)
- Authentication Method:** RSA Signature
- Certificate Name:** fortigate
- Local ID:** (empty field)
- Advanced Options:** (Dialup Group, Peer, XAUTH, Nat Traversal, DPD)

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

Menu: VPN -> IPSec, tab Phase 1

- Enter into the field **Gateway Name** a descriptive name for the remote VPN gateway.
- Set **Remote Gateway** to **Dialup User**.
- Set **Mode** to **Main (ID protection)**. The mGuard does not support *Aggressive Mode* due to security reason.
- **P1 Proposal:** We've chosen 3DES and SHA1 for this interoperability test.
- **DH Group:** We've chosen DH Group 5 for this interoperability test.
- **Authentication Method:** Select whether you want to use **Preshared Key** or **RSA Signature** (Certificates). In this case we need to select **RSA Signature**.
- **Certificate Name:** Select the local certificate.

##### 4.1.2 Phase 2 Configuration

The required entries for the phase 2 configuration are the same as already described in chapter "Phase 2 Configuration".

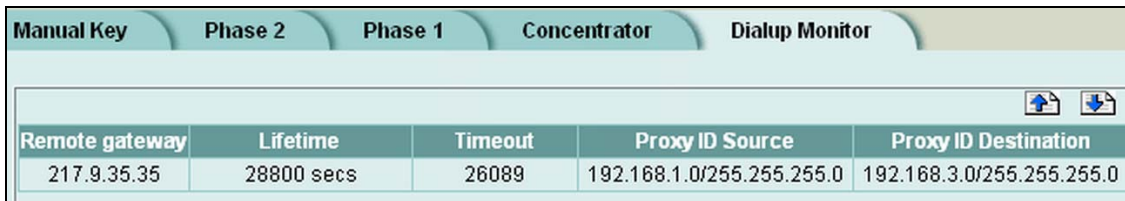
### **4.1.3 Firewall Encryption Policy**

The required entries for the configuration of the firewall encryption policy are the same as already described in chapter "Firewall Encryption Policy".

**Note:** If the VPN subnet of the remote system is unknown, as it is the case for Dial-up connections, then you may specify **WAN1\_all** as **Destination**. This is equivalent to the network IP 0.0.0.0/0.0.0.0.

### **4.2 Dialup Monitor**

The Dialup Monitor displays all successful established connections.



Remote gateway	Lifetime	Timeout	Proxy ID Source	Proxy ID Destination
217.9.35.35	28800 secs	26089	192.168.1.0/255.255.255.0	192.168.3.0/255.255.255.0

*Menu: VPN -> IPSec, tab "Dialup Monitor"*

## 5 Configuration of the mGuard

- Select **VPN -> Connections** from the menu and click at **New**.
- Enter a descriptive name for the connection and click at **Edit**.
- The following screen appears:

The screenshot shows the configuration page for a VPN connection. The title is "VPN > Connections > Connection vpn to fortigate". The form includes the following fields and sections:

- A descriptive name for the connection:** vpn to fortigate
- Enabled:** Yes
- Address of the remote site's VPN gateway (either an IP address, a hostname, or %any):** 80.81.28.251
- Connection type:** Tunnel (Net <-> Net)
- Connection startup:** Start connection to... ..remote VPN gateway.
- ISAKMP SA (Key Exchange):**
  - Authentication method:** Pre-Shared Secret (with a Configure button)
  - Encryption Algorithm:** 3DES-168
  - Hash Algorithm:** All algorithms
- IPsec SA (Data Exchange):**
  - Encryption Algorithm:** 3DES-168
  - Hash Algorithm:** All algorithms
- Perfect Forward Secrecy (PFS) (The remote site must have the same entry. Activation is recommended due to security reasons.):** Yes
- Tunnel Settings:**
  - Local network address:** 192.168.3.0
  - The appropriate local netmask:** 255.255.255.0
  - The virtual IP which will be used by the client in Stealth mode:** 192.168.3.1
  - Remote network address:** 192.168.1.0
  - The appropriate remote netmask:** 255.255.255.0
- Firewall Incoming (untrusted port):**

Protocol	From IP	From Port	To IP	To Port	Action	Log
All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	No

Log entries for unknown connection attempts: No
- Firewall Outgoing (trusted port):**

Protocol	From IP	From Port	To IP	To Port	Action	Log
All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	No

Log entries for unknown connection attempts: No

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

*Menu: VPN -> Connections*

- **Address of the remote site's VPN gateway:** Enter the external IP-address of the FortiGate (in our example 80.81.28.251).
- **Connection type:** We want to establish a VPN-tunnel between the mGuard and the FortiGate. Therefore we need to specify **Tunnel (Net <-> Net)** as connection type.
- **Connection Startup:** The mGuard should initiate the connection. Therefore we select **Start connection to ...**
- **Authentication method:**
  - Pre-shared Keys: If you use PSK then select **Pre-shared Secret**. Click at **Configure** and enter the shared secret you defined at the FortiGate.
  - X.509 Certificate: If you use PKI select **X.509 Certificate**. Click at **Configure** and import the local certificate of the FortiGate.
- **Encryption Algorithm and Hash Algorithm (ISAKMP SA and IPsec SA):** These settings must correspond to the settings on the FortiGate.
- **Perfect Forward Secrecy (PFS):** This value must correspond to the settings on the FortiGate. The mGuard chooses the correct DH Group automatically.
- **Tunnel settings / local network and netmask:** These parameters are used for specifying the subnet of the VPN-tunnel at the mGuard (in our example 192.168.3.0/255.255.255.0). Those values must correspond to the internal network of the mGuard.

## ***Interop Guide – VPN connection between mGuard and FortiGate-60***

---

- **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 are used for specifying the subnet of the VPN-tunnel on the FortiGate (in our example 192.168.1.0/255.255.255.0). Those values must correspond to the internal network of the FortiGate.

Click at **OK** after entering the required data. If the mGuard is in *Router-Mode* then it will try to establish the VPN connection immediately.

## 6 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**).

VPN > IPsec Status						
Connection Name	Connection			ISAKMP State	IPsec State	
Gateway	Gateway	10.0.0.133		10.0.0.199	STATE_MAIN_R3 (sent MR3, ISAKMP SA established)	STATE_QUICK_R2 (IPsec SA established)
	Traffic	172.16.1.0/24 /		192.168.0.0/24 /		
	ID	C=de, ST=de, L=Berlin, O=Innominate, OU=Technical Support, CN=mGuard, E=support@innominate.com		C=de, ST=de, L=Berlin, O=Innominate, OU=Technical Support, CN=Astero, E=support@innominate.com		
Update						

*Menu: VPN -> IPsec Status*

On the FortiGate select **VPN -> IPsec, Phase 2** from the menu to get the info about the status of the VPN connection. It is either UP or DOWN.

Manual Key	Phase 2	Phase 1	Concentrator	Dialup Monitor	
Tunnel Name	Remote Gateway	Lifetime(sec/kb)	Status	Timeout	Modify
vpn_mguard	217.9.35.35	28800/NA	Up	28501	

*Menu: VPN -> IPsec, Phase 2*

### 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/certificates.
- Mismatched IKE SA policy parameters. Compare the "ISAKMP SA (Data exchange)" settings on the mGuard (menu: VPN -> Connection) with the settings of the specified "P1 Proposal" on the FortiGate (menu: VPN -> IPsec, Phase 1, select the gateway and click "edit")

### 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 IPSec policy parameters. Compare the "IPSec SA (Data exchange)" settings on the mGuard (menu: VPN -> Connection) with the settings of the specified "P2 Proposal" on the FortiGate (menu: VPN -> IPsec, Phase 2, select the VPN and click "edit")
- Mismatched tunnel (subnet) parameters. Compare the following parameters:
  - mGuard tunnel settings: local network address = FortiGate -> Policy for VPN: Dest. Network
  - mGuard tunnel settings: remote network address = FortiGate -> Policy for VPN: Source Network.