



# movianVPN™

*A handheld VPN client specifically designed for mobile and wireless devices*

**Version 1.1.2**  
**Check Point VPN-1**

## **Server Configuration Guide**



Certicom(R), Certicom logos, movian (tm), movianVPN (tm) are trademarks of Certicom Corp. All other trademarks used are the property of their respective owners.

The *Server Configuration Guide* describes how to configure various VPN servers for use with **movianVPN**.

Other documentation provided with **movianVPN** includes the *movianVPN User's Guide*. The *User's Guide* describes how to install, configure, and use **movianVPN**.

### General Inquiry

The **movianVPN** general inquiry may be contacted at 510-780-5100. For further product information visit our website at [www.moviansecurity.com](http://www.moviansecurity.com).

ALL INFORMATION CONTAINED IN THIS DOCUMENT ARE PROVIDED "AS IS" WITHOUT WARRANTY OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. CERTICOM DISCLAIMS ANY LEGAL LIABILITY OR RESPONSIBILITY FOR THE ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION, PROCEDURE, METHOD, APPARATUS, PRODUCT, OR PROCESS POSTED HERE. NEITHER CERTICOM, ITS EMPLOYEES, NOR ITS ASSOCIATES ASSUMES ANY RESPONSIBILITY FOR LOSS OR DAMAGES RESULTING FROM THE USE OF INFORMATION CONTAINED IN THE DOCUMENTATION. CERTICOM ASSUMES NO RESPONSIBILITY FOR ERRORS OR OMISSIONS IN THIS DOCUMENTATION.

WITH RESPECT TO ONLY LIMITATION OF DIRECT DAMAGES, UNLESS SPECIFICALLY STATED OTHERWISE IN A LICENSE AGREEMENT EXECUTED BETWEEN YOU AND CERTICOM, YOU AGREE THAT ANY LIABILITY ON THE PART OF CERTICOM FOR BREACH OF THE WARRANTIES CONTAINED HEREIN OR ANY OF THE OTHER PROVISIONS OF THIS AGREEMENT OR ANY OTHER BREACH GIVING RISE TO LIABILITY OR IN ANY OTHER WAY ARISING OUT OF OR RELATED TO THIS AGREEMENT FOR ANY CAUSE OF ACTION WHATSOEVER AND REGARDLESS OF THE FORM OF ACTION (INCLUDING BREACH OF CONTRACT, STRICT LIABILITY, TORT INCLUDING NEGLIGENCE OR ANY OTHER LEGAL OR EQUITABLE THEORY), SHALL BE LIMITED TO YOUR DIRECT DAMAGES IN AN AMOUNT NOT TO EXCEED ONE (\$1.00) US DOLLAR

YOU AGREE THAT IN NO EVENT WILL CERTICOM BE LIABLE FOR DAMAGES IN RESPECT OF INCIDENTAL, ORDINARY, PUNITIVE, EXEMPLARY, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES EVEN IF CERTICOM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES INCLUDING, BUT NOT LIMITED TO, BUSINESS INTERRUPTION, LOST BUSINESS REVENUE, LOST PROFITS, FAILURE TO REALIZE EXPECTED SAVINGS, ECONOMIC LOSS, LOSS OF DATA, LOSS OF BUSINESS OPPORTUNITY OR ANY CLAIM AGAINST YOU BY ANY OTHER PARTY. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE LIMITATIONS ON IMPLIED WARRANTIES OR THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

BY USING THIS DOCUMENTATION, YOU AGREE TO BE BOUND BY THE TERMS AS STATED HEREIN. IF YOU DO NOT ACCEPT THESE TERMS AND CONDITIONS, YOU MUST DELETE THIS DOCUMENT AND NOT MAKE ANY USE OF IT.

ADDITIONAL TERMS AND CONDITIONS MAY APPLY TO YOU AS PER THE SOFTWARE LICENSE AGREEMENT THAT YOU MAY HAVE EXECUTED WITH CERTICOM.

### Copyright Notice

© Certicom Corp. 2000, 2001. All rights reserved. This documentation contains Certicom's proprietary information and any use and distribution are limited to authorized licensees of Certicom. Any unauthorized use, reproduction, and distribution of this documentation is strictly prohibited by law."

"Certicom(R), Certicom logos, movian (tm), movianVPN (tm) are trademarks of Certicom Corp. The movianVPN is covered by one or more of the following U.S. Patents: 6,078,667 , 6,049,815, 5,999,626, 5,955,717, 5,933,504, 5,896,455, 5,889,865, 5,787,028, 5,761,305, 5,600,725, 4,745,568, and corresponding foreign patents. Additional patents pending.



## Table of Contents

### Introduction

|                                       |   |
|---------------------------------------|---|
| Overview of the movianVPN             | 1 |
| <i>How the Client Works</i>           | 1 |
| <i>Features and Benefits</i>          | 1 |
| Overview of the Configuration Process | 3 |

### Configuring the Check Point VPN-1 Server

|                                     |    |
|-------------------------------------|----|
| Introduction                        | 5  |
| <i>The Configuration Process</i>    | 6  |
| Adding Groups and Users             | 7  |
| <i>Adding Groups</i>                | 7  |
| <i>Adding Templates</i>             | 7  |
| <i>Adding Users</i>                 | 8  |
| Configuring VPN Client Access Rules | 9  |
| Configuring the Firewall Policy     | 10 |
| Managing Network Objects            | 11 |
| Enabling IP Forwarding              | 13 |



---

# 1 Introduction

*This chapter is an overview of the process of configuring a Virtual Private Network (VPN) for use with the **movianVPN**. The following sections are included:*

- Overview of **movianVPN**
- Overview of the Configuration Process

---

## Overview of the **movianVPN**

The Certicom **Handheld VPN Client** is a fully configurable GUI-based application you can use to securely connect to a VPN over a wired or wireless connection. With **movianVPN**, you can access and exchange e-mail, as well as acquire Sales Force Automation and Enterprise Resource Planning data with little risk of the information being intercepted or of unauthorized users penetrating your system.

### How the Client Works

Using **movianVPN**, you can connect to a VPN via a wireless network or with a conventional telephone line that dials into an Internet Service Provider. When you connect to the VPN, the VPN gateway encrypts the information using IPSec and sends it through the tunnel to **movianVPN**. **movianVPN** then decrypts the message. Note that this is a two-way process — any information you send using **movianVPN** is encrypted before it reaches the tunnel, and is decrypted by the VPN gateway.

Once connected, you can use the software on your Palm™ organizer or Win CE device to access the information you need. You can send and receive messages with an e-mail client, or you can download the latest corporate information with a Web browser.

### Features and Benefits

**movianVPN** offers the following features and benefits:

- An intuitive graphical user interface which allows you to easily configure the Client and connect to a VPN.
- Uses a 163-bit Elliptic Curve Cryptosystem (ECC) algorithm, as well as 768-bit and 1024-bit Diffie-Hellman algorithms. These algorithms can quickly generate keys and secure the data sent through IP tunnels. ECC provides a high level of

security with less code and a smaller encryption key than other well-known encryption methods. It also ensures fast connections to gateways supporting ECC. Diffie-Hellman also provides strong security, and ensures interoperability.

- Use of an Internet Key Exchange (IKE)-based IPsec protocol.
- Runs on both major hand-held platforms: the Palm™ organizer and the PocketPC™ (Win CE).



## Overview of the Configuration Process

Before remote users can communicate with a VPN using the **movianVPN**, you must modify the configuration of the target VPN. Specifically:

- Configuring the internal and external interfaces with the appropriate IP addresses.
- Configuring the public interface and default gateway.
- Creating and applying client policies and filters.
- Setting up a pool of IP addresses.
- Enabling IPSec and IKE for a user group or set of user groups.

---

**Note:** The parameters you must configure will differ depending on the VPN server you are using, and on your needs.

---



---

# 2 Configuring the Check Point VPN-1 Server

*This chapter explains how to configure the Check Point VPN-1 server for use with the movianVPN. The following sections are included:*

- Introduction
- Adding Groups and Users
- Configuring VPN Client Access Rules
- Configuring the Firewall Policy
- Managing Network Objects
- Enabling IP Forwarding

---

## Introduction

Check Point VPN-1 does not interoperate with **movianVPN** out of the box. You must configure the interfaces and security settings on the VPN before users can make connections with **movianVPN**.

Before you configure Check Point VPN-1 for use with **movianVPN**:

- Install the Check Point software on the appropriate computer.
- Set up the default access rules. This includes specifying a name for the default network object, configuring an IP address and network mask, and enabling automatic network address translation (NAT).
- Know the IP address and subnet mask of the VPN.
- Have a list of the names of your users.

---

**Note:** There are versions of Check Point VPN-1 for Windows NT and UNIX. This chapter covers the configuration of Windows NT server. For information on configuring the UNIX version, refer to the appropriate Check Point documentation.

---

## The Configuration Process

Configuring Check Point VPN-1 to work with **movianVPN** involves:

- Adding Groups and Users
- Configuring VPN Client Access Rules
- Configuring the Firewall Policy
- Managing Network Objects
- Enabling IP Forwarding

---

**Note:** This chapter only covers the configuration tasks specific to interoperability with the **movianVPN**. For detailed configuration information, refer to the *appropriate Check Point documentation*.

---



## Adding Groups and Users

For users to access the VPN, you must populate the system with groups and users. Adding groups and users involves:

- Adding Groups
- Adding Templates
- Adding Users

### Adding Groups

A group is a set of users who have common privileges to access a VPN. You control access to various parts of a network by assigning access privileges to each user group. You should create groups according to the tasks the users in that group perform.

To add a group:

1. Log into Check Point VPN-1 using the Policy Editor. For more information on logging in, see the documentation from Check Point.
2. Select **Users** from the **Manage** menu. The Users dialog appears.
3. Click **New**, then select **Group** from the popup list. The Groups dialog appears.
4. Type a name for the group in the **Name** field.
5. If necessary, type a description for the group in the **Comment** field.
6. Click **OK**.

### Adding Templates

A template is a user profile containing parameters that are common to all members of a group. You can use a template to quickly add users to the VPN. Any users derived from the template will inherit the template's settings.

To add a template:

1. Select **Users** from the **Manage** menu. The Users dialog appears.
2. Click **New**, then select **Template** from the popup list. The User Definition Template dialog appears.
3. Type a name for the template in the **Template** field.
4. If necessary, type a description of the template in the **Comment** field.
5. Click the **Groups** tab.
6. In the **Available Groups** list, click the name of the group you created earlier, then click **Add>**. The group is added to the template.
7. Click the **Location** tab.
8. In the Network Objects list, click **Any** then click **Add>** to add the object to the list of sources. This setting allows users to access the VPN from any location.

9. Click **Any** then click **Add>** to add the object to the list of destinations. This setting allows packets to travel to any destination IP address.
10. Click the **Time** tab, then do the following:
  - In the **Day of week** area, click the days of the week on which users can access the VPN.
  - In the **Time of day** area, type the hours during which users can access the VPN in the **From** and **To** fields. These times must be in 24 hour format. For example, **00:00** and **23:59**.
11. Click the **Encryption** tab, then do the following:
  - In the **Client Encryption Methods** area, click the **IKE** checkbox then click **Edit**. The IKE Properties dialog appears.
  - Click the **Password** box to enable password prompting.
12. Click the **Encryption** tab, then do the following:
  - Click the **Encryption + Data Integrity (ESP)** radio button.
  - Click the **MD5** radio button.
  - Select **3DES** from the **Encryption Algorithm** dropdown list.
13. Click **OK** to close the dialog. You are returned to the User Definition Template dialog.
14. Click **OK** to close the User Definition Template dialog.
15. Click **Install** to save the changes. The Install User Database dialog appears.
16. Select the object in which you want to install the database from the list.
17. Click **OK** to return to the Users dialog.

## Adding Users

To add a user:

1. On the Users dialog, click **New** then select the name of the group you created earlier from the dropdown list. The User Properties dialog appears.
2. Type the name of the new user in the **Name** field.
3. Click the **Encryption** tab.
4. If it is not already selected, click the **IKE** checkbox.
5. Click **Edit**. The IKE Properties dialog appears.
6. Type a password for the user in the **Password** field, then click **OK** to close the dialog.
7. Click **OK** to close the User Properties dialog.
8. Click **Install** to save the changes. The Install User Database dialog appears.
9. Select the object in which you want to install the database from the list.
10. Click **OK** to return to the Users dialog.
11. Repeat steps 1 to 10 for each new user you want to add.



## Configuring VPN Client Access Rules

The client access rules determine what data can move in and out of the VPN, as well as when and from where remote users can access the system

To configure VPN client access rules:

1. Select **Add Rule** from the **Edit** menu. From the popup list that appears, select one of the following:
  - **Bottom**—add the rule to the bottom of the list.
  - **Top**—add the rule at the top of the list.
  - **After**—add the new rule after the current rule.
  - **Before**—add the new rule before the current rule.
2. The new rule is added to the list. Right click the **Source** column of the new rule, then select **Add** from the popup list.
3. Select the name of the group you created earlier from the list, then click **OK**.
4. Leave the entries in the **Destination** and **Service** columns as they are. These settings, respectively, allow the VPN to connect to any IP address and allow all packets to pass through the firewall.

---

**Note:** If you need to restrict access, choose another option from the **Service** column by right clicking.

---

5. Right click **Action** and select **Client Encrypt**. This forces the firewall to accept only encrypted packets from **movianVPN**.
6. If you want to log debugging information, right click the **Track** column and select one of the following options:
  - **Long**—logs detailed debugging information.
  - **Short**—logs brief debugging information.
7. Select **Save** from the **File** menu to save the changes.

## Configuring the Firewall Policy

The firewall policy controls how the VPN's firewall deals with incoming and outgoing traffic.

To configure the firewall policy:

1. Select **Policy** from the **Properties** menu. The Properties Setup dialog appears.
2. Click the **Desktop Security** tab.
3. Clear the **Respond to Unauthenticated Topology Requests (IKE and FWZ)** checkbox to prevent the firewall module from responding to topology requests from SecureRemote clients.
4. Click **OK** to close the Properties Setup dialog.
5. Select **Install** from the **Policy** menu.
6. Select the firewall object from the list, then click **OK** to save the changes.



## Managing Network Objects

In Check Point VPN-1, a network object can include the following:

- Workstations
- Gateways
- Routers
- Networks
- Switches
- Firewalls
- Domains

Managing network objects involves adding them to a user group, then configuring the objects.

To manage network objects:

1. Select **Network Object** from the **Manage** menu. The Network Objects dialog appears.
2. Select the group you created earlier, then click **Edit**. The Group Properties dialog appears.
3. Select the firewall and localnet objects (created when you installed the Check Point software and performed preliminary configuration) from the list. Click **Add**.
4. Click **OK** to close the Group Properties dialog.
5. On the Network Objects dialog, click the firewall object then click **Edit**. The Workstation Properties dialog appears.
6. Click the **Interfaces** tab.
7. If necessary, add a new interface by clicking **Add**. The Interface Properties dialog appears. You can edit the following fields:
  - **Name**—the name of the new interface.
  - **Net Address**—the IP address of the VPN.
  - **Net Mask**—the subnet mask of the VPN.
8. Click the **Security** tab.
9. Click the **This net** radio button. This setting prevents IP spoofing.
10. Click **OK** to close the Interface Properties dialog.
11. Click the **VPN** tab.
12. Click the **Other** radio button, then select the group you defined earlier from the list.
13. Click the **IKE** checkbox in the list of defined encryption schemes.
14. Click **Edit**. The IKE Properties dialog appears.

15. Click the **Pre-Shared Secret** checkbox, then click **OK** to close the IKE Properties dialog.
16. Click **OK** to save the network object. You are returned to the Network Object dialog.
17. Click **Close** to close the Network Object dialog.
18. Select **Install** from the **Policy** menu.
19. Click **Install** to save the changes. The Install User Database dialog appears.
20. Select the object in which you want to install the database from the list, then click **OK**.



## Enabling IP Forwarding

IP forwarding (also call IP routing) allows the VPN to route packets to other IP addresses. In order for the firewall to work, you must first enable IP forwarding.

To enable IP forwarding:

1. Select **Settings>Control Panel** from the Windows Start menu. The Control Panel appears.
2. Double click **Network**. The Network dialog appears.
3. Click the **Protocols** tab.
4. Select **TCP/IP** from the list of network protocols.
5. Click **Properties**. The TCP/IP Properties dialog appears.
6. Click the **Routing** tab.
7. Click the **Enable IP Forwarding** checkbox.
8. Click **OK**, then click **Close** on the TCP/IP Properties dialog.
9. Reboot the system for the changes to take effect.

