

**Entrust® Products and Check Point™ VPN-1® NG**

# **Integration Guide**

**Document Issue: 1.2**

**Date: May 2003**



**The information is subject to change as Entrust reserves the right to, without notice, make changes to its products as progress in engineering or manufacturing methods or circumstances may warrant.**

Confidential.

Contains proprietary information of Entrust, Inc.

Copyright© 2003 Entrust and its licensors. All rights reserved.

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. All other Entrust product names and service names are trademarks of Entrust. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS, WARRANTIES AND/OR CONDITIONS OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A SPECIFIC PURPOSE.

# Contents

**Chapter 1**  
**Introduction . . . . . 7**

- Revision History . . . . . 8
- Audience . . . . . 8
- Purpose . . . . . 8
- General Information on Naming Conventions . . . . . 8
- Architecture . . . . . 10

**Chapter 2**  
**Preparation . . . . . 13**

- System and Software Requirements . . . . . 14
- User Administration Skill . . . . . 16
- Installation Environment . . . . . 16
- Modifying the Entrust.ini file . . . . . 17
- Windows 2000 Client Setup . . . . . 19

**Chapter 3**  
**Configuring the VPN-1 NG FP-1 for use with Entrust Products . . . . . 21**

- Introduction . . . . . 22
- Modifying Entrust-CA Service on Firewall . . . . . 23
- Creating Certificate Authority Server Object . . . . . 25
- Creating CA/Directory Object . . . . . 30
- Creating Internal Network Object . . . . . 32
- Modifying Firewall Object . . . . . 33
- What to do if You Need to Re-enroll the Firewall Certificate . . . . . 48
- Creating the LDAP Account Unit on the Firewall . . . . . 51

Creating LDAP Group . . . . .	51
Creating LDAP Template . . . . .	53
Creating LDAP Account Unit . . . . .	56
Creating the External LDAP Group . . . . .	60
Creating Rule Base . . . . .	61
Installing the Security Policy on the Firewall . . . . .	62

**Chapter 4**  
**Configuring the VPN-1® SecuRemote NG Client . . . . . 63**

Creating the VPN-1 SecuRemote Client User in Entrust Authority™ Security Manager Administration . . . . .	64
Creating an IPSec Tunnel using Pre-Shared Secrets (Optional) . . . . .	69
Self-Extracting or Configurable Installation of VPN-1 SecuRemote . . . . .	76
Selecting the Entrust.ini . . . . .	77
Selecting Entrust Entelligence™ Desktop Manager in VPN-1 SecuRemote . . . . .	78
Creating the Entrust digital ID for the VPN-1 SecuRemote Client . . . . .	78
Downloading the Firewall Topology . . . . .	82
Switching to Client Connect Mode from Transparent Mode . . . . .	84
Authenticating to Create the IPSec Tunnel using Transparent Mode . . . . .	88
Key Updates . . . . .	89

**Chapter 5**  
**Defining Access Controls based on User DN . . . . . 91**

Overview of Method Used . . . . .	92
Sample Setup . . . . .	92

**Chapter 6**  
**Working with an Entrust Subordinate CA . . . . . 97**

How to setup Entrust Subordinate CA with VPN-1 NG FP-1 . . . . .	98
--	----

**Chapter 7**

<b>How do you know if it is working? . . . . .</b>	<b>99</b>
How do you know if it is working? . . . . .	100
<b>Chapter 8</b>	
<b>Troubleshooting . . . . .</b>	<b>101</b>
Error Login to Entrust CMS . . . . .	102
Failed to register key (-3236) ASN.1 encoding/decoding failure . . . . .	103
Failed to register key: Internal Error: (-1666) . . . . .	104
Users Authenticate Successfully but cannot Access the Internal Network . . . . .	105
Error: Communication with gateway (Gateway Name) at site xxx.xxx.xxx.xxx failed . . . . .	105
Error: Site xxx.xxx.xxx.xxx says that it is not a Certificate Authority. . . . .	106
Negotiation with gateway at site xxx.xxx.xxx.xxx has failed. Certificate is revoked. . . . .	106
Negotiations with gateway at site xxx.xxx.xxx.xxx has failed. User (DN) unknown. . . . .	107
Could not validate the Certificate used by gateway . . . . .	108
(-11530) Client was expecting a DN change . . . . .	109
Cannot Complete Certificate Chain . . . . .	110
The Digital Certificate could not be Verified . . . . .	110
<b>Chapter 9</b>	
<b>Known Issues . . . . .</b>	<b>113</b>
Known Issues . . . . .	114
Microsoft Active Directory Support . . . . .	115
<b>Chapter 10</b>	
<b>Appendix A - Additional Reference Material . . . . .</b>	<b>117</b>
Entrust Documentation . . . . .	118
Check Point Documentation . . . . .	120
<b>Chapter 11</b>	
<b>Appendix B - Sample Entrust.ini files . . . . .</b>	<b>121</b>

Entrust.ini File . . . . . 122

# Chapter 1

## Introduction

This guide is intended as a tool to assist customers deploying the Check Point VPN-1® NG FP-1 with Entrust products.

# Revision History

This integration guide has gone through revisions and it is important to know and understand the different revisions that have occurred. Below is a list of the revisions and the changes that have been made to the guide.

Revision	Date	Description
1.1	June 2002	Original release.
1.2	May 20, 2003	The information about anonymous the anonymous read access in Active Directory clarified. Also revision history added.

## Audience

The intended target audience is technically oriented and tasked with getting the products up and running. The document assumes the reader has access to relevant documentation from both Entrust and Check Point and is able to perform a basic installation of both products.

## Purpose

This document will focus on the integration points between Entrust and Check Point products. The primary goal is to establish a secure VPN connection between a Check Point VPN-1 SecuRemote Client and the VPN-1 NG FP-1 using digital certificates for authentication and access control. The resulting configuration is suitable for developing familiarity with the operation of Entrust software with the VPN-1 NG FP-1. It is also intended to serve as a baseline from which a configuration suited to the customer's environment can be tailored for production usage.

# General Information on Naming Conventions

In conjunction with the name change from Entrust Technologies Inc. to Entrust, Inc. the names of Entrust software has changed. Throughout this guide reference will be made to the new naming conventions. However when using older material you may see references to the older naming conventions. This section will act as a partial guide to assist you in this.

## Sample Naming Convention - Entrust

Old Product Name	New Product	New Product Name
	Name First Occurence	Subsequent Occurences
Entrust/Authority	Entrust Authority™ Security Manager	Security Manager
Entrust/RA	Entrust Authority™ Security Manager Administration	Security Manager Administration
Entrust/Master Control	Entrust Authority™ Security Manager Control	Security Manager Control
Entrust/VPN Connector	Entrust Authority™ Enrollment Server for VPN	Enrollment Server for VPN
Entrust/AutoRA	Entrust Authority™ Self-Administration Server	Self-Administration Server
Entrust/Entelligence	Entrust Entelligence™ Desktop Manager	Desktop Manager
Entrust/Desktop Designer	Entrust Entelligence™ Installation Designer	Installation Designer

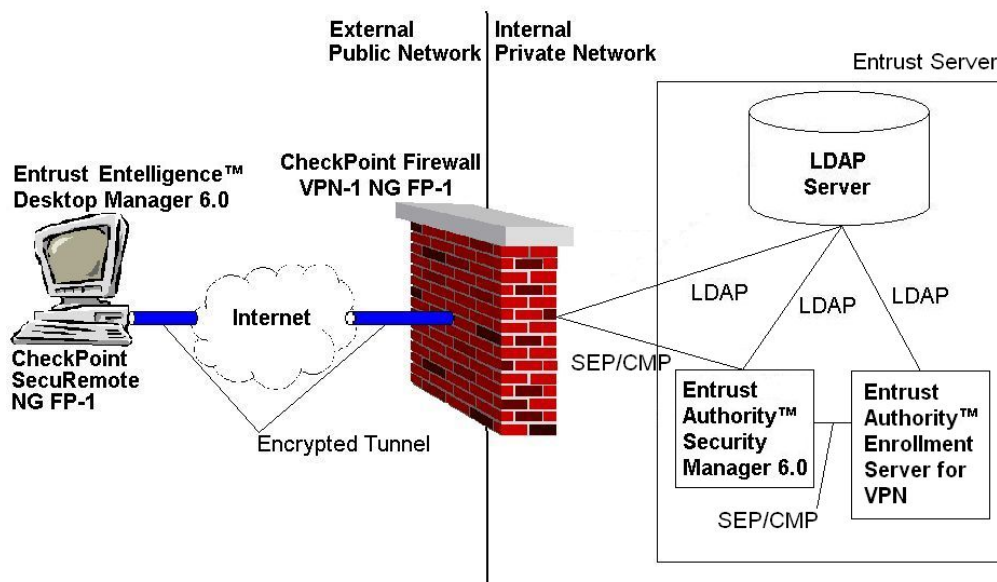
## Sample Naming Convention - Check Point

First Occurence	Subsequent Occurences
-----------------	-----------------------

# Architecture

The architecture is straightforward, as shown in the following diagram:

## Topology



The elements of the architecture are:

- Check Point VPN-1 NG FP-1

The Firewall Gateway PC. As part of this exercise the reader will configure network objects for Entrust, and install a digital certificate.

- Check Point VPN-1 SecuRemote NG FP-1 Client and Entrust Entelligence™ Desktop Manager 6.0

The VPN client PC. As part of this exercise the reader will create and install Check Point and Entrust® software packages. The reader will also obtain a digital certificate for the client.

- **Entrust Server**

This PC is used to issue and manage digital certificates for both the VPN-1 firewall and the VPN-1 client. Software on this machine includes: Entrust Authority™ Security Manager 6.0, Microsoft Active directory as a stand alone LDAP repository, and an Informix database.

For production systems the Entrust Authority™ Enrollment Server for VPN should not be installed on the same machine as the Security Manager. This document describes a system with both products installed on the same machine. For lab environments this configuration is adequate.



# Chapter 2

## Preparation

The following sections describe pre-requisites and preparations for installation and configuration.

# System and Software Requirements

Installing the system components requires certain minimum hardware and software configuration steps on dedicated machines.

Consistent time and dates across all devices and PCs is essential. Certificate authorization and revocation information validity is partially based on system time and date. Different time zones between clients and server are not affected as long as those time zones are configured correctly.

## Entrust server

For simplicity and cost effectiveness a single machine running Windows 2000 Server will host all infrastructure software, including Security Manager, Enrollment Server for VPN, Microsoft Active Directory, and Informix database.

### System requirements for this machine are:

- 128 Mbytes of RAM
- Pentium 300 or better
- One 2X or faster CD-ROM drive
- TCP/IP stack installed
- 10 Gbyte Hard Drive
- 2 Hard Drive partitions formatted as NTFS

### Software requirements for this machine are:

- Windows 2000 Server and Service Pack 1
- Security Manager 6.0
- Microsoft Active Directory

Refer to the release notes for the Security Manager 6.0 that reference useful information on various documents that can be used in assisting you in installing and configuring the Security Manager.

**The following information documents system specifications used during testing. Please refer to Check Point documentation for current supported platforms and minimum system requirements.**

**The following system specifications were used for both the Management Console and VPN/Firewall-1 modules.**

- Operating System - Windows 2000 Server Service Pack 1 and Nokia 300 Appliance Hardware with IPSO 3.4.2
- Disk Space - 40 Mbytes
- Memory - 128 Mbytes

**The following system specifications were used for the VPN-1 NG FP-1 GUI (Check Point VPN-1 SecuRemote NG FP-1) client:**

- Operating System - Windows 2000 Professional and Service Pack 1
- Disk space - 40 Mbytes
- Memory - 128 Mbytes
- Check Point VPN-1 SecuRemote NG FP-1 (build 51057) client
- Desktop Manager 6.0

#### **Enrollment Server for VPN machine**

**The following system specifications were used for the Enrollment Server for VPN.**

- Operating System - Windows 2000 Server and Service Pack 1
- Disk Space - 10 Mbytes
- Memory - 128 Mbytes
- Enrollment Server for VPN 6.0

[Note: Please refer to the various release notes or install guides for the software being installed for the latest on OS and system requirements. The URL to find the release notes of Check Point NG FP-1 is [http://www.CheckPoint.com/support/technical/documents/docs\\_ngfp1.html](http://www.CheckPoint.com/support/technical/documents/docs_ngfp1.html) (Remember username and password will be required)]

Information on Check Point NG FP-1 for Nokia Appliance Hardware can be found at [http://www.CheckPoint.com/support/technical/documents/docs\\_nokia.html](http://www.CheckPoint.com/support/technical/documents/docs_nokia.html) (Username and password required).

## User Administration Skill

It is assumed that the installer and administrator is an experienced system administrator or network administrator with appropriate education and training, who knows how to install, configure, and manage basic internetworking systems.

Familiarity with the basic concepts of PKI is a requirement for this configuration. Step by step instructions include basic configuration of the VPN-1 NG FP-1 but it would be beneficial to have read and understood the documentation provided with the Check Point Software. Also a familiarity with the software would be an asset.

A familiarity with Windows 2000 system configuration and management is a must.

## Installation Environment

For simplicity of this exercise the three machines used are directly connected. While this does not reflect a normally routed Internet and/or enterprise network, it is sufficient to demonstrate the concepts and operations involved when using digital certificates.

**A Security Manager infrastructure consists of 3 major support systems:**

An LDAP Directory is used by Security Manager to store public certificate information for client and server public access. Encryption certificates, certificate revocation lists and policy certificates are all publicly hosted through this support system.

While this guide documents the use of Microsoft Active Directory, Entrust® Software support other Directory products. Current Entrust-Ready information is found on the Entrust Partner Solutions web site. (<http://www.entrust.com/partners/>)

### **Informix database**

A relational database is used by Security Manager to store information about Entrust users and the infrastructure. This data is encrypted.

## Security Manager and Entrust Authority™ Security Manager Administration

Security Manager is the Certification Authority of the system. Its main functions are to create, manage and enforce user certificates and policies.

Security Manager Administration is the graphical interface to the Security Manager system. It is used by Security Officers and Administrators to create, manage and configure the Security Manager.

Additional support systems include:

### Desktop Manager

Desktop Manager works with Security Manager to automate key management for clients transparently. Client keys and certificates are stored in an Entrust key store called an Entrust digital ID. Desktop Manager can encrypt, decrypt, sign and verify secure data with the keys and certificates stored in the client Entrust digital ID.

### Enrollment Server for VPN

Enrollment Server for VPN is an extension of the Security Manager. It lets you issue certificates to virtual private network (VPN) devices such as routers, gateways and firewalls that use PKCS#10 or Simple Certificate Enrollment Protocol (SCEP).

Note: Entrust does not recommend or support the use of Check Point's 'Entrust/PKI' enrollment feature within Check Point VPN-1 NG. This feature is built using an Entrust Toolkit which is no longer supported. The use of Entrust Authority Enrollment Server for VPN 6.0 with Check Point's 'OPSEC PKI' feature is the recommended and supported enrollment method for Check Point VPN-1 NG.

**Note: For more information on setting up the Security Manager refer to the guides that come with the software and additional information located on the Entrust web site at <https://www.entrust.com/support/> (Username and password are required). Refer to the Appendix at the back of the document for additional reference material.**

# Modifying the Entrust.ini file

When using VPN-1 NG FP-1 and Microsoft Active Directory with Security Manager 6.0 there are some minor modifications that are required to the entrust.ini file used by the VPN-1 SecuRemote client.

Active Directory makes extensive use of Domain Components (DC) attribute. Make the following changes in the entrust.ini to add support for DC.

- 1 Get a copy of the entrust.ini file from the Security Manager machine. (In this

environment it will be located in the WINNT directory of that machine)

- 2 Open the entrust.ini file in a text editor, for example Notepad.
- 3 The following sections already exist. You will need to add the bottom line of each section so the three sections look like the following.

**[OIDAlias]**

; AliasName=AlgName

domainComponent=dc

**[OIDTable]**

; AlgName=Numeric Object Identifier

dc=0.9.2342.19200300.100.1.25

**[X500AttrSyntax]**

; X500AttributeType=X500SyntaxName

dc=IA5StringSyntax

VPN-1 NG FP-1 and VPN-1 SecuRemote requires that FIPS Mode operation is disabled (see Troubleshooting guide for details). To do this:

- 1 In the same entrust.ini file locate the section at the end of the file while opened in a text editor.

[FIPS Mode]

FipsMode=1

- 2 To turn FIPS mode check off simply change the value of FipsMode from 1 to 0.

[FIPS Mode]

FipsMode=0

- 3 Now save the entrust.ini file and then distribute it to the VPN-1 SecuRemote users.

Note that Entrust does not recommend turning off FIPS Mode for the entrust.ini

file used by the Security Manager.

## Windows 2000 Client Setup

In this setup the VPN-1 SecuRemote client will need to be able to:

- Log into the Domain where the Security Manager is located OR
- You will need to enable "anonymous bind" in Active Directory.

This will allow the user to use Entelligence to update the user's keys. If neither is set then the user will be able to search the directory and see their entry, but will not be able to see their own certificate. Since Entelligence and Security Manager use the absence of the user's certificate in the directory to flag the Change DN state, Entelligence will start a change DN session with Security Manager. Since the user is not really in a change DN state, Security Manager will reject the attempt and Entelligence will return the following error to the user: **"(-11530) Client was expecting a DN change but new certificate from CA did not contain a DN change"**

**Note: This occurs with a Windows 2000 client with Microsoft Active Directory.**

Your company's security policy and system architecture will dictate which of the following methods is most suitable.

### Method A - Logging into the Domain

In order to accomplish this you may need to open up some ports on the firewall. These ports include:

- 1 Kerberos (UDP port 88): the FireWall-1 Kerberos port has a different port; create a new UDP service
- 2 NetBIOS traffic: a predefined NBT group with nbdatagram, nbname, and nbssession
- 3 LDAP for Active Directory usage: the predefined LDAP service TCP port 389
- 4 NTP: UDP port 123; the predefined service ntp-udp
- 5 TCP: port 135. The clients contact the Domain Controller on this port, then receive a random high port in the back connection

However it should be noted that this would expose these ports on your firewall. There are ways of doing this securely that can be found on the Check Point site. The URL to the Check Point SecureKnowledge is <https://support.Check Point.com>. Note you are required to have a username and password.

### **Method B - Using Anonymous Bind on the Active Directory**

In testing this VPN Solution we enable the anonymous bind in Microsoft Active Directory for the CA Entry in order for the Gateways to communicate to the directory to fetch CRLs. However you should look at the security issues if you plan to open up the Active Directory in this manner.

When you configured the Microsoft Active Directory with Entrust you ran a program called "entadconfig.exe". When you ran this program there is a screen called "Grant Anonymous Read Access" displayed in the wizard. One of the options is:

#### **"Grant anonymous read access to the CA Entry and all its sub-entries."**

It is this selection which gives the gateway anonymous read access to the CA Entry in which the CRL is contained.

Also on this screen is the option to allow anonymous read access to user, and computer entries. This did not need to be selected. This option has broader implications than the first option, mainly because it's a permission inherited throughout the domain. If you're using applications that can't use NTLM or Kerberos, and these applications don't require access to public key information, Entrust recommends you not select Grant anonymous read access to user, contact and computer entries in Active Directory.

NOTE: Refer to the Check Point and Entrust web sites for updates on integration with Active Directory.

# Chapter 3

## Configuring the VPN-1 NG FP-1 for use with Entrust Products

This section will explain the configuration required for the VPN-1 NG FP-1 in order for it to work with Entrust products.

# Introduction

There are basically 5 steps to the entire process.

- 1 Make sure there is proper network connectivity between the firewall to the Security Manager, LDAP Directory, and the Secure Remote client machines. You can do this by pinging each of the machines on each end to the other machine, and then vice versa.
- 2 Installation of the Entrust Authority Security Manager and Enrollment Server for VPN products and an LDAP server. Make sure that users can be added and that they can be initialized through client software such as Entelligence or VPN-1 SecuRemote. Also you will need to make sure the following is applied:
  - When configuring your cryptographic information, make sure that your "Certification Authority Key Pair Algorithm" is set to one of the RSA options. Do not select the DSA algorithm.
  - The directory must be able to handle the LDAPV2 protocol.

**Note: Entrust does not recommend or support the use of Check Point's 'Entrust/PKI' enrollment feature within Check Point VPN-1 NG. This feature is built using an Entrust Toolkit which is no longer supported. The use of Entrust Authority Enrollment Server for VPN 6.0 with Check Point's 'OPSEC PKI' feature is the recommended and supported enrollment method for Check Point VPN-1 NG.**

- 3 Installation of the VPN-1 NG Firewall and check for its functionality.
- 4 Installation of the Secure Remote Client and check for its functionality. You will need a copy of the entrust.ini file, and a digital ID either created on the Secure Remote client side, or the Security Manager Administration.
- 5 Testing the connection using the Secure Remote client and having that user authenticate to the firewall.

**[Note: Whenever you make changes to the information on the VPN-1 NG FP-1 you will need to re-install the policy by selecting from the menu bar Policy > Install. Then select which target you would like to install the policy to. You will then see a status of the install in which it should come back successful.]**

Check Point NG FP-1 Docs

General Guides -

[http://www.checkpoint.com/support/technical/documents/docs\\_ngfp1.html](http://www.checkpoint.com/support/technical/documents/docs_ngfp1.html)

Nokia Appliance Hardware Platform -

[http://www.checkpoint.com/support/technical/documents/docs\\_nokia.html](http://www.checkpoint.com/support/technical/documents/docs_nokia.html)

Security Manager 6.0 Docs

[https://www.entrust.com/support/documentation/product\\_docs.cfm?folderID=495](https://www.entrust.com/support/documentation/product_docs.cfm?folderID=495)

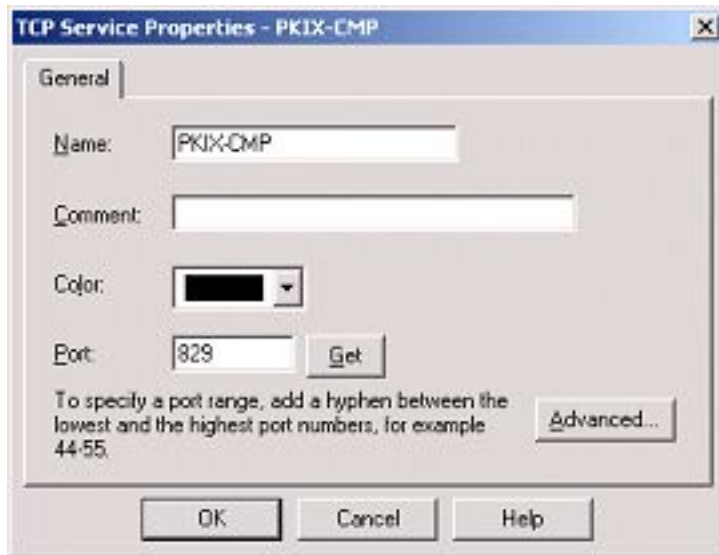
## Modifying Entrust-CA Service on Firewall

You will need to create this because VPN-1 does not know about the 6.0 PKI PKIX-CMP tcp protocol of port 829. This is useful in case you are to limit specific service access to clients and will include the Entrust-CA service in this rule. The steps for creating this are as follows:

- 1 From the Firewall policy editor screen menu bar select **Manage** and then **Services**.
- 2 In the **Services** window, select on **New** and then select **TCP** from the drop down menu.

- 3 Enter in a name for this service such as PKIX-CMP and then enter the port of **829**, and select **OK** to finish. (Note: The names for the various objects cannot contain a whitespace. Therefore if you need to separate words in the name then use "-" or "\_", such as the example above).

### Creating PKIX Service in VPN-1 NG FP-1

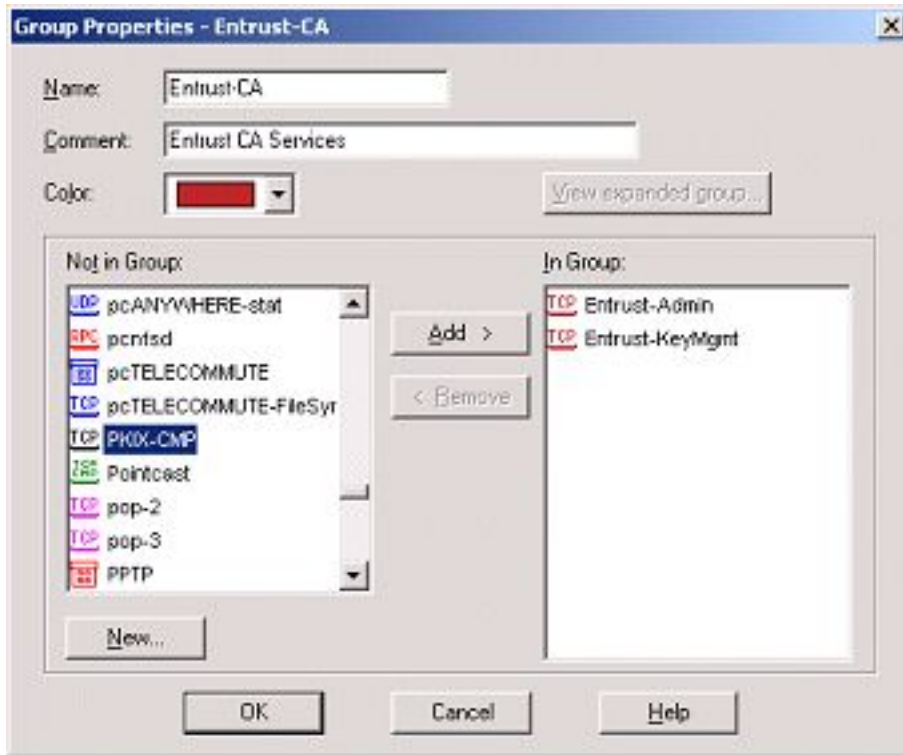


Once this is done you will have to add this service to the Entrust-CA service. The steps for creating this are as follows:

- 1 Scroll down the Services window and select the service for Entrust-CA. Then select **Edit**.
- 2 Scroll down the list of Services and find the **PKIX-CMP** service you created above, and add this to the group **Entrust-CA** and select **OK** to finish.

- 3 Select **Close** to Finish.

### Adding PKIX Service to the Entrust-CA Service



## Creating Certificate Authority Server Object

You need to define the Certificate Authority (CA) on the firewall. This will be needed to enroll the firewall certificate later, and to also hold the CA certificate.

### OPSEC Enrollment Method

The main difference in this enrollment method, compared to the PKIX-CMP enrollment method in previous versions of Check Point VPN-1, is the use of the Enrollment Server for VPN to retrieve both the Firewall Certificate and the Security Manager Certificate.

To create the Certificate Authority (CA) Server Object you:

- 1 From the menu bar of the Policy editor, select **Manage** and then **Servers**.

- 2 Select **New** and then select the **CA** option.
- 3 Once the CA properties screen appears, enter the name you are going to use for the CA Server object and then select **OPSEC PKI** for the **CA-Type**.

### **OPSEC CA Server Object - General**



- 4 Then select the **OPSEC PKI** tab.

### **OPSEC CA Server Object - PKI**



- 5 In this tab you will need to get the CA Certificate into the Server Object by selecting **Get**. Then in the browse window you will need to browse to the location of the CA certificate.

For the Enrollment Server for VPN the CA Certificate is located by default at **C:\Program Files\Entrust\Enrollment Server for VPN\Data\vpnconcacert.pem**. If your Enrollment Server for VPN is located on a different machine then you will need to copy this file over.

Note: In this section you can obtain your CRL either through an LDAP Server (which require an LDAP Account Unit) or through an HTTP Server. In this example the LDAP Server will be used using an LDAP Account Unit configured later.

- 6 Then when you select the CA Certificate you get a screen such as the one below. Select **OK** to accept the Certificate if it is the right one.

### **OPSEC CA Server Object - CA Certificate**



- 7 Then select the **Advanced** tab. In this tab you can select whether or not to cache CRLs that are retrieved for validation. If not selected then it will need to fetch a new CRL each time a certificate needs to be validated.

### **OPSEC CA Server Object - Advanced**



- 8 Select **OK**.

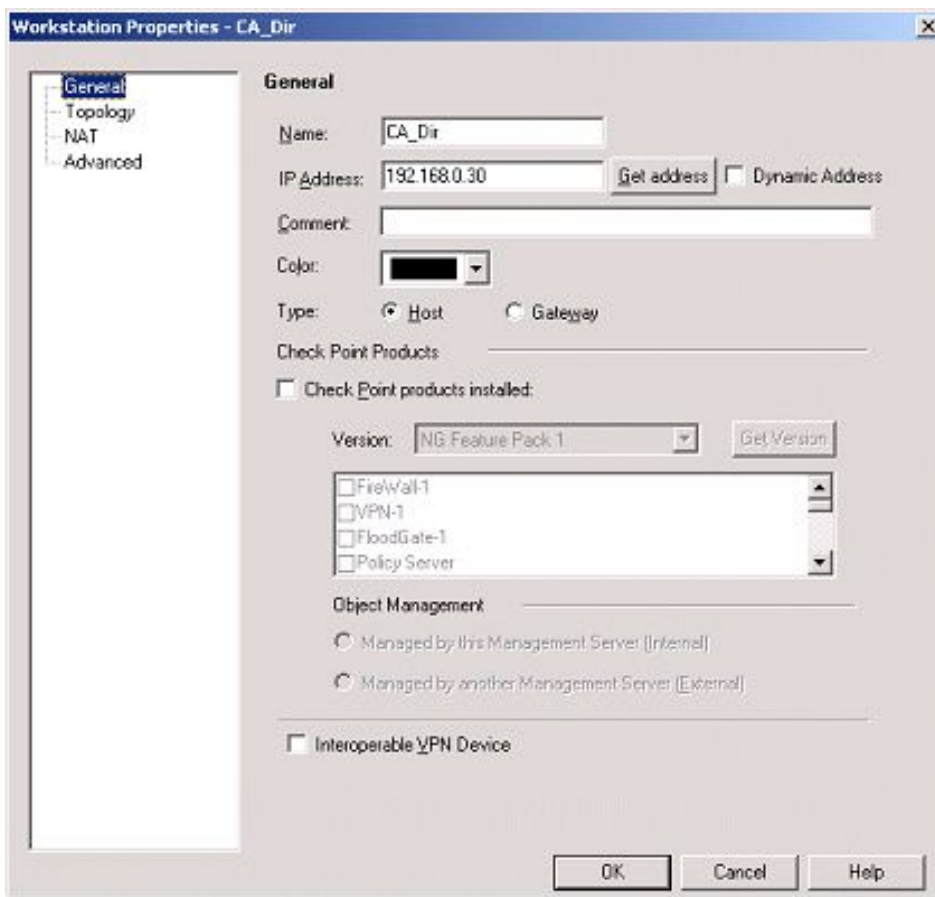
# Creating CA/Directory Object

In order to create your Rule Base and Addressing Translations you will have to setup various network objects. The steps for creating these objects are described in the next few sections.

## To Create the CA/Directory Object

- 1 From the menu bar of the Policy Editor, select **Manage** then select **Network Objects**. In the network objects box, select **New** and then select **Workstation**. In the **General** tab enter in the **name** for this object (ie: CA\_Dir) then enter in the **IP Address** for the CA/Directory server.

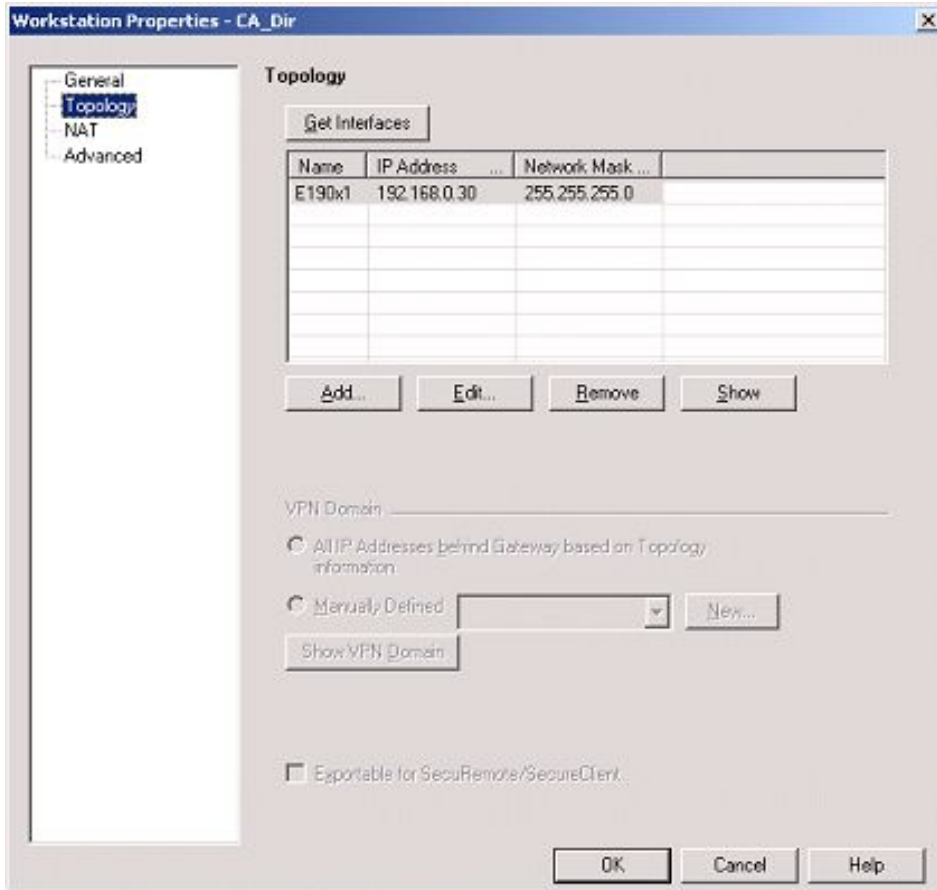
## Entrust CA/Directory Object - General



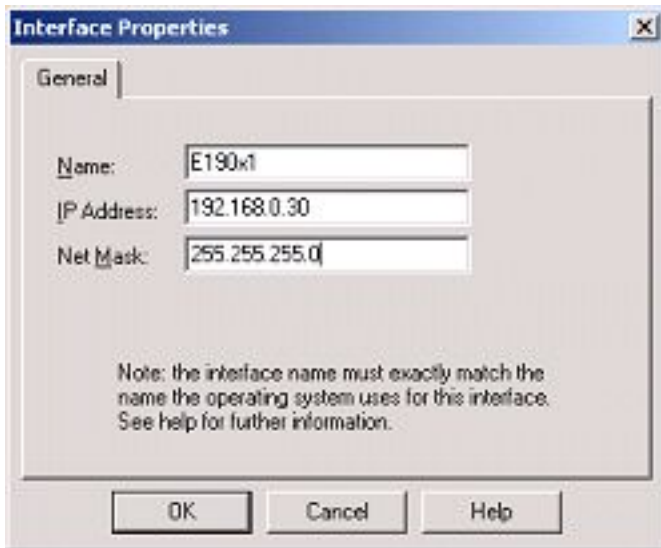
The screenshot shows the 'Workstation Properties - CA\_Dir' dialog box. The 'General' tab is selected in the left-hand pane. The 'Name' field contains 'CA\_Dir'. The 'IP Address' field contains '192.168.0.30', with a 'Get address' button and a 'Dynamic Address' checkbox. The 'Comment' field is empty. The 'Color' field is a black color selector. The 'Type' is set to 'Host' (selected with a radio button) and 'Gateway' is unselected. The 'Check Point Products' section has a 'Check Point products installed' checkbox, which is unchecked. Below it, the 'Version' is set to 'NG Feature Pack 1' with a 'Get Version' button. A list box contains 'FireWall-1', 'VPN-1', 'FloodGate-1', and 'Policy Server', all with unchecked checkboxes. The 'Object Management' section has two radio buttons: 'Managed by this Management Server [Internal]' (selected) and 'Managed by another Management Server [External]'. At the bottom, there is an unchecked checkbox for 'Interoperable VPN Device'. The 'OK', 'Cancel', and 'Help' buttons are at the bottom right.

2. Select the **Topology** section on the left side of the window. Select **Add** to enter the **name**, **IP Address** and **Subnet Mask** for the CA and Directory server.

### Entrust CA/Directory Object - Topology



## Entrust CA/Directory Object - Topology - Interface



[Note: If your Entrust CA and LDAP Server are on different machines then you will need to create a separate, unique workstation object for each.]

- 3 Select **OK** to finish.

## Creating Internal Network Object

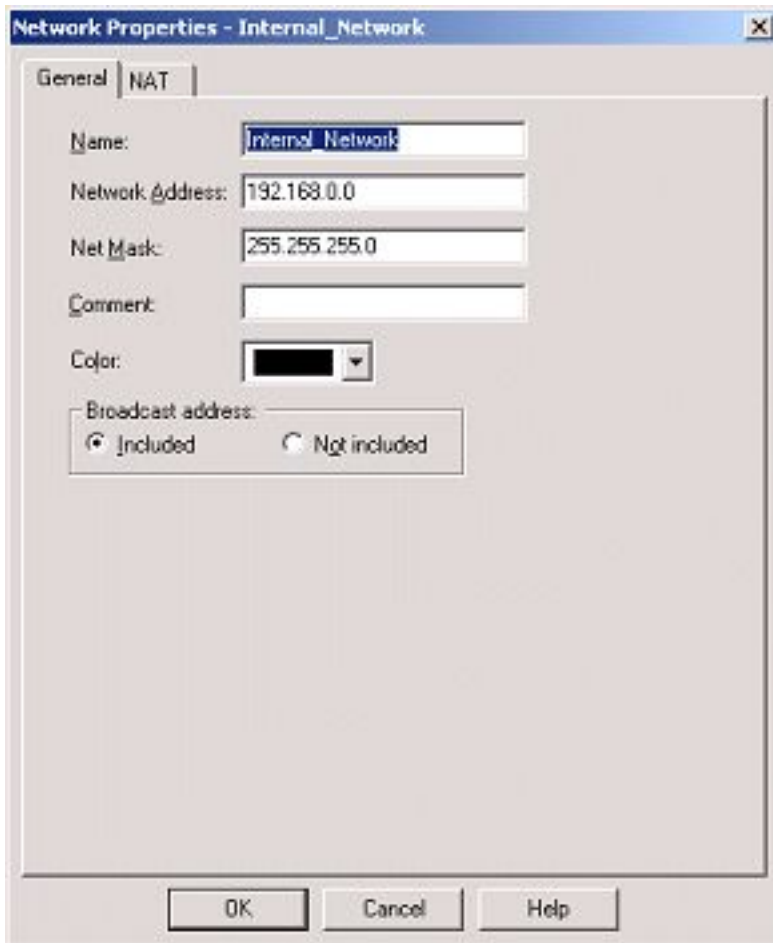
You will need to define an internal Network object to act as your encryption domain.

To create the internal Network object

- 1 From the menu bar of the Policy Editor, select **Manage** and then select **Network Objects**. In the Network Objects window select **New** and then **Network**.

- 2 In the Network Properties screen, enter a name for the object, and specify the **Network Address** for the encryption domain (intranet), and the appropriate **Net Mask**.

### Internal Network Object - General



- 3 The select **OK** to finish.

## Modifying Firewall Object

Next you will need to modify the firewall object. If you have the Firewall Management and the Firewall on the same machine, you will only need one. If they are on different machines then you will have to create two. For this setup they are both on the same machine. To create the Firewall object:

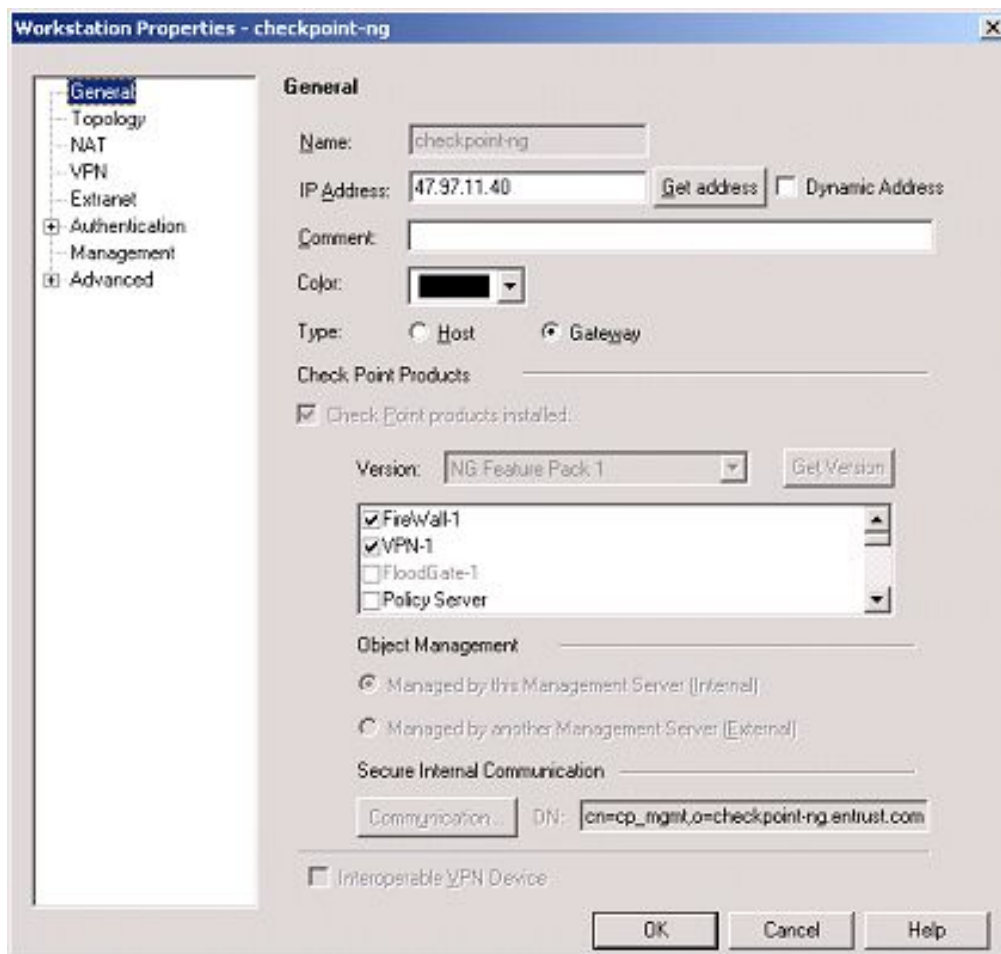
By default the installation of VPN-1 NG FP-1 will create a Firewall object for you. Therefore we are going to be modifying it here to use Entrust.

The following steps show how to modify it to use Entrust. From the menu bar of the policy editor, select on **Manage** then the **Network Objects**. Then select the **Firewall** object and select **Edit**.

### General Section

The General Section should already be configured. Refer to the diagram below for an example.

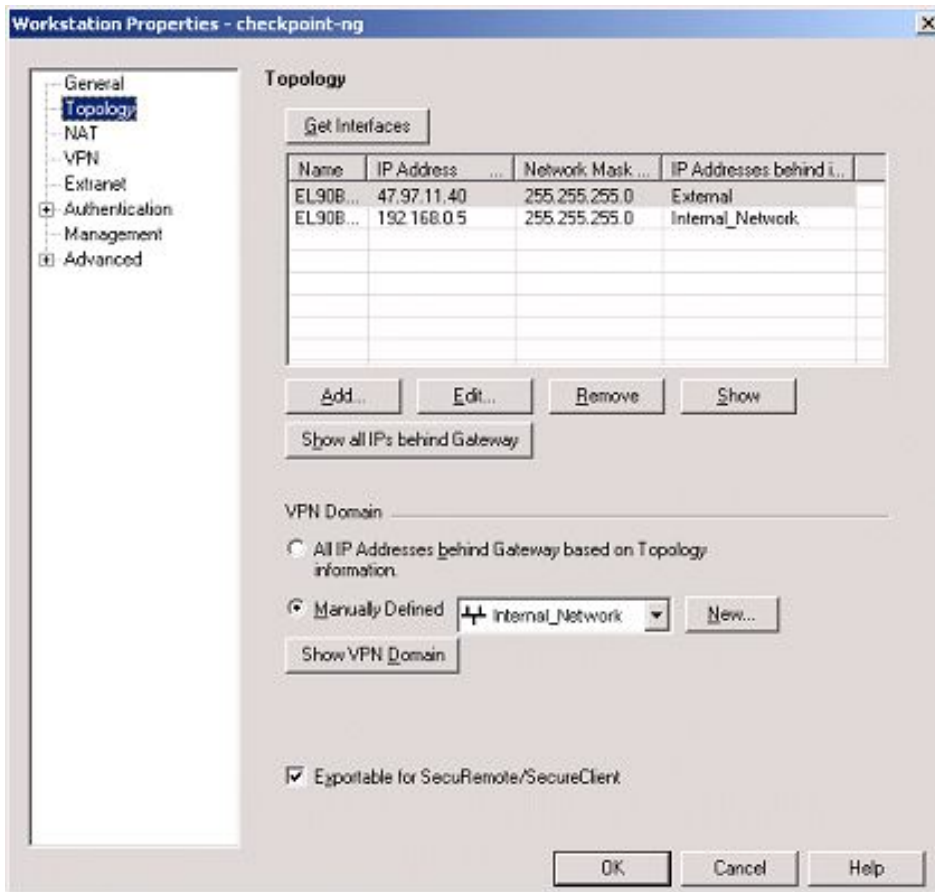
### Firewall Object - General



## Topology Section

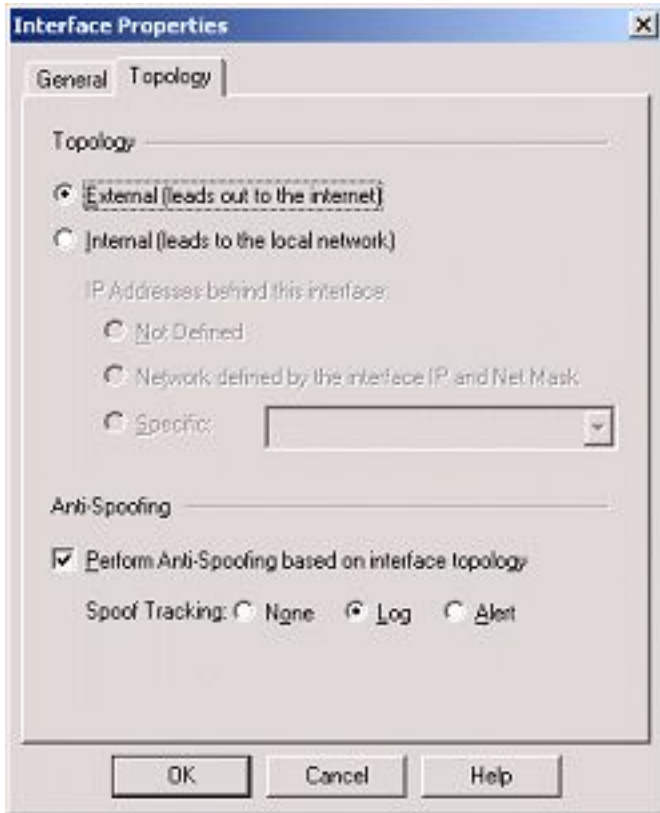
- 1 Select the **Topology Section**. Here you will see the IP Addresses of the NIC cards on the firewall. What you will need to do at this point is to make sure the "**IP Addresses behind interface**" are defined.

## Firewall Object - Topology



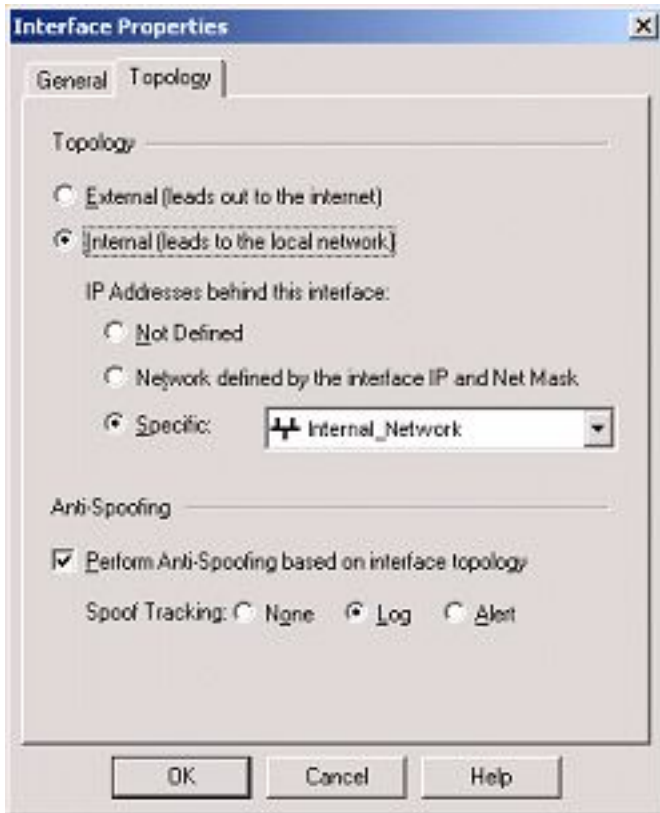
2. Select the **External NIC interface**, and select **Edit**. In the **Topology** tab select "**External (leads out to the Internet)**" and Select "**Perform Anti-Spoofing based on interface topology**" to perform anti-spoofing on the interface. Then Select **OK**.

### Firewall Object - Topology - External Interface



- 3 Select the **Internal NIC interface**, and select **Edit**. In the **Topology** tab select "**Internal (leads to the local network)**" and then select **Specific** in which you will then select the **Internal Network Object (Encryption Domain)** that you defined earlier in the drop down box. Also select "**Perform Anti-Spoofing based on interface topology**" to perform anti-spoofing on the interface. Then Select **OK**.

### Firewall Object - Topology - Internal Interface



- 4 Perform this also on any other interfaces that you may have if you are using more than 2.
- 5 Then in the **VPN Domain** you would select **Manually Defined** and again select the **Internal Network Object (Encryption Domain)** that you defined earlier in the drop down box.
- 6 To have VPN-1 SecuRemote users be able to download the Topology of the Firewall object you must select **Exportable for VPN-1 SecuRemote/SecureClient**, otherwise the client will not be able to communicate to the internal network.

## VPN Section

This is the section in which you will create the Firewall's digital ID.

### To generate the Firewall Digital ID using Entrust Authority Enrollment Server for VPN 6.0 (OPSEC)

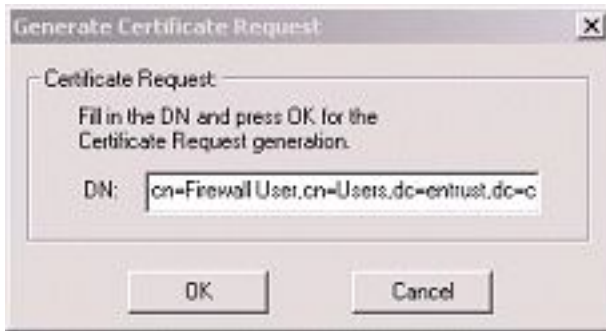
- 1 In this section you will initialize the Entrust digital ID for the Firewall object. Under **Certificate List** select **Add**.
- 2 In the **Certificate Properties** window enter in a **Nickname** for the firewall certificate and then select the **Certificate Authority** you created earlier (for OPsec) on the drop-down list. Once this is complete you will need to generate the PKCS#10 request for the Firewall to get its certificate signed by the Security Manager. To do this select **Generate**.

### Generating Firewall Certificate



- 3 Once you selected **Generate** you will be prompted to enter in the **dn** of the firewall digital ID. It is only necessary to include the Common Name of the dn (cn=Firewall User). When you read the request in the Enrollment Server you will select the rest of the dn from the searchbase selected. Select **OK**

### DN for Firewall Certificate



- 4 You will then see the following displayed if successful. Select **OK**.

### Successful Reply



- 5 Now select View on the Certificate Properties window. The complete PKCS#10 request generated by the Firewall will be displayed. Simply take this and copy it to the clipboard (ctrl-c).

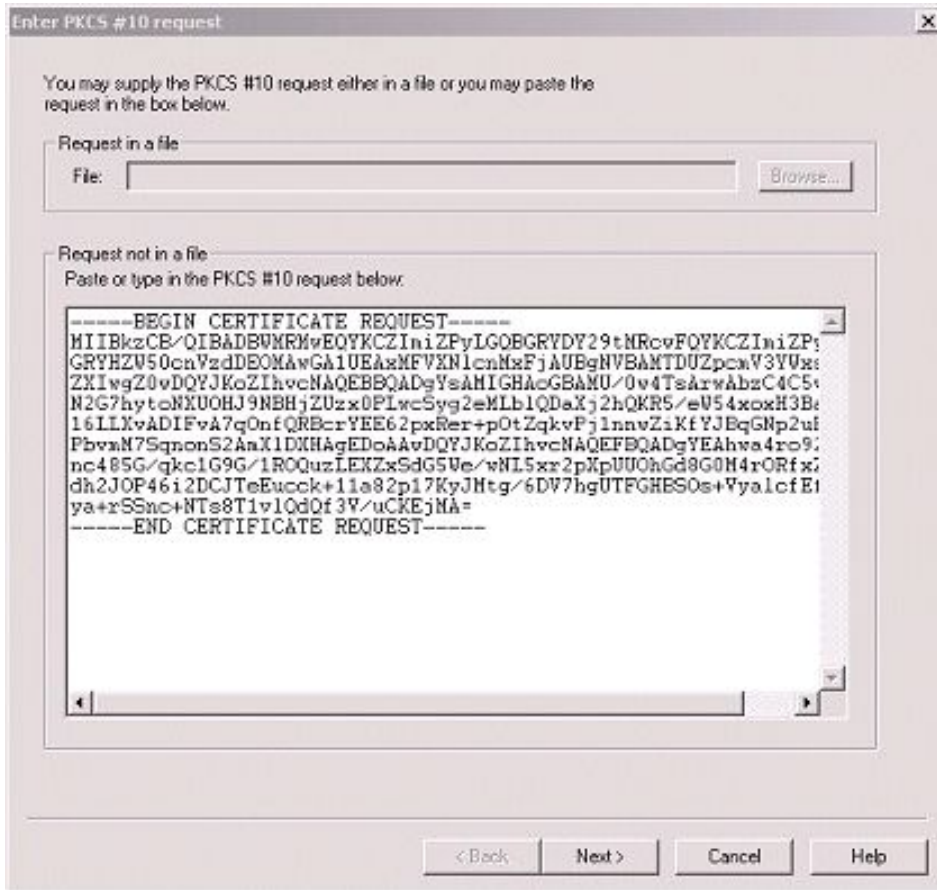
If your Enrollment Server for VPN is not located on the same machine as your firewall's Policy Editor, then you will need to save this information to a file. Open up a text editor and then paste the information in. Then save the file and copy this over to the Enrollment Server for VPN machine. The extension can be left as a txt extension.

### PKCS#10 Request for Firewall Certificate



- 6 Log into the Enrollment Server for VPN and then select from the menu bar **Request >> Read PKCS #10..** In this screen either paste in the request from step 5 above into the window or if you copied over the file select Browse and then select the file then select **Open**. Select **Next**.

### Reading the PKCS#10 Reply in Enrollment Server for VPN



- 7 You will then see the information displayed about the Firewall Certificate request. Select the correct searchbase and then select **Next**.

### Information Contained in PKCS#10 Request

**PKCS #10 Request Information**

Contents:

Searchbase:

Common name:

Serial number:

Description:

Subject alternate names:

Fingerprints:

MD5:

SHA1:

When processing this request:

Use the searchbase contained in the request.

Use this searchbase

Publish certificate to directory

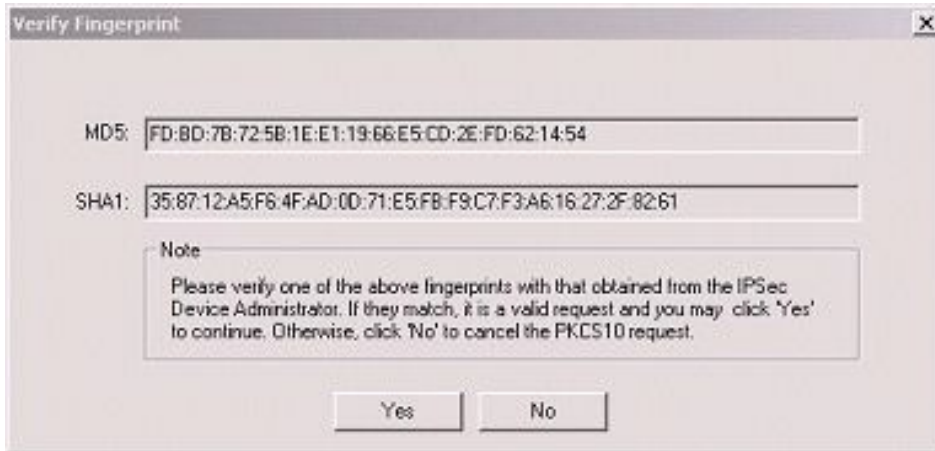
Wrap the output with PKCS-7

Include CA Certificates in PKCS-7 wrap

< Back   Next >   Cancel   Help

- At this point it will display the fingerprint of the certificate request to authenticate it with the device admin to validate the request. If this is the correct one then select **Yes**.

### **FingerPrint for PKCS#7 Reply**



- You will then have the PKCS#7 reply generate on the Enrollment Server. However at this point there is no BEGIN or END CERTIFICATE REQUEST header/footer. Therefore it will be necessary to add these in before importing the PKCS#7 reply into the Firewall Object. Select Save to file, and then enter the information of the path and name for it to be saved as.

### PKCS#7 Reply from Enrollment Server for VPN



Open the file in a text editor and then add

-----BEGIN CERTIFICATE REQUEST-----

to the beginning of the file and add

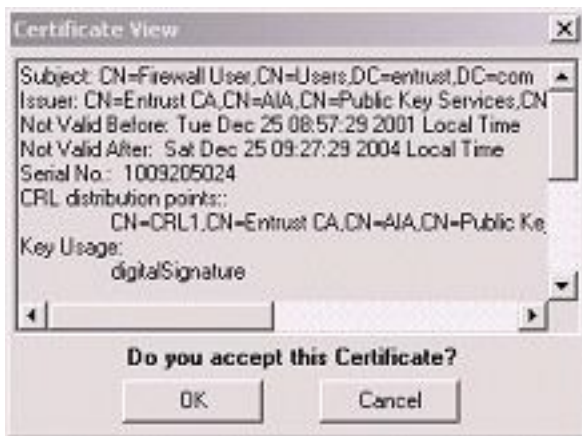
-----END CERTIFICATE REQUEST-----

to the end of the file. Your file should have the same format as the example below. Once this is done then save the file and copy it over to the Policy Editor machine.

```
-----BEGIN CERTIFICATE REQUEST-----
MIID1DCCAz2gAwIBAgIEPCc/IDANBgkqhkiG9w0BAQUFADCBmJEtMBEGCgmSjomT
8ixkARkWA2NvbTEXMBUGCgmSjomT8ixkARkWB2VudHJlc3QxYjAUBgNVBAMTDUNv
bmZpZ3VyYXRpb24xETAPBgNVBAMTCFN1cnZpY2VzMRwwGgYDVQQDExNQdWJsaWMG
S2V5IFN1cnZpY2VzMQwwCgYDVQQDEwNBSUExEzARBgNVBAMTCkVudHJlc3QgQ0Ew
HhcNMDEzMjI1MTM1NzI5WhcNMDEzMjI1MTQyNzI5WjBWMRMwEQYKCCZImiZPyLGQB
GRYDY29tMrcwFQYKCCZImiZPyLGQBGRYHZW50cnVzdDEOMAwGA1UEAxMFVXN1cnMx
FjAUBgNVBAMTDUzpcmV3YWxsIFVzZXIwZ0Z0DQYJKoZIhvcNAQEBBQADgYsAMIGH
AoGBAMU/0w4TsArwAbzC4C5vb8sON2G7hytonXUOHJ9NBHjZUzx0PLwcSyg2eMLb
lQDaXj2hQKR5/eW54xoxH3BaWK3N16LLXvADIFvA7qOnfQRbcrYEE62pxRer+pOt
ZqkvPjlnnwZiKfYJBqGNp2uHQsVzPbvmM7SqnonS2AmXlDXHAgEdo4IBajCCAwyw
CwYDVR0PBAQDAGCgMCsGA1UdEAQkMCKADzIwMDEzMjI1MTM1NzI5WoEPMjAwNDAX
MzExODI3MjlaMIHDBGNVHR8EgbswgbgwbWggBKgga+kgawwgakxEzARBgoJkiaJk/
IsZAEZFgNjb20xZmZAVBgoJkiaJk/IsZAEZFgdlbnRydXN0MRyYwFAyDVQQDEw1D
b25maWdlcmF0aW9uMREwDwYDVQQDEwhTZXJ2aWNlc2EcmBoGA1UEAxMTUHVibG1j
IETleSBTZXJ2aWNlc2EMMAoGA1UEAxMDQU1BMRMwEQYDVQQDEwFbnRydXN0IENB
MQ0wCwYDVQQDEwRDUkwMB8GA1UdIwQYMBaAFEOaIdL9VozE15NyrCNMzefuFViy
MB0GA1UdDgQWBRRrJ5nBFVCaz/o64/VeriX9NAXr/zAJBgNVHRMEAjaAMBkGCSqG
SIb2fQdBAAQMMAAobBFY2LjADAgSwMA0GCSqGSIb3DQEBBQUAA4GBAEq0i5rATkh6
AGg/RPQzNPNzgc15iIQnfJvneN1L1GeVd9dnhG9G3XKEJwrGHLBsQQ1asCoxrUSZ
eM3FmgKmX5pzNyYmoO+FEME/vsyJlmXvJo9dHgTgixRjP7DBJia2ca+NUUZf06g
l/1lnciEMzALadlusp5cUVpMz1ZBpu3D
-----END CERTIFICATE REQUEST-----
```

- On the Policy Editor machine with the Firewall Object's Certificate property window opened you will need to select **Get**. Then browse to the location of the PKCS#7 reply from above and select it. You will then be asked if you want to accept this certificate. If this is the correct one then select **OK**.

### Retrieving the PKCS#7 Reply in the Firewall



- 11 If there was a problem with the PKCS#7 reply (such as the begin and end header/footer missing) you would see an error like the one below. You will need to look at the PKCS#7 reply to make sure it is valid (with header/footer).

### **Error Generated by Missing Header and Footer**



### **Editing IKE Properties on the VPN Section**

- 1 You will need to select the Encryption schemes. In the section **Encryption Schemes** select **IKE** and then select **Edit** under this window.
- 2 If you are using the Strong version of VPN-1 NG FP-1 and the VPN-1 SecuRemote then select **3DES** and deselect the remaining **Support key exchange encryption with:**.

- 3 For the **Support data integrity with:** select **SHA1**.

### Firewall Object - VPN - IKE Properties



- 4 Below in **Support authentication methods:** select **Public Key Signatures** and then select **Specify** to the right of this.
- 5 This will display the **Allowed Certificates** window to define which certificates to use in IKE negotiations with a locally managed peer gateway. The options you have are:
  - **The gateway can use any of its certificates** — VPN-1 NG FP-1 will automatically select a Certificate Authority.
  - **The gateway must use a certificate issued by this Certificate Authority** — The gateway will use certificates issued by the Certificate Authority selected from the drop-down list.

In this example the option **The gateway must use a certificate issued by this Certificate Authority** was selected and the **Entrust CA** object created earlier is selected.

Which one you select will be determined by your setup. Once this is selected then select **OK** to save.

### Firewall Object - VPN - IKE - CA Property



- 6 Select **OK**.
- 7 Select **Close** to finish.

## What to do if You Need to Re-enroll the Firewall Certificate

This is not required for the initial setup of the VPN-1 NG FP-1, but will be required later.

Digital certificates expire after a pre-determined period of time - typically one to two years depending on corporate policy. When using Check Point's OPSEC PKI feature administrators must track certificate expiry dates and re-enroll for new certificates before they expire. Use the Security Manager Administration or Enrollment Server for VPN consoles to find certificates nearing expiry. To re-enroll for a new firewall certificate:

- 1 Log into the **Security Manager Administration** and then **search** and find the Firewall User created earlier.
- 2 **Double-click** on the user entry and select the **Certificate List** tab and check to make sure the certificate for the firewall is **revoked/expired**.
- 3 Select **OK**.

- 4 Log into the **Policy Editor** on the VPN-1 NG FP-1.
- 5 **Select** the firewall object that contains the certificate that you are recovering.
- 6 Select the **VPN section**.
- 7 Now select the **certificate** under the **Certificate List** section that belongs to the firewall user with the Security Manager (**Do not select the one for the internal CA**).
- 8 Once selected (highlighted) select **Edit**.
- 9 On this screen select **Generate**.
- 10 It will then warn you "**You already have a key. Do you want to generate a new one?**", select **Yes**.
- 11 Another warning will display, "**The generation of the certificate for the workstation cannot be undone, unless you click Remove. Are you sure you want to continue?**", select **Yes**.
- 12 You will be prompted to enter in the **dn** of the firewall digital ID. Include the Common Name of the dn (cn=Firewall User). Typically the Common Name of the firewall will not change during re-enrollment. When you read the request in the Enrollment Server you will select the rest of the dn from the searchbase selected. Select **OK**.
- 13 Here you should see the response "**Certificate Request created successfully**". Select **OK**.
- 14 Now select View on the Certificate Properties window. The complete PKCS#10 request generated by the Firewall will be displayed. Simply take this and copy it to the clipboard (ctrl-c).

If your Enrollment Server for VPN is not located on the same machine as your firewall's Policy Editor, then you will need to save this information to a file. Open up a text editor and then paste the information in. Then save the file and copy this over to the Enrollment Server for VPN machine. The extension can be left as a txt extension.

- 15 Log into the Enrollment Server for VPN and then select from the menu bar **Request >> Read PKCS #10**.. In this screen either paste in the request from step 14 above into the window or if you copied over the file select Browse and then

select the file then select **Open**. Select **Next**.

- 16 You will then see the information displayed about the Firewall Certificate request. Select the correct searchbase and then select **Next**.
- 17 At this point it will display the fingerprint of the certificate request to authenticate it with the device admin to validate the request. If this is the correct one then select **Yes**.
- 18 You will then have the PKCS#7 reply generate on the Enrollment Server. However at this point there is no BEGIN or END CERTIFICATE REQUEST header/footer. Therefore it will be necessary to add these in before importing the PKCS#7 reply into the Firewall Object. Select Save to file, and then enter the information of the path and name for it to be saved as.

Open the file in a text editor and then add

```
-----BEGIN CERTIFICATE REQUEST-----
```

to the beginning of the file and add

```
-----END CERTIFICATE REQUEST-----
```

to the end of the file. Your file should have the same format as the example below. Once this is done then save the file and copy it over to the Policy Editor machine.

```
-----BEGIN CERTIFICATE REQUEST-----
MIID1DCCAz2gAwIBAgIEPCC/IDANBgkqhkiG9w0BAQUFADCBmJEtMBEGCgmSJomT8ixkARkWA2NvbTEXMBUGCgmSJomT8ixkARkWB2VudHJlc3QxZjAUBgNVBAMTDUNvbmZpZ3VyYXRpb24xETAPBgNVBAMTCFNlcnZpY2VzMRwwGgYDVQQDExNQdWJsaWMgS2V5IFNlcnZpY2VzMQwwCgYDVQQDEwNBSUExEzARBgNVBAMTCkVudHJlc3QgQ0EwHhcNMDEzMjI1MTM1NzI5WhcNMDEzMjI1MTM1NzI5WjBWMRMwEQYKCCZImiZPyLGQBGRYDY29tMRCwFQYKCCZImiZPyLQBGRYHZW50cnVzdDEOMAwGA1UEAxMFVXNlcnMxZjAUBgNVBAMTDUZpcmV3YWxsIFVzZXIwZ0wDQYJKoZIhvcNAQEBBQADgYsAMIGHAoGBAMU/0w4TsArwAbzC4C5vb8sON2G7hytONXUOHJ9NBHjZUzx0PLwcSyyg2eMLblQDaXj2hQKR5/eW54xoxH3BaWK3N16LLXvADIFvA7qOnfQRBcrYEE62pxRer+pOtZqkvPjlnnwZikfYJBqGNp2uHQsVzPbvM7SqnonS2AmX1DXHAgEDo4IBajCCAwywCwYDVR0PBAQDAGCgMCsGA1UdEAQkMCKADzIwMDEzMjI1MTM1NzI5WoEPMjAwNDAMzExODI3MjlaMIHDBgNVHR8EgbswgbgwbWggbKggg+kgawwgakxEzARBgoJkiaJk/IsZAEZFgNjb20xZzAVBgoJkiaJk/IsZAEZFgdlbnRydXN0MRYwFAYDVQQDEw1Db25maWdlcmF0aw9uMREwDwYDVQQDEwhTZXJ2aWNlczEcmBoGA1UEAxMTUHVhbiBGljIEt1eSBTZXJ2aWNlczEEMMAoGA1UEAxMDQU1BMRMwEQYDVQQDEwFbnRydXN0IENBMQ0wCwYDVQQDEwRDUkwMB8GA1UdIwQYMBaAFEOaIdL9VOze15NyrCNMzefuFVIyMB0GA1UdDgQWBBRrJ5nBFVCaz/o64/VeriX9NAXr/zAJBgNVHRMEAjAAMBkGCSqGSIb2fQdBAAMMAobBFY2LjADAgSwMA0GCSqGSIb3DQEBBQUAA4GBAEq0i5rATkh6AGg/RPQzNPNzgc15iIQnfJvneN1L1GeVd9dnhG9G3XKEJwrGHLBsQQ1asCoxrUSZem3FmgKmX5pzNyYvmo0+FEME/vsyJlmXvJo9dHgTgixRjP7DBJia2ca+NUUZFO6q1/llnciEMzALadlusp5cUVpMz1ZBpu3D
-----END CERTIFICATE REQUEST-----
```

- 19 On the Policy Editor machine with the Firewall Object's Certificate property window opened you will need to select **Get**. Then browse to the location of the PKCS#7 reply from above and select it. You will then be asked if you want to

accept this certificate. If this is the correct one then select **OK**.

- 20 At this point you should be successful in recovering the Firewall certificate. Select **OK** to close.
- 21 Select **OK** to finish.

## Creating the LDAP Account Unit on the Firewall

The next few sections will outline the steps involved in configuring an LDAP Account Unit in order to authenticate users to the firewall and fetch CRLs from the LDAP server.

### Creating LDAP Group

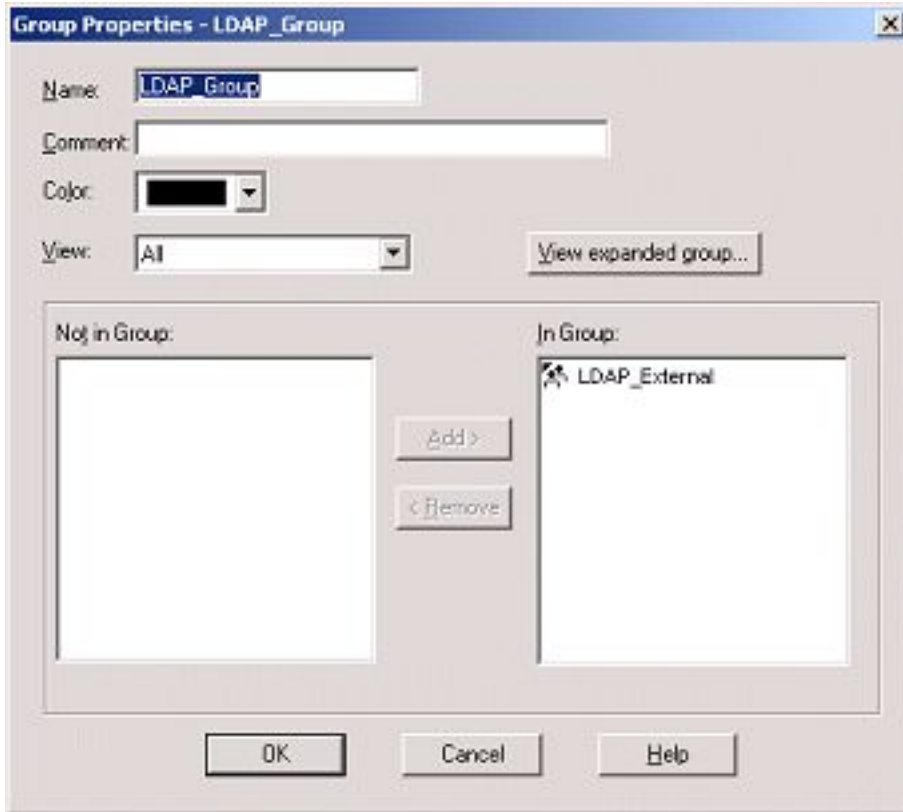
The first step in this process is to define a Group for the Account Unit to use. After this you will need to define the Template, LDAP Account Unit object, group and an external LDAP group for the LDAP Account Unit.

To create the group for the LDAP Account Unit:

- 1 From the menu bar of the policy editor, select on **Manage** then the **Users and Administrators ..** selection.
- 2 Select **New** then select **Group ...**

- 3 Give a **name** for the group being created.

### Group for LDAP Account Unit



- 4 After you have created the External LDAP Group for the Account Unit you will need to select it from the **Not in Group:** field in the properties of this group and select **Add**. You will be reminded of this in the section **Creating External LDAP Group**.
- 5 Select **OK**.
- 6 Select **Close** to finish.

## Creating LDAP Template

The next step in this process will be to define a Template for the LDAP Account Unit to use. The template will reveal such information as the authentication method, access time, location, expiration date to use for the users being authenticated.

To create the template for the LDAP Account Unit:

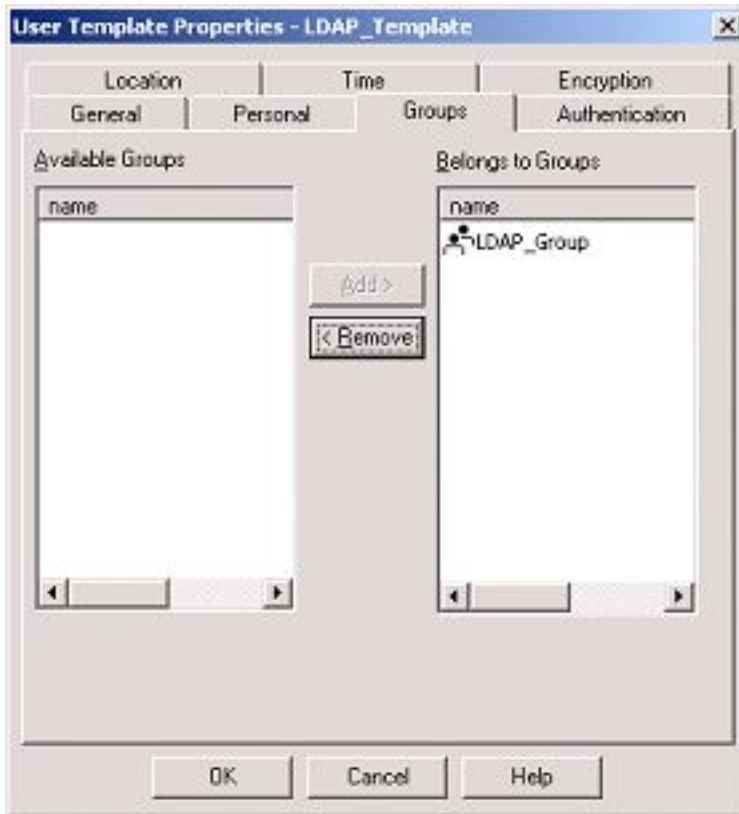
- 1 From the menu bar of the policy editor, select on **Manage** then the **Users and Administrators ..** selection.
- 2 Select **New** then select **Template ..**
- 3 In the **General** tab give a **name** for the template being created.

### LDAP Account Unit Template - General



- 4 From the **Groups** tab select the **Group** you created earlier from the list of **Available Groups** and **ADD** to **Belongs to Groups**.

### LDAP Account Unit Template - Groups



- 5 The **Encryption** tab is where you indicate the Encryption Method for the users. Here select **IKE** for the **Client Encryption Method**. Then select **Edit**. In the **IKE Properties** screen select **Public Key** in the **Authentication** tab. Then in the **Encryption** tab make sure that **Transform** is **Encryption+Data Integrity (ESP)**, **Data Integrity** is **SHA1** and the **Encryption Algorithm** is **3DES**. Select **OK**.

### LDAP Account Unit Template - Encryption IKE Authentication



### LDAP Account Unit Template - Encryption IKE



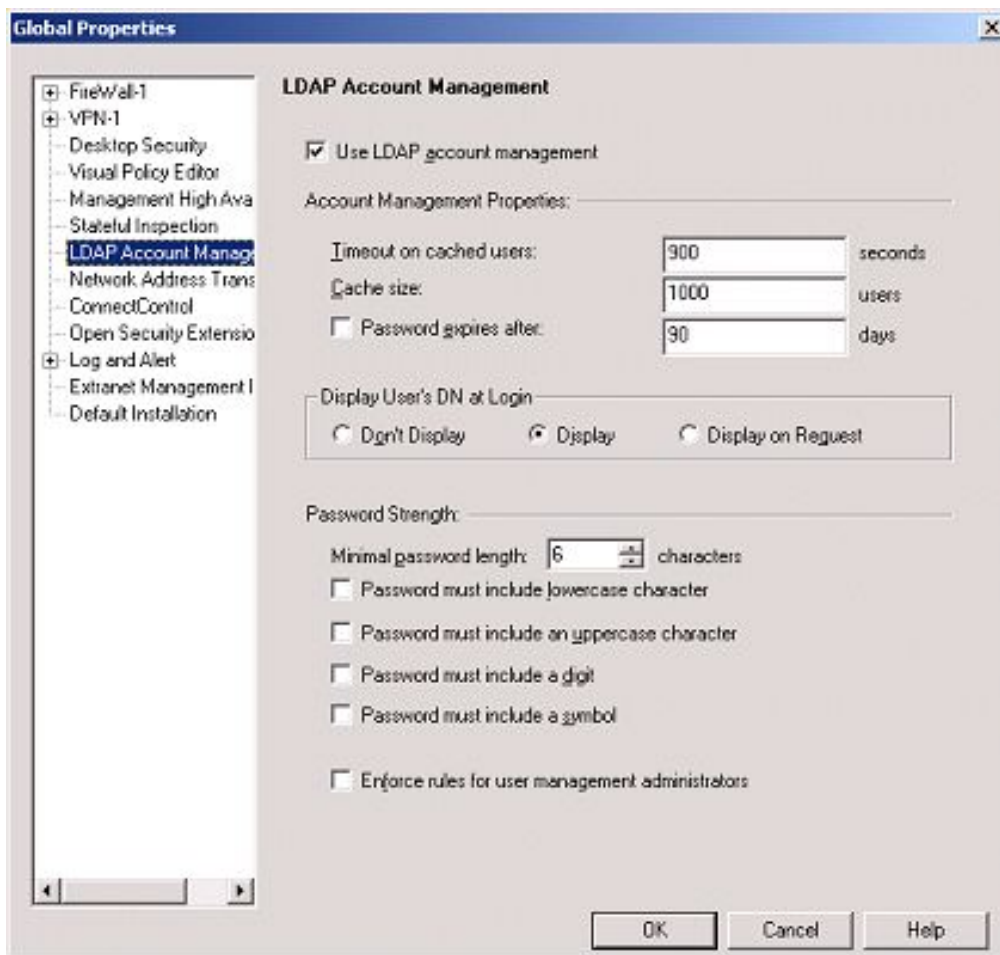
- 6 Select **OK**.

7 Select **Close** to finish.

## Creating LDAP Account Unit

Before creating the LDAP Account Unit, you will need to go to the menu bar in the Policy Editor and select **Policy >> Global Properties**. Then select **LDAP Account Management** section and in this screen select **Use LDAP Account Management**. Select **OK**.

### Firewall Policy - Global Properties - LDAP Account Management

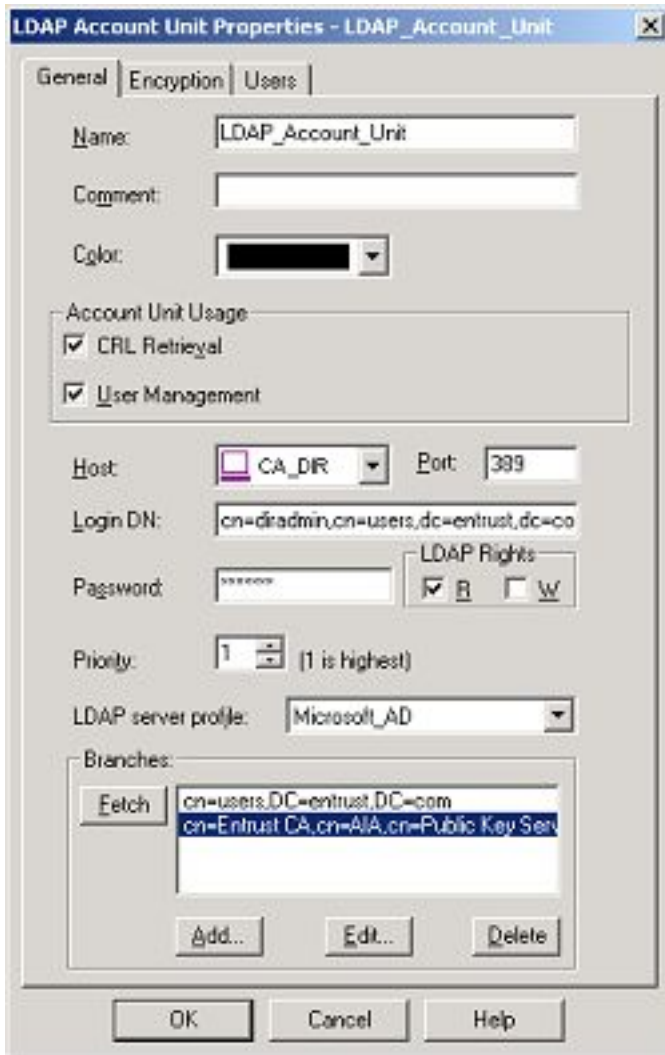


To create the LDAP Account Unit:

1 From the menu bar of the Policy editor, select **Manage** and then **Servers**.

- 2 Select on **New** and then select the **LDAP Account Unit ..** option.
- 3 Enter a **name** for the LDAP Account Unit being created.

### LDAP Account Unit Object - General



- 4 For the Account Unit Usage make sure **CRL Retrieval** and **User Management** are selected.
- 5 For the **Host** select the **CA/Directory object** (or if using separate machines the Directory object) that you created earlier.
- 6 The port to the Directory (LDAP Server) by default is **389**. Enter the correct value

here.

- 7 Next you will need to enter the **DN** of the **Directory Administrator** to bind to the directory. In the example **cn=diradmin,cn=users,dc=entrust,dc=com** was used. The Directory Administrator was created earlier in the section **Creating Firewall User in Entrust RA**.
- 8 Enter the **Password** for the directory administrator entered in the previous step.
- 9 Select the **LDAP rights** for the user binding to the directory. **Note** do not select **Write** access to the LDAP Server as you are just **reading** the information in the directory and not changing it.
- 10 Select the **LDAP Server digital ID type**. For this example we are using Microsoft Active Directory and therefore **Microsoft\_AD** is selected.
- 11 Then select **Fetch** to add the branches of the users to be authenticated against. If this cannot be resolved then see the section later on troubleshooting. You may want to try adding branches manually, but this indicates a problem.

Also note that if you are using Microsoft Active Directory, the CRL Distribution Points will be located under the CA entry in the directory which is usually different from the location of the users. Therefore it is important to **add the CA entry branch** if the FETCH command does not retrieve the CA branch (the location where Active Directory stores the CRL). The simplest way to find out where the CA entry is to open the entrust.ini file up in a text editor. Then under the section **[Entrust Settings]** you will find an entry such as:

**CA Distinguished Name=cn=Entrust CA,cn=AIA,cn=Public Key Services,cn=Services,cn=Configuration,dc=entrust,dc=com**

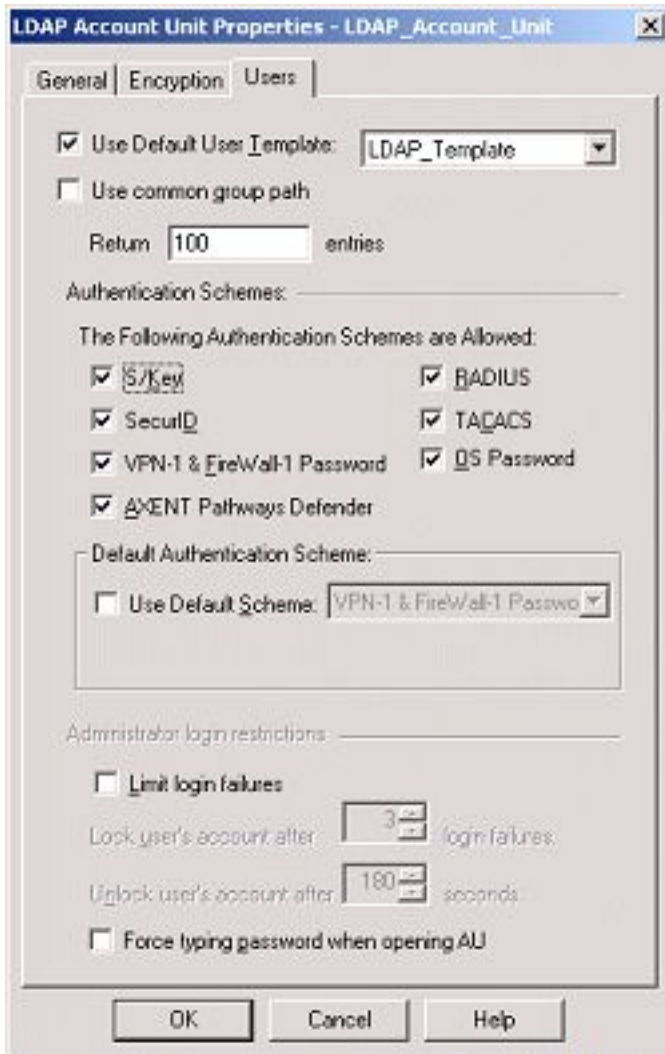
What you will then need to do is select everything to the right of the first equal sign (=) and to the end of dc=com and copy this into your clipboard (**Ctrl-C**). Then in this LDAP Account Unit screen select ADD for the branches and paste (**Ctrl-V**) in the branch like the one below (**Note: this branch will usually be different for each CA**):

**cn=Entrust CA,cn=AIA,cn=Public Key Services,cn=Services,cn=Configuration,dc=entrust,dc=com**

This will then allow you to fetch CRLs later when needed to authenticate users. Select **OK**.

- Then in the **Users** tab, select **Use Default User Template** and then select the template that you created earlier for the LDAP Account Unit.

### LDAP Account Unit Object - Users



- Select **OK**.
- Select **Close** to finish.

## Creating the External LDAP Group

The last step for configuring the LDAP Account Unit is to create an External LDAP Group. To create the External LDAP Group:

- 1 From the menu bar of the policy editor, select on **Manage** then the **Users and Administrators ..** selection.
- 2 select on **New** and then select the **External Group ..** option.

### External LDAP Group

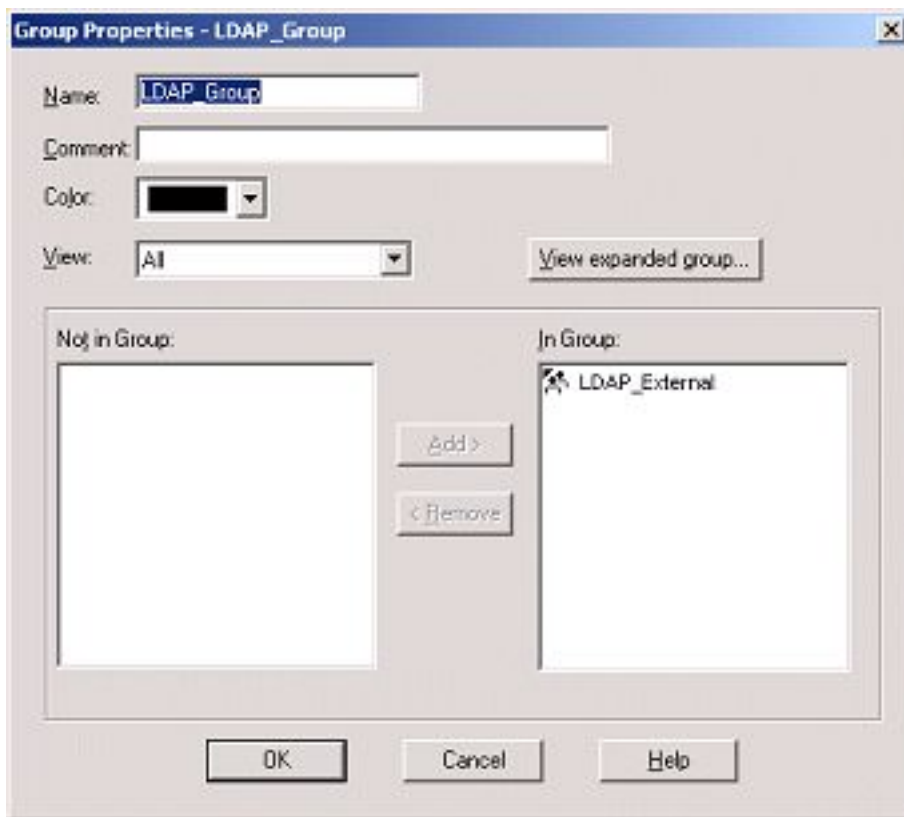


- 3 Enter a **name** to be used for this External LDAP Group.
- 4 Select the **Account Unit** created earlier in the **drop-down list**.
- 5 You can then select the **Group's Scope** however for this example it was left at **All Account Unit's Users**. How specific you want this would determine on your setup.

- 6 Select **OK**.
- 7 Select **Close** to finish.

[Note: Now at this point you will need to open up the properties of the first group that you created. From the menu bar of the policy editor, select on 'Manage' then the "Users and Administrators .." selection. Then select the group and select Edit. In the "Not in Group" section select the External LDAP Group and then Add this to the "In Group". Then select OK.]

### Placing External LDAP Group in LDAP Group



## Creating Rule Base

To tie all the objects created to a security policy it will be necessary to create a Rule Base. When creating the rule base you will need to have users belonging to a group to be able to authenticate to the Firewall and gain restricted access to your network. Each corporation will have different security policies which govern what users are permitted

to do, so each will be different.

At this point you will need to create a rule base that will allow users to authenticate and gain restricted access to your internal network using their Entrust digital id's. The Check Point guides have examples of rule bases used for authenticating with certificates.

## Installing the Security Policy on the Firewall

Once you have made the changes to the firewall and rules added you will then need to install/re-install the policy so that users can get your public keys and be able to download the firewall's topology. To do this select **Policy** from the menu bar and then select **Install**. For more details on the options available in installing the policy refer to the **Check Point Management Guide.pdf** in the section **Installing the Security Policy**

# Chapter 4

## Configuring the VPN-1® SecuRemote NG Client

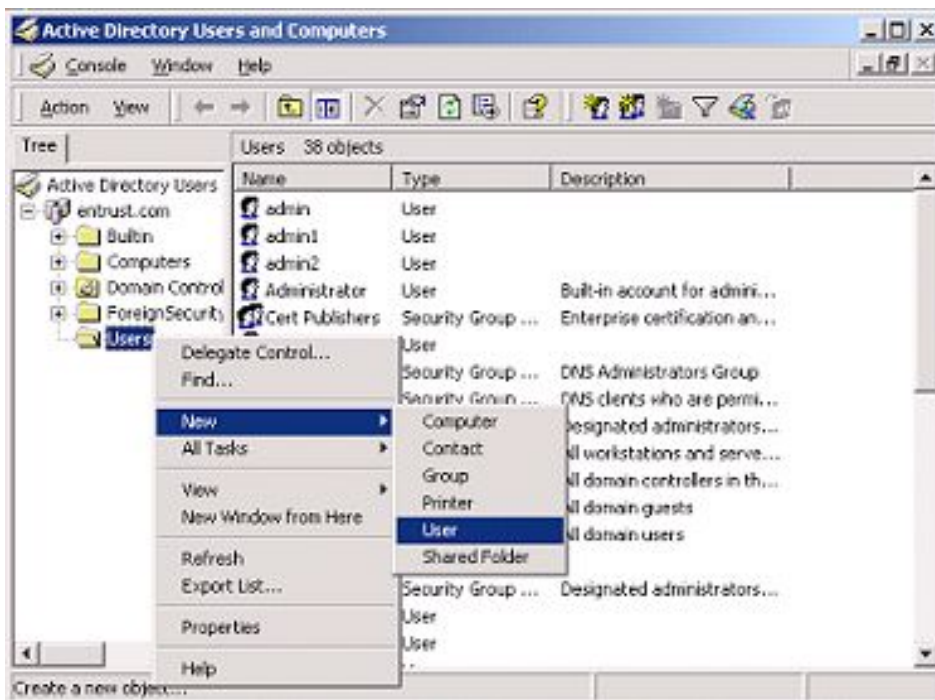
The following sections outline how you would configure VPN-1 SecuRemote and Desktop Manager client in order to authenticate to the VPN-1 NG FP-1.

# Creating the VPN-1 SecuRemote Client User in Entrust Authority™ Security Manager Administration

You have to create a regular end user with an enterprise certificate for the VPN-1 SecuRemote user. To do this, you must:

- 1 **Add** the user in Active Directory first (**Start >> Programs >> Administrative Tools >> Active Directory Users and Computers**). Then select the container to add the user to and then right-click and select **New >> User**.

## Adding User in Active Directory



Add in the **First, Last and User logon name**. Select **Next**.

### Adding User in Active Directory - New Object

The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: entrust.com/Users'. Below this, there are several input fields:

- First name:** SecuRemote
- Last name:** One
- Full name:** SecuRemote One
- User logon name:** Secureone (text) and @entrust.com (dropdown)
- User logon name (pre-Windows 2000):** ENTRUST0\ (text) and Secureone (text)

At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Enter in a password for the user and then select the appropriate options for the password in your setup. Select **Next**.

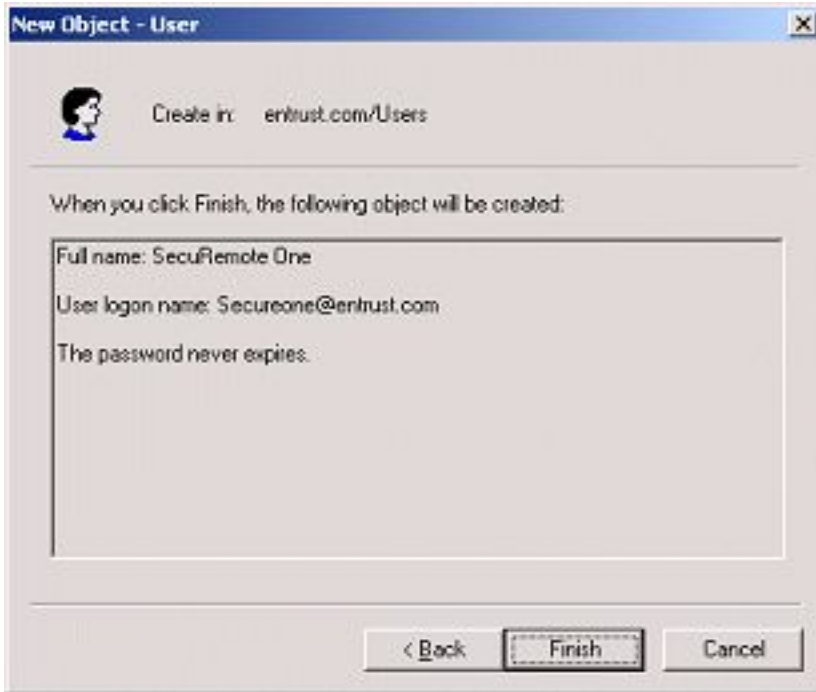
### Adding User in Active Directory - Password



The screenshot shows a Windows dialog box titled "New Object - User". At the top left, there is a user icon and the text "Create in: entrust.com/Users". Below this, there are two text input fields: "Password" and "Confirm password", both containing masked characters (dots). Underneath the input fields are four checkboxes with the following labels: "User must change password at next logon", "User cannot change password", "Password never expires" (which is checked), and "Account is disabled". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

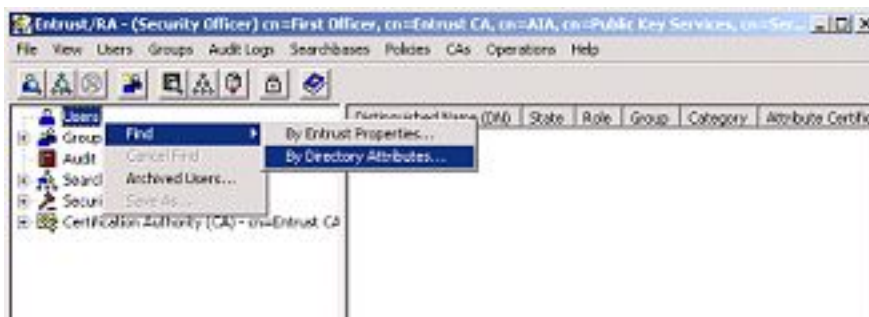
Then if the information is correct for the user then select **Finish**.

### Adding User in Active Directory - Finish



- 2 Log into the **Security Manager Administration**.
- 3 Do a Search of Users by Directory Attributes (**Right-click users** and select **Select By Directory Attributes**. Make sure to select the correct searchbase and add in any values for the search fields or you can leave them with the wildcard symbol (\*) and then click Find).

### Selecting Search in Entrust RA



## Directory Search in Entrust RA



- 4 Double-click on the user to open their **User Property** screen. Here make any changes you need to add (example: dn information, key update options, etc.) to suit your corporate policy.
- 5 Select **OK**. This will prompt you for authorization of this operation.
- 6 At this point you will get a **reference number** and **authorization code**. You can use this to create the user's digital ID.

**[Note: You will need to determine how you will create the user digital ID. Depending on your setup this could be accomplished in at least two different methods.]**

- 1 Creating the digital ID on the Security Manager Administration machine and then sending the user their digital ID, in a secure manner.
- 2 Use the reference number and authorization code created earlier, to create the digital ID remotely on the client machine. Since the sample configuration described in this document places the Security Manager and directory behind the firewall, you would first need to establish an IPSec tunnel with the firewall using IKE (pre-shared secrets) with a username and password. Certificate enrollment with Security Manager could then occur through this tunnel and subsequent connections would be authenticated using digital certificates. See the section below on Creating an IPSec Tunnel using Pre-shared Secrets for details.
- 3 Using the Entrust Authority Self-Administration Server to create the profile either

on the server or client side through the browser. For more details on this please contact your Entrust representative.

## Creating an IPSec Tunnel using Pre-Shared Secrets (Optional)

This section will outline a alternative method to establish a temporary IPSec tunnel with limited access rights to remotely create an Entrust digital ID.

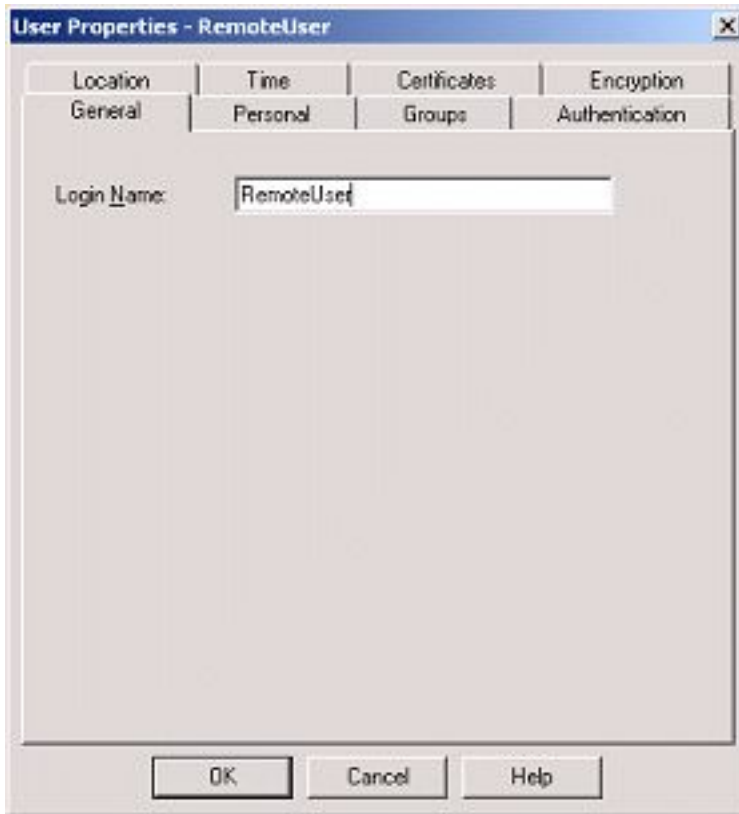
Steps are: define a user, a group that this user belongs to, a rule in the Rule Base defining this group and possibly some modifications to the Firewall's object properties. Once these configuration steps are complete end-users can use the chosen username/password to enable remote enrollment. Enrollment is described further on in the document.

### Creating the User

- 1 In the **Policy Editor** on the Firewall select **Manage >> Users and Administrators ...**
- 2 On the **User** screen select **New >> User by Template >> Default**.

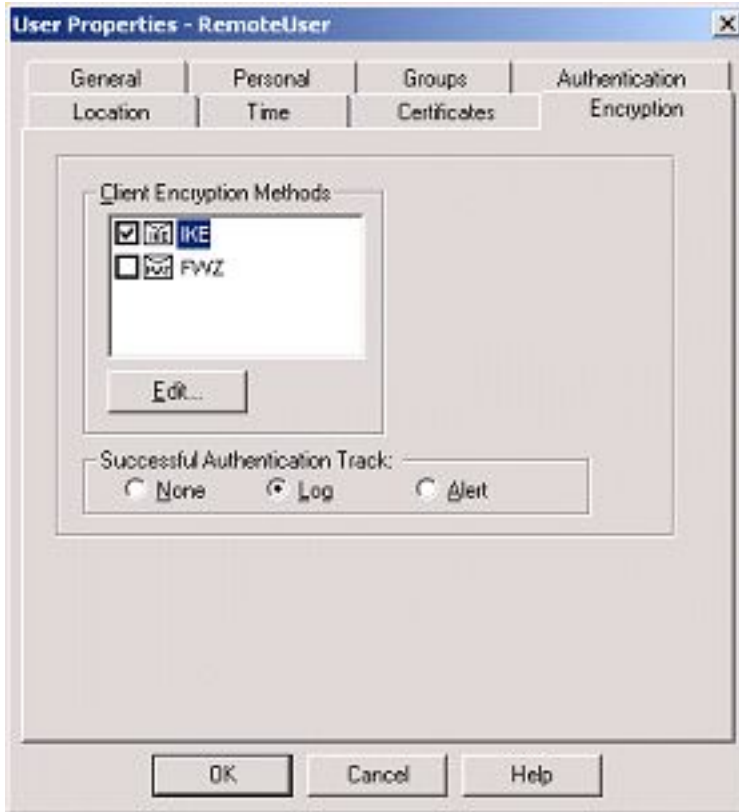
- 3 In the **General** tab enter in a **name** for the user. Then select the **Encryption** tab.

### **General Tab for Remote Users**



- 4 In the **Encryption** tab select **IKE** and then select **Edit**.

### Encryption Tab for Remote Users



- 5 On the **IKE Properties** screen select **Password (Pre-shared secret)**. Then enter in a **secret password** and then confirm the password. Select **OK**.

### **Password for Pre-Shared Secret**



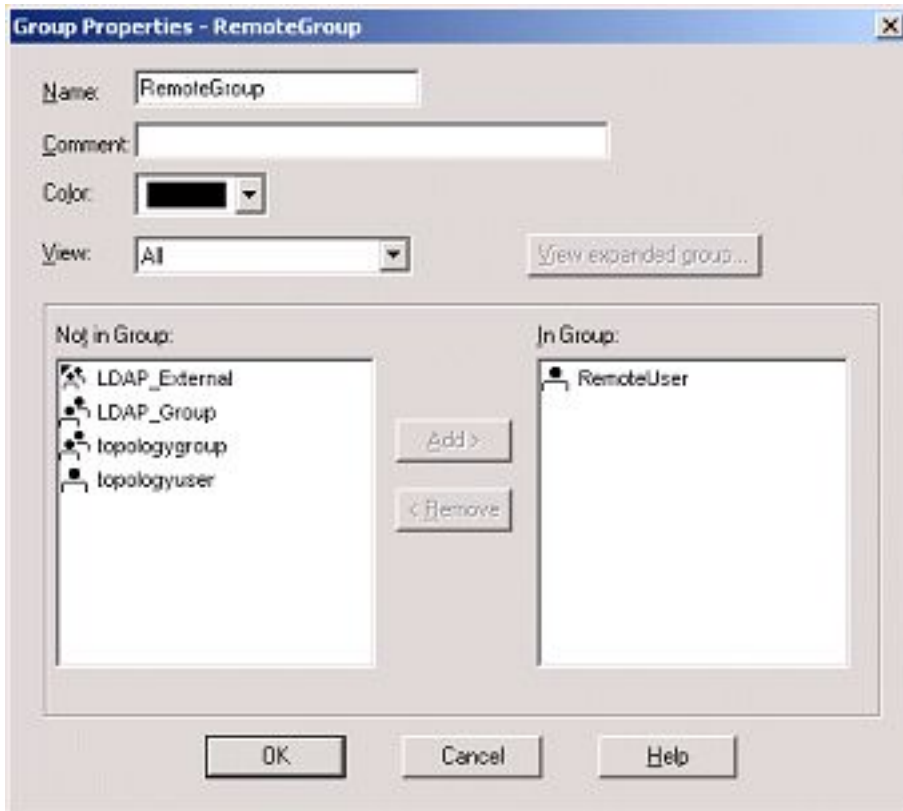
- 6 Select **OK** to finish.

### **Creating the Group**

- 1 In the **Policy Editor** on the Firewall select **Manage >> Users and Administrators ...**
- 2 On the **User** screen select **New >> Group**.
- 3 In the **Group Properties** screen enter in a **name** for the group.

- 4 Then from the **Not In Group** column select the user created above and select **Add>**.

### Remote Group Property



- 5 Select **OK** to finish.

### Modifying the Firewall Object

- 1 In the **Policy Editor** on the Firewall select **Manage >> Network Objects**.
- 2 In the **Network Objects** screen then select the **firewall object** and then **Edit**.
- 3 In the **VPN Section** select **Edit** for the **IKE Encryption Scheme**.

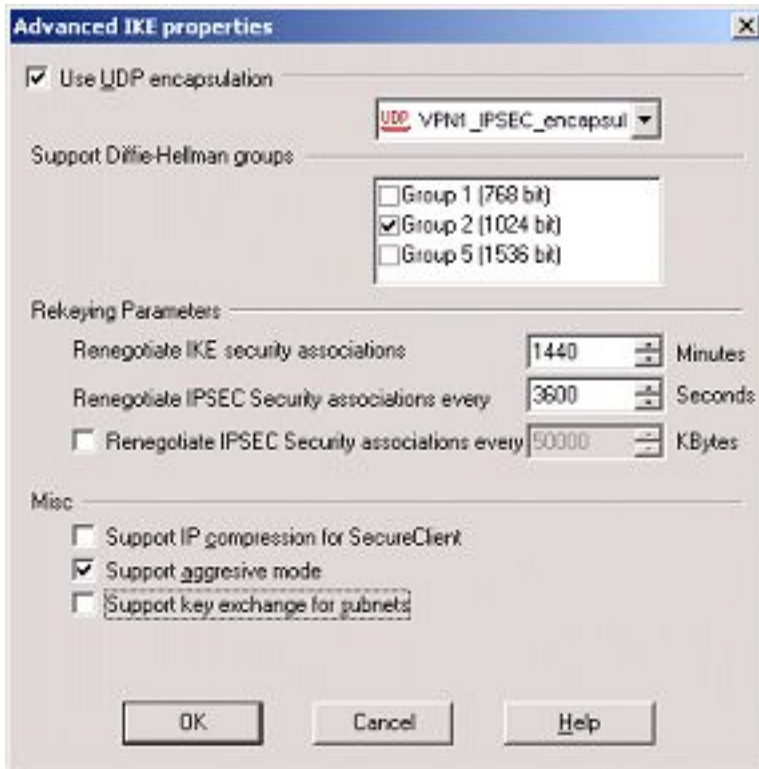
- 4 Make sure that **VPN-1 & Firewall-1 authentication for VPN-1 SecuRemote/SecureClient (Hybrid Mode)** is selected and then select **Advanced**.

### IKE Properties



- 5 In the **Advanced IKE properties** screen make sure that **Support aggressive mode** is selected in the **Misc** section.

### Advanced Properties



- 6 Select **OK**.
- 7 Select **OK**.
- 8 Select **OK** to finish.

### Rule Base

To tie these objects together you define a Rule in the Rule Base to allow the user to authenticate using Pre-Shared secrets.

### Authenticating with Pre-Shared Secrets

When users connect to the Firewall to create their Entrust digital ID they will be prompted to Authenticate themselves by providing the username and password of the pre-shared secret. To do this de-select **Use Certificate** and then enter in the **username**

(of the user created earlier - not the group name) and the **password** (of the same user created earlier). Then select **OK**. You should then receive an acknowledgement that the user is authenticated. At this point you will be able to finish creating your Entrust digital ID.

### Login with Pre-Shared Secrets



## Self-Extracting or Configurable Installation of VPN-1 SecuRemote

When downloading the VPN-1 SecuRemote client software from the Check Point web site you have the option of downloading the package in two installation types:

- **Self-Extracting Installation**
- **Configurable Installation**

The Configurable Installation allows you to add customized entrust.ini, userc.c and product.ini files to suit your environment. Refer to the VPN-1 SecuRemote release notes for more details.

To download the VPN-1 SecuRemote client (Self-Extracting or Configurable Installation) go to the Check Point web site at [http://www.CheckPoint.com/techsupport/downloads\\_sr.html](http://www.CheckPoint.com/techsupport/downloads_sr.html).

# Selecting the Entrust.ini

VPN-1 SecuRemote retrieves Entrust configuration details from the `entrust.ini` file. The following steps detail how to select the correct `entrust.ini` from within VPN-1 SecuRemote.

- 1 **Install VPN-1 SecuRemote NG** on the client machine, and reboot.
- 2 At this point the client would need to obtain a copy of the **entrust.ini** file from the Security Manager machine. (Depending on how you setup your install package this could be contained in the custom install of the VPN-1 SecuRemote client - or just added with it).

**Note:** The installation of VPN-1 SecuRemote NG may overwrite any existing `entrust.ini` file in the `WINNT` directory. This is controlled using the `OverwriteEntINI` setting (0=don't overwrite, 1=overwrite) in the Check Point `product.ini` file in its Configurable installation. Therefore it is important to check and make sure before proceeding that the `entrust.ini` file in the `WINNT` is the correct one.

- 3 The client would then place the **entrust.ini** file in the `WINNT` directory. (This will be the default location that Desktop Manager looks for the `entrust.ini` file.)
- 4 Then open up VPN-1 SecuRemote (**by double-clicking on the VPN-1 SecuRemote icon in the system tray**) and then select from the menu bar (**Certificates >> Select\_INI file**).

## VPN-1 SecuRemote Icon



- 5 Then **browse** to the location of the **entrust.ini** file in your `WINNT` directory.

# Selecting Entrust Entelligence™ Desktop Manager in VPN-1 SecuRemote

In VPN-1 SecuRemote you have the option to use the Desktop Manager Login screen (if Desktop Manager is installed on the machine) or VPN-1 SecuRemote Login screen when authenticating.

## Desktop Manager is not installed

Ensure that you have selected (on the menu bar **Certificates >> Enable/Disable Entrust Entelligence ..**) "**Don't use Entrust Entelligence in the future**". This is selected by default in the installation of VPN-1 SecuRemote. The VPN-1 SecuRemote login screen is now available for authentication.

If you need to create/recover your Entrust digital ID then you would simply select from the menu bar **Certificates >>** (Create or Recover) depending on which operation you need to perform. This would then invoke the VPN-1 SecuRemote User screen in which you would then fill in the necessary details.

## When you have both Desktop Manager and VPN-1 SecuRemote on the Client machine

Here you have two options.

### Select "**Don't use Entrust Entelligence in the future**"

This will allow you to use the VPN-1 SecuRemote login screen when authenticating, however you will still use the Desktop Manager wizard for digital ID creation/recovery.

### De-Select "**Don't use Entrust Entelligence in the future**"

This will allow you to use the Entrust Login when authenticating, as well as the Desktop Manager wizard for digital ID creation/recovery.

# Creating the Entrust digital ID for the VPN-1 SecuRemote Client

Once you have decided on the method for creating the Entrust digital ID, you will need to follow one of the following methods.

## Method 1 - Creating the Entrust digital ID on the Security Manager Administration.

- 1 Once the user has been added to the Active Directory and enabled for Entrust (as outlined earlier) you will need to select the user once again.

- 2 Now **right-click** on the user and select **Create digital ID**.
- 3 Enter in the **name** for the digital ID (this does not have to match the dn of the user, but should identify the user as to not cause confusion), location to save the digital ID and the password used to unlock the digital ID. (**Note: Use the Password Rules >> button to display the rules being used for setting the password**).

### Creating digital ID on the Security Manager Administration



- 4 Now you will need to securely transfer the digital ID to the VPN-1 SecuRemote user machine.

### Method 2 - Creating the Entrust digital ID remotely on the VPN-1 SecuRemote Client.

- 1 Securely distribute the reference number and authorization code to the end user. See the Entrust/Admin guide for more information on secure distribution techniques.

- 2 Establish an IPSec tunnel with the VPN-1 NG FP-1 on VPN-1 SecuRemote, using a **username** and **password** setup on the firewall as outlined earlier in the section **Creating an IPSec Tunnel using Pre-Shared Secrets**.
- 3 Once the tunnel is established then we can create the Entrust digital ID. On the menu bar of the VPN-1 SecuRemote client window select (**Certificates >> Create**).
- 4 **If You Do Not Have Desktop Manager Installed on the Machine**

This will then launch the Create User window. Follow the instructions entering in the name, path and password for the Entrust digital ID.

### **Creating digital ID Remotely on VPN-1 SecuRemote (SecuRemote)**

The screenshot shows the 'Create User' dialog box with the following details:

- Title Bar:** Create User
- Save Profile as:**
  - Save to file (with a 'Browse...' button)
  - Save to hardware token:
  - Text field: D:\Test Profiles\Secure 1.epf
- Please select a password for your profile:**
  - User Password: [masked]
  - Verify Password: [masked]
- Please specify your profile parameters:**
  - Reference Number: 99359583
  - Authorization Code: GCQB-6w/R9-FGT8
- Buttons:** OK, Cancel, Help

5 **OR If You Have Desktop Manager Installed on the Machine**

This will launch the Desktop Manager digital ID Creation Wizard. Simply follow the steps and enter in the information to complete the digital ID creation.

**Creating digital ID Remotely on VPN-1 SecuRemote (Entrust)**

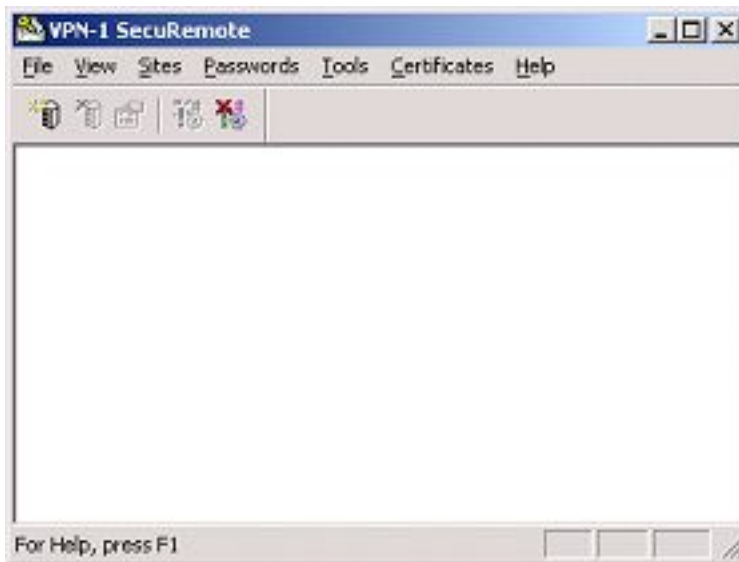


# Downloading the Firewall Topology

In order to communicate with the Firewall, you will need to download the topology information that you need for the communication. To do this:

- 1 In the VPN-1 SecuRemote client window, from the menu bar select (**Sites >> Create New**).

## VPN-1 SecuRemote Client Window



- 2 Enter in the IP Address of the external interface of the VPN-1 NG FP-1 that you are going to authenticate with. Then select **OK**. Refer to Check Point documentation for methods of avoiding this step by distributing a **userc.c** file with a customized installation package.
- 3 In the VPN-1 SecuRemote Authentication window you will need to select the digital ID you created earlier to authenticate with. (Depending on the method of creating the digital ID you may have to browse to the location where you stored your digital ID, for first time use.)

- 4 Enter in the **password** to unlock your Entrust digital ID.

### VPN-1 SecuRemote Login Screen



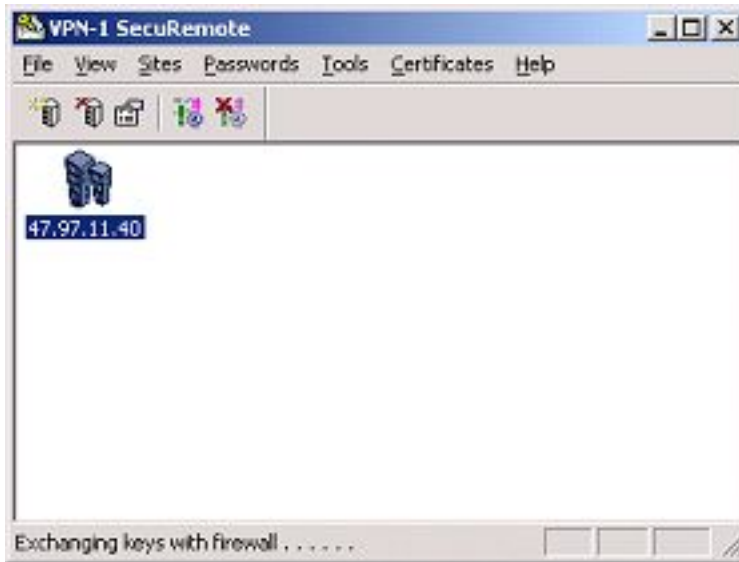
- 5 You will then have to verify the **DN information** of the VPN-1 NG FP-1 as given to the remote client by the VPN-1 NG FP-1 Administrator. If it is valid then select **OK**.

### Verifying the DN of VPN-1 NG FP-1



- 6 At this point you have downloaded the site topology needed to connect and establish your IPSec tunnel.

### VPN-1 SecuRemote Window with Site Topology



## Switching to Client Connect Mode from Transparent Mode

VPN-1 NG FP-1 allows VPN-1 SecuRemote to use a new mode called "**Connect Mode**". This allows the client to **connect** to the firewall (establish the IPSec tunnel) or **disconnect** from the firewall (take down the IPSec tunnel) manually. By default the VPN-1 SecuRemote client is already in Transparent mode. In testing this configuration **Connect Mode** was used to establish the IPSec tunnel. Therefore the remaining sections will make use of this method.

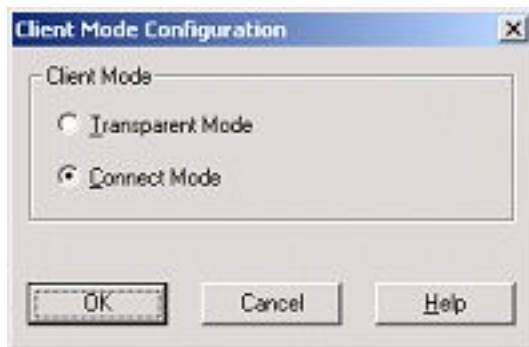
However to note either mode will work in establishing the IPSec tunnel. The big difference is in how it is done. Connect mode offers a manual connect/disconnect of the IPSec tunnel, whereas Transparent mode has the connection made for the client behind the scenes as the client initiates communication with the Firewall.

**Note: You must already have downloaded the site topology before switching to this mode.**

To switch from transparent mode (which is the default mode in the installation) to connect mode simply do the following:

- 1 Bring up your VPN-1 SecuRemote window (**Left-click** on the **VPN-1 SecuRemote icon** in the system tray).
- 2 Select from the menu bar (**Tools >> Configure Client Mode ..**)
- 3 Select **Connect Mode** and select **OK**.

### **Client Connect Mode**



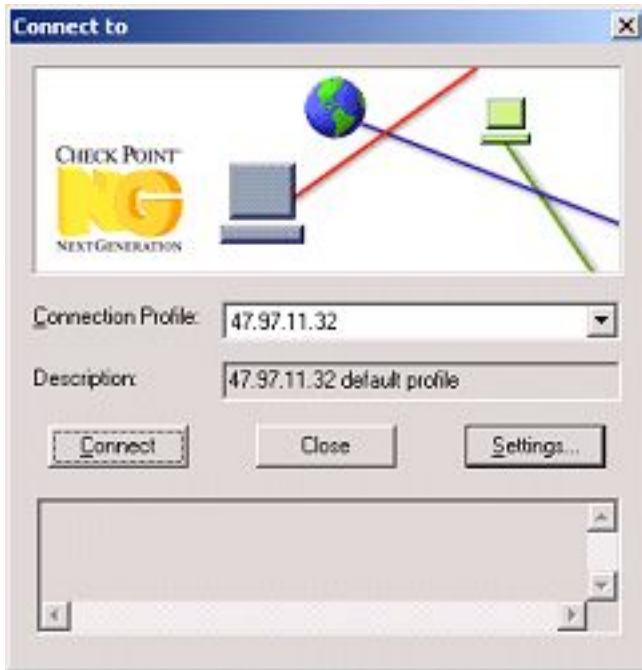
- 4 You will then have to **restart** VPN-1 SecuRemote for this change to take effect.
- 5 **Right-click** the **VPN-1 SecuRemote icon** in system tray and select **Stop VPN-1 SecuRemote**.
- 6 Select VPN-1 SecuRemote from your **Start > Programs > Check Point VPN-1 SecuRemote > SecuRemote** (or **shortcut** on your desktop).

You have now switched to the Connect Mode of the client.

## To Connect to the Firewall

- 1 **Left-click** on the **VPN-1 SecuRemote icon** in the system tray.
- 2 In the **Connect to** window select your **Connection digital ID** of the firewall that you want to connect to.

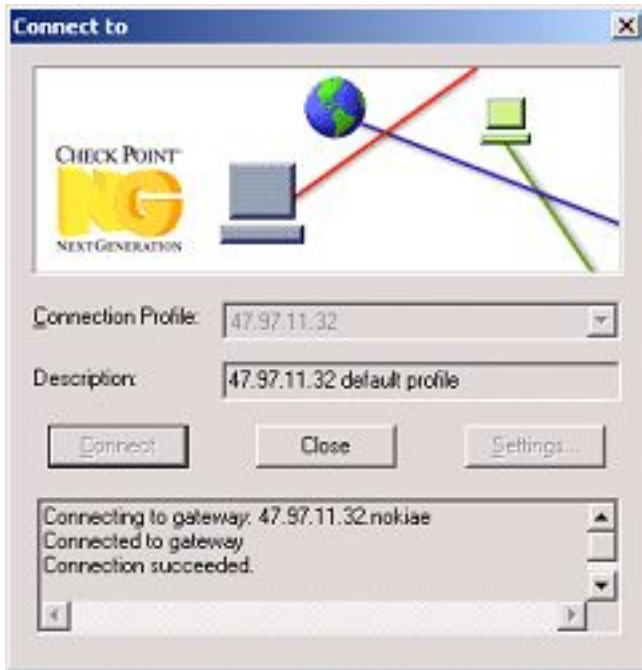
### Connect Window



- 3 Select **Connect**.
- 4 Authenticate to the firewall by logging into it in at the prompt.

- 5 If authentication is successful the **Connect to** window will disappear. At this point you should have access to your internal network.

### Client Connect Message



## To Disconnect from the Firewall

- 1 **Left-click** on the **VPN-1 SecuRemote icon** in the system tray.
- 2 Here a **VPN-1 SecuRemote Connection Status** window will be displayed. Simply select **Disconnect** and your IPsec tunnel is removed.

### Client Disconnect



**Note:** Transparent mode will not require the user to manually connect to the firewall. When data is sent to the firewall that needs to be encrypted it will trigger authentication and establish the IPsec tunnel.

## Authenticating to Create the IPsec Tunnel using Transparent Mode

As mentioned earlier Transparent Mode is the default mode (unless customised differently) for the VPN-1 SecuRemote client. You will need to explore and decide the mode you want your VPN-1 SecuRemote clients to use. You only need to use one, as both are not required together to establish the IPsec tunnel.

If using Transparent mode with VPN-1 SecuRemote, and you are ready to establish an IPSec tunnel with your Entrust digital certificate to communicate securely with your VPN, then refer to the following sections.

To establish/authenticate the tunnel:

- 1 If VPN-1 SecuRemote client is running then as soon as you communicate with the Firewall (Telnet, FTP, Ping, etc.) you will be prompted to authenticate yourself.
- 2 When this happens you will see the VPN-1 SecuRemote (or Desktop Manager) login prompt. Select your **Entrust digital ID** and enter the **password**. Click **OK**.
- 3 At this point you should see a response back from the firewall saying that you have been authenticated. If you get an error, then refer to the section at the end on Troubleshooting or refer to the following knowledge bases.

**Entrust Knowledge Base - <https://www.entrust.com/support/> (Select Knowledge Base)**

**Check Point SecureKnowledge Base - <http://support.checkpoint.com/login.html>**

### **Authentication to VPN-1 NG FP-1**



- 4 If successful you should be able to gain access to your internal network.

## **Key Updates**

The tested version of the VPN-1 SecuRemote client does not take advantage of some of the Entrust features, such as automatic key updates, since it operates in what Entrust refers to as "Offline" mode. Once the VPN connection is established and the Authority Security Manager and Directory are accessible, Desktop Manager can be used to switch to 'online mode', or "Connected to Entrust". To do this (**right-click** on Entrust key icon in system tray and select **Log In to Entrust**, making sure to have "**work off-line**" **deselected**). If you are in a key update period, you will be notified that your keys have

been updated.

Note: That the testing of this with the Desktop Manager installed had the option **Don't Use Entrust Intelligence in the Future** deselected on the VPN-1 SecuRemote client.

# Chapter 5

## Defining Access Controls based on User DN

Once a user is authenticated, the next step is to determine where they can go and what they can do, also known as authorization and entitlements. Check Point provides mechanisms to achieve this built around groups. This chapter describes some examples of how users are assigned to groups based on the information contained in their Digital ID, specifically in their Distinguished Name or DN.

# Overview of Method Used

This method makes use of Groups, External Groups, LDAP Account Units, Templates and Rules in the Rule Base.

## Groups

A group is used to define a group of users that you want to have the same restrictions/access. It is this group that you will include in the Rule Base granting/restricting access.

## External Groups

External Groups will become members of the Groups, but will also define the LDAP Account Unit that you will use to bind to your LDAP Server to fetch the information at the branch level indicated. Here you will also be able to place restrictions on the DN (ie. Searchbase where the user was created) for access. You can also restrict within the group (branch) by using a prefix filter.

## LDAP Account Units

This is where you indicate the location of the LDAP Server, login information to bind with the LDAP Server, branches to fetch, and template to use.

## Templates

Here is where you indicate the use of Public Key encryption along with other details such as Access Times, Source, Destination, etc.

## Rule Base

The rules in the Rule Base will grant or restrict access to the various groups. Groups can be placed in the Source of the rules, then restricting their Destination and Service, while having to Encrypt the data.

# Sample Setup

This section will outline a simple setup between two groups of users.

- PKI Users
- Firewall Administrators

In this example the DN (branch) of each group is as follows:

- PKI Users - ou=PKI Users, dc=Entrust, dc=com
- Firewall Administrators - ou=FW Admin, dc=Entrust, dc=com

### Creating or Modifying an LDAP Account Unit

Unless you are using multiple LDAP Servers you will only require one LDAP Account Unit for this sample. If you have already configured your LDAP Account Unit then you can simply modify this, instead of creating a new one. If this is the case then **skip to step 9** only.

- 1 If you have not already created an LDAP Account Unit you will need to change your Global Policy to include User Management in the LDAP Account. Select **Policy >> Global Properties ...** Here select the **LDAP Account Management link** on the left. Select the **Use LDAP account management** option.
- 2 For the PKI Users and the Firewall Administrators simply create a group for each on the Policy Editor for the Firewall. (**Manage >> Servers >> New >> LDAP Account Unit**)
- 3 Enter in a **name** for the LDAP Account Unit (Example: LDAP\_Account).
- 4 Select both **CRL Retrieval** and **User Management** from the "Account Unit Usage" section.
- 5 In the **Host** drop-down list select the **LDAP Server object** that you have created earlier in this guide.
- 6 Enter in the **DN** and **Password** for the user that you are going to bind to the directory.
- 7 Select the **LDAP Rights** that this user has.
- 8 Select the **LDAP Server digital ID** to the LDAP Server that you are using. (Example: Microsoft\_AD)
- 9 Under Branches select **ADD** and add the branch for the groups that you are using. (Example: PKI Users - ou=PKI Users, dc=Entrust, dc=com and Firewall Administrators - ou=FW Admin, dc=Entrust, dc=com).
- 10 On the **Users** tab select Use Default User Template: and select the Template that

you will create later. (example: VPN\_Template)

- 11 Select **OK** to save.

### Creating External Groups

- 1 For the PKI Users and the Firewall Administrators create a group for each on the Policy Editor for the Firewall. (**Manage >> Users and Administrators >> New >> External Group ..**).
- 2 Enter the **Name** for each **External Group** (Example: PKI\_External and FWA\_External).
- 3 In **Account Unit** select the Account Unit you created or modified above. (Example: LDAP\_Account).
- 4 Then select the option under **Group's Scope** to **Only Subtree** and then select the branch that you enter in the LDAP Account Unit to match the group's DN.

### Creating the Groups

- 1 For the PKI Users and the Firewall Administrators simply create a group for each on the Policy Editor for the Firewall. (**Manage >> Users and Administrators >> New >> Group**)
- 2 Enter the **Name** for each group (Example: PKI\_Group and FWA\_Group).
- 3 In the **Not In Group** select the **External Group** that you created earlier (Example: PKI\_External for PKI\_Group and FWA\_External for FWA\_Group).
- 4 Save each by selecting **OK**.

### Creating Template

Unless you want to change the Access Times, etc. you will only require one template.

- 1 For the PKI Users and the Firewall Administrators simply create a group for each on the Policy Editor for the Firewall. (**Manage >> Users and Administrators >> New >> Template**).

- 2 Give the template a **Login Name** on the **General** Tab. (Example: VPN\_Template)
- 3 On the **Groups** tab, select in the **Available Groups** column the groups (**Not External Groups**) that you created earlier (Example: PKI\_Group and FWA\_Group) and then **ADD** these.
- 4 On the **Encryption** Tab select **IKE** for the **Client Encryption Method** and then select **EDIT**. Making sure that you select **Public Key** in this new window.
- 5 Select **OK**.
- 6 Select **OK** to save.

### Rules in the Rule Base

Once you have this setup then the next step is to add rules to your rule base to grant/restrict the users access to the internal network. Such as restricting the PKI\_Group to the Security Manager machine only and the FWA\_Group to both the Policy Editor machine of the Firewall and Security Manager. You can further restrict the access of services they are allowed in the rule base. The same example could be used to limit access to protected resources such as web servers, email, etc.

### Testing Results

Once you have installed the new policy on the firewall with the above additions, you have then restricted access to each of these groups. To test this out simply create different users in each of these groups. Then once you have the client's digital ID, log into the Firewall with each digital ID. What you will notice is that the user in the PKI Users branch will have access to the Security Manager machine but not to the the VPN-1 NG FP-1 Policy Editor machine. Also the user from the FW Admin branch will have access to both the VPN-1 NG FP-1 Policy Editor machine and the Security Manager machine.

These mechanisms can be used to build access control rules.



# Chapter 6

## Working with an Entrust Subordinate CA

This section will discuss the use of Entrust Subordinate CAs with VPN-1 NG FP-1. Also note that in testing, both the Entrust Root and Subordinate CA shared the same Active Directory. Each had its own CA entry in the directory.

# How to setup Entrust Subordinate CA with VPN-1 NG FP-1

Configuration is much the same as with the Root CA (check the documentation in the guides that come with your Security Manager software on how to setup an Entrust Subordinate CA).

The previous setup with a Root CA required at minimum two user certificates.

- 1 One for the Firewall itself (along with retrieving the Root CA certificate in the CA Server object created).
- 2 One for the VPN-1 SecuRemote Client user.

For the Subordinate CA this will be the same. However the certificates for both will have to come from the Subordinate CA itself. So once you have the Subordinate CA configured and working, simply make sure you use the `entrust.ini` file from the subordinate CA, and digital IDs created from it.

**Note: Testing was with Desktop Manager 6.0 with the patch 46190EN along with the VPN-1 SecuRemote NG FP-1 on the client workstation. If you did not include Desktop Manager on the client machine and then created the Entrust digital ID you will only have the digital ID's \*.pch (policy certificate) and \*.epf (user digital ID) created. Then when you try and authenticate to the VPN-1 NG FP-1 (using Subordinate Certificates) you would receive the error:**

**The digital certificate could not be verified. Possibly the signer's key file has not been imported into your personal address book.**

Therefore with this version of VPN-1 SecuRemote you need Desktop Manager included to work in a heirarchy.

# Chapter 7

## How do you know if it is working?

# How do you know if it is working?

This section lists some brief tests that can be done to confirm if your configuration is working. This is not an absolute list.

- 1 Download/Update the Site Topology from the VPN-1 NG FP-1 successfully.
- 2 Authenticate a user to the VPN-1 NG FP-1 using Entrust digital certificates successfully.
- 3 Have access to your internal network (where you did not have access before authenticating).
- 4 Revoke the certificate of a test user and push a new CRL to the LDAP Server. Then try to authenticate as this user to the firewall. If you have the firewall configured so that the cached information of the user is not kept or not for a long period of time, then it should state the user's certificate is revoked and not allow you to establish an IPSec tunnel. (Refer to the section on **Creating Certificate Authority Server Object** for the information on the settings for the CRL retrieval)

# Chapter 8

## Troubleshooting

This section is a guide to assist you in case you run into problems along the way. This is not an exhaustive list of errors but should help guide you to a resolution. Refer to the Entrust Support web site ([www.entrust.com](http://www.entrust.com)) and the Check Point Web Site ([www.checkpoint.com](http://www.checkpoint.com)) [user id and password required for both] for the latest updates and error listings.

# Error Login to Entrust CMS

## Problem

When trying to initialize or recover the Firewall object certificate using the Entrust/PKI method you get the error:

## Error Login to Entrust CMS

### genkey Key creation failed for (firewall machine name)

There will be no information contained in the CA log files (manager.log and mgraudit.log) on the Security Manager machine, and the operation of initializing/recovering the Firewall digital ID fails.

## Solution

Note that the use of the Entrust/PKI enrollment method is no longer supported by Entrust. This tech note is provided for completeness since the feature still appears in Check Point GUI's.

The entrust.ini file being used by the VPN-1 NG FP-1 has Fips Mode turned on.

### [FIPS Mode]

#### FipsMode=1

Therefore the VPN-1 NG FP-1 fails on the FIPS Mode check and cannot login into the Entrust CMS toolkit. To solve this problem you will need to modify the entrust.ini file and change the value above from 1 to 0.

#### FipsMode=0

To put this change into effect you will need to reselect the entrust.ini file for the Entrust CA server object that you created earlier.

- 1 Select **Manage > Servers** from the Menu Bar of the VPN-1 NG FP-1.
- 2 **Double-click**(or select the object and then select **Edit**) on the **Entrust CA** server object created earlier.
- 3 Select the **Entrust PKI** tab and select **Get** under the "**Configuration**" selection to select the **entrust.ini** file.
- 4 Browse to the location of the modified **entrust.ini** file, select it and select **Open**.

5 select OK.

When this is done then retry to initialize/recover the Firewall user.

## Failed to register key (-3236) ASN.1 encoding/decoding failure

### Problem

When trying to initialize or recover the Firewall object certificate you get the error:

#### Failed to register key (-3236) ASN.1 encoding/decoding failure

In the manager.log file on the CA you will see something like:

```
[-02923 Infrastructure Error.] Received PKIX error message from '(Reference Number Used)' [-996, '(-996)'].
```

In the mgraudit.log file you will see something like:

```
[-07805 PKIX key recovery request error.] Event: Done to > '(Reference Number Used)' : Received PKIX error from '(Reference Number Used)' [-996, '(-996)'].
```

```
[-07866 Failed to receive key recovery acknowledgment from the client application. The new user certificate has been revoked.]
```

This example was for recovering the user, but the same results would occur for initializing the user as well.

### Solution

Note that the use of the Entrust/PKI enrollment method is no longer supported by Entrust. This tech note is provided for completeness since the feature still appears in Check Point GUI's.

The problem here is that the Client Application (VPN-1 NG FP-1) made a request to the Security Manager to have its digital ID initialized/recovered. Since we are using Microsoft Active Directory (DC components) the reply back to the client application was not understood. Therefore the Security Manager failed to get a response back from the Client and revoked the client's certificate.

The entrust.ini file does not have the information contained (or is partially missing or incorrect) for DC Components. Therefore check back to the section "**Modifying the Entrust.ini file**" in the Chapter on **Preparation** to make the necessary changes.

Once the entrust.ini file is modified then:

- 1 Select **Manage > Servers** from the Menu Bar of the VPN-1 NG FP-1.
- 2 **Double-click** (or select the object and then select **Edit**) on the **Entrust CA** server object created earlier.
- 3 Select the **Entrust PKI** tab and select **Get** under the "**Configuration**" selection to select the **entrust.ini** file.
- 4 Browse to the location of the modified **entrust.ini** file, select it and select **Open**.
- 5 select **OK**.

You will then need to set the VPN-1 NG FP-1 User into Key Recovery. (Check the Entrust Admin Guide for details on Key Recovery) Then recover the firewall user's certificate on the Firewall object.

## Failed to register key: Internal Error: (-1666)

### Problem

When trying to initialize or recover the Firewall object certificate you get the error:

**Failed to register key: Internal Error: (-1666)**

On the Security Manager in the manager.log you see:

**[-02908 The system time at the key management service and the client application differ by more than 2 hours.]**

### Solution

Note that the use of the Entrust/PKI enrollment method is no longer supported by Entrust. This tech note is provided for completeness since the feature still appears in Check Point GUI's.

The problem here is that the client machine (VPN-1 NG FP-1) and the Security Manager are out of sync by more than 2 hours (the buffer Entrust allows). Therefore you would check the DATE/TIME/TIME ZONE on the client machine and compare that to the Security Manager machine.

When changing the DATE/TIME/TIME ZONE it is best to change it on the client application (if it does not mind a time change). As changing the time on the Security Manager can throw certificates out of their validity period. If you need to change the time on the Security Manager machine it is best to check with Entrust Support to see if this will cause any problems for you.

## Users Authenticate Successfully but cannot Access the Internal Network

There could be a number of reasons for this. However here are a couple to check out.

- 1 It maybe possible that the flag "**Exportable for VPN-1 SecuRemote/SecureClient**" was **not** selected under the **Firewall Network** object in the **Topology** section. If not then the VPN-1 SecuRemote client does not know about the network topology and cannot gain access. Check this **flag** and then select **OK**. After this you will have to **install/re-install** a new Policy on the Check Point Firewall. Refer to the section **Installing the Security Policy on the Firewall** in this guide.
- 2 Are there network issues beyond the firewall itself. In otherwords the VPN-1 SecuRemote client can get to the Firewall to authenticate but could not find its destination. Always check the Log Viewer on the VPN-1 NG FP-1 to give you more clues to the problem.

## Error: Communication with gateway (Gateway Name) at site xxx.xxx.xxx.xxx failed

### Problem

There could be many reasons why this error occurs. Some of them include:

- 1 Network connectivity is not established between the client and firewall.
- 2 The firewall has lost connection to the LDAP Server and as a result the Firewall logs reports the action being dropped because user is unknown.
- 3 The VPN-1 NG FP-1 is down.

## Solutions

You will need to check the following.

- 1 There is connectivity between the firewall and client.
- 2 Check to see if there is connectivity between the firewall and LDAP server.
- 3 Check to see if the Firewall services are running.

# Error: Site xxx.xxx.xxx.xxx says that it is not a Certificate Authority.

## Problem

When trying to download the topology of the VPN-1 NG FP-1 onto the VPN-1 SecuRemote machine you receive the error:

**Error: Site xxx.xxx.xxx.xxx says that it is not a Certificate Authority.**

## Solution

On the VPN-1 NG FP-1 from the menu bar (**Policy >> Global Policy**) in the **Desktop Security** section "**Respond to unauthenticated topology requests (IKE and FWZ)**," is selected. You will need to **deselect** this option and then **re-install** the Policy on the Firewall.

# Negotiation with gateway at site xxx.xxx.xxx.xxx has failed. Certificate is revoked.

## Problem

As the error suggests the client cannot authenticate to the firewall because their Entrust certificate is revoked. When authenticating to the firewall it checks the Entrust CRL to see if the user's certificate is revoked. If it is then it will display the error:

**Negotiation with gateway at site xxx.xxx.xxx.xxx has failed. Certificate is revoked. (DN of the user revoked)**

when the user tries to authenticate.

### Solution

The user will have to be recovered through the Security Manager Administration. Again the process can be completed on the Security Manager Administration and the new digital ID then sent to the client, or they can establish a tunnel to the Firewall and use the **authorization code** and **reference number** to complete the Recovery (On the VPN-1 SecuRemote window you would select **Certificates >> Recover**).

Once the user is recovered they should be able to authenticate to the firewall.

## Negotiations with gateway at site xxx.xxx.xxx.xxx has failed. User (DN) unknown.

### Problem

When you try authenticating to the VPN-1 NG FP-1 you receive the error:

**Negotiations with gateway at site xxx.xxx.xxx.xxx has failed. User (DN) unknown.**

Therefore the client is unable to authenticate.

### Solution

The problem is the LDAP Account Unit is trying to find this user in the LDAP Server and cannot. This could be caused by many different reasons.

- 1 The user is not in the LDAP server. Check and make sure the user Exists.
- 2 The information contained on the LDAP Account Unit is incorrect. This would be especially true if all users where having this problem. Check the properties on the firewall for the LDAP Account Unit that you created. Such as the dn and password of the directory administrator that you are binding with. The directory object that you have selected and port number. Also the branch(es) that you are fetching. If the branch is lower than the level the user is on it will not see the user.

One of the tests you can perform is to select the "**Users**" tab in the left-hand pane of the **Policy Editor** window.



Here you will see the **LDAP Account Units** that you have defined. Simply **double-click** on your **LDAP Account Unit** and it will then **bind** to your LDAP server. It will then display the branches that it fetches. From here **double-click** on the level where the users are added and then check to the **right-hand** window pane to see if you see the user listed. If not then the user may not exist or is in the wrong branch.

If you receive an error "**Binding to LDAP Server: Failed to bind to the LDAP server - wrong password or wrong login dn**", then go back and check the LDAP Account Unit defined to make sure the **Directory Administrator information** is correct.

- 3 There maybe some network problems getting to the LDAP Server.

## Could not validate the Certificate used by gateway

### Problem

This error came as a result of our testing of the environment. We were testing what would happen when we had the Firewall certificate set for key expiry and then allowed the certificate to expire. Since this was the last test of the day we did not reset the key update options nor did we recover back the certificate. The next day we then started by trying to authenticate to the firewall with the VPN-1 SecuRemote client. As a result we got the error on the client:

**Could not validate the Certificate used by gateway xxx.xxx.xxx.xxx at site xxx.xxx.xxx.xxx CA Certificate is missing in the token.**

On the firewall log viewer we saw:

**IKE: Main Mode Received Notification from Peer: invalid certificate**

When we checked the status of the Firewall certificate in the Security Manager Administration we discovered the certificate was expired and we have not recovered the digital ID.

### Solution

To solve this problem you would need to **recover** the firewall certificate if it has **expired**, in the Security Manager Administration. Also before recovering the firewall certificate take a look at the **Key Update** options for that user (**Double-click** this user and bring up their **property screen** (in Security Manager Administration) and then select the "**Key Update Options**" tab). Make sure you have the correct options selected here before you recover the digital ID.

Once the digital ID was recovered back to the firewall, it resolved our problem.

## **(-11530) Client was expecting a DN change**

### **Problem**

During logging into Entrust Login through the IPSec tunnel the user may experience the error:

**"(-11530) Client was expecting a DN change but new certificate from CA did not contain a DN change"**

The cause here is that the user in Entrust can see their directory entry but cannot find their certificate in this directory entry. As a result Entrust believes the user is set to a state of **"DN Change"**. However the account information on the CA itself does not indicate this. The problem is the client does not have sufficient access to the directory to be able to view their certificate.

### **Solution**

The solution is simple in nature, give the client permission to view their certificate. However it is complicated by the nature of giving this permission. As stated in the beginning of this document there are two possible methods:

- 1 Have them login to the domain.
- 2 Give users anonymous read access to the Directory.

In either case the solution will depend on your setup and corporate policy on security.

**Note: For more troubleshooting information you can use the Entrust and Check Point Knowledge bases located at:**

**Entrust Knowledge Base - <https://www.entrust.com/support/>**

**(Here to search the knowledge base select "Knowledge Base".)**

**Check Point SecureKnowledge Base - <http://support.Check Point.com/login.html>**

**(Username and password required for both)**

# Cannot Complete Certificate Chain

## Problem

When trying to authenticate a user on VPN-1 SecuRemote client with VPN-1 NG FP-1 using a Subordinate CA you receive the error:

**Negotiation with gateway XXX at site xxx.xxx.xxx.xxx has failed. Cannot complete certificate chain (User DN).**

One of the causes of this could be that the digital ID you are trying to authenticate to the firewall with is a digital ID created with the Root CA. The firewall certificate has its certificate with the Subordinate CA. Therefore when it looks at the certificate that it is signed with (verifying) it does not know about the certificate chain of the Subordinate to the Root CA. Also in this test both the Root CA and Subordinate CA had entries in the same Microsoft Active Directory.

## Solution

Make sure the digital ID being used is with the same CA (Subordinate or Root).

# The Digital Certificate could not be Verified

## Problem

When using VPN-1 SecuRemote NG FP-1 without Desktop Manager on the client machine and using certificates in an Entrust CA Hierarchy, the user authenticating may see the following error displayed:

**The digital certificate could not be verified. Possibly the signer's key file has not been imported into your personal address book.**

The problem is associated to the files that the client has created and cached to the local system. With VPN-1 SecuRemote NG FP-1 only on the machine the client will only be able to create the user's files **\*.epf** and **\*.pch** associated with the user's digital ID. Therefore it will not have information about the **CRL** and **ARL** that is associated with the CA Hierarchy and not be able to verify the signature from the Subordinate CA.

## Solution

The solution would be to install the Desktop Manager 6.0 (patch 46190EN) client on the client machine as well. Then when the user creates their digital ID they will also create the **\*.epf**, **\*.pch**, **\*.xcc**, **\*.pab**, **\*.ckl**, **\*.crl**, **\*.cch**, **\*.arl** files associated with this digital ID.





# Chapter 9

## Known Issues

This section contains a small list of known issues relating to the present setup of using VPN-1 NG FP-1.

# Known Issues

The following are known issues at time of writing for customers using Check Point NG FP1 with Entrust products. Refer to the Entrust Support Knowledge Base ([www.entrust.com](http://www.entrust.com)) [Username and Password required] for current status.

## Issue 1 - Using Entrust Entelligence with the VPN-1 SecuRemote NG client build number 51057.

- 1 When you have deselected '**Don't use Entrust Entelligence in the Future**' (**Certificates > Enable/Disable Entrust Entelligence** on the VPN-1 SecuRemote client) and therefore will use the Entrust Entelligence login screen to authenticate. At this point the **Browse** button becomes **disabled**, not allowing you to select your Entrust digital ID.

### Workaround

Use the **Entrust Key Icon** in the system tray to login to Entrust **off-line** first. (**Right-click** then '**Log In to Entrust**'. Then make sure '**Work Off-line**' is selected.) Then **log out** of Entrust from the **Entrust Key Icon**.

At this point you will then have the correct digital ID on the Entrust Login screen when authenticating.

**Note: Check Point has a hotfix available (SHF\_DT\_FP1\_0001.zip) if you are running VPN-1 SecuRemote NG FP-1 and using a version 5.x of the Entrust/PKI. Contact Check Point Support. This hotfix resolves this issue.**

- 2 After authenticating the IPSec tunnel, VPN-1 SecuRemote does not log you into Entrust Entelligence. This is a known issue reported on the Check Point site with the work around as applying the Hot Fix from Check Point (as discussed in the previous issue).

Another workaround to this issue you can manually login on-line or off-line to Entrust after you established the IPSec tunnel. (**Right-click** on **key icon** in system tray and select **Login To Entrust**).

**Note: Check Point has a hotfix available (SHF\_DT\_FP1\_0001.zip) if you are running VPN-1 SecuRemote NG FP-1 and using a version 5.x of the Entrust/PKI. Contact Check Point Support. This hotfix resolves this issue.**

Both of these fixes are scheduled to be included in VPN-1 SecuRemote NG FP-2.

## Issue 2 - VPN-1 SecuRemote Only Installed on the Client Machine

VPN-1 SecuRemote NG (build 51057) does not allow Entrust users without Entelligence Desktop Manager installed to change from offline to online operations. To enable online operations, such as Entrust's automatic key update, with this version of VPN-1 SecuRemote NG, Entelligence Desktop Manager must be installed.

## Issue 3 - Trying to get Entrust/SignOn working with VPN-1 SecuRemote

At present Entrust/SignOn will not work with VPN-1 SecuRemote NG FP-1. This is due to be fixed in the FP-3 release of VPN-1 SecuRemote NG.

# Microsoft Active Directory Support

Binding to the Microsoft Active Directory can be accomplished through either Windows Authentication (by default) or by anonymous bind. Anonymous binding is not enabled by default in Active Directory. For the purposes of this solution guide anonymous read access was granted on the Active Directory for two reasons:

- 1 The version of Check Point VPN-1 tested (NG FP1) did not natively support Active Directory and therefore without anonymous read access it could not bind to the directory to retrieve CRLs.
- 2 If the client does not make use of Windows Authentication when they log into their computer they will not be able to bind to the Active Directory and thus will not be able to go On-Line with Entrust for key management. Note this requires that the `entrust.ini` is configured for anonymous bind to Active Directory using

**AuthMethod=anonymous**

on the client `entrust.ini` file under the section **[Directory Connection Settings]**.

When using VPN in a Microsoft Active Directory environment you should be aware of the compatibility of both the Gateway and Client when rolling this out. Verify how the specific version of the VPN product works with Active Directory and also check the Entrust Support Web Site (<https://www.entrust.com/support/>) for updates.



# Chapter 10

## Appendix A - Additional Reference Material

# Entrust Documentation

In addition to the documentation provided on the software CD's, many documents are available on the Entrust Support Web Site ([www.entrust.com/support/](http://www.entrust.com/support/)). The following are documents relevant to customers deploying Entrust with Check Point VPN Products.

## Entrust Security Manager 6.0

### Release Notes

[Location -  
[https://www.entrust.com/support/documentation/product\\_docs.cfm?folderID=745](https://www.entrust.com/support/documentation/product_docs.cfm?folderID=745)]

- **ReadMe 6.0 for Windows OR ReadMe 6.0 for UNIX**

### User Guides

[Location -  
[https://www.entrust.com/support/documentation/product\\_docs.cfm?folderID=746](https://www.entrust.com/support/documentation/product_docs.cfm?folderID=746)]

- **Installing Entrust/PKI 6.0 on Windows OR Installing Entrust/PKI 6.0 on UNIX**
- **Administering Entrust/PKI 6.0 on UNIX OR Administering Entrust/PKI 6.0 on Windows**
- **Using Entrust/PKI 6.0 on Windows OR Using Entrust/PKI 6.0 on UNIX**

### White Papers

[Location -  
[https://www.entrust.com/support/documentation/product\\_docs.cfm?folderID=747](https://www.entrust.com/support/documentation/product_docs.cfm?folderID=747)]

- **Using Microsoft Active Directory**
- **Schema Requirements with Active Directory**

## Entrust Authority Enrollment Server for VPN

The documentation for this can be found directly on the CD or on the computer once installed (c:\Program Files\Entrust\Enrollment Server for VPN\)

- **user\_guide.pdf**
- **release\_notes.pdf**

### **Entrust Authority Self-Administration Server**

The documentation for this can be found directly on the CD or on the computer once installed (c:\Program Files\Entrust\Self-Administration Server\Documentation\)

- **release\_notes**
- **Self-Administration Server Guide**

### **Desktop Manager 6.0**

[Location -  
[https://www.entrust.com/support/documentation/product\\_docs.cfm?folderID=560](https://www.entrust.com/support/documentation/product_docs.cfm?folderID=560)]

- **Quick Start Guide**
- **ReadMe 6.0**

### **Desktop Manager 6.0 SP1**

[Location -  
[https://www.entrust.com/support/documentation/product\\_docs.cfm?folderID=730](https://www.entrust.com/support/documentation/product_docs.cfm?folderID=730)]

- **Release Notes**

# Check Point Documentation

See the Check Point Support Web Site (<http://www.checkpoint.com/support/technical/documents/index.html>) for the following useful documents.

## Check Point NG FP-1

[Location - [http://www.checkpoint.com/support/technical/documents/docs\\_ngfp1.html](http://www.checkpoint.com/support/technical/documents/docs_ngfp1.html)]

- **NG FP1 Getting Started**
- **NG FP1 Management Guide**
- **NG FP1 User Management Guide**
- **NG FP1 Reference Guide**
- **FireWall-1 NG FP1**
- **Virtual Private Networks NG FP1**
- **Connect Mode/ Office Mode**
- **VPN-1 SecuRemote/ SecureClient NG FP1 Administration Guide**

## Release Notes

- **VPN-1 SecuRemote/ SecureClient NG FP1 Build 51057**
- **NG FP1 Suite**

## Nokia Documentation at Check Point

[Location - [http://www.checkpoint.com/support/technical/documents/docs\\_nokia.html](http://www.checkpoint.com/support/technical/documents/docs_nokia.html)]

# Chapter 11

## Appendix B - Sample Entrust.ini files

This section contains an example of entrust.ini file that were used in the testing of this environment.

# Entrust.ini File

Below is a sample of the entrust.ini file used for the VPN-1 SecuRemote client.

```
[Entrust Settings]
; the long timeout is needed for first time init with luna ca
ClientSocketTimeout=240
Authority=192.168.0.30+829
Manager=192.168.0.30+709
Server=192.168.0.30+389
Defaultdigital IDLocation=
EncryptWith=Cast
ClientType=Heavy
MaximumCrossCertNodes=20
CrossCertCACacheSize=5
ArlCacheEnabled=1
CrossCertCRLCacheSize=8
CrossCertCACacheEnabled=1
CrossCertARLCacheSize=8
CrossCertDebug=0
CrlCacheEnabled=1
CertificateCacheEnabled=1
CertificateCacheSize=50
SearchBase=cn=Users,dc=entrust,dc=com
SigningKey=RSA-1024
; by default session credentials are valid for 1 week
DefaultCredentials_time_req=604800
DefaultContext_time_req=3600
ProgDir=
InstallDir=
CA Distinguished Name=cn=Entrust CA,cn=AIA,cn=Public Key
Services,cn=Services,cn=Configuration,dc=entrust,dc=com

[Directory Connection Settings]
DirectoryProtocol=LDAPV3
DirectorySearchSizeLimit=300
DirectoryOperationTimeLimit=30
DirectoryConnectTimeLimit=30
UseBinaryOptionDefaults=0
PreventFilterOptions=1
AuthMethod=WinAuth,anonymous
LDAPModifyOperation=Replace

[X500 Search Data Structure]
data0=sn,Last Name,24

[X500 Group Data Structure]
data0=cn,Name,30,d

[X500 Display Data Structure]
data0=cn,Name,30,d
data1=sn,N/A,30

[X500 Sorting Data Structure]
data0=sn,N/A,30

[OIDAlias]
; AliasName=AlgName
domainComponent=dc

[OIDTable]
; AlgName=Numeric Object Identifier
dc=0.9.2342.19200300.100.1.25
```

```

[X500AttrSyntax]
; X500AttributeType=X500SyntaxName
dc=IA5StringSyntax

[PEMAlgNames]
; PEM Algorithm Name=X.500 Algorithm Name
[DOS Extensions]
BAT=34
C=36
TXT=15
CMD=34
COM=34
CPP=36
CSV=10
CXX=36
DBF=25
DIF=11
DLL=34
DOC=14
EPS=29
EXE=34
H=36
MPC=18
MPP=16
MPV=19
MPW=20
MPX=17
PM4=26
PPT=32
PT4=27
PUB=21
RDY=24
RTF=15
SIT=30
SLK=07
STY=15
SYS=34
TEM=27
TIF=28
TPL=27
TXT=35
WK1=09
WK3=33
WKS=08
WRD=15
XLA=05
XLC=01
XLM=10
XLS=09
XLT=06
XLW=04
FRM=37
MID=38
PDF=39
LSO=40
ILY=41
IFM=42
IPK=43

[Mac Types]
01=XCEL,XLC3; MS Excel 3.0 Chart
02=XCEL,XLS3; MS Excel 3.0 Spreadsheet
03=XCEL,XLM3; MS Excel 3.0 Macrosheet
04=XCEL,XLW3; MS Excel 3.0 Workspace
05=XCEL,XLA; MS Excel 3.0 Add-in MacroFile
06=XCEL,SLM3; MS Excel 3.0 Template File

```

```

07=XCEL,TEXT; MS Excel 3.0
08=XCEL,XLC4; MS Excel 4.0 Chart
09=XCEL,XLS4; MS Excel 4.0 Spreadsheet
10=XCEL,XLM4; MS Excel 4.0 Macrosheet
11=XCEL,XLW4; MS Excel 4.0 WorkSpace
12=XCEL,XLA; MS Excel 4.0 Add-in MacroFile
13=XCEL,XLT; MS Excel 4.0 Template File
09=XCEL,XLS5; Excel 5.0 workbook, template
09=XCEL,XLS; Excel 2.2 worksheet
14=MSWD,WDBN; MS Word 5.1 Document
15=MSWD,TEXT; MS Word 5.1 Document
14=MSWD,W6BN; Word 6.0 document
14=FraB,FASL; FrameBuilder 4.0.2 document
15=MSWD,RTF; Word rich text format
15=LMAN,TEXT; Word 2.x, WordPerfect 5.0, 5.1 (DOS) 5.x (Windows)
16=MSPJ,MPP; MS Project 3.0
17=MSPJ,MPX; MS Project 3.0 Exchange File
18=MSPJ,MPC; MS Project 3.0
19=MSPJ,MPV; MS Project 3.0 Calendars
20=MSPJ,MPW; MS Project 3.0 Views
21=ALD3,ALB3; Pagemaker 3.0 Publication
22=ALD3,ALT3; Pagemaker 3.0 Template
23=ALD3,TIFF; Pagemaker 3.0 Tiff Graphics
24=MORE,TEXT; Symantec More File
25=FOX+,F+DB; FoxBase Plus
26=ALD4,ALB4; Pagemaker 4.0 Publication
27=ALD4,ALT4; Pagemaker 4.0 Template
28=ALD4,TIFF; Pagemaker 4.0 Tiff Graphics
29=ARTZ,EPSF; Adobe Illustrator
30=SIT!,SIT!; Aladdin Stuffit
31=PPT2,SLD2; MS PowerPoint 2.0
32=PPT3,SLD3; MS PowerPoint 3.0, 4.0 Presentations
33=L123,LWK3; Lotus 1-2-3
34=LMAN,DEXE; LMAN Executables
35=ttxt,TEXT; Teach Text Document
36=KAHL,TEXT; Symantec Think-C Source File
37=Fram,FASL; FrameMaker Document
38=QmdF,TRAK; QuickTime Midi
39=CARO,PDF; Adobe Acrobat Reader
40=EMAG,EM3F; EMAGIC Logic song file
41=IDes,ILay; Informed Designer Form Template
42=IMgr,IDoc; Informed Filler Form Data
43=IMgr,IPkg; Informed Filler Package
[ASH Information]
ASHServer=192.168.0.30
ASHPort=710
ASHdn=cn = ASH Service,cn=Entrust CA,cn=AIA,cn=Public Key
Services,cn=Services,cn=Configuration,dc=entrust,dc=com
PKIVersion=5

[Login Strings]
Message=<None>

[FIPS Mode]
EtAdmapiName=etadmapi
FipsMode=0
etadmapiAuth=DES-MAC,64,603BDC13C5DA9D23:CAST3-MAC,64,64,A9A4799FFA90098F
entrustraAuth=DES-MAC,64,3033E4EC36CD61E8:CAST3-MAC,64,64,0088BF3B895028A9
EntadminAuth=DES-MAC,64,3033E4EC36CD61E8:CAST3-MAC,64,64,0088BF3B895028A9
entadminName=entrustRA

```