

# Keon Ready Implementation Guide



## Keon Ready Implementation Guide

### FireWall-1/VPN-1 v4.1

Last Modified October 17, 2000

#### 1. Partner Information

Partner Name	Check Point Software Technologies
Web Site	<a href="http://www.checkpoint.com">www.checkpoint.com</a>
Product Name	FireWall-1 / VPN-1
Version & Platform	4.1 for WindowsNT, Solaris, HP/UX, and AIX
Product Description	FireWall-1/VPN-1 is an award winning, comprehensive application suite that integrates access control, authentication, encryption, network address translation, content security, auditing, and connection control. The suite is unified by Check Point's OPSEC policy management framework, which provides integration and enterprise management for FW-1/VPN-1 and many third-party network security applications. It is available on Sun, Hewlett-Packard, and IBM UNIX-based systems, WindowsNT systems, Bay Networks routers, Xylan and Ipsilon Networks switches, U.S. Robotics remote access servers, and TimeStep hardware encryption devices.
Keon Integration	Certificate Server

#### 2. Contact Information

	Pre-Sales	Post-Sales
Name	Check Point Resellers	Check Point Technical Support
E-mail	<a href="mailto:Info@checkpoint.com">Info@checkpoint.com</a>	<a href="mailto:Support@checkpoint.com">Support@checkpoint.com</a>
Phone	650-628-2000	800-429-4391
Web	<a href="http://www.checkpoint.com/sales/index.html">http://www.checkpoint.com/sales/index.html</a>	<a href="http://www.checkpoint.com/techsupport">http://www.checkpoint.com/techsupport</a>

### 3. Product Requirements

- **Operating systems:**  
Microsoft Windows NT 4.0 (SP3 or higher)  
Sun Solaris 2.6, Solaris 7 (32 bit mode only)  
HP-UX 10.20, 11. 0 (32 bit mode only)  
IBM AIX 4.2.1, 4.3.2
- **Disk space:** 40 MB
- **Memory**
  - **Management Server & Enforcement Module:** 64MB minimum, 128MB recommended
  - **SecuRemote/SecureClient:** 32MB
- **Network interface**  
ATM  
Ethernet  
Fast Ethernet  
FDDI  
Token Ring
- **Version of Keon Certificate Server tested:**  
KCS 5.5 on Windows NT v4.0 with SP5. CRL checking does not work with KCS 5.0.
- **Version(s) of partner software tested:**  
Check Point FireWall-1/VPN-1 4.1 with SP1 and SP2. Also known as Check Point 2000.
- **GUI / Window environments supported:**  
FireWall-1 management runs on Windows and Motif UNIX environments.
- **What software is required at the remote user's desktop to allow PKI or Keon support?  
What version of the software is required?**  
Check Point SecuRemote or SecureClient version 4.1 or later.

## Keon Ready Implementation Guide

### 4. Product Configuration

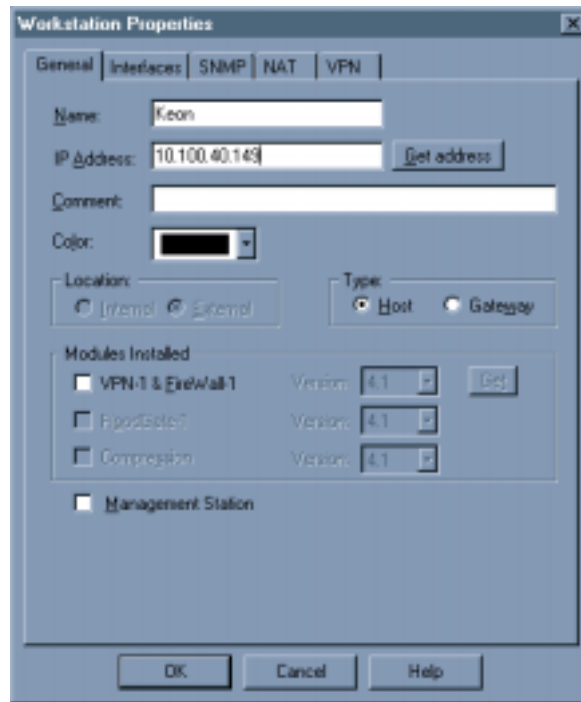
The goal of this section is to show you how to configure Check Point FireWall-1 to authentication VPN users with Keon certificates. Please reference the Check Point 2000 CD-ROM for helpful documents on this subject (Docs > FireWall-1).

**Prerequisite:** Make sure you can authenticate with either a password or IKE shared secret, and can successfully establish a VPN tunnel. Before introducing certificates, configure the firewall for IKE authentication using a shared secret or for FWZ. Refer to the FireWall-1 documentation for details on how to do this.

**A. Create a Workstation object on FireWall-1.** From the Check Point Policy Editor, go to Manage > Network Objects > New > Workstation.

- **Name:** host name(s) of system(s) running KCS and/or LDAP (typically this is the same system).
- **IP Address:** Click on the 'Get Address' box to make sure that name resolution is working properly. If an address does not come back. Contact your network administrator to correct this issue before continuing.
- **Comment:** (optional)
- **Color:** (optional)
- **Location:** N/A
- **Type:** Host. Please see 'Help' on more info for this field.
- **Modules Installed / Management Station:** N/A. Typically there is no Check Point software running on this box.

There are no other configuration parameters needed. Everything that you need to configure is shown in the screen shot. You will not need to access any other tab except for 'General'.



**B. Create an LDAP object on FireWall-1.** From the Check Point Policy Editor, go to Manage > Servers > New > LDAP Account Unit.

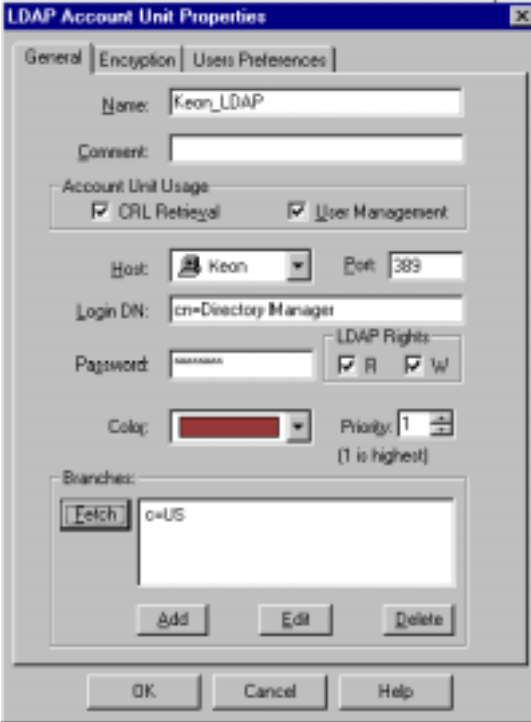
- **Name:** This is a 'friendly name' it does not have to match any TCP/IP naming convention on your network. Use a naming scheme that is easy for you to remember, such as <computername\_LDAP>.
- **Comment:** (optional)
- **Account Unit Usage:** Check both 'CRL Retrieval' and 'User Management'.

## Keon Ready Implementation Guide

- **Host:** From the drop list, select the system that we created in step 1.
- **Port:** 389
- **Login DN:** cn=Directory Manager
- **Password:** (Password for above. If you installed KCS 5.5 in “typical” mode the password is your MEK password)
- **LDAP Rights:** Check both 'R' and 'W'.
- **Color:** (optional)
- **Priority:** 1
- **Branches:** Click 'Fetch'.

There are no other configuration parameters needed. Everything that you need to configure is shown in the screen shot. You will not need to access any other tab except for 'General'.

**IMPORTANT:** Login DN and Password is very important. They need to be correct. Clicking 'Fetch' and getting a return value of 'c=US' does not mean that it was successful. Be sure that they are indeed correct.



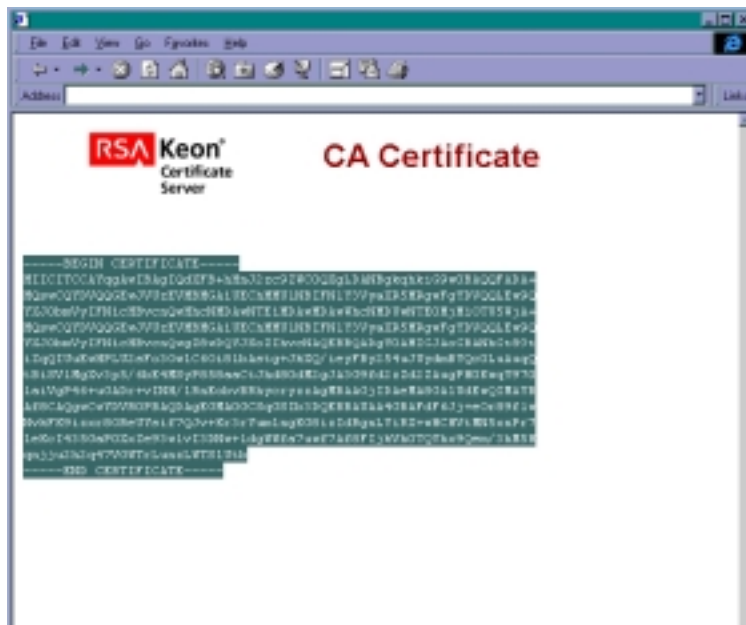
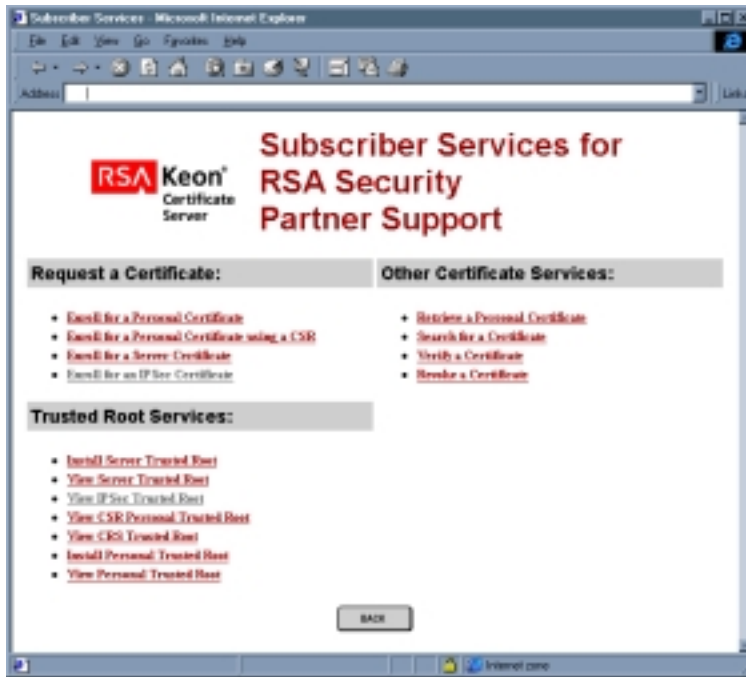
The screenshot shows the 'LDAP Account Unit Properties' dialog box with the 'General' tab selected. The fields are filled with the following values:

- Name: Keon\_LDAP
- Comment: (empty)
- Account Unit Usage:  CRL Retrieval,  User Management
- Host: Keon (dropdown)
- Port: 389
- Login DN: cn=Directory Manager
- Password: (masked)
- LDAP Rights:  R,  W
- Color: (red dropdown)
- Priority: 1 (1 is highest)
- Branches: A table with one entry: 'c=US' (The 'Fetch' button is highlighted).

Buttons at the bottom: Add, Edit, Delete, OK, Cancel, Help.

## Keon Ready Implementation Guide

**C. Obtain IPsec Trusted Root from CA (Certificate Authority).** From the Keon Certificate Servers' Subscriber Services page, click on 'View IPsec Trusted Root'. Copy/Paste certificate text to a temporary file that will be needed later in step 4. Make sure to highlight text beginning with '-----BEGIN CERTIFICATE-----' and ending with '-----END CERTIFICATE-----'



## Keon Ready Implementation Guide

**D. Create a CA instance on FireWall-1.** From the Check Point Policy Editor, go to Manage > Servers > New > CA.

### **GENERAL tab:**

**Name:** This is a 'friendly name' it does not have to match any TCP/IP naming convention on your network. Use a naming scheme that is easy for you to remember, such as <computername\_CA>.

**Comment:** (optional)

**Color:** (optional)

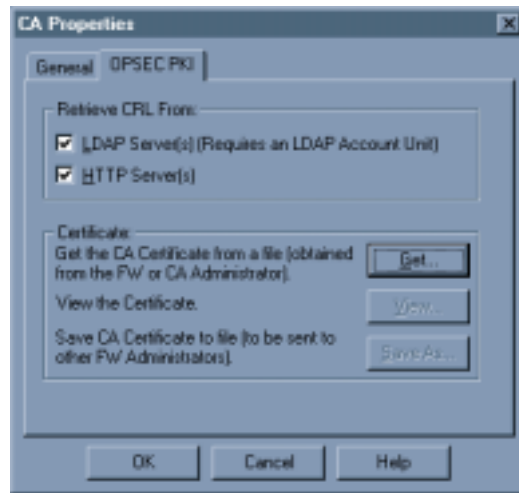
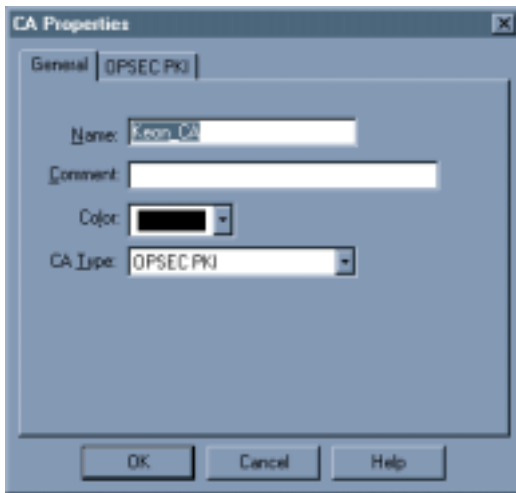
**CA Type:** From the drop list, select OPSEC PKI.

Now, click on the OPSEC PKI tab.

### **OPSEC PKI tab:**

**Retrieve CRL From:** Check both LDAP Servers and HTTP Servers.

**Certificate:** Click 'Get' and point to the temporary file we created in step 3 containing the IPSec Trusted Root certificate.

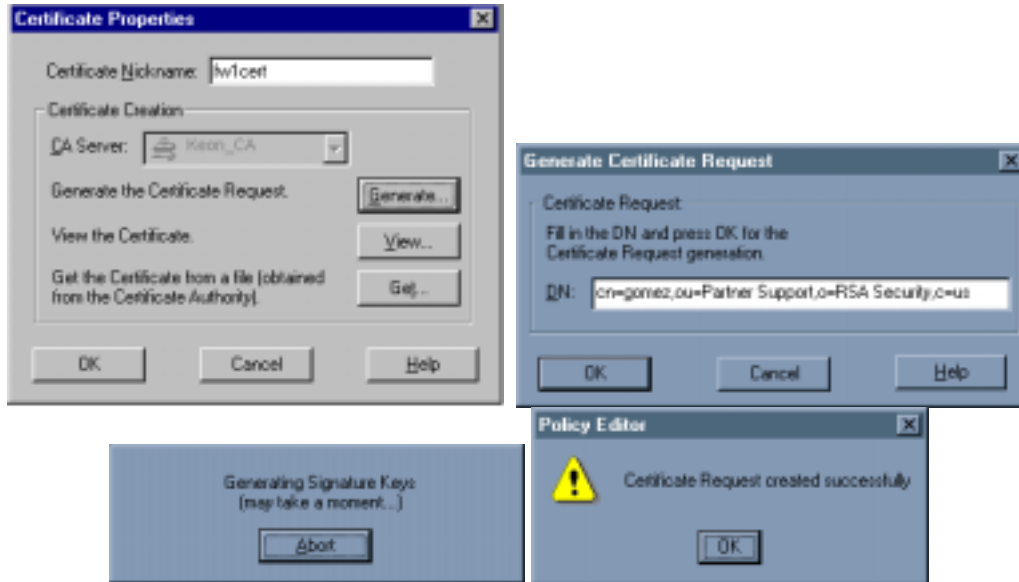


## Keon Ready Implementation Guide

E. **Generate a CSR (Certificate Signing Request) for an IPSec certificate on FireWall-1.** From the Check Point Policy Editor, go to Manage > Network Objects > (Select FireWall-1 instance) > Edit > Certificates tab > Add.

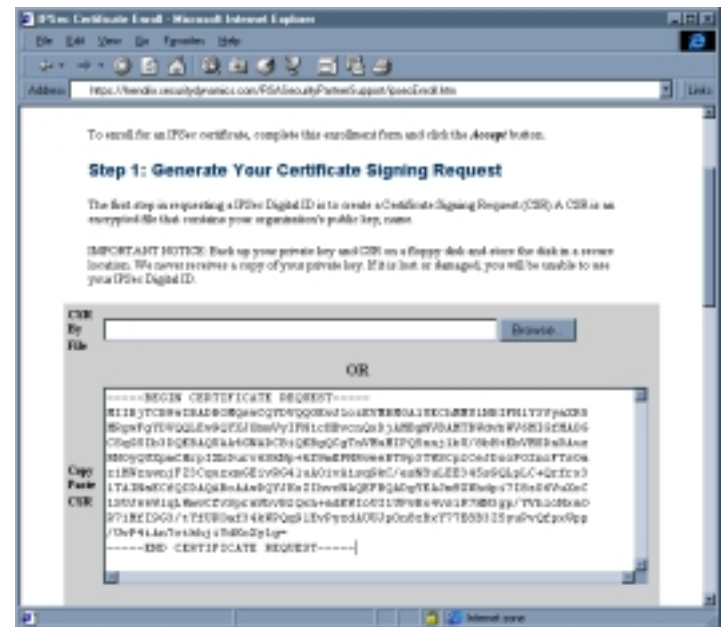
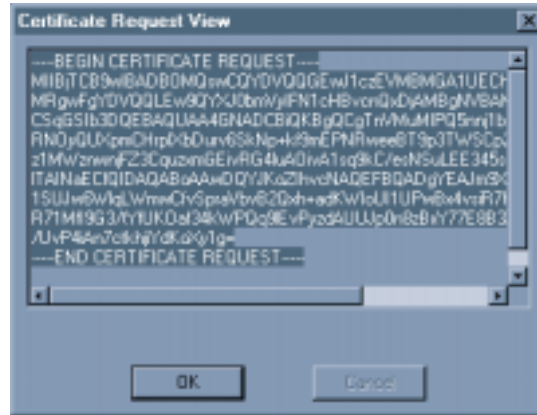
- **Certificate Properties window.** In the Certificates Property window specify a nickname for the certificate. You must specify a nickname for each certificate because a workstation can have more than one certificate. Also, from the drop down box, select the Keon CA that you created in the previous step.
- **Generate Certificate Request window.** Fill in the DN information...cn=<host name>,ou=<jurisdiction sub name>,o=<jurisdiction name>,c=us

**Note:** In some cases, these entries are case (i.e c=us versus c=US) and format (i.e. spaces and commas) sensitive.



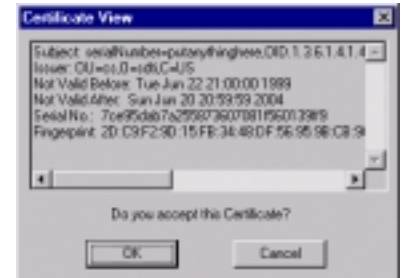
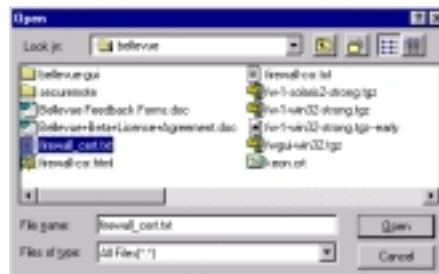
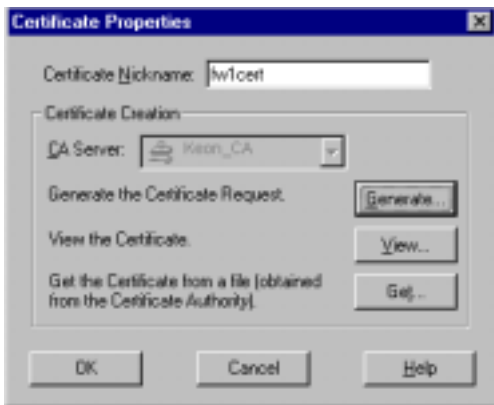
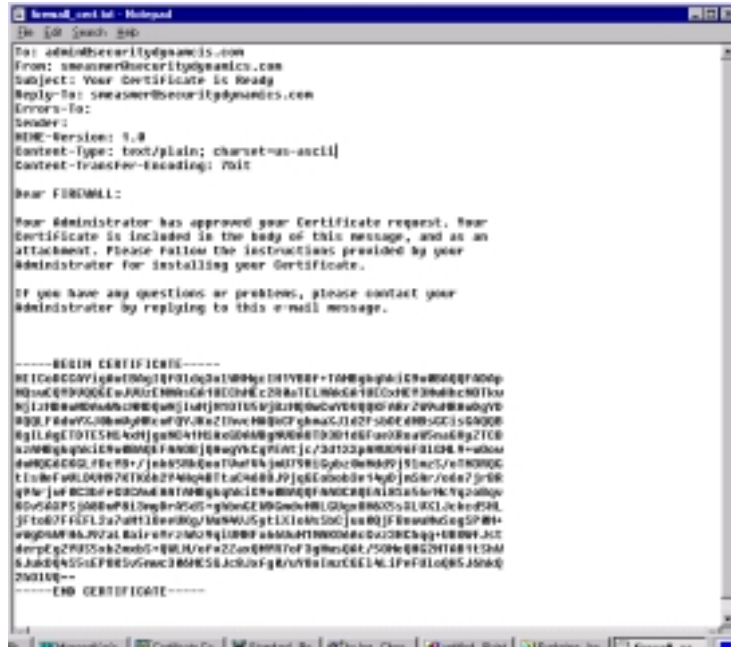
## Keon Ready Implementation Guide

**F. Request IPsec certificate from the CA using the CSR.** After generating the CSR, go to the Check Point Policy Editor, Manage > Network Objects > (Select FireWall-1 instance) > Edit > Certificates tab, click on 'View'. Highlight and copy contents to the clipboard (Ctrl - c). Be sure to highlight text beginning with '-----BEGIN CERTIFICATE REQUEST-----' and ending with '-----END CERTIFICATE REQUEST-----'. Access the Keon Certificate Servers' Subscriber Services page; click on 'Enroll for an IPsec Certificate'. Paste (Ctrl -v) the CSR into the field 'Copy Paste CSR' and fill out the rest of the required information on the form. Click Accept.



## Keon Ready Implementation Guide

**G. Obtain IPsec certificate from the CA.** The request will then be approved by the Keon Certificate Administrator and mailed back to the requestor. Copy the contents of this email to a file. Go to the Firewall to you were in step F....from the Check Point Policy Editor, go to Manage > Network Objects > (Select FireWall-1 instance) > Edit > Certificates tab > Select certificate which at this point should have a status of 'unsigned' > click on 'Edit'. Click 'Get' and point to the email file you just created.



## Keon Ready Implementation Guide

**H. Configure FireWall-1 to use certificates for VPN encryption authentication.** From the Check Point Policy Editor, go to Manage > Network Objects > (Select FireWall-1 instance) > Edit > VPN tab.

The image displays three overlapping configuration windows from the Check Point Policy Editor:

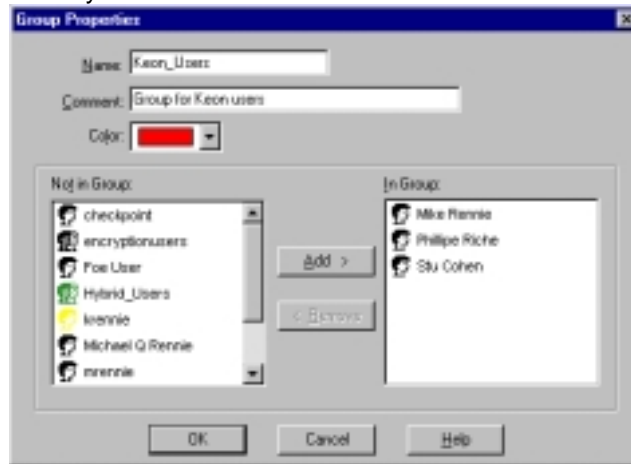
- Workstation Properties:** Shows the 'VPN' tab with 'Encryption schemes defined' including IKE, Manual IPSEC, SHIP, and PVAZ. The 'Domain' is set to 'encryptiondomain'.
- IKE Properties:** Shows 'Support key exchange encryption with' (YES, CAST, 3DES) and 'Support data integrity with' (MD5, SHA1). Authentication methods include 'Pre-Shared Secret', 'Public Key Signatures', and 'VPN-1 & FireWall-1 authentication for SecuRemote Hybrid Model'.
- Public Key Matching Criteria:** Shows 'Certificate presented by this object' with a dropdown menu set to 'Any'.

Below these windows is the 'test - Policy Editor' window, which contains a table of security policies:

No.	Source	Destination	Service	Action	Track	Install On	Time
1	Any	Any	MBT NFS secured	accept		Gateways	Any
2	remote-users@Any	Any	Any	Client Encrypt	Long	Gateways	Any
3	Any	Any	Any	drop		Gateways	Any

## Keon Ready Implementation Guide

**I. Create a group.** From the Check Point Policy Editor, go to Manage > Users > New > Group. This group will be used to reference all users being authenticated by Keon certificates.



**Name** - the group's name

**Comment** - descriptive text. This text is displayed on the bottom of the Network Object window when this group is selected.

**Color** - Color of the group's icon. Select the desired color from the drop-down list.

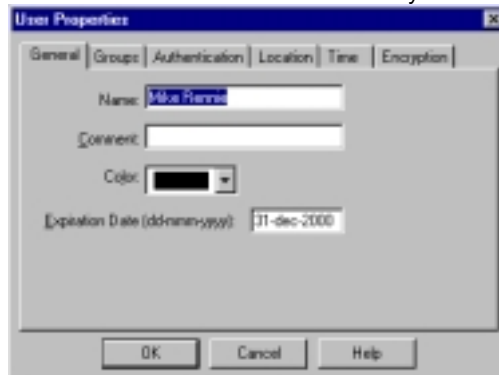
**Not In Group** - Objects which do not belong to the group

**In Group** - Objects included in the group.

**J. Create a user.** From the Check Point Policy Editor, go to Manage > Users > New > Default. This user will authenticate via Keon certificates. You will need to configure 4 out of the 6 tabs within this screen.

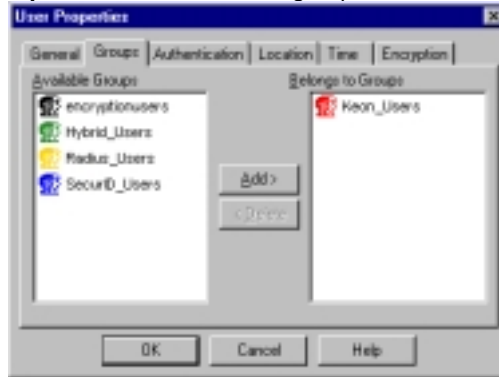
**Note:** Instead of creating a FireWall-1 user account for each individual Keon user, you can create a default FireWall-1 user called 'generic\*'. All users that do not have a FireWall-1 user account will automatically be authenticated via Keon certificates.

**General tab:** Choose a name that matches the matches the syntax of the CN in your certificate.

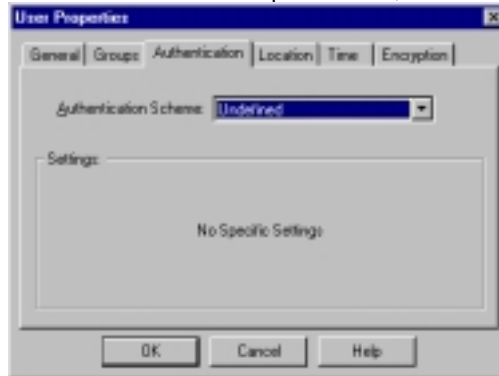


## Keon Ready Implementation Guide

**Groups tab:** Select and Add group created in step 1.



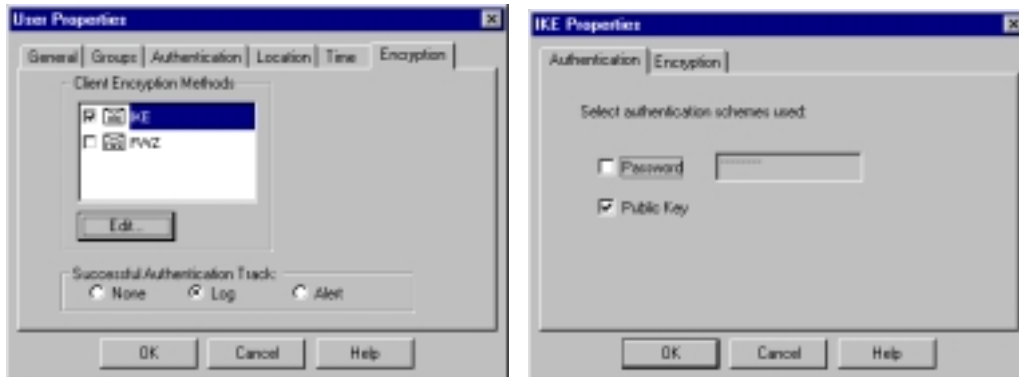
**Authentication tab:** From the drop down box, choose Undefined.



**Location tab:** OPTIONAL

**Time tab:** OPTIONAL

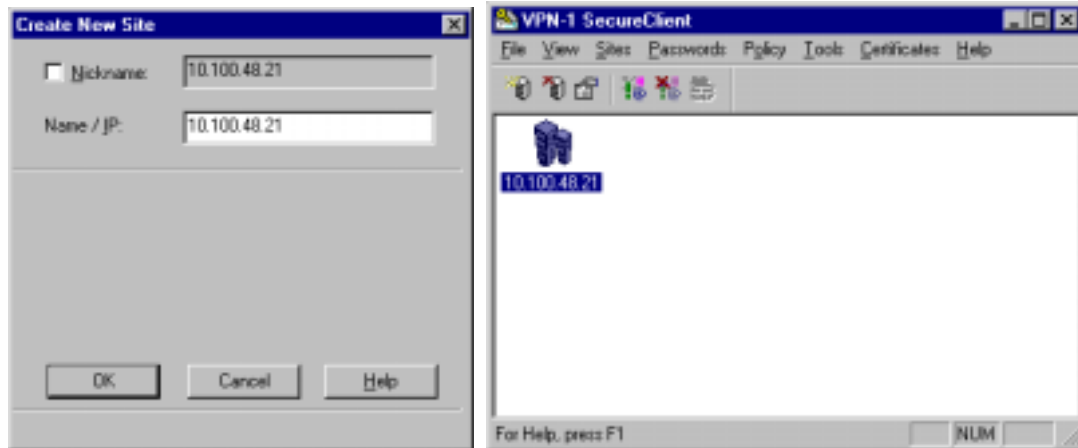
**Encryption tab:** Check the box to the left of 'IKE', click Edit. The IKE Properties window will come up. In the Authentication tab, check the box for Public Key. This will enable the use of certificates with the IKE encryption scheme.



## Keon Ready Implementation Guide

### Configuring SecuRemote/SecureClient:

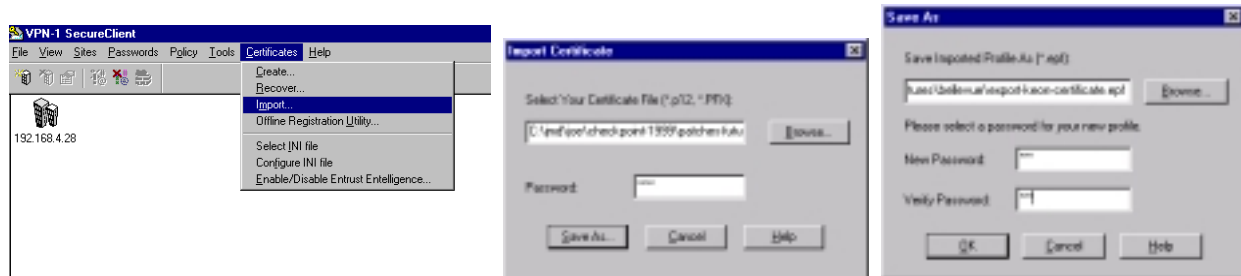
- **Install SecuRemote/SecureClient software on client PC's.** Refer to Check Point documentation for installation of SecureClient and/or SecuRemote VPN client software.
- **Create Site.** On the client software, go to Sites > Create New. Enter the IP address of the system running FireWall-1 / VPN-1. Click OK.



- **Configure SecuRemote/SecureClient for IKE encryption.** On the client software, go to Tools > Encryption Scheme > IKE. Click OK.

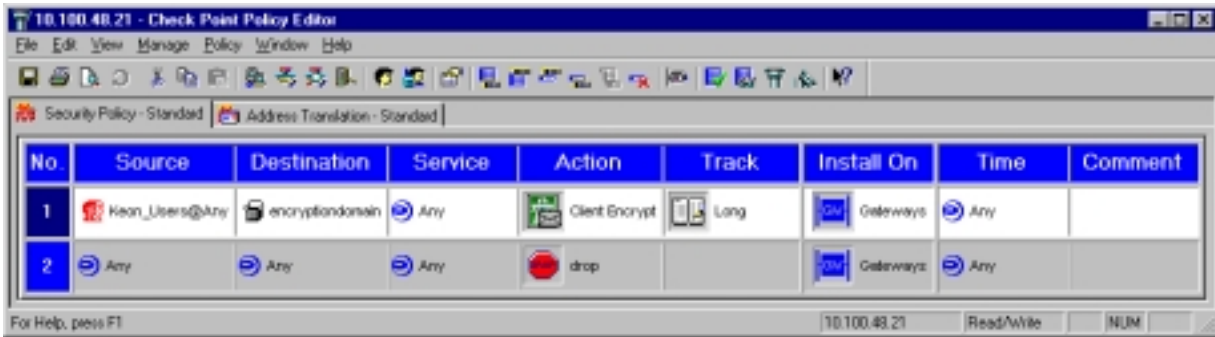


- On the SecureClient / SecuRemote client PC, use a web browser to enroll and obtain a personal certificate from the Keon CA (this may require a rule on the firewall to allow this traffic). Also install the server's Trusted Root Certificate to the browser (this is required for the next step).
- Use the browser to export this certificate to a file in PKCS#12 format. It MUST contain the users private key, the users' certificate and the issuing CA's certificate.
- Import the PKCS#12 file (this converts it to a .epf file). Save it to the PC's hard drive.

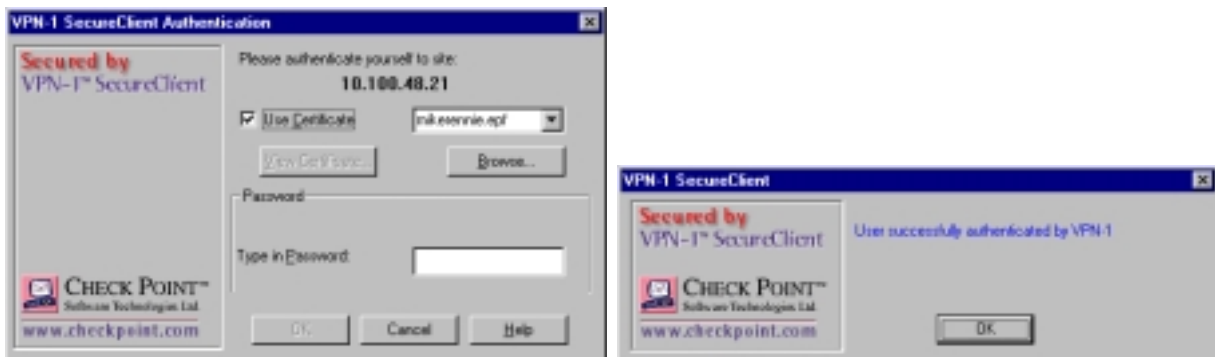


## Keon Ready Implementation Guide

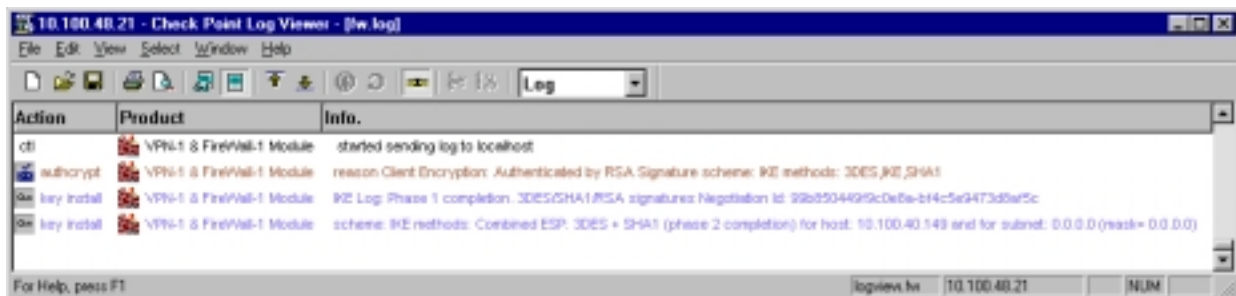
- **Create rule set.** Below is an example of a simple rule set that requires client PCs that want to pass through the firewall to use SecuRemote/SecureClient to encrypt the connections. Rule #1 challenge users in the Keon\_Users group and creates an encrypted tunnel. Rule #4 drops all other packets. Similar to other authentication methods, Keon certificate support is established by the user definitions and how the rule is created.



- **Complete.** Upon generating traffic between the SecureClient / SecurRemote client and a system through the firewall, you will be able to authenticate using the certificate, and establish an IPSec tunnel. The password you are prompted for is that one you created after importing the PKCS#12 file. Here is a sample of the prompts from SecureClient 4.1:



Successful entry in Check Point Log Viewer from above attempt:



## 5. Certification Checklist

Test Case	Personal	Server	IPSec
<b>PKCS#10 Enrollment via CSR:</b>			
Generate PKCS#10 Request	<input type="text"/>	<input type="text"/>	<input type="text" value="P"/>
Process PKCS#10 Request	<input type="text"/>	<input type="text"/>	<input type="text" value="P"/>
<b>Manual Enrollment:</b>			
Request Certificate	<input type="text" value="P"/>	<input type="text"/>	<input type="text"/>
Process Certificate Request	<input type="text" value="P"/>	<input type="text"/>	<input type="text"/>
<b>Import Certificate</b>			
Import PKCS#7 Certificate	<input type="text" value="P"/>	<input type="text"/>	<input type="text"/>
Import via cut & paste	<input type="text"/>	<input type="text"/>	<input type="text" value="P"/>
View & verify Certificate	<input type="text" value="P"/>	<input type="text"/>	<input type="text" value="P"/>
Install trusted root Certificate	<input type="text" value="P"/>	<input type="text"/>	<input type="text" value="P"/>
<b>Certificate Usage</b>			
Use certificate for authentication	<input type="text" value="P"/>	<input type="text"/>	<input type="text" value="P"/>
Use certificate for encryption	<input type="text" value="P"/>	<input type="text"/>	<input type="text" value="P"/>
<b>LDAP Support (if applicable)</b>			
Name lookup & certificate retrieval	<input type="text"/>	<input type="text"/>	<input type="text"/>
Revocation recognized via CRL	<input type="text" value="P"/>	<input type="text"/>	<input type="text"/>

**P**=Pass **X**=Fail **N/A**=Non-available function

## Keon Ready Implementation Guide

### 6. Additional Notes

- **Shared secrets.** Before getting certificate-based IPSec working, make sure you can establish a tunnel between SecuRemote/SecureClient and the firewall with shared secrets - this has nothing to do with Keon but will assure everything else about the firewall & VPN setup are correct.
- **Certificate Revocation List (CRL).** If you see errors in your log about CRL retrievals, you must correct them before certificate-based IPSec will work. Check your LDAP to make sure there is one. If not, manually force a CRL replication via the KEON system management page <local signer management>.
- **Certificate Authority.** When configuring a CA server in the firewall gateway, make sure to check the LDAP retrieval box, not just the HTTP box
- **LDAP Server.** You must configure an LDAP server and the firewall must be able to retrieve CRLs from it or you won't be able to do certificate-based IPSec.
- **Generating a Certificate Signing Request (CSR).** When enrolling for your firewall's IPSec certificate, make sure the certificate's distinguished name's O, OU, etc. match how your KCS jurisdiction is named so the CRL checking will work properly. The CSR request is case sensitive and it must match your root O and OU.
- **Usernames.** The CN in the user's certificate must match a user defined on the firewall, and that user definition must allow for certificate-based authentication. Most users will enroll for a certificate with First and Last Name, however, most VPNs users are created with a user domain name. You must make sure that the full user first name and last name is the login name.
- **generic\* user.** Instead of creating a FireWall-1 user account for each individual user, you can create and configure a default FireWall-1 user called 'generic\*' that will use certificates. All users that do not have a FireWall-1 user account will then automatically be authenticated by certificates.
- **Hybrid mode.** Hybrid Mode IKE authentication allows for the use of SecurID tokens in the use of IKE versus FWZ encryption. To enable this capability, a Certificate Authority has to be configured and trusted. At the time of this writing, Check Point does not support the use of KCS 5.0 or 5.5 for use with Hybrid mode IKE.
- **CA hierarchies.** SecuRemote/SecureClient does not support CA hierarchies
- **Importing certificates into SecuRemote/Secure Client.** When importing the PKCS #12 file into SecuRemote/SecureClient it MUST contain the users private key, the users' certificate and the issuing CA's cert.