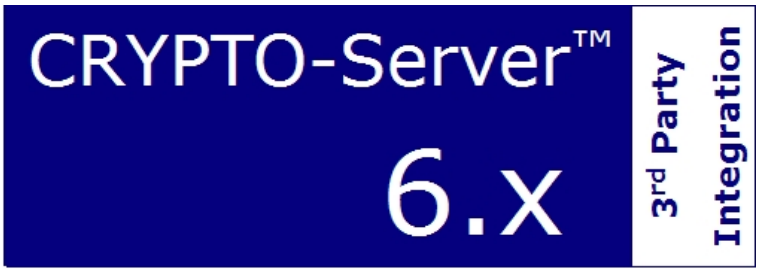


Check Point FW-1/VPN-1 NG/FP3

Implementation Guide

Check Point VPN-1 NG/FP3 Overview

This documentation is an overview and necessary steps in configuring Check Point VPN-1 NG/FP3 for use with CRYPTO-MAS and CRYPTOCard tokens.

Check Point VPN-1 NG/FP3 is used to create an encrypted tunnel between host and destination. CRYPTO-MAS works in conjunction with the Check Point VPN-1 NG/FP3 to replace static passwords with strong two-factor authentication that prevents the use of lost, stolen, shared, or easily guessed passwords when establishing a connection to gain access to protected resources.

With CRYPTO-MAS acting as the authentication server for a VPN enabled resource, an authenticated connection sequence would be as follows:

1. The Firewall / VPN logon prompts the user for their logon name and their CRYPTOCard generated PIN + One-time password.

2. The incoming RADIUS authentication request is relayed over to the CRYPTO-MAS Server. This is shown in Figure 1 below.

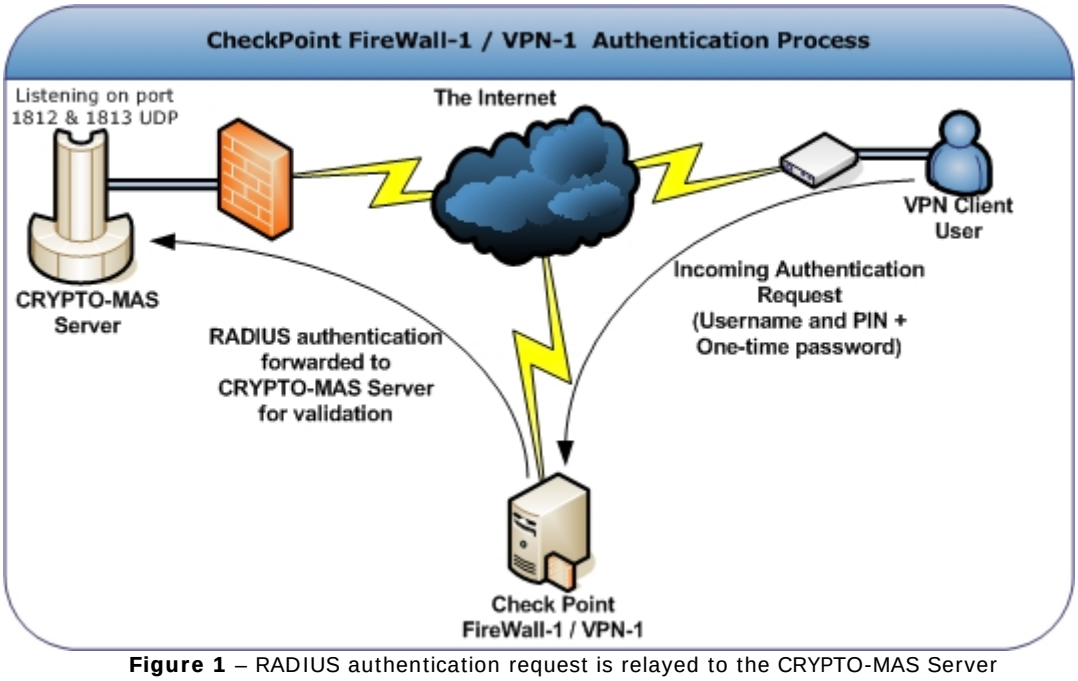


Figure 1 – RADIUS authentication request is relayed to the CRYPTO-MAS Server

3. The CRYPTO-MAS Server examines the incoming packet. If the user exists, it then checks the token associated with the user for the expected PIN + One-time password.

4. Once the PIN + One-time password is verified against the user's token and it is valid, it will then send an access accepted. This is illustrated in Figure 2 below.

The user does not exist, or the PIN + One-time password is incorrect it will send an access reject.

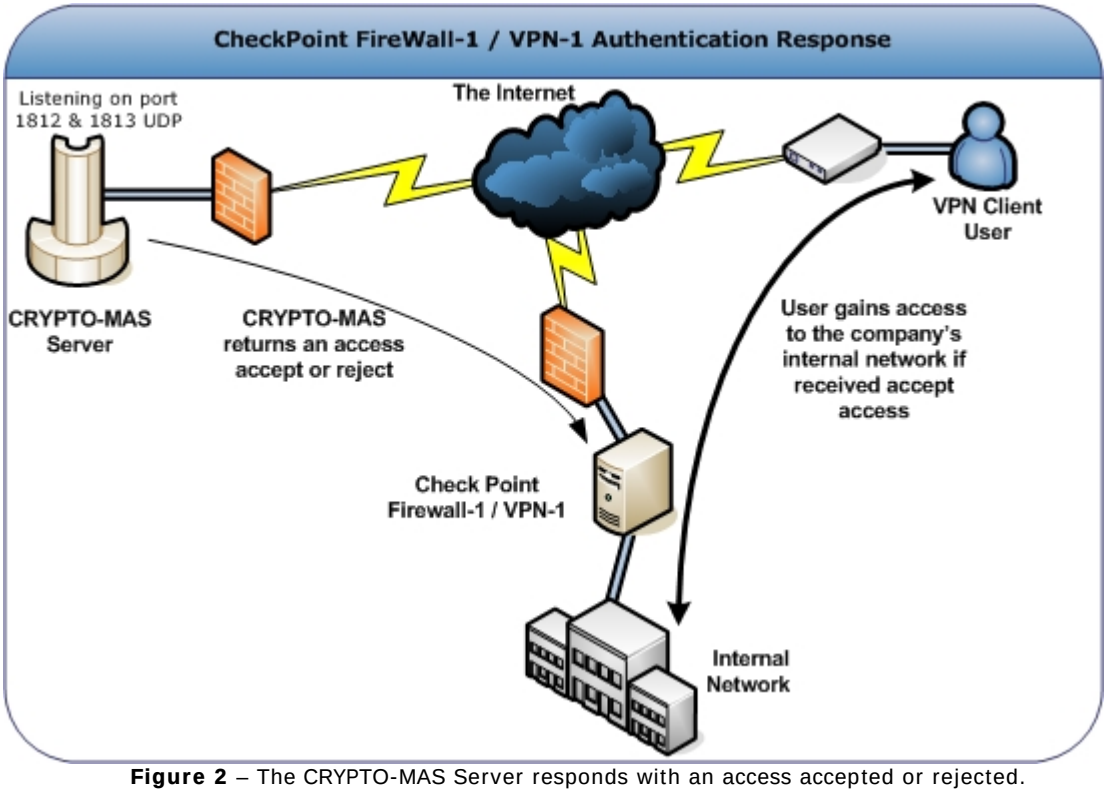


Figure 2 – The CRYPTO-MAS Server responds with an access accepted or rejected.

Compatibility

For compatibility issues with Check Point and this documentation, please configure and use Check Point VPN-1 version NG/FP3. All revisions after NG/FP3 have not been tested.

Prerequisites

The following systems must be installed and operational prior to configuring Check Point to use CRYPTOCard authentication.

- Ensure that end users can authenticate through Check Point VPN with a static password before configuring Check Point to use CRYPTOCard authentication.
- An initialized CRYPTOCard token assigned to a valid CRYPTOCard user.

The following CRYPTO-MAS server information is also required:

Primary CRYPTO-MAS RADIUS Server Fully Qualified Hostname or IP Address:	
Secondary CRYPTO-MAS RADIUS Server Fully Qualified Hostname or IP Address (**OPTIONAL**):	
CRYPTO-MAS RADIUS Authentication port number:	
CRYPTO-MAS RADIUS Accounting port number (**OPTIONAL**):	
CRYPTO-MAS RADIUS Shared Secret:	

Configure Check Point FW-1 and VPN-1

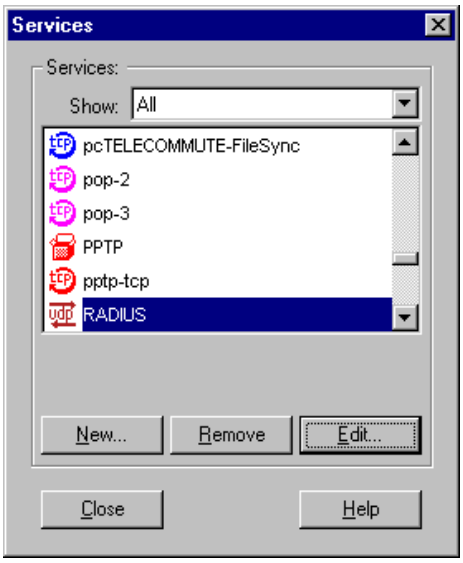
The following steps are required to complete the configuration of the FW-1 and VPN-1

- Configure the RADIUS server port (default 1812)
- Enable RADIUS Authentication.
- Configure the VPN-1 settings & IKE Encryption
- Create an authentication group
- Add CRYPTOCard users in FireWall-1/VPN-1
- Configure the Rule Set

Configuring a RADIUS port in Check Point FireWall-1 / VPN-1

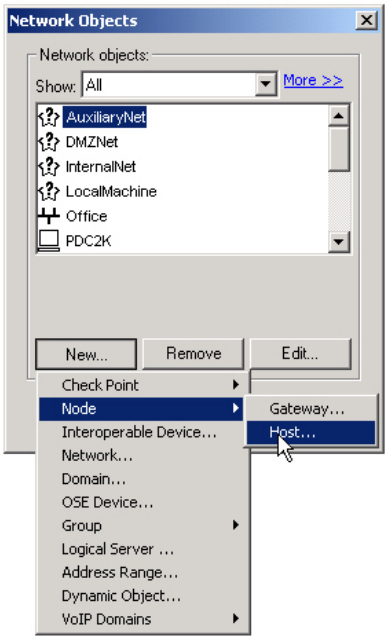
Check Point FireWall-1 / VPN-1 needs to be configured to use port 1812 so it can exchange RADIUS packets with the CRYPTO-MAS Server.

By default Firewall-1 uses port 1645. The RADIUS standards group has since changed the official port value to 1812. Newer O/S releases have implemented port 1812 for RADIUS.



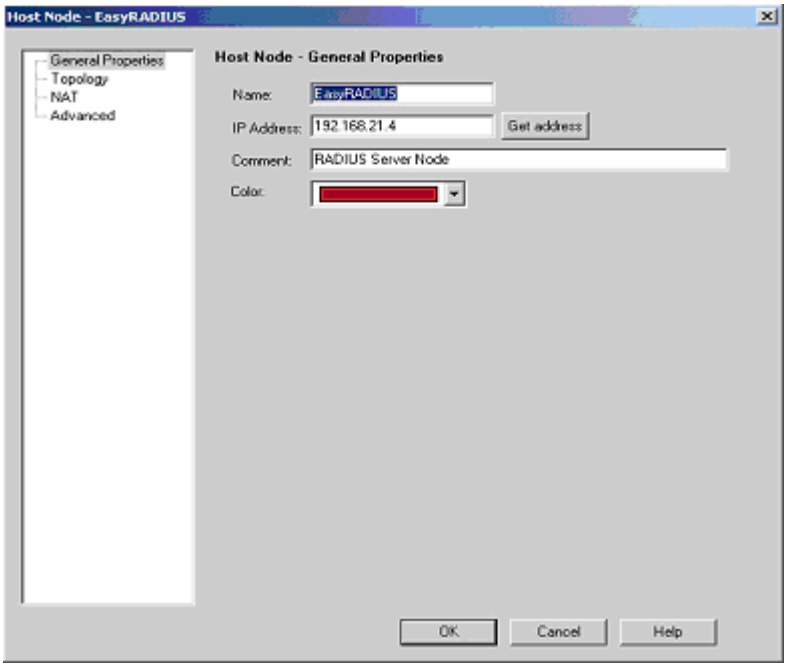
Defining the RADIUS Workstation in Check Point FireWall-1 / VPN-1

Define the IP Address of the CRYPTO-MAS Server on the Check Point FireWall-1 / VPN-1 machine. Fill in the information for the CRYPTO-MAS RADIUS server obtained from the prerequisites section.



From the Check Point SmartDashboard, Select Network Objects from the Manage Menu:

- Click New
- Node
- Host
- Under General Properties, enter the Host Node Properties:
- Name
- IP Address of CRYPTO-MAS Server
- Comment
- Color
- Click OK
- Then Close

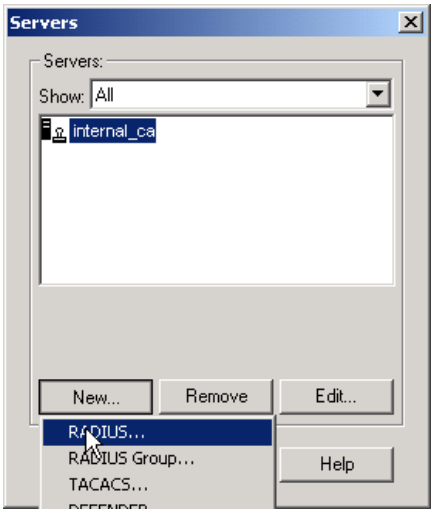


Defining the RADIUS Server in FireWall-1/VPN-1

On the system that is running Check Point FireWall-1 / VPN-1, you will need to define the CRYPTO-MAS Server machine (IP Address).

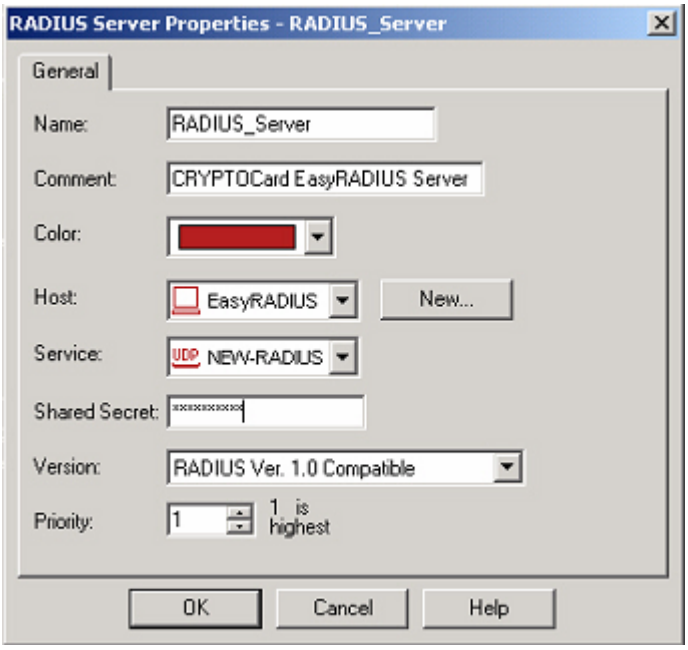
From the Check Point™ SmartDashboard, open:
Manage Menu

- Choose Servers
- In the Servers window, click New
- Select RADIUS

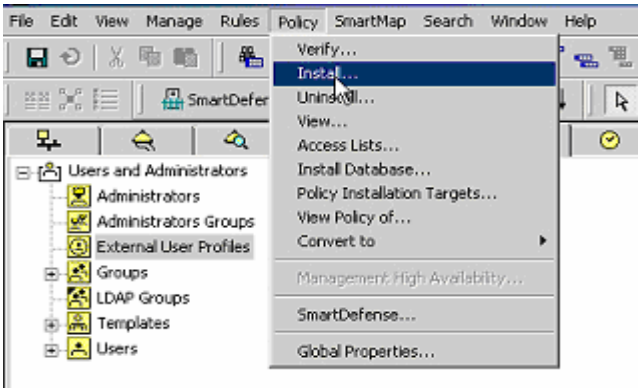


Define the CRYPTO-MAS Server Properties:

- Name.
- Comment.
- Color.
- Host (this should be the Host Node you defined in the previous section)
- Service (NEW-RADIUS may be selected if the RADIUS server is using port 1812).
- The Shared Secret entered must match the Shared Secret that is defined in the Prerequisites section.
- Version
- When choosing your RADIUS protocol version, you can select either RADIUS Version 1.0 or RADIUS Version 2.0.
- Click OK, then Close



Click the Policy menu then choose Install.



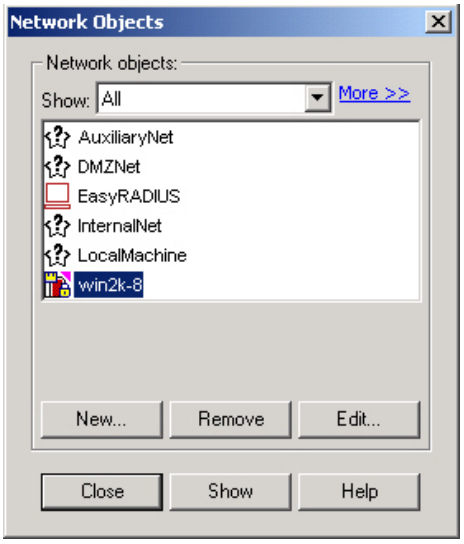
Enabling RADIUS Authentication on FireWall-1 / VPN-1

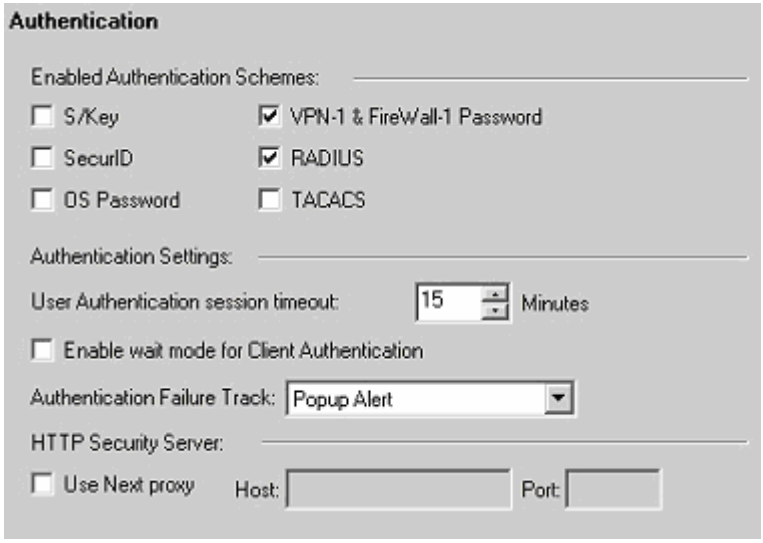
From the Check Point SmartDashboard Go to the Manage Menu and choose:

- Network Objects
- Select the FireWall-1 / VPN-1 object (in this case it's win2k-8)
- Click Edit

Under General Properties:

- Select Authentication
- Verify the VPN-1 & FireWall-1 Password and RADIUS boxes are checked



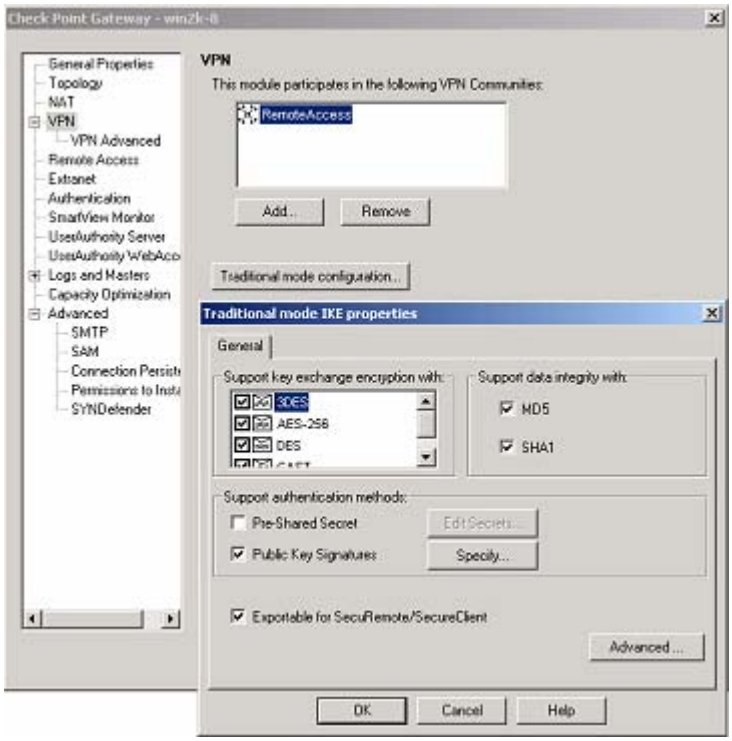


Configuring the VPN-1 settings & IKE Encryption

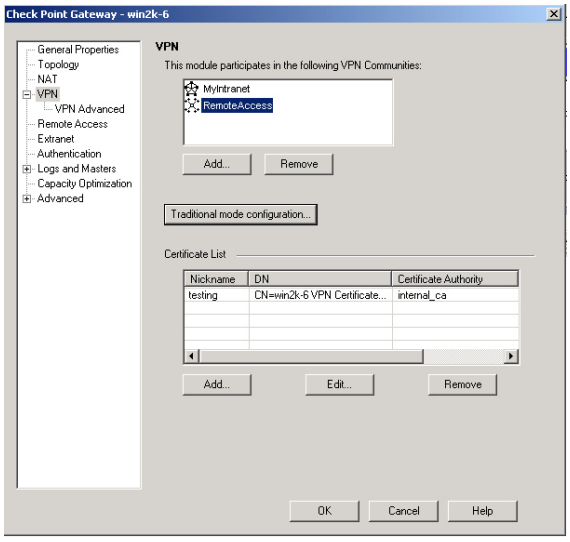
The following steps allow the SecuRemote end-users to download the VPN-1 topology from the FireWall, and to encrypt connections to the Inside network.

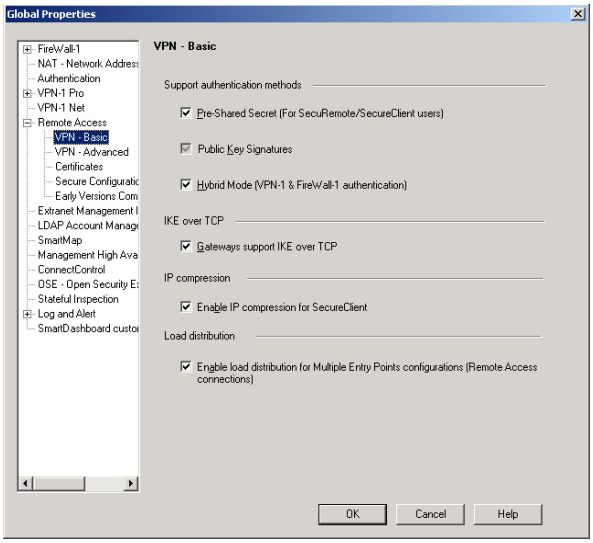
From the FireWall-1 / VPN-1 network object, under General Properties choose:

- VPN
- Select your VPN Community (RemoteAccess)
- Click 'Traditional mode configuration'
- Place a check in the box next to 'Exportable for SecuRemote/SecureClient'.



In the VPN section under General Properties verify that a Certificate exists in the Certificate List. Verify that Hybrid Mode Authentication has been enabled. Select Policy, Global Policy, Remote Access, VPN – Basic. Under Support authentication methods verify that Hybrid Mode has been checkmarked.





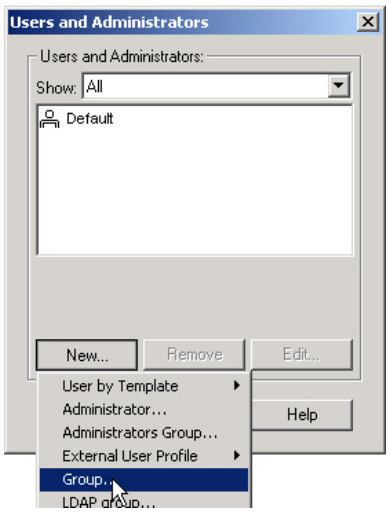
Creating an Authentication Group (VPN-1)

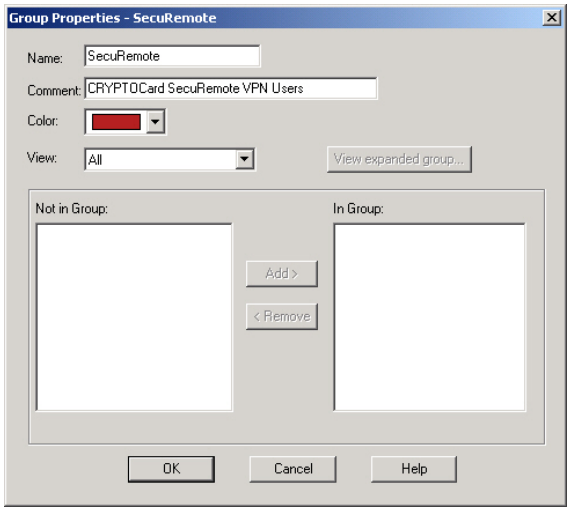
From the Manage Menu, select:

- Users and Administrators
- Click New
- Select Group

This group will be used to reference all users being authenticated the CRYPTO-MAS Server. In the Group Properties box enter the:

- Name
- Comment
- Color for the group
- Click OK



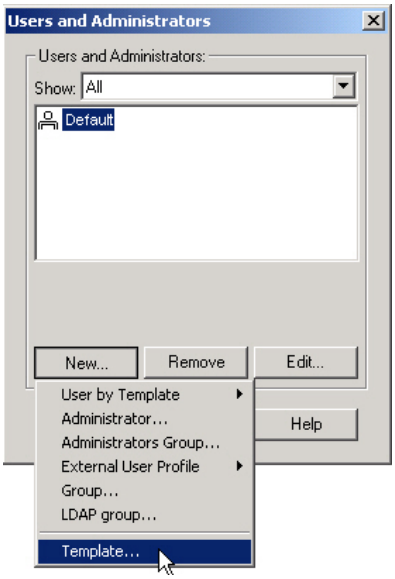


Adding CRYPTOCard Users in FireWall-1 / VPN-1

CRYPTOCard token users can be configured to use RADIUS authentication in two methods on the FireWall-1 / VPN-1. Each CRYPTOCard token user can be added to the FireWall-1 / VPN-1 database individually, or a generic user entry can be configured. Use the method that best meets your network authentication requirements.

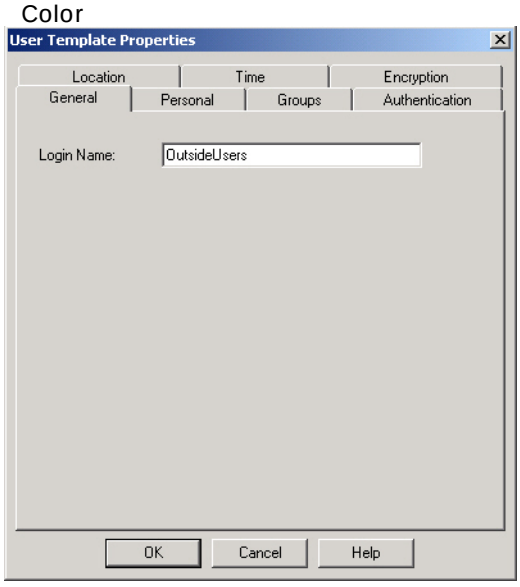
In the Check Point SmartDashboard, select:

- Users and Administrators from the Manage Menu
- Click New
- Template



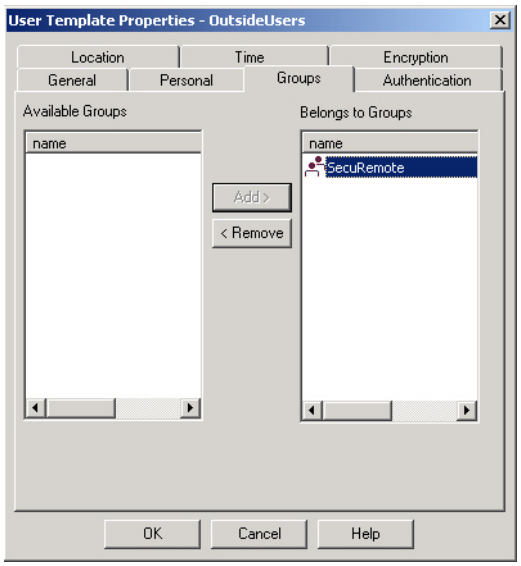
In the User Template Properties dialog box, under the General Tab, define:

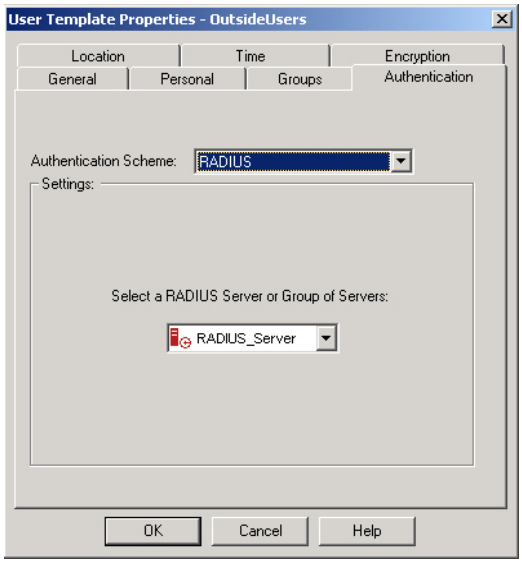
- Login Name
- Click the Personal Tab
- Define Expiration Date
- Comment
- Color



Click on the:

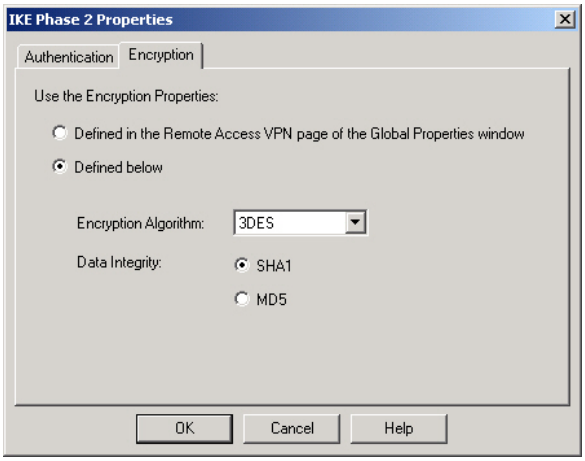
- Groups Tab
- Select the SecuRemote group
- Click Add button
- Click on the Authentication Tab
- Define the Authentication Scheme as RADIUS
- Select the RADIUS Server that's created in the previous section

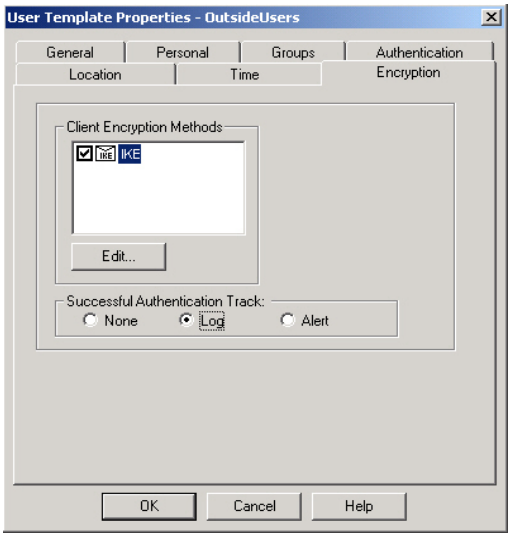




Click on the:

- Location Tab and Time Tab
- Define these settings as per your network security policy
- Select the Encryption Tab
- Check the box to the left of 'IKE'
- Click the Edit button to configure the IKE Encryption settings
- Select the Encryption Tab to validate the Encryption Algorithm
- Click the Install button to add the user to the FireWall-1® user database
- Close Users and Administrators dialog box

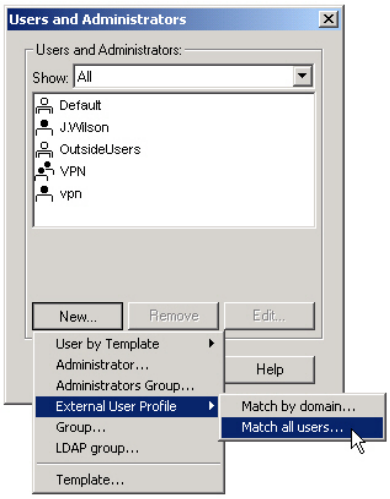


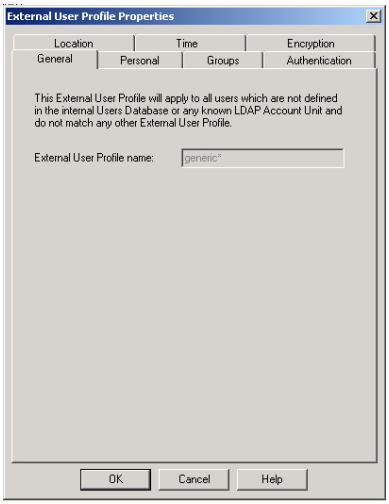


Configuring a Generic User Entry

From the Users and Administrators window:

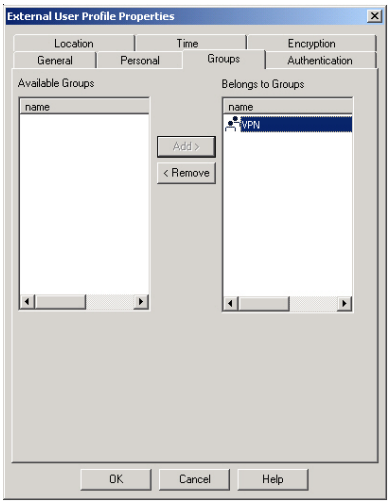
- Click New
- External User Profile
- Choose Match all users





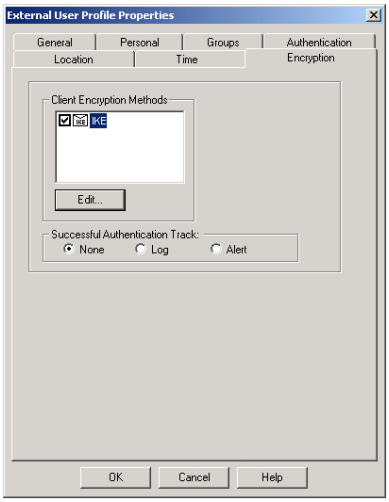
In the External User Profile Properties window:

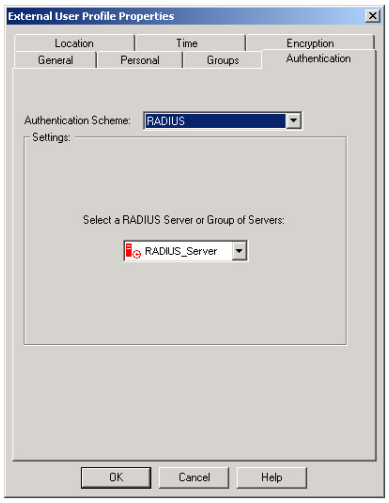
- Select the VPN tab then
- Add the appropriate Group



On the Authentication tab choose:

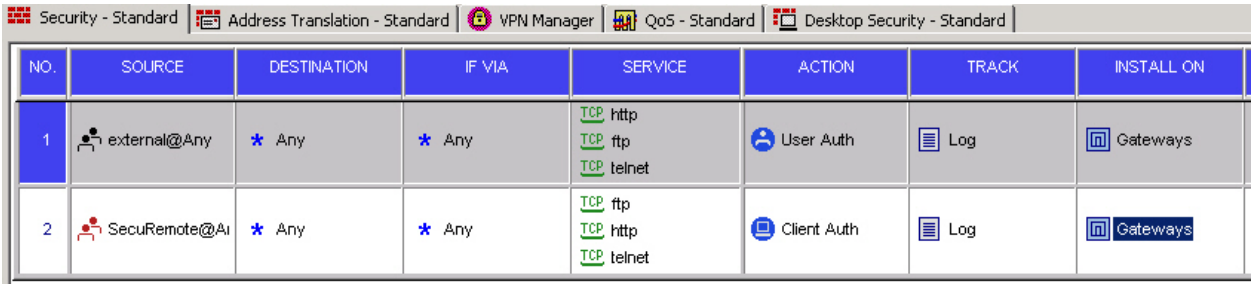
- RADIUS as the Authentication Scheme
- Select the RADIUS Server
- Select the Encryption tab
- Place a checkmark in IKE





Creating a FireWall-1 / VPN-1 Rule Set

Below is an example of two simple rule sets that will require users to authenticate with CRYPTOCard tokens. Configure the rule sets as per your network requirements.



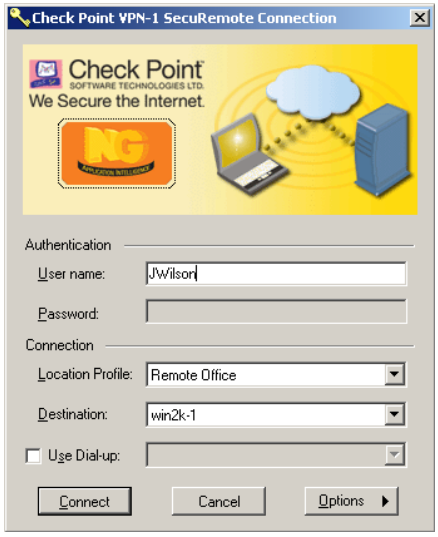
- The first rule states that anyone in the group External is must be 'Authenticated' to be able to use HTTP, FTP, or Telnet. Authentication may be via RADIUS or FireWall-1's internal database.
- The second rule has the SecuRemote group that contains users configured to use RADIUS as their authentication method when using the FTP, HTTP, or Telnet services.

Once you have established your rules, connect to the service using a CRYPTOCard username and response generated from your token.

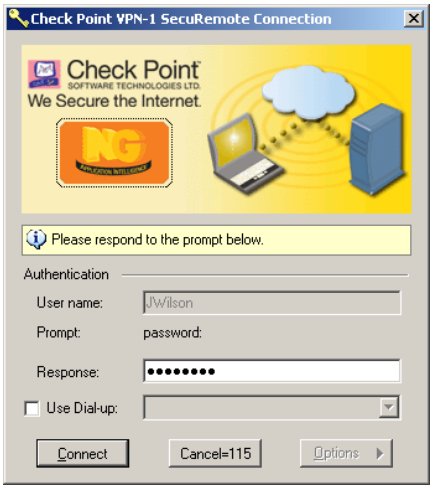
Connect using SecuRemote

After installing SecuRemote /Secure Client and configuring it to connect to the VPN-1 / FW-1 gateway, the end-user will be able to connect to the gateway using their CRYPTOCard token.
Using the connection configured above, launch the SecuRemote connection.

Enter the CRYPTOCard username then click connect.



Enter the PIN + One-time password in the password field, and click OK.



Once the VPN-1 / FW-1 gateway has verified the username and password with the CRYPTO-MAS Server, the secure tunnel will be established.

Solution Overview

Summary	
Product Name	Check Point VPN-1
Vendor Site	http://www.checkpoint.com/
Supported VPN Client Software	Windows VPN Client (Windows Default Check Point VPN-1 SecuRemote Connection Client
Authentication Method	RADIUS Authentication
Supported RADIUS Functionality for Check Point	
RADIUS Authentication Encryption	PAP
Authentication Method	One-time password Challenge-response Static Password
New PIN Mode	User changeable Alphanumeric 4-8 digit PIN User changeable Numeric 4-8 digit PIN

Trademarks

Publication History

Date	Changes
October 27, 2006	Initial Draft
November 9, 2006	Global Draft
November 29, 2006	Minor Revision