

Check Point Software Technologies LTD.

FireWall-1 Version 4.0 How To Configure Authenticated & Encrypted SecuRemote Topology Downloads from a Firewall Module

Authored By: Lewis Colascione – Regional Technical Manager
Date: August 17, 1999
Purpose: To describe and Document how to configure Encrypted & Authenticated SecuRemote topology downloads from a Firewall-1 enforcement module.

Check Point Software Technologies LTD.

Firewall-1 v4.0 provisions the ability to download the SecuRemote topology in an authenticated & encrypted fashion from the Firewall Module enforcement point rather than the Management Server. This addresses the issue of a Management Server being distributed inside a hidden non routable network. Also using the default method of fetching the topology information from a Management Server that is addressable on the Internet without Authentication and Encryption means anyone can access this Topology information, and it is transmitted in the clear.

This can be done if you are using IKE/IPSEC for SecuRemote or any of the FWZ supported schemes. This document outlines the procedure to enable your existing SecuRemote FWZ users to get updates and define site information from a Firewall Module. This solves the issue that may occur when you split your Management Server and Firewall module to different servers.

NOTE: If you already using IKE/IPSEC for SecuRemote users then you will only need to perform Step #4.

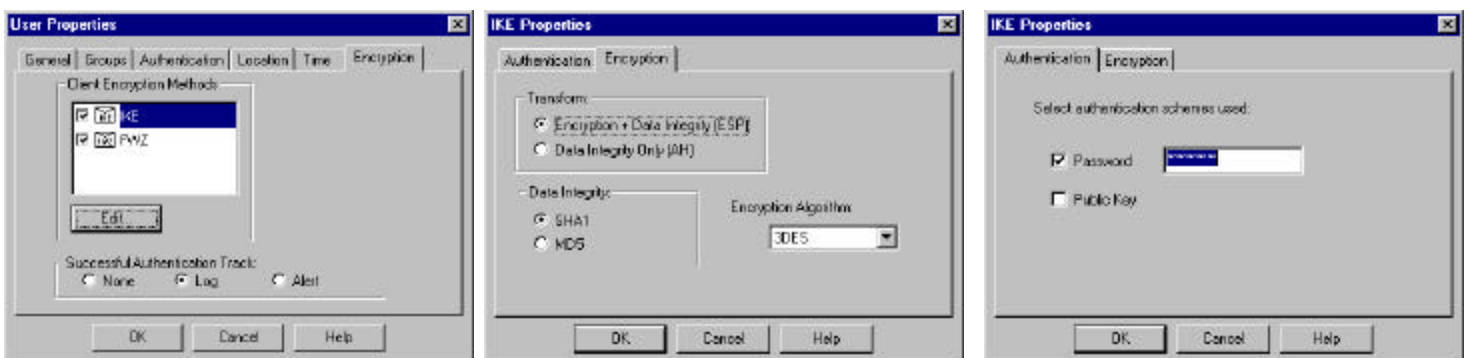
First you must do one of 2 things;

- 1) Create a user ID to be used for the Topology Download authentication challenge.
- 2) Edit your existing users to enable IKE with a shared secret.

Firewall-1 uses the IKE to perform the user challenge and establish an SSL link from the SecuRemote user to the Firewall Module for obtaining the topology information.

4) Create a specific user for Topology Downloads.

- a) Using the user editor create a new default user. *Manage -> Users -> New -> Default*
- b) Go right to the encryption tab and enable IKE.
- c) Edit the IKE properties and select Password Authentication
- d) Enter a password that your users will use for Topology Downloads.
- e) De select the Public Key dialog.
- f) Save and install the user database. NOTE: you do not need to put the user in any groups.

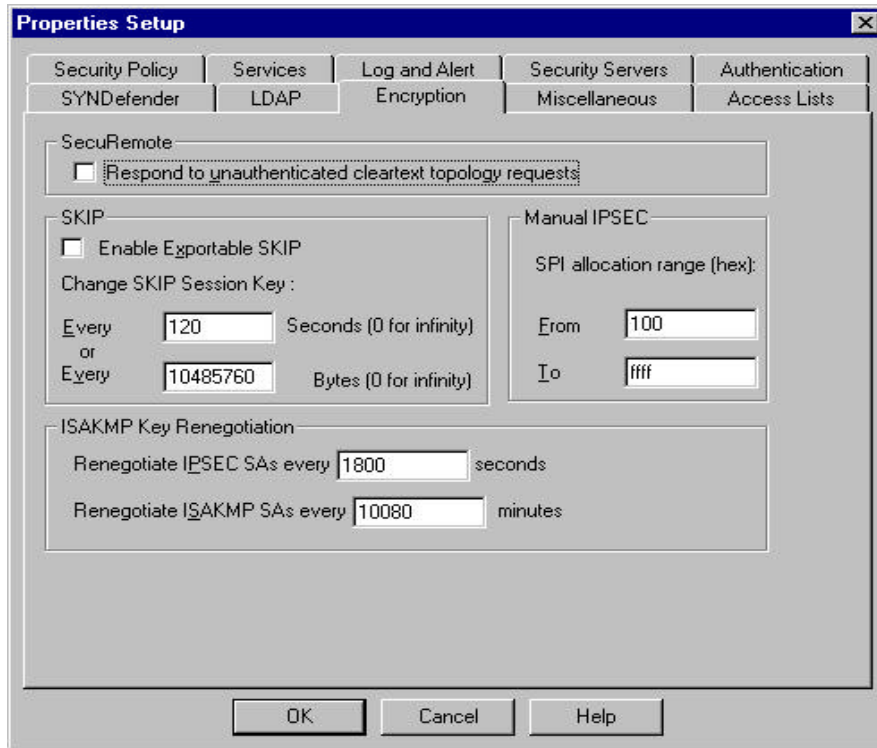


4) Editing an existing user for authenticated topology.

- a) Edit the existing user profile.
- b) Follow from step (b) on the previous instructions.

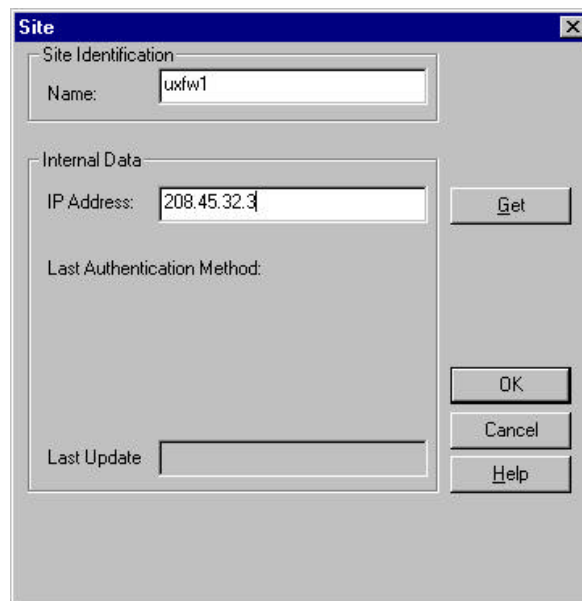
3) Next you must tell the Firewall to accept only Authenticated Topology Downloads;

- a) In the Policy Editor go to *Policy -> Properties -> Encryption* and uncheck the box that allows Firewall-1 to respond to non-authenticated topology requests.

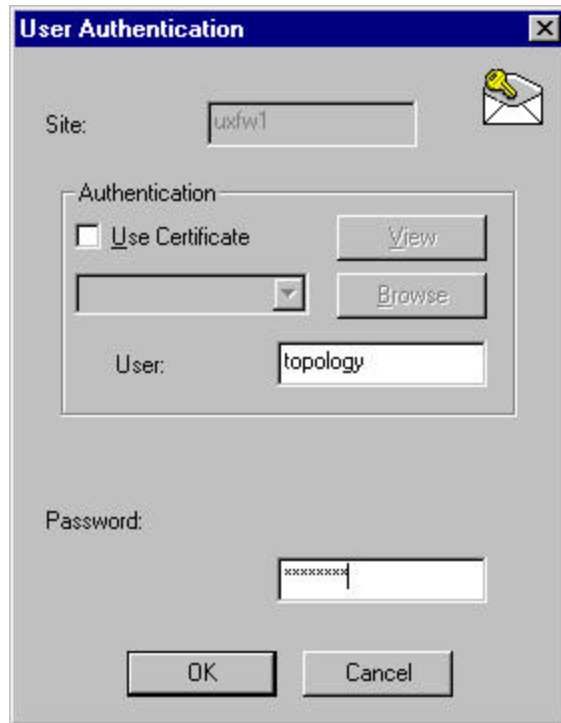


- b) Install the security policy *Policy -> Install*.

4) Now have your v4.0 or higher SecuRemote user attempt a SecuRemote topology download or update their existing site information from the Firewall Module.



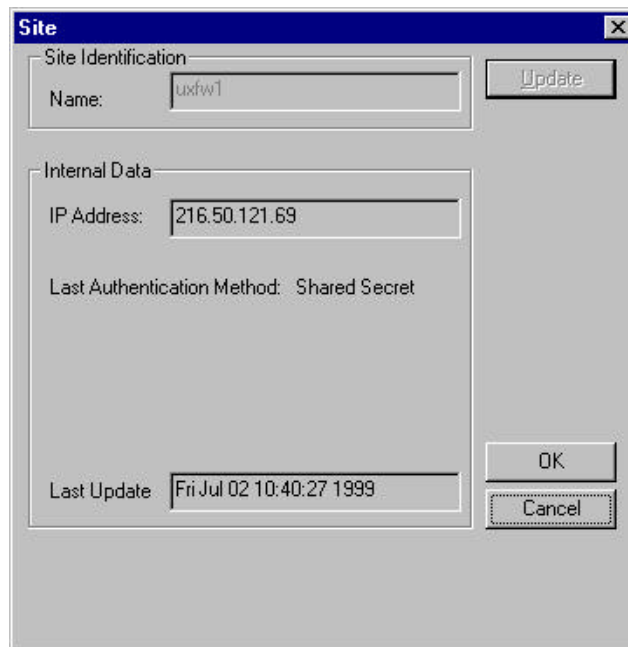
The user will receive an IKE challenge for the topology change. They must enter the ID and PW of the new topology user you created or their ID and the shared secret you gave them when you modified their user profile.



The 'User Authentication' dialog box features a title bar with a close button. The 'Site' field contains 'uxfw1' and has a key icon to its right. The 'Authentication' section includes an unchecked 'Use Certificate' checkbox, a 'View' button, a dropdown menu, and a 'Browse' button. The 'User' field is set to 'topology'. The 'Password' field is masked with 'xxxxxxx'. At the bottom are 'OK' and 'Cancel' buttons.

The Site definition window Last Authentication method will change to Shared Secret Scheme;

The result will be an authenticated encrypted topology download with method of Shared Secret instead of FWZ.



The 'Site' configuration dialog box has a title bar with a close button. It is divided into 'Site Identification' and 'Internal Data' sections. The 'Name' field is 'uxfw1' with an 'Update' button. The 'IP Address' field is '216.50.121.69'. The 'Last Authentication Method' is 'Shared Secret'. The 'Last Update' field shows 'Fri Jul 02 10:40:27 1999'. 'OK' and 'Cancel' buttons are at the bottom right.