

# **Check Point Software Technologies LTD.**

## **Quick Install: ACE Server Setup Procedure FireWall-1 v3.0**

## **Quick Install: ACE Server Setup Procedure FireWall-1 v3.0**

The FireWall-1 software uses the standard client library of the ACE/Server. The Firewall needs to be defined as an ACE Client. Follow these steps to configure your FireWall-1 Gateway to interface with your Security Dynamics ACE Server.

- 1) On the ACE Server configure the Gateway system as an ACE Client.

**NOTE:** Be sure that the ACE server and the client (FW-1) system each refer to the clients hostname/ip-address pair. This pair is derived from the following:

**UNIX:** /etc/hosts file  
/etc/nodename file

**NT:** \winnt\system32\drivers\etc\hosts  
Computer name

- 2) On the ACE server generate the sdconf.rec file.
- 3) Copy the sdconf.rec file to one of the following locations:

**UNIX:** /var/ace

**NT:** %SystemRoot%\system32

- 4) Restart the FireWall.
- 5) When adding users add them in parallel to the FireWall and the ACE Server unless you are using the Generic User feature in 3.0. A description follows.

**NOTE:** The new PIN option is supported with Firewall-1 v3.0.

**NOTE:** In order for DES encryption between the ACE server and the FireWall you must have the DES version of FireWall-1, and a DES encryption license for the management station.

### **Generic Users:**

If you have already defined a large number of users in an external database, you can define these users in FireWall-1 either by entering them manually or by importing them using the *fw dbimport comand* (see "User Database - Importing and Exporting" of FireWall-1 Architecture and Administration). In either case, all the users will be defined and maintained in both databases.

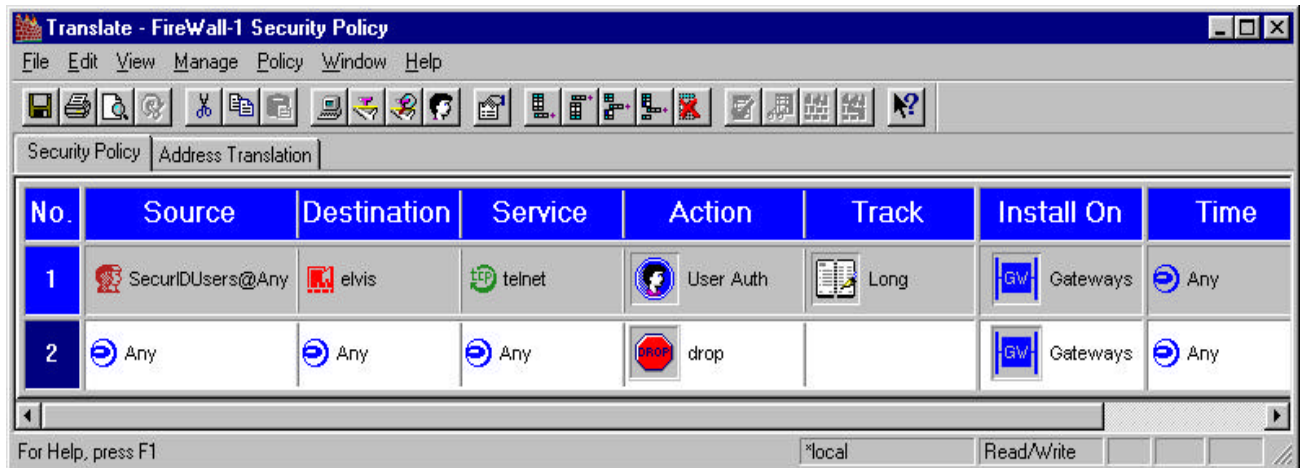
You can avoid the burden of maintaining multiple user databases by defining a user named "generic\*" whom FireWall-1 treats in a special way. FireWall-1 applies the restrictions specified in the User Properties window (for example, those defined in the Location and Time tabs), but for authentication purposes, uses the name typed in by the user instead of "generic\*." In this way, the external authentication server "sees" the user's real name and authenticates him or her accordingly.

#### **Example:**

Definition

For example, suppose you have already defined a large number of users to the Security Dynamics database and they are all authenticating themselves with their SecurID cards. Now, you want to integrate this authentication with FireWall-1, but you do not want to define all your SecurID users in the FireWall-1 User Database. You can use the generic user feature as follows:

1. Define a user group named (for example) SecurIDUsers.
2. Define a user named generic\* as a member of SecurIDUsers.



3. Specify SecurID as the Authentication Scheme for generic\*.
4. Add a rule to the Rule Base similar to this:
5. Install the Security Policy.

**Usage:**

Suppose that Alice is a SecurID user, but she is not defined in the FireWall-1 User Database. When she TELNETs to elvis (and the above rule is applied), the following sequence of events takes place:

1. FireWall-1 prompts Alice for her user name.
2. Alice enters her name.
3. FireWall-1 determines that Alice is an unknown user.
4. FireWall-1 determines that there is a user named generic\* defined in the User Database, whose Authentication Method is SecurID.

**NOTE:** If there is no user named generic\*, FireWall-1 issues the "illegal user name" error message and disallows the connection.

5. FireWall-1 prompts Alice to enter her SecurID password.
6. Alice enters her SecurID password.

7. FireWall-1 contacts the SecurID server and asks to authenticate user Alice, supplying the password Alice entered.

8. The SecurID server notifies FireWall-1 whether Alice was successfully authenticated.

9. FireWall-1 either allows or disallows the connection, based on whether Alice was successfully authenticated.

**Notes:**

1. By using this feature with an external server, you disable FireWall-1's ability to detect invalid user names.

The responsibility of authenticating the user is passed to the external server. You will only get an alert or log if the authentication fails on the external server. Without this option, it is possible to get an alert or log when an invalid user name is entered.

2. By default, all the users defined in the external server are allowed access.

There is no way to treat the users differently (but see item 3 below). The System Administrator should carefully consider the implications of allowing this blanket access.

3. If you wish to deny access to a specific user, define that user in the FireWall-1 User Database and set the user's Authentication Scheme to Undefined.

4. To disable this feature, delete generic\* from the FireWall-1 User Database, or set generic\*'s Authentication Scheme to Undefined.

5. This feature does not work with the S/Key and FireWall-1 Password Authentication Schemes.

The user generic\* will always fail S/Key and FireWall-1 Password authentication, because these schemes are implemented directly by FireWall-1 and not by external servers, so their users must be defined in the FireWall-1 User Database.

Nevertheless, there is still an advantage to be gained by defining a user generic\* with the FireWall-1 Password Authentication Scheme. An attacker who guesses at a user name will not see the error message "unknown user." Instead, the attacker will see a message indicating that the authentication failed, and will not know whether it is the name or the password that is invalid.

6. generic\* cannot be used as the name of a real user.