IBM SecureWay® Firewall for AIX®

Setup and Installation

Version 4 Release 1

IBM SecureWay® Firewall for AIX®

Setup and Installation

Version 4 Release 1

Note

Before using this information and the product it supports, be sure to read the general information under “Appendix. Notices” on page 15.

Sixth Edition (September 1999)

This edition applies to Version 4 Release 1 of the IBM SecureWay Firewall for AIX (product number 5697-F48).

Contents

Chapter 1. Installing the IBM® SecureWay® Firewall for AIX®

This book will tell you how to setup and install the latest version of the IBM® SecureWay® Firewall for AIX®. Before you install the IBM SecureWay Firewall for AIX version 4.1, read “Migrating to the IBM Firewall V4R1” and “Before You Begin”. Following this section, are instructions which tell you how to use the SMIT menus in AIX/6000® to install the IBM Firewall from its distribution media.

Migrating to the IBM Firewall V4R1

If you are using a previous version of the IBM Firewall, first migrate your system to AIX version 4.3.2, and then uninstall your previous version of the Firewall before installing the IBM SecureWay Firewall for AIX V4R1.

Tunnels

Migration of tunnels is automatic and the way it is performed depends your your setup.

1. If there is no firewall installed on the AIX machine, but you were using IPSec tunnels from native AIX, then the tunnels are migrated from the tunnel database because the format of the database has changed. In addition, because there is no support for old headers, IBM tunnels, IPv6 tunnels, and tunnels whose mode is transport, the migration is restricted as follows:
   - tunnel mode
   - IPv4
   - manual tunnel
   - new header
2. If there was an earlier installation of the Firewall, then there can be no AIX IPSec tunnels database, because AIX IPSec and the Firewall have been mutually exclusive from the beginning. Firewalls do not use transport mode (although end systems may). The IBM Firewall has only supported old headers and IPv4. Because we no longer support IBM tunnels, the migration criteria are:
   - manual tunnel
   - KEYED_MD5 is migrated to HMAC_MD5
   - DES_CBC_8 and DES_CBC_4 are migrated to DES_CBC (which is the same thing as DES_CBC_8, but _4 is not generally thought to be useful.
   - CDMF remains CDMF
   - The tunnel IDs will typically change, so if there are filter rules or services with tunnel IDs, they are mapped from the old values to the new ones.

The files are backed up in `/etc/security/FW.savetunnel` in case there is a problem.

Before You Begin

The following checklist helps you plan the IBM Firewall:

- Ensure that you have the required hardware and software needed to install the IBM Firewall. The amount of time required for installation varies depending upon the hardware configuration and the installation media. See “Prerequisite Software and Hardware” for information.
- **Installation causes significant changes to your system. We recommend that you back up your system before you install the IBM Firewall if you want to restore your system to its original state.**
- If the AIX Common Desktop Environment is installed on your system, the firewall installation deactivates and disables it.
- Before you install the IBM Firewall, disable any remotely installed file systems such as NFS, AFS, or DFS.
- Verify that all interfaces are configured and TCP/IP routing tables are defined before installing the IBM Firewall.

Prerequisite Software and Hardware

This section describes the programs and hardware, including memory and disk space, needed by the IBM Firewall.

Software

To install and use the IBM SecureWay Firewall 4.0 for AIX, you must have the following software installed:

- IBM AIX/6000 Version 4.3.2 and the Java Development Kit for AIX, available at **http://www.ibm.com/java/jdk/download** or IBM AIX/6000 Version 4.3.2.
- If you plan to use SNMP, you must install the System View Agent for AIX SNMP Mapper and you should install `bos.net.tcp.server` for the `snmpinfo` command.

By using User-Supplied Authentication, you can build any user-selected form of authentication. If you use User-Supplied Authentication, you must compile your code on an AIX machine compatible with the version of the firewall it is intended to run on.

Hardware

IBM Firewall requires the following hardware configuration.

System Unit

A RISC System/6000® that is supported by the AIX/6000 Version 4.3.2 operating system, excluding shared memory multiprocessors.

Peripheral Devices

Communication Hardware: You can use any communication hardware interface supported by the TCP/IP protocol stack to make the network connections.

In order to be effective as a firewall program, the IBM Firewall must have at least two network interfaces:

- One network interface connects the secure, internal network that the firewall protects.

- The other network interface connects to the nonsecure, outside network or Internet.

The interfaces that have been tested are Token Ring and Ethernet. Other interfaces that should work are:

- Local Area Network adapter for AIX
- X.25
- ATM
- SLIP
- FDDI

Recommended Hardware for Pager Support Notification: You need the following hardware for pager support notification:

- IBM modem or Hayes compatible modem
- A supported pager
- The service provider must support the TAP protocol

Disk Space Requirements: The recommended disk space for this product is:

- Base Firewall - 73MB
- Netscape Browser - 10MB
- xlC Runtime Environment (for SCCS) - 26MB
- AIX 4.3.2 patches - 66MB
- Java Runtime Environment (AIX 4.3.2) - 16MB
- SystemView packages - 5MB
- Report Utilities 1MB
- Approximately 50MB of free disk space for log files. Depending upon the amount of logging done by your firewall, you may need more disk space.

Memory Requirements: The recommended memory for the IBM Firewall is at least 64MB.

Security Authentication Devices

The IBM Firewall directly supports the following security devices that provide remote authentication of your users. You will need one secureID token per user that needs to be authenticated.

Security Dynamics SecurID Card:

- Model SD200 (standard card without buttons)
- PINPAD (card with buttons)

Refer to your Security Dynamics ACE Server documentation for for more information.

Hardening for AIX System Configuration

During installation, hardening maximizes security and efficiency. After installing the IBM Firewall software, including the configuration files, the installation starts editing the system resources that might compromise security.

Hardening is irreversible so you may want to back up your system before you install the IBM Firewall.

Hardening does the following:

- If the AIX Common Desktop Environment is installed on the system, the IBM Firewall installation disables it.
- The IBM Firewall installation removes all unnecessary programs from *inittab*, like nfs and printer daemons.
- System startup invokes only specific firewall daemons. Unnecessary daemons create a security risk.
- All functions that are not required are removed from *inetd*. Only proxy ftp, proxy telnet function, and the remote configuration server are included.
- All logins are disabled for users except root, daemon, bin, adm, nobody, and any previous IBM Firewall users.
- Owners are set to *nobody* and permissions are zeroed out for unowned files and directories.
- Any previous IBM Firewall users are migrated to this new version.
- Unsecure applications, like tftp and rlogind, are disabled.
- The file system integrity checker database is generated.

Installing the IBM Firewall Using SMIT

The System Management Interface Tool (SMIT) provides menus and online help to guide you through installing the IBM Firewall. If you are not familiar with SMIT, refer to *AIX/6000 General Concepts and Procedures for IBM RISC System/6000* for more information.

When you install the IBM Firewall, SMIT installs all the files from the IBM Firewall distribution media. Later, you can configure the functions you want to use and remove the others.

Before you begin the installation, if you have a previous version of the Firewall installed, you need to uninstall it before installing IBM Firewall V4R1.

Log into AIX/6000 as user **root** (the system administrator) with the appropriate password and set the language environment, as described in "Setting the Language Environment for AIX/6000".

Setting the Language Environment for AIX/6000

On AIX/6000, set the language environment to access the catalog. The base firewall is provided with U.S English (en_US codepage) catalogs. The catalogs for all other supported languages are separately installable.

See "Using SMIT to Select Your Language Environment" to select a language environment, if you have not already done so. Note, the AIX default selection of "Generic C", which sets $LANG to C, causes installation of the IBM Firewall to fail.

Using SMIT to Select Your Language Environment

1. Enter `smit mle_cc_set_hdr` at the AIX command line.
2. Click List to get a list of languages.
3. Scroll to select the desired language (the base firewall ISO8859-1 en_US code page).

4. Click OK.

   A dialog appears.
5. It may be necessary to install additional language support filesets from the AIX installation media. If so, fill in the INPUT device/directory for software field.
6. Click List to see a list of input devices.
7. Move the cursor to select an input device.

   If any additional filesets are necessary, SMIT will automatically install them from your media.
8. Click OK.
9. Reboot for these changes to take effect.

Installing the IBM Firewall

After you have selected your language environment, you are ready to install the IBM Firewall.

1. Insert the IBM Firewall CD-ROM into the CD-ROM drive.
2. Start the installation program by entering `smit install_package` on the command line.

   The *Install and Update Software Package Name* panel appears.
3. Click List.
4. Select the `/dev/cd0` option from the list to install the IBM Firewall from the CD-ROM drive.
5. Click OK.

   The *Multi Select List* panel appears.
6. Select FW. Then select from the following options:
   - EFM
     - IBM Enterprise Management System (a Firewall that manages other Firewalls)
   - FW
     - Base IBM SecureWay Firewall
     - IBM SecureWay Firewall Common Libraries and Catalogs
     - IBM SecureWay Firewall HTTP Proxy
     - IBM SecureWay Firewall Remote Configuration Client
     - IBM SecureWay Firewall Report Generation Utilities
   - Netscape
     - Netscape Communicator
   - nsauditor
     - Network Security Auditor
   - sva
     - System View Agent for AIX
     - System View Agent for AIX SNMP Mapper
7. Select Base IBM Firewall. If you would like to have the IBM Firewall configuration client, select the Configuration Client too. The Netscape Communicator is included when you install the configuration client. **Report Utilities** and **Configuration Client** are separate installable packages, which you can install on non-firewall machines.
8. Click Enter after making all selections.

The previous SMIT menu reappears with the IBM Firewall selected.

Click Enter to start the installation. The next screen asks whether you want to continue.

9. Click Enter; SMIT installs the selected items.
10. When the installation is complete, select Exit SMIT from the Exit menu or press F12 to Exit.

    The SMIT window is closed.

If you have installed the IBM Base Firewall:

- Be sure to **REBOOT** your system before proceeding. When you reboot, the Firewall filter is active using the default filter rules described in the *IBM SecureWay Firewall for AIX User's Guide*.
- After you reboot, configure firewall filter rules to permit and deny specific IP traffic. Please refer to the *IBM SecureWay Firewall for AIX User's Guide* in order to configure a usable firewall.
- XLOCK circumvents firewall authentication. Therefore, if you want to use XLOCK, issue the command `chuser SYSTEM=compat root:`. The system will prompt for a password at logon, in addition to the firewall authentication, which can also be password.
- After you install the IBM Firewall on your disk, read the *README* file, which contains any updates to product installation instructions and functions. The *README* file is accessible through the main IBM Firewall configuration client panel. Click Help on the main configuration client panel and choose Read Me from the dropdown list.
- After you log onto the IBM Firewall for the first time, the setup wizard appears automatically. It aids you with the initial configuration of the Firewall. It is especially helpful if you do not have extensive knowledge of the firewall configuration because it enables you to have a basic firewall configuration up and running quickly after installation. See the *IBM SecureWay Firewall for AIX User's Guide* for more information.

Configuring the IBM Firewall from a Remote Configuration Client

In order to configure the IBM Firewall from a remote configuration client (one that is not installed on the same machine as the IBM Firewall), you must do the following:

1. Reboot and log into the AIX machine where the IBM Firewall is installed.
2. Using either SMIT or smitty select:

   ```
   Security & Users
       Users
          Change/Show Characteristics
   ```

3. Select root and set *User can LOGIN REMOTELY?* to true.
4. Type the following command on the prompt:

   ```
   fwcfgsrv cmd=change localonly=no
   ```

5. Type the following command on the prompt:

   ```
   fwuser cmd=change username=root remauth=password remadmin=password
   ```

Chapter 2. Installing the Triple DES Feature

If you are in a country that allows stronger encryption, you may be eligible to upgrade your IBM Firewall V4R1 with the Triple DES feature.

You can install the Triple DES feature from a web site. See the IBM Firewall product README file for more information about this web site.

1. Start the installation program by entering *SMIT* at the command line.
2. Select *Software Installation and Maintenance*.
3. Select *Install and Update Software*.
4. Select *Install and Update from the Latest Available Software*.
5. Enter the file path location for the triple DES feature.
6. Click *OK*.
7. On the *Software to Install* menu, click *List*.
8. From the *Multi-Select List*, choose:

   ```
   bos.crypto-priv
     +4.3.2.0 Triple DES Encryption for IP Security
   ```

9. Click *OK*.
10. Reboot your machine.

Chapter 3. Removing the Installed Packages

This section describes how to disable your firewall and remove the IBM Firewall and the configuration client from your AIX system.

Note: If you remove the installed packages, hardening will not be reversed.

Start the removal of the installation program by entering `smitty install_remove` at the AIX command line. You will get the Remove Installed Software menu.

1. From SMIT press F4 to get a list.
2. Move the cursor to select the software you want to remove. Press F7. Then press Enter.
3. In the PREVIEW only field, use the tab key to get **No**.
4. In the REMOVE dependent software field, use the tab key to get **Yes**.
5. Click Enter.
6. SMIT asks you to confirm the removal of the IBM Firewall.
7. Click Enter to remove the IBM Firewall.

   Note: Please reboot your system, after you remove the firewall code, to remove active filters from memory.

User **root** has been restored as a regular AIX user

Chapter 4. Installing the IBM SecureWay Firewall Client for Windows

This section tells you how to install the IBM SecureWay Firewall client on a Windows machine so that you can remotely configure the IBM Firewall for AIX.

Before you install the IBM Firewall Client do the following:

Prerequisite Software and Hardware

This section describes the programs and hardware, including memory and disk space, needed by the IBM Firewall client.

Software

To install and use the IBM Firewall Client, you must have Microsoft Windows NT Version 4.0, Windows 95, or Windows 98 installed.

Minimum Hardware Configuration

IBM Firewall Client requires the following hardware configuration.

System Unit

- Pentium Processor 100MHz
- 32MB RAM
- 1GB hard drive

Disk Space Requirements

The recommended disk space for this product is:

- Configuration Client - 60MB
- Netscape Browser - 15MB
- Report Utilities - 3MB
- Socks Monitor - 4MB

Note: These disk space requirements are based upon installing on a FAT partition of less than 512MB. If your FAT partition is more than 512MB, then the space used on your hard drive can be more than the given requirements above.

Installing the IBM Firewall Client

1. Click Start or specify *x:\nt40\en_US\Client\setup.exe* from the command line, where *x:* is your CDROM drive.
2. Click Run.
3. Click OK to start the installation program.
4. Click Next and the copyright statement is displayed.
5. Click OK. You are given the option to install the Netscape Communicator program.

6. When the Netscape Communicator installation has completed, click OK to continue.

   After you install Netscape, the IBM Firewall install program continues.
7. From the IBM Firewall Client Installation Options dialog, select the items you want to install from the components list.
8. Click Next.
9. Double-check your configuration; click Next.
10. Click Finish to exit installation.

Reboot your system.

Note that the configuration client displays help by using the default program associated with .html files. If you choose to install Netscape Communicator 4.07 as provided with the IBM Firewall, you will need to manually associate .html files with Netscape. See *associating file types with programs* in the Windows help utility for details.

Chapter 5. Installing the IBM Firewall Documentation

To install the following documentation:

- *IBM SecureWay Firewall for AIX Setup and Installation*
- *IBM SecureWay Firewall for AIX User's Guide*
- *IBM SecureWay Firewall for AIX Reference*
- *A Comprehensive Guide to Virtual Private Networks, Volume 1: IBM Firewall, Servers and Client Solutions* (a redbook)

download the following files from the `books/en_US` directory on the IBM Firewall CDROM to your workstation:

- *fwinstal.pdf* - (this book)
- *fwuser.pdf*
- *fwref.pdf*
- *fwinstal.html* - (this book)
- *fwvpnrbk.pdf* - available in English only from the English directory

Use the Adobe Acrobat Reader Version 3.0 to view these books. If you do not have the Adobe Acrobat Reader installed, you can go to the Adobe Web Site at: **www.adobe.com/prodindex/acrobat/** to learn more about the Adobe Acrobat Reader and to get a copy.

You can also order a hardcopy of the *IBM SecureWay Firewall for AIX User's Guide, GC31-8419-03* and the *IBM SecureWay Firewall for AIX Reference, SC31-8418-03*.

Appendix. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Department TL3B/ Building 062
P.O. Box 12195
3039 Cornwallis

Research Triangle Park, NC 27709-2195
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

IBM is required to include the following statements in order to distribute portions of this document and the software described herein to which contributions have been made by the University of California and NEC Systems Laboratory.

This product includes software developed by the University of California, Berkeley and its contributors.

This product contains code licensed from RSA Data Security Incorporated.

Trademarks

The following terms are trademarks of the IBM corporation in the United States or other countries or both:

- AIX
- AIX/6000
- SecureWay
- IBM
- RISC/6000
- RISC System/6000

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States and/or other countries.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States and/or other countries.

Other company, product, and service names may be trademarks or service marks of others.

Readers' Comments — We'd Like to Hear from You

IBM SecureWay® Firewall for AIX®
Setup and Installation

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	□	□	□	□	□

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	□	□	□	□	□
Complete	□	□	□	□	□
Easy to find	□	□	□	□	□
Easy to understand	□	□	□	□	□
Well organized	□	□	□	□	□
Applicable to your tasks	□	□	□	□	□

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? □ Yes □ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.

Readers' Comments — We'd Like to Hear from You

Cut or Fold
Along Line

Fold and Tape

Please do not staple

Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Information Development
Department CGMD / Bldg 500
P.O. Box 12195
Research Triangle Park, NC
27709-9990

Fold and Tape

Please do not staple

Fold and Tape

Cut or Fold
Along Line

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.