IBM ®

IBM eNetwork Firewall V3.2 for AIX and for Windows NT — Internet Security Offering

Overview

A firewall allows an organization to establish security policies, allowing only authorized communications between networks inside and outside of their organization. IBM continues its worldwide leadership for Internet security offerings by adding Firewall for Windows NT™ to Firewall for AIX® in a new and enhanced release.

IBM Firewall V3.2 for AIX and Firewall V3.2 for Windows NT programs are both provided on a single CDROM to allow customers to choose the product that best meets the configuration needs of their organization. Every Firewall program package and program package upgrade will include the Security Dynamics Ace/Server with a two-user license.

This release of Firewall includes menu and message support for eight National Languages in addition to English. The support applies to both AIX and Windows NT. All eight language translations are on the CDROM.

Firewall V3.2 for AIX is an extension to Firewall V3.1 for AIX. Refer to Software Announcement 297-122, dated April 30, 1997. The remote client that ships with the Firewall now has support for additional authentication methods. Firewall V3.2 for Windows NT is a new offering based on Firewall for AIX.

Management capabilities make creating and distributing your security policies throughout the organization secure, yet simple. Using a graphical user interface (GUI) written in Java™, an administrator can remotely create policies for multiple firewalls and then activate them worldwide. With different authorization levels, central administrators can establish corporate policies, while remote administrators meet local needs.

IBM Firewall supports all three standard methods of firewalling: circuit-level gateways, application proxies, and advanced filtering.

Firewall for Windows NT currently provides Network Address Translation (NAT) functionality with Application Proxies and SOCKS Circuit Level Gateway. IBM will additionally provide NAT via the expert filter function. For availability and shipment information, refer to the firewall Web page at:

http://www.software.ibm.com /enetwork/firewall

To make the IBM Firewall easier to acquire for small organizations or departments of larger companies, we now offer pricing based on the number of host addresses per Firewall server. An entry-level program for up to 25 host addresses per Firewall server is now available to make implementing security more affordable.

The IBM Firewall also includes software developed by RSA and the University of California, Berkeley, and its contributors.

Intended Customers

Private and public enterprises that deal in sensitive or proprietary data. Examples of such industries include banking, government, healthcare, and research. Examples of sensitive data include personnel data, credit reports, business financial data, new product development, and government intelligence.

At a Glance

IBM's Firewall V3.2 for AIX and for Windows NT includes:

- All leading firewall architectures

- Common administration of AIX and Windows NT Firewalls

- Java-based GUI for remote management and administration

- Hardening of the operating system

- National Language Support

- Realtime log monitor, reporting, and SafeMail proxy

- Multi-level authorizations

Key Prerequisites

The Netscape Navigator, a Java-enabled browser, is required to use the Firewall GUI.

The Microsoft Accelerator Package is required for the IPSEC remote client on Windows® 95. The feature applies to Firewall for AIX.

Planned Availability Dates

- April 17, 1998, for Firewall V3.2

- May 15, 1998, for Firewall V3.2 Windows NT National Language support

- Targeted for June 30, 1998, for Firewall V3.2 Windows NT NAT enhancement

---

Description

Firewall V3.2 for AIX and Firewall V3.2 for Windows NT are network security "firewall" programs for RS/6000™ or Intel® Pentium® processor machines. In essence, a firewall is a blockade between a secure, internal private network and another (non-secure) network or the Internet. The firewall has two main functions:

- To prevent users in your own network from freely exchanging information with users outside your network.

- To prevent users who are outside your network from coming in to compromise or attack your network.

Normally, hosts in a secure network cannot access the outside network. This reduces the risk of being intruded upon by unauthorized users from the Internet but denies Internet accessibility to users within the secure network. Without Internet accessibility, users in the secure network cannot use important tools such as Telnet, FTP, Gopher, and World Wide Web to access the resources available on the Internet. The IBM Firewall offers a secure access to the Internet, with the capability of being very selective as to who it lets in.

In order to control access between your network and the Internet and facilitate authorized transactions, IBM provides these services and barriers:

New Functions in Firewall V3.2 for AIX:

- IPSEC Remote Client on Windows 95 ─ This function is installed on the client to encrypt all of the data that flows between the client and the firewall. It is extremely useful for remote users, users on the road, remote sales force on the road, people working from home, and so on.

  A No-Charge Function ─ Three main benefits:

  - This does not tie a client to a specific ISP. The TCP/IP address that is assigned by your ISP is irrelevant. You can change ISPs and TCP/IP addresses without having an affect on the operation of this function.

  - Supports the IPSEC standard.

    -- Uses 56-bit DES key, which provides data confidentiality, data integrity, and authentication

    -- Also supports CDMF

  - Authentication can now be done with a full range of choices that include DES-encrypted password and one-time password (for example S-Key or security token).

- The AIX and Windows NT Firewalls can be administered from an AIX, Windows NT, or Windows 95 remote configuration client.

Firewall V3.2 for Windows NT Includes the Following Functional Capabilities:

- Application proxies

  - FTP
  - Telnet
  - HTTP

- Transparent Proxy for Telnet and FTP ─ This is a transparent proxy function for the Telnet and FTP protocols which provides a seamless access by the firewall without prompting for userid and password. It is a configurable option that only allows for processing from the secure side of the firewall to the non-secure side of the firewall.

- HTTP proxy ─ Seamless Internet access for WWW browsers without the need for Socks.

- Socks Server

  - Support for Socks Version 5
  - Authentication of clients
  - Supports many TCP protocols

- IP Address Pricing Per Firewall Server ─ New pricing levels have been established based on the number of IP addresses initiating outbound session requests through the firewall per Firewall server. The new levels per Firewall server are:

  - 25 IP addresses (entry)
  - 50 IP addresses (small)
  - 250 IP addresses (medium)
  - Unrestricted IP addresses (unlimited)

- GUI Administration ─ A Java-based GUI to administer one or more remote Firewalls or a local Firewall:

  - For remote administration, encryption is done on a Windows NT machine via SSL:

    -- The administrator is authenticated with a password before accessing a Firewall.

    -- All traffic is encrypted between the administrator's workstation and the Firewall, thus protecting the confidentiality of the data.

  - For local administration, authentication can be done with a full range of choices that include: Firewall password, NT logon password, and one-time password schemes such as Secure Net Key Cards and Security Dynamics' SecurID Card.

  - Prevents multiple administrators from changing configuration files at the same time.

  - Applets are required on the administrator's workstations.

  - Java applets are secure because they are installed and run on the client. They are not downloaded across the network.

  - The AIX and Windows NT Firewalls can be administered from an AIX, Windows NT, or Windows 95 remote configuration client.

- Filtering

  - Ability to permit or deny traffic on a packet-by-packet basis

  - Filter rules by time-of-day (TOD), date, and day of week

  - No limit on the number of filter rules

- Report Utilities

  - Logfile is formatted with tags that allow the user to generate reports.

  - Utilities are provided to build tables and import them into an SQL data base engine.

  - Sample queries will be provided.

  - The Syslog will remain available, providing compatibility with existing customer report generation.

- SafeMail Mail Proxy

  - Supports SMTP and mime extensions.
  - Mail is not stored on the Firewall.

- Private side domain names are hidden on outbound mail.

- Administration Level by Function

  - Administrative activities are categorized by product function.

  - Specify what functions an administrator can configure.

  - Each administrator's actions are logged with their userid.

  - The administrators do not require root logon level.

- Real-Time Log Monitor

  - Log monitor notifies the administrator of a detected threshold condition on a real-time basis.

  - The monitor looks at each item as it is written to the log, therefore, not missing any events due to time periods.

- Default User Authentication — Provides an API to which customers can write in order to perform user-supplied authentication. If a userid has not been defined at the firewall, the firewall will attempt to call a user-supplied authentication method to validate the ID.

- Password Rules

  - Administrators can logon with their own userids or with the root logon to administer the Firewall.

  - Some of the new password rules are:

    -- Number of failed logons before user account is locked

    -- Number of days to warn user before password expires

    -- Number of passwords before you can reuse them

    -- Number of weeks before password can be reused

- SMP Support

- Firewall for Windows NT does not support virtual private networks (VPNs) at this time. Therefore, neither DES nor CDMF data transfer encryption is provided.

Year 2000

This product is Year 2000 ready. When used in accordance with its associated documentation, it is capable of correctly processing, providing, and/or receiving date data within and between the 20th and 21st centuries, provided all other products (for example, software, hardware, and firmware) used with the product properly exchange accurate date data with it.

Reference Information

Evaluation: Once the product has become generally available, the IBM Firewall for AIX CDMF encryption version and Firewall V3.2 for Windows NT will be available for evaluation at no charge via electronic download from the Internet at:

http://www.software.ibm.com /enetwork/firewall

After 60 days, the functions are automatically disabled.

For those who want to continue to use the IBM Firewall after the 60-day evaluation period, it must be ordered for a fee.

Trademarks

RS/6000 is a trademark of International Business Machines Corporation in the United States or other countries or both.
AIX is a registered trademark of International Business Machines Corporation in the United States or other countries or both.
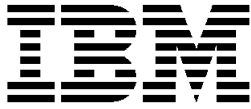Intel and Pentium are registered trademarks of Intel Corporation.
Windows NT is a trademark of Microsoft Corporation.
Microsoft and Windows are registered trademarks of Microsoft Corporation.
Java is a trademark of Sun Microsystems, Inc.
Other company, product, and service names may be trademarks or service marks of others.

Education Support

The following courses will be available.

Course Title	Course Number
Internet Security and Firewall Planning	N3202
IBM Firewall for AIX	N3203
IBM Firewall for NT Implementation Lab	N3204

Visit the following Web site for additional information:

http://www.software.ibm.com /enetwork/firewall

The appropriate curriculum will be updated, as necessary, to include the enhancements described in this announcement.

Publications

No publications are shipped with this program.

The following publications can be ordered after availability. To order, contact your IBM representative.

Title	Order Number
IBM eNetwork Firewall for AIX® NT User's Guide	GC31-8419
IBM eNetwork Firewall for AIX Reference Guide	SC31-8418
IBM eNetwork Firewall for Windows NT™ User's Guide	GC31-8658
IBM eNetwork Firewall for Windows NT Reference Guide	SC31-8659
Protect and Survive using IBM Firewall for AIX	SG24-2577

In addition, you can use the IBM Internet Firewall Web site:

http://www.software.ibm.com /enetwork/firewall

to download, view, and print the firewall publications in HTML format and in PDF (portable document format). For printing PDF files, you'll need the Adobe Acrobat Reader, which is available through:

http://www.adobe.com/prodindex/acrobat/

Displayable Softcopy Publications: The following English and translated publications are offered in softcopy form. The displayable manuals are included as part of the basic machine-readable material at no additional charge. The files are shipped on the same media type as the basic machine-readable material (CD-ROM).

These files can be used with the PDF (Print Document Facility), in conjunction with the ADOBE Acrobat Reader licensed programs, in any of the supported environments to create unmodified printed copies of the manuals. Terms and conditions for use of the machine-readable files are shipped with the files.

- IBM eNetwork Firewall for AIX User's Guide
- IBM eNetwork Firewall for AIX Reference Guide
- IBM eNetwork Firewall for Windows NT User's Guide
- IBM eNetwork Firewall for Windows NT Reference Guide

Technical Information

Specified Operating Environment

Hardware Requirements:

For Firewall on AIX:

- An RS/6000™ including IBM Power Series® Family with the AIX Version 4.2.1 or 4.3 operating system, excluding shared memory multiprocessors

For Firewall on Windows NT:

- A single, dual, or four-processor Intel® Pentium® 133 MHz machine

Firewall for both AIX and Windows NT requires:

- A minimum of 64 MB of memory

- Approximately 100 MB of free disk space for the following:

  - 50 MB for the base Firewall, Netscape Navigator, SystemView®, Report Utilities, and AIX or Windows NT patches

  - 50 MB for log files

    Depending on how you configure your Firewall, your storage needs for logs will vary. For example, if you record little data in the log file, you might need as little as 1 MB of log storage per day. However, if you implement a full Socks Firewall, you could need as much as 30 MB per day for log files. Assuming you want to keep seven days worth of logs, this is 210 MB disk space for logs.

- A CD-ROM drive for product installation

- Peripheral devices:

  - Mouse, trackball, TrackPoint®, and pen

    Although all functions can be performed with the keyboard, a pointing device is also recommended

- At least two network adapters, for the IBM Firewall to be effective as a firewall program

  - Supported by TCP/IP protocol stack.

This announcement is provided for your information only. For additional information, contact your IBM representative, call 800-IBM-4YOU, or visit the IBM home page at: http://www.ibm.com.

- One network adapter connects the secure, internal network that the firewall protects

- The other network adapter connects the non-secure, outside network or Internet

- Adapters:

    -- All adapters supported by NDIS including Token Ring and Ethernet
    -- Local Area Network Adapter (AIX Only)
    -- X.25, ATM, FDDI, or S/390® (AIX Only)

- IBM modem or Hayes compatible for pager support

- Supported pager (TAP protocol)

- Communication hardware interface supported by TCP/IP protocol stack

- IBM PC or compatible that is supported by the Microsoft® Windows® 95 operating system (required for AIX IPSEC remote client only)

Software Requirements: To install and use the IBM Firewall Version 3.2 for AIX, you must have the following programs installed:

- IBM AIX/6000® Version 4.3 or 4.2.1 and AIX 4.2 Bonus Pak.

- Microsoft Windows 95 in support of IPSEC remote client.

- Microsoft ISDN Accelerator Pack (required for IPSEC remote client only). The ISDN Accelerator Pack can be downloaded from:

    http://www.microsoft.com/windows /download/msisdn11.exe

- Netscape Navigator Java™ Browser V3.0 or higher.

To install and use the IBM Firewall Version 3.2 for Windows NT, you must have the following programs installed:

- Windows NT Server V4.0

- Windows NT Service Pack 3

The following Microsoft corrective service hotfixes should be installed:

- For ndis_fix, q156655 (required for SMP support)

- For dns_fix, q169461 (required for DNS support)

- simptcp_fix, q154460 (improved security)

- teardrop2_fix, q179129 (improved security)

These fixes should be installed in the listed sequence.

The English versions of these hotfixes are currently available from Microsoft, Inc.

Some hotfixes may not be available for select language versions of Windows NT V4.0. Availability of hotfixes from Microsoft, Inc. may impact function and security for national language versions of the Firewall for Windows NT. For additional information on Microsoft hotfixes, refer to:

http://www.microsoft.com/Support

Compatibility: Security Authentication Devices ─You can use the IBM Firewall V3.2 for AIX and for Windows NT with the following security devices to provide remote authentication of your users:

- AssureNet Pathways SecureNet Key Card

- Model SNK-010
- Model SNK-004

- Security Dynamics SecurID Card

- Model SD200
- PINPAD

Packaging: The IBM Firewall V3.2 for AIX and for Windows NT package includes:

- One CD-ROM containing:

    - IBM Firewall product
    - Report Utilities
    - Configuration Client
    - English Netscape Navigator for AIX
    - English Netscape Navigator for Windows
    - The following softcopy publications:

        -- IBM Firewall for AIX User's Guide in all nine languages

        -- IBM Firewall for AIX Reference Guide in all nine languages

        -- Protect and Survive using IBM Firewall for AIX in English

    - The following English softcopy publications. Translated versions also will be on the CD-ROM that ships the Firewall for Windows NT national languages.
        -- IBM Firewall for Windows NT User's Guide
        -- IBM Firewall for Windows NT Reference Guide

- Where are the Books Brochure

- Firewall Installation Booklet in the appropriate language

- Proof of License

- Program License Agreement

- License Information Booklet

- Registration Card (must be returned for customer contact)

- Security Dynamics Ace/Server package including:

    - Two CD-ROMS containing Ace/Server code and product documentation

    - Three diskettes containing:

        -- SoftID code for two users
        -- License for Ace/Server
        -- Seed records for SoftID

    - Quick Start document and registration card

    - Postcard to receive two free key fobs

Security, Auditability, and Control

The security and auditability features of Firewall V3.2 for AIX and for Windows NT include the following:

- User identification/authentication
- Secured network
- Intrusion alarm
- Error log tracking
- Real time log monitor
- Report utilities
- Secured passwords

In addition, Firewall V3.2 for AIX includes:

- Virtual private networks

- IPSEC for remote client with strong authentication
- Configuration file checksum monitor

The customer is responsible for evaluation, selection, and implementation of security features, administrative procedures, and appropriate controls in application systems and communication facilities.

Ordering Information

IBM Firewall V3.2 for AIX and for Windows NT has one charge unit (install), and is orderable as a program package. These firewall units are also available at upgrade prices for those customers licensed for IBM Firewall V3.2, IBM Firewall V3.1 for AIX, and Internet Connection Secured Network Gateway V2 (ICSNG) or non-IBM Firewalls.

The IBM Firewall is offered at four usage levels (Entry, Small, Medium, and Unlimited). Ordering a program package entitles one server for either Entry (25 IP addresses), Small (50 IP addresses), Medium (250 IP addresses), or Unlimited (unrestricted IP addresses). Upgrades from Firewall V3.2 are allowed from Entry, Small, or Medium to a higher usage level of Firewall V3.2. Upgrades from Firewall V3.1 are allowed to the same usage level of Firewall V3.2; for example, Small to Small.

The following program packages include DES and CDMF encryption on AIX.

Description	Order Type Number	Feature Number	Part Number
Firewall V3.2 for AIX and Windows NT, Entry	5801-AAR	7213	04L4962
Firewall V3.2 for AIX and Windows NT, Small	5801-AAR	7214	04L0992
Firewall V3.2 for AIX and Windows NT, Medium	5801-AAR	7215	04L0993
Firewall V3.2 for AIX and Windows NT, Unlimited	5801-AAR	7216	04L0994

Upgrades: Upgrades to IBM Firewall V3.2 for AIX and Windows NT are allowed from IBM Firewall V3.1, Internet Connection Secured Network Gateway (ICSNG) V2.1 and V2.2 or non-IBM firewalls, and from smaller V3.2 programs to larger V3.2 programs. Upgrades from Firewall V3.1 are no charge. Upgrades are allowed from any language to any language.

The following upgrades to Firewall V3.2 include DES & CDMF encryption on AIX.

Description	Order Type Number	Feature Number	Part Number
Firewall V3.2 Upgrade V3.1 Small to V3.2 Small	5803-AAR	4590	04L4565
Firewall V3.2 Upgrade V3.1 Medium to V3.2 Medium	5803-AAR	4591	04L4566
Firewall V3.2 Upgrade V3.1 Unlimited to V3.2 Unlimited	5803-AAR	4592	04L4567
Firewall V3.2 Upgrade ICSNG V2 or non-IBM Firewall to V3.2 Entry	5803-AAR	1110	04L7535
Firewall V3.2 Upgrade ICSNG V2 or non-IBM Firewall to V3.2 Small	5803-AAR	4587	04L4562
Firewall V3.2 Upgrade ICSNG V2 or non-IBM Firewall to V3.2 Medium	5803-AAR	4588	04L4563
Firewall V3.2 Upgrade ICSNG V2 or non-IBM Firewall to V3.2 Unlimited	5803-AAR	4589	04L4564
Firewall V3.2 Upgrade V3.2 Entry to V3.2 Small	5803-AAR	4593	04L4971
Firewall V3.2 Upgrade V3.2 Entry to V3.2 Medium	5803-AAR	4594	04L4972
Firewall V3.2 Upgrade V3.2 Entry to V3.2 Unlimited	5803-AAR	4595	04L4973
Firewall V3.2 Upgrade V3.2 Small to V3.2 Medium	5803-AAR	4596	04L4568
Firewall V3.2 Upgrade V3.2 Small to V3.2 Unlimited	5803-AAR	4597	04L4569
Firewall V3.2 Upgrade V3.2 Medium to V3.2 Unlimited	5803-AAR	4598	04L4570

Upgrade Protection (Entitled Customers): Customers who have previously acquired Software Advantage Upgrade Protection, as shown in the table below, will automatically receive their program package or upgrade shortly after general availability.

Description	Upgrade Protection One-Time Charge Part Number	Quarterly Charge Part Number	Program Package Part Number
Upgrade Protection for:			
Firewall V3.1 for AIX 56-Bit DES & CDMF, Small	84H7740	84H7741	04L0992
Firewall V3.1 for AIX 56-Bit DES & CDMF, Medium	84H7742	84H7743	04L0993
Firewall V3.1 for AIX 56-Bit DES & CDMF, Unlimited	33H4303	33H4304	04L0994

Terms and Conditions

Licensing: IBM International Program License Agreement. Proofs of Entitlement (PoE) are required for all authorized use.

Limited Warranty Applies: Yes

Program Services: Available until January 31, 2001

Money-back Guarantee: Two months, money-back guarantee for program packages

Copy and Use on Home/Portable Computer: No

Usage Restriction: Yes. Charges for these programs are based upon the resources that they use or manage. The total number of resources used or being managed may not exceed the number authorized by the applicable Proof of Entitlement. If the total exceeds the quantity in the Proof of Entitlement, the customer must notify IBM or their reseller as stated in the IPLA.

Support Line: Personal Systems

AIX

Complimentary Introductory Support: Not available for OS/2® platform

Length of time:	60 days
Must be part of solution with:	RS/6000 brand system acquired from IBM
Applies to:	First installation in customer enterprise

Upgrades: Customers may acquire upgrades up to the currently authorized level of use of the qualifying programs.

Volume Orders: Volume licensing part numbers and prices will be announced on April 28, 1998.

Entitled Upgrade for Current SW Advantage Upgrade Protection Licensees: Yes

Entitled Upgrade for Current AIX/UNIX® Upgrade Protection Licensees: No

Variable Charges Apply: No

Charges

Description	Part Number	One-Time Charge	Monthly Optional Support Line Charge
The following Program Packages include DES and CDMF encryption on AIX.			
Firewall V3.2 for AIX and Windows NT, Entry	04L4962	$ 2,499	$230
Firewall V3.2 for AIX and Windows NT, Small	04L0992	4,499	230
Firewall V3.2 for AIX and Windows NT, Medium	04L0993	9,499	230
Firewall V3.2 for AIX and Windows NT, Unlimited	04L0994	16,500	230
The following upgrades to Firewall V3.2 include DES & CDMF encryption on AIX.			
Firewall V3.2 Upgrade V3.1 Small to V3.2 Small	04L4565	0	230
Firewall V3.2 Upgrade V3.1 Medium to V3.2 Medium	04L4566	0	230
Firewall V3.2 Upgrade V3.1 Unl to V3.2 Unl	04L4567	0	230
Firewall V3.2 Upgrade ICSNG V2 or non-IBM Firewall to V3.2 Entry	04L7535	599	230
Firewall V3.2 Upgrade ICSNG V2 or non-IBM Firewall to V3.2 Small	04L4562	999	230
Firewall V3.2 Upgrade ICSNG V2 or non-IBM Firewall to V3.2 Medium	04L4563	2,999	230
Firewall V3.2 Upgrade ICSNG V2 or non-IBM Firewall to V3.2 Unlimited	04L4564	5,499	230
Firewall V3.2 Upgrade V3.2 Entry to V3.2 Small	04L4971	1,999	230
Firewall V3.2 Upgrade V3.2 Entry to V3.2 Medium	04L4972	6,999	230
Firewall V3.2 Upgrade V3.2 Entry to V3.2 Unl	04L4973	13,999	230
Firewall V3.2 Upgrade V3.2 Small to V3.2 Medium	04L4568	4,999	230
Firewall V3.2 Upgrade V3.2 Small to V3.2 Unl	04L4569	11,999	230
Firewall V3.2 Upgrade V3.2 Medium to V3.2 Unl	04L4570	6,999	230

Note: Volume licensing part numbers and prices will be announced on April 28, 1998.