



Product Description

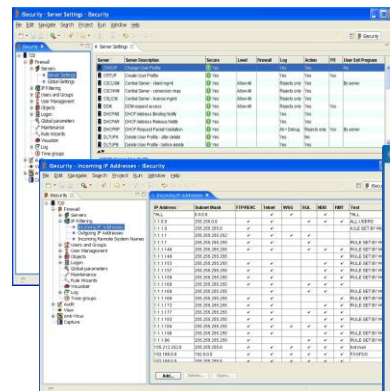
Firewall protects and secures all types of access, to and from the iSeries, within or outside the organization, under all types of communication protocols. This robust, cost-effective security solution is by far the most intuitive and easy-to-use security software product on the market today. As part of iSecurity's Intrusion Detection and Prevention system, Firewall manages user profile status, secures entry via pre-defined entry points, and profiles activity by time. Its "top-down" functional design and intuitive logic creates a work environment that even iSeries novices can master in minutes. Firewall features a user-friendly, Java-based GUI in addition to the traditional green-screen interface.

The Firewall Solution

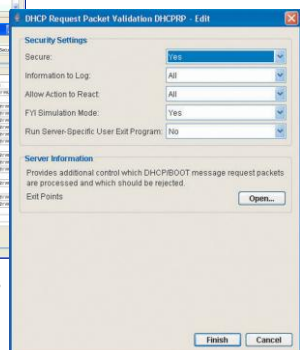
Technological advances of recent years have compelled IBM to open up the iSeries and its OS/400 operating system to the rest of the world. This new "openness" brought with it many of the security risks inherent in distributed environments. System administrators need to equip themselves with a new generation of security tools to combat these evolving threats. Firewall is just such a tool. It enhances native OS/400 by controlling access via all known external sources and controlling precisely what users are permitted to do once access is granted.

Firewall is designed for clarity, simplicity, and ease-of-use. Its unique "Best Fit" algorithm saves you precious work time by eliminating the need for pre-defined security rule priorities. The software automatically selects and dynamically applies the most suitable and efficient rules, thereby minimizing throughput delays. In addition, Firewall rule wizards greatly simplify the security definition process, extracting and summarizing data (IFS and native objects, IPs, users, etc.) from the history logs and then displaying the actual transaction statistics alongside current rules. The user may then choose to modify rules based on the data or create new rules – all from one convenient screen.

Firewall works together with Action to automatically trigger alert messages and immediate corrective actions when an intrusion or other security breach is detected.



Server-specific configuration settings



Server security protects all 49 security-related exit points

Clear, easy navigation through hierarchy-based levels provide for quick, streamlined usage

Key Features

Firewall Protection

- > Incoming and outgoing TCP/IP address filtering for Internet, FTP, REXEC, Telnet, and DHCP
- > Subnet mask filtering
- > Remote system (SNA) firewall protection for DDM, DRDA and Passthrough operations
- > Powerful Intrusion Detection that enables Firewall to trigger proactive responses to the security administrator by MSGQ and email
- > DHCP request packet validation

User Security

- > User-to-server security for all server functions and exit points
- > Prevents users from performing specific actions, irrespective of access method or of location
- > Verb support provides control over the execution of commands for specific servers
- > Internal profile groups simplify rule creation for specific groups of users
- > DDM/DRDA security including pre- and post- validation user swapping

- > Protection over user signon from Telnet – limits user access to specific IPs and terminals
- > Login control, including alternate user name support, for FTP, REXEC, WSG and Pass-through
- > User-definable exit program support (global and per server)
- > User management and statistics tools ease system and security tasks

Object Security

- > Controls object access at the level of specific action, such as read, write, delete, rename, run etc.
- > Secures native O/S 400 and IFS objects
- > Protects files, libraries, programs, commands, data queues and print files
- > Definable rule exceptions for specific users

History Logs and Reports

- > Total user control over which transactions are logged and displayed
- > Many pre-defined queries and reports
- > Powerful report generator
- > Wizard to generate accurate reports from Firewall log
- > Redirecting output to an output file for further processing
- > Print all Firewall definitions for review and documentation
- > Flexible report scheduler enables reports processing at off peak
- > Modify rules directly from Firewall log

Benefits

- > Protects all iSeries exit points and servers - more than any other product on the market!
- > Protects all communication protocols (TCP/IP, FTP, Telnet, WSG, Passthrough, etc.)
- > Superior human engineering makes Firewall incredibly easy to understand and learn, even for non-technical system administrators
- > Precisely controls what users may do after access is granted – unlike standard firewall products
- > “Best-Fit” algorithm minimizes throughput delays by rapidly and efficiently applying security rules
- > Rule Wizards dramatically simplify security rule definition
- > State-of-the-art intrusion detection guards against hacker attacks
- > Standard firewall protection provides IP address and SNA name filtering
- > Subnet mask filtering for all IP addresses – one rule can protect an entire workgroup or LAN
- > Protects both native and IFS objects – all of your databases are secured
- > Remote logon security limits IP address to specific users at specific times
- > Automatic signon with alternate user profile (usually with restricted authorities) enhances security when authorized users connect from remote locations
- > Powerful report generator and scheduler

Basic Security

Protect all 53 exit points by determining how servers are to be protected and what level of access control is desired.

Firewall Security

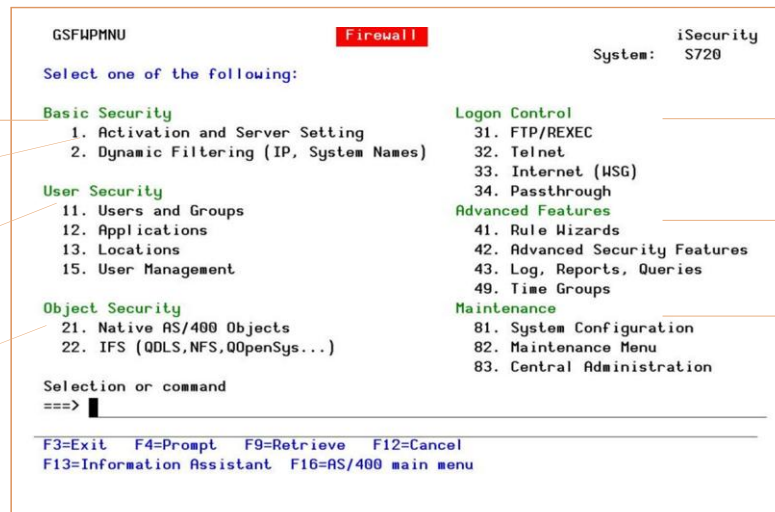
Control activity from or outbound to specific IP addresses

User Security

Control individual servers by users, profiles, groups and Firewall user groups

Object Security

Define security rules for files, libraries, data queues, printer files, programs, commands and IFS objects



The screenshot shows the main menu of the iSecurity Firewall application. At the top, it says 'GSFHPMNU' and 'Firewall'. The system name is 'iSecurity' and the system number is 'S720'. Below this, it says 'Select one of the following:'. The menu is organized into several categories:

- Basic Security**
 - 1. Activation and Server Setting
 - 2. Dynamic Filtering (IP, System Names)
- User Security**
 - 11. Users and Groups
 - 12. Applications
 - 13. Locations
 - 15. User Management
- Object Security**
 - 21. Native AS/400 Objects
 - 22. IFS (QDLS, NFS, QOpenSys...)
- Logon Control**
 - 31. FTP/REXEC
 - 32. Telnet
 - 33. Internet (WSG)
 - 34. Passthrough
- Advanced Features**
 - 41. Rule Wizards
 - 42. Advanced Security Features
 - 43. Log, Reports, Queries
 - 49. Time Groups
- Maintenance**
 - 81. System Configuration
 - 82. Maintenance Menu
 - 83. Central Administration

At the bottom, there is a prompt 'Selection or command' followed by '==>'. Below that, there are function key definitions: F3=Exit, F4=Prompt, F9=Retrieve, F12=Cancel, F13=Information Assistant, F16=AS/400 main menu.

Logon Control

Define attributes for specific combinations of IP addresses (or SNA names) and user profiles

Advanced Features

Reporting features provide queries and reports for system activity traceability

Maintenance

Features include Emergency Override, which enables overriding existing security rules temporarily - useful in responding quickly to sudden security breaches

AH Technology Pty Ltd.

7 Illowa St Malvern East, Vic., 3145
PO Box 205, Malvern, Vic., 3144, Australia.
Tel: +613 9885-4877 • Fax: +613 8678-0665

