



Firewall

Exit Point Monitoring

Firewall

Firewall protects and secures remote access to and from the IBM i. 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 prevention system, Firewall manages authorized user access which would usually not include command line access to locally execute powerful commands. By exploiting the exit point vulnerability that exists in the IBM i platform, users can perform unauthorized activity using remote TCP/IP applications, protocols and services designed to connect to the server remotely.

Firewall's "top-down" functional design and intuitive logic creates a work environment that IBM i administrators, security professionals, auditors and senior management can master easily. Firewall features a user-friendly, Java-based GUI (Graphical User Interface) in addition to the traditional 5250 green-screen interface.

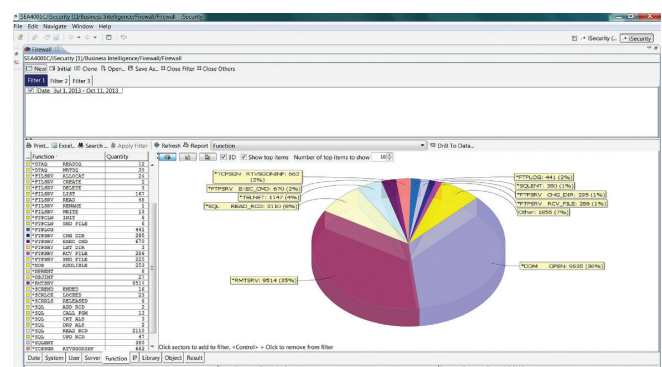
THE FIREWALL SOLUTION

Technological advances of recent years forced IBM to open up the IBM i data to the rest of the world. This new access to IBM i data opens the door to many security risks inherent in distributed environments. System administrators and security managers need to equip themselves with a new generation of security tools to combat these evolving modern threats.

Firewall enhances the native IBM i by controlling access via known external sources and controlling precisely what users are permitted to do once access is granted.

KEY FEATURES

- Incoming and outgoing TCP/IP address filtering for Internet, FTP, REXEC, Telnet, and DHCP
- Exit FYI mode and enter Intrusion Prevention mode one exit point at a time
- Remote system (SNA) firewall protection for DDM, DRDA and Pass-through operations
- Intrusion Prevention System initiates alerts and proactive responses, which are sent to the security administrator via MSGQ, email or text message.
- User Management capabilities containing comprehensive information and management of all user profiles
- Terminal screen security that protects unattended terminal screens, including PCs running terminal emulation software, from unauthorized use
- Built-in business intelligence tool that enables IT managers to graphically analyze security related system activity quickly and easily



Firewall Business Intelligence Tool

USER SECURITY

- User-to-server security for all server functions and exit points
- Verb support provides control over the execution of commands for specific servers
- User management and statistics tools ease system and security tasks
- Login control, including alternate user name support, for FTP, REXEC, WSG and Pass-through
- User-definable exit program support (global and per server)
- Internal profile groups simplify rule creation for specific groups of users DDM/DRDA security including pre and post validation user swapping Protection over user sign-on from Telnet - limits user access to specific IP's and terminals

OBJECT SECURITY

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

SERVER-SPECIFIC CONFIGURATION SETTINGS

- 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 security related IBM i exit points and servers - more than any other product on the market
- Protects all communication protocols (TCP/IP, FTP, Telnet, WSG, Pass-through, etc.)
- Precisely controls what users may perform 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 definitions
- State-of-the-art intrusion prevention guards against hackers
- Protects both native and IFS objects - all of your databases are secured

Date	Time	Result	Operation mode	Server	Decision level	Message ID
Nov 5, 2013	7:27:46 AM	Allowed	*FYI	TCP Signon Server	USSRV=User authority	GRE2170 *TCPGSG *FYIP All
Nov 5, 2013	7:27:48 AM	Rejected	*FYI	Remote Command/Program Call	OBNTV=Object authority-Native	GRE6053 *RMTSRV *FYIP De
Nov 5, 2013	7:28:00 AM	Rejected	*FYI	FTP Server Logon	GSFTP=FTP logon	GRE6021 *FTPLG *FYIP Den
Nov 5, 2013	7:28:00 AM	Rejected	*FYI	FTP Server-Incoming Rqst Validation	OBNTV=Object authority-Native	GRE6031 *FTPSRV *FYIP Den
Nov 5, 2013	7:28:01 AM	Rejected	*FYI	FTP Server-Incoming Rqst Validation	OBNTV=Object authority-Native	GRE6031 *FTPSRV *FYIP Den
Nov 5, 2013	7:28:02 AM	Allowed	*FYI	FTP Server-Incoming Rqst Validation	OBNTV=Object authority-Native	GRE7051 *FTPSRV *FYIP Allo
Nov 5, 2013	7:28:02 AM	Rejected	*FYI	FTP Server-Incoming Rqst Validation	USVRB=User authority-to verb	GRE6032 *FTPSRV *FYIP Den
Nov 5, 2013	7:28:02 AM	Rejected	*FYI	FTP Server-Incoming Rqst Validation	USVRB=User authority-to verb	GRE6032 *FTPSRV *FYIP Den
Nov 5, 2013	7:28:02 AM	Rejected	*FYI	FTP Server-Incoming Rqst Validation	USVRB=User authority-to verb	GRE6032 *FTPSRV *FYIP Den
Nov 5, 2013	7:28:06 AM	Rejected	*FYI	FTP Server-Incoming Rqst Validation	USVRB=User authority-to verb	GRE6032 *FTPSRV *FYIP Den
Nov 5, 2013	7:28:46 AM	Allowed	*FYI	Database Server - entry	USSRV=User authority	GRE7006 *SQLENT *FYIP All
Nov 5, 2013	7:28:46 AM	Rejected	*FYI	Database Server - data base access	USSRV=User authority	GRE7002 *NDB *FYIP Allowe
Nov 5, 2013	7:28:46 AM	Rejected	*FYI	Database Server - SQL access & Showcse	OBNTV=Object authority-Native	GRE6041 *SQL *FYIP Denied
Nov 5, 2013	8:02:09 AM	Allowed	*FYI	Telnet Device Initialization	GSTEL=Telnet logon	GRE7080 *TELNET *FYIP Allc
Nov 5, 2013	8:05:00 AM	Allowed	*FYI	Create User Profile		GRE7240 *CRTUP *FYIP User
Nov 5, 2013	8:05:01 AM	Allowed	*FYI	Change User Profile - alter change		GRE7230 *CHGUP *FYIP Use
Nov 5, 2013	8:05:01 AM	Allowed	*FYI	Delete User Profile - before delete		GRE7260 *DLTUPR *FYIP Use
Nov 5, 2013	8:05:03 AM	Allowed	*FYI	Delete User Profile - after delete		GRE7250 *DLTUPA *FYIP Use
Nov 5, 2013	8:44:35 AM	Rejected	*FYI	TCP Signon Server	FWIPA=Dynamic Filtering IP address	GRE6170 *TCPGSG *FYIP De
Nov 5, 2013	8:44:40 AM	Allowed	*FYI	Telnet Device Initialization	GSTEL=Telnet logon	GRE7080 *TELNET *FYIP Allc
Nov 5, 2013	10:52:11 AM	Allowed	*FYI	TCP Signon Server	USSRV=User authority	GRE2170 *TCPGSG *FYIP All
Nov 5, 2013	10:52:12 AM	Allowed	*FYI	Database Server - entry	USSRV=User authority	GRE7006 *SQLENT *FYIP All
Nov 5, 2013	10:52:12 AM	Allowed	*FYI	Remote Command/Program Call	OBNTV=Object authority-Native	GRE7051 *RMTSRV *FYIP All
Nov 5, 2013	10:52:16 AM	Allowed	*FYI	Remote Command/Program Call	OBNTV=Object authority-Native	GRE7051 *RMTSRV *FYIP All
Nov 5, 2013	10:52:17 AM	Allowed	*FYI	Remote Command/Program Call	OBNTV=Object authority-Native	GRE7051 *RMTSRV *FYIP All
Nov 5, 2013	10:52:17 AM	Allowed	*FYI	Remote Command/Program Call	OBNTV=Object authority-Native	GRE7051 *RMTSRV *FYIP All
Nov 5, 2013	10:52:17 AM	Allowed	*FYI	Remote Command/Program Call	OBNTV=Object authority-Native	GRE7051 *RMTSRV *FYIP All
Nov 5, 2013	10:52:17 AM	Allowed	*FYI	Remote Command/Program Call	OBNTV=Object authority-Native	GRE7051 *RMTSRV *FYIP All

Firewall Log

Server	Secure	Security level	Log
SQL - Database Server - SQL access & Showcse	By verb	Full (User+Object)	No change
SELECT	Read record	Allow	
INSERT	Add record	Reject	
UPDATE	Update record	Reject	
DELETE	Delete record	Reject	
CREATE TABLE	Create file	Reject	
CREATE INDEX	Create file	Reject	
CREATE VIEW	Create file	Reject	
CREATE ALIAS	Create file	Reject	
DROP TABLE	Delete file	Reject	
DROP INDEX	Delete file	Allow	
DROP VIEW	Delete file	Allow	
DROP ALIAS	Delete file	Allow	
RENAME	Rename file	Allow	
CALL	Call program	Allow	
CREATE COLLECTION/DATABASE/SCHEMA		Allow	
CREATE PROCEDURE		Allow	
DROP COLLECTION/DATABASE/SCHEMA		Allow	
DROP PROCEDURE		Allow	
ALTER TABLE	File - Other	Allow	
COMMENT ON		Allow	
LABEL ON	File - Other	Allow	
LOCK TABLE	File - Other	Allow	
DROP PACKAGE		Allow	
GRANT PACKAGE		Allow	
GRANT TABLE	File - Other	Allow	
REVOKE PACKAGE		Allow	
REVOKE TABLE	File - Other	Allow	

Firewall User Management GUI

- Remote logon security limits IP address to specific users
- Automatic sign-on with alternate user profile (usually with restricted authorities) enhances security when authorized users connect from remote locations
- Powerful report generator and scheduler
- Robust log functions as a table with ability to filter, sort, organize and present data