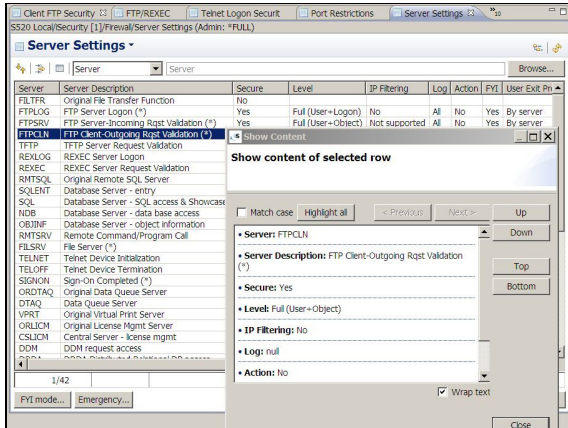


## Complete Network Access, User, Workstation & Virus Protection



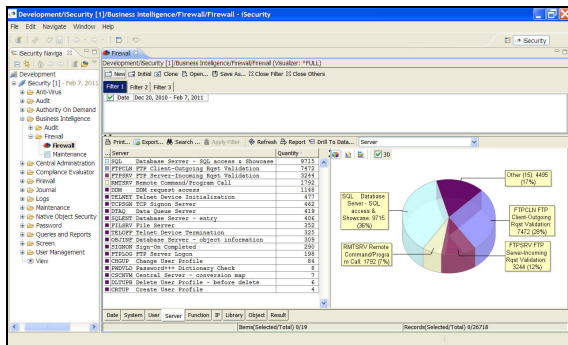
**Firewall Server Settings**

The iSecurity™ Prevention Pack provides optimal protection against infiltration of the IBM i, whether from the external network, from inside the organization, by PC-type viruses and more.

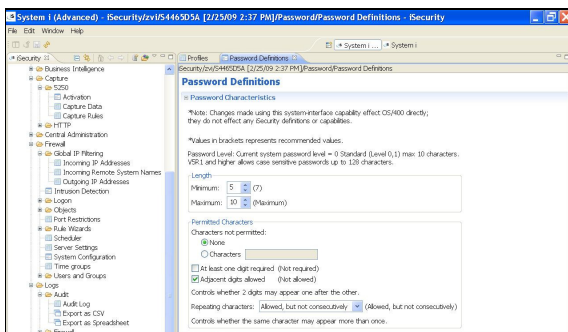
The Prevention Pack includes real-time network monitoring and intrusion detection, user and password management, protection of unattended workstations, and GUI-based “drill down” capabilities for analyzing and investigating network accesses via all possible servers.

### Prevention Pack Features

- Full GUI and Green-Screen support
- Prevention of data loss, unauthorized data alteration, and exposure of data
- Complete user profile and password management capabilities
- Automatic dispatch of Intrusion Detection System (IDS) alerts by e-mail, operator messages, Syslog, SNMP, SMS, etc.
- Simulation mode allows safe implementation of network access rules into production mode
- Wizards enable automatic generation and subsequent fine-tuning of security rules based on actual network activity
- Comprehensive review of server security status
- Network access log information stored in a unique security data warehouse for extremely efficient online investigation and pinpointing of security breaches by IP, date, system, object, library, server, function, Rejected/Accepted, etc.
- Easy customization to meet site requirements and specifications
- Access to critical data and processes only by relevant personnel



**Visualizer Graphical Analysis of Firewall Log**



**Password Definitions Screen**

## Prevention Pack Solutions

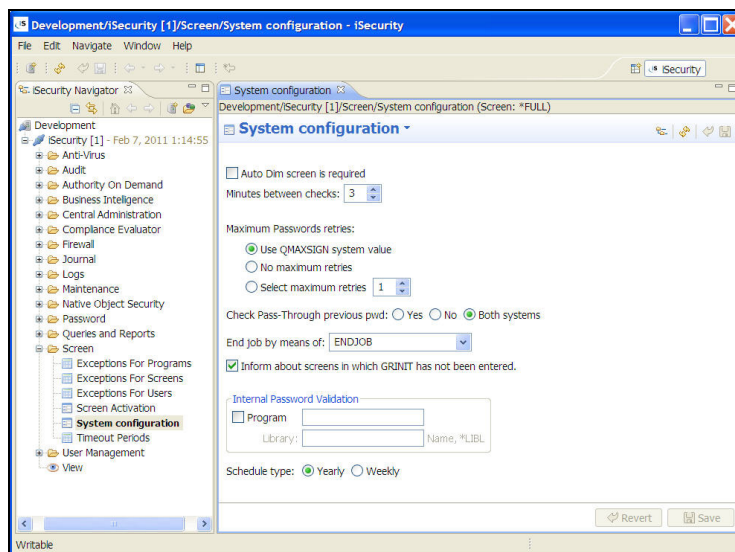
**Firewall** - Secures every type of access to and from the IBM i through predefined entry points, including internal and external access, under every type of communication protocol (TCP/IP, FTP, Telnet, etc.). Easy-to-use wizard defines network access rules based upon past network access events; simulation (FYI) mode allows for checking and verifying rules prior to implementation.

**Visualizer for Firewall** - Provides business intelligence oriented, at-a-glance graphic views of log data collected by Firewall, enabling IT managers to analyze security-related system activity and pinpoint details regarding suspected security breaches.

**Password** - Combines all OS/400 password management capabilities and contains tools to block the use of easy-to-crack passwords. Supports site-specific dictionaries to prevent company or product-related passwords.

**Screen** - Protects unattended terminal screens and workstations, running terminal emulation software, against unauthorized use. Locks terminal screens automatically and asks for the user password if terminal remains unused for a specified period of time.

**Assessment** - Analyzes security definitions and values based on key parameters (network access, system auditing, user activity, and sign-on attributes). Generates reports, shows overall system security status, and suggests corrective actions or specific iSecurity solutions. Generates Executive Summary highlights scores in more than 10 security-related categories.



Screen System Configuration