CASE STUDY

IBM i Network Access Control & Segmentation

Asian Banking Institution *Anonymized | Confidential*

Client Profile

Industry	Banking
Region	Asia
Environment	IBM i — 5 LPARs supporting digital banking, payment systems, and financial applications
Security Scope	IBM i Network Access Control & Segmentation
Assessment Type	Internal Security Hardening & Regulatory Compliance Initiative

The Challenge

The client's IBM i infrastructure supported critical banking operations and processed highly sensitive financial data accessed by internal users, external applications, vendors, and partner systems. As cybersecurity and regulatory requirements increased, the bank identified a significant need for tighter network-level access controls specifically for IBM i services.

Lack of Granular IBM i Network Security

The organization lacked the ability to:

- Restrict access by user profile
- Control connections based on IP address or subnet
- Limit access to specific IBM i services and ports
- Separate production and administrative access paths
- Rapidly create temporary or emergency access rules

Any authorized network user could potentially attempt connections to IBM i services such as: FTP, ODBC, DRDA, DDM, Remote Command, Telnet, Native IBM i interfaces.

Operational Complexity

The banking environment changed frequently due to:

- New vendors and fintech integrations
- Temporary project access requirements
- Remote administration needs
- Regulatory segmentation policies

The IT security team required a solution that allowed rapid rule creation and deployment without operational delays or complex network changes.

Compliance & Security Requirements

The solution is needed to:

- Operate natively on IBM i
- Support rapid policy changes and rule deployment
- Minimize disruption to banking operations
- Strengthen segmentation around sensitive financial systems
- Improve visibility into IBM i network activity

Solution Deployed

Raz-Lee deployed iSecurity Firewall across all IBM i partitions.

iSecurity Firewall

Implemented IBM i-native network access control and segmentation directly at the IBM i interface layer:

- Restricting access by user profile, IP address, subnet, protocol, and time of day
- Controlling access to IBM i services including FTP, ODBC, DRDA, Telnet, and Remote Command while Monitoring inbound connection attempts in real time
- Creating segmentation policies around critical banking applications and sensitive data
- Create new access rules within minutes
- Deploy temporary vendor or project access rapidly
- Modify policies without application changes
- Respond immediately to emerging threats or operational requests
- Implement granular controls without relying on external firewall teams

This flexibility significantly reduced operational bottlenecks and accelerated security response times.

Results

- Strengthened IBM i network segmentation and access control
- Reduced unauthorized connection exposure across banking systems
- Improved visibility into IBM i network activity and access attempts
- Accelerated deployment of security policies and temporary access rules
- Enabled rapid response to operational and security requirements
- Deployment completed without disruption to production banking services

The organization significantly improved IBM i network security while maintaining the agility required in a fast-moving banking environment.

Key QSA Feedback

> *“One of the biggest advantages for our team was the speed and simplicity of rule creation. We were able to implement granular IBM i access controls in minutes instead of waiting through lengthy network firewall change processes. Raz-Lee Firewall gave us both security and operational flexibility.”*

— Infrastructure Security Manager (paraphrased)