

CASE STUDY

Firewall Assessment Achieves Compliance & Enhances Network Security for State Agency

The state agency, which has broad responsibility across multiple industries, relied on the expertise of the AIS Network Information Security and Risk Management Team to perform a comprehensive firewall assessment to strengthen network security, meet audit requirements, and ensure best practices. The team's work brought the agency's firewall configuration up to industry standards and provided new firewall rule documentation.

Client

A \$124 million Virginia State Agency has authority over a wide range of business and economic interests.

Challenge

State agencies must adhere to the highest standards across all their operations. The firewall is the first line of defense in an agency's network security. To ensure that the agency satisfied information security audit requirements and industry best practices, the agency's CIO engaged AISN cybersecurity engineers to assess the organization's Cisco firewalls across multiple locations and recommend configuration, implementation, management, and security policy enhancements.

Solution

AISN provided engineers with experience with U.S. Department of Defense security protocol and the Cisco Adaptive Security Appliance family of security devices. Using a combination of automated scripts and manual techniques, AISN assessed the agency's configuration and construction for each firewall location, identifying and recommending detailed corrections for multiple rules and obsolete services within regulations. AISN engineers reviewed the agency's IT Firewall Standard v2.0 to determine alignment with applicable industry standards such as NIST 800-41r1, SEC 501-11.2, and the Center for Internet Security Cisco Firewall Benchmark.

Results

Agency personnel cleaned up outdated firewall rules based on AISN's best practice recommendations to enhance firewall configuration, implementation, and management. All gaps, issues, or problems were documented along with the recommended corrections, options for consideration, and an implementation plan, putting the agency on a path to achieve full compliance and strengthened network security. AISN also aligned the agency IT Firewall Policies with identified industry standards and agency IT Security Policies, which required overhauling its written firewall rules documentation.

