

Web and Email Security for 20,000 Users and 2 Billion Connections per day

The Objective

A large Federal organization with 10,000 local employees, 6 regional offices and 7800 seasonal field representatives requested assistance with the implementation of a web and email security solution. The Cisco IronPort email and web security solutions selected for this purpose are designed to secure organizations of all sizes, and are built from the ground up and deployed at the gateway to protect networks, and enable a perimeter defense so that Internet threats never make it to employees' desktops.

The Challenge

The Network Support Organization (NSO) needed to provide safe web and mail access to their almost 20,000 employees. The NSO knew it needed to increase its security measures to defend against damaging malware and ensure full compliance with acceptable use policies by limiting access to suspect URL's. The NSO also had management issues with the large amount of proxy servers that were being used in their Citrix environment. Seamless application access and consistent security were critical to protect all of the users in this "borderless" network environment. The two data centers received 2 billion web connections a day during peak loads and required traffic monitoring and load balancing with the option to monitor the system locally as well as remotely.

The Solution

With thousands of users accessing its system, the customer sought a single-source security solution that would provide robust defense, including reliable URL filtering and virus scanning to shield it from malware, spyware, and downloads from malicious websites designed to compromise networks. NFF installed, configured, customized, and maintained the Cisco IronPort enterprise solution for web and email security, replacing the former Websense product. This provided the client with:

- High-performance protection and defense against spyware and web-based threats
- Web usage controls, as well as URL, web reputation, and malware filtering
- Advanced application and visibility controls
- High speed web proxy, along with integrated caching and content acceleration capabilities
- Unique outbound threat monitoring
- Enforcement of acceptable use and security policies over native passive FTP and HTTP's decrypted data



- Comprehensive management and reporting capabilities with multiple deployment modes, robust real-time and historical reports, through a user friendly graphical interface

The Result

Since deploying the Cisco IronPort Solution, the client reports:

- Improved URL filtering utilizing rapid parsing and vectoring capabilities of the IronPort engine
- Increased security through application usage monitoring and controls
- Less risk of delays to legitimate email
- Decline in spam and virus related IT Service Desk calls, releasing IT to focus more on business enablement projects
- Improved operational capabilities to re-design, reconfigure and customize appliances to address dynamic email and web security requirements

About NFF

NFF is a Technology Solutions provider, specializing in Data Center Virtualization, Unified Communications, and Secured Network Infrastructure. NFF's proficiency and experience allow our customers to depend on us as a single source for planning, deployment and long-term support of their complex projects. We provide Network Assessments, Technology Design and Integration, Software and Database Services, and Staff Augmentation. We have the unique ability to take a project from ideation to design, implementation, and ongoing support, all under one roof. For more information visit www.nffinc.com.