CASE STUDY

Supporting Automation and Saving $100M at One of the World's Largest Financial Institutions

Several years ago, one of the world's largest financial institutions put out a request for proposals (RFP) to replace its legacy firewall infrastructure. The company has a very centralized IT infrastructure: A global technology group provides IT services to all business units around the world. The initiative would ultimately replace the company's entire enterprise firewall infrastructure.

There were several reasons behind this initiative and its timing. For one thing, the company regularly reviews all its technologies to make sure they support enterprise strategies and requirements. Second, the firm was concurrently embarking on a massive automation initiative and needed the firewall infrastructure to support this undertaking. Finally, the incumbent firewalls—all from a single vendor—were having scalability problems in the firm's massive infrastructure. Specifically, the window of time during which all offices worldwide were closed for the weekend was often not long enough to complete updates. As a result, many updates were not being completed at all, increasing risk to the company.

Fortinet was invited to respond to the RFP along with several other major firewall vendors. The firm has a very thorough review process that includes extensive discussions and exhaustive proofs of concept (POCs) for each vendor. After months of written responses to questions and several deep-dive sessions with Fortinet engineers at the company's IT headquarters, Fortinet supplied equipment for a comprehensive, eight-week POC.

Assessing the Firm's Key Priorities

As the firm's network team went through the various POC processes of each vendor, it looked at a wide variety of features and functionality, but ultimately focused on several factors that aligned with the company's overall business strategy. One big priority focused on the need for deep firewall integration with its chosen automation platform, Red Hat Ansible. The new firewalls also needed to support specific elements of the automation project, including provisioning, upgrades, and clusters of upgrades—without downtime.

The firm operates one of the biggest centralized networks in the world, and scalability was a primary concern.

Details

Customer: Leading U.S.-based Financial Services Firm

Business Impact

- Projected $100 million in cost savings and productivity improvements over five years
- Increased hardware-based firewall resiliency without adding staff
- Significant savings and deployment advantages in staging charges for hardware via automated provisioning

A second priority was scalability. The company operates one of the biggest centralized networks in the world, and some technology solutions simply do not work well at that scale—even those designed with large enterprises in mind. With that in mind, the firm's POCs are designed to simulate the massive scale of its infrastructure and to test for strains in the system.

A third priority was performance—another problem the company was starting to experience with its incumbent firewalls. A fourth priority was the firm's confidence in the executive leadership and engineering strength of each vendor—their ability to deliver on future needs that might not be on anyone's radar today.

A fifth priority was management, where FortiManager proved to be a significant upgrade over the legacy vendor's management tool. Specifically, the firm was experiencing extraordinarily long update windows that were spilling into production hours when common, often small updates were applied to the environment. In contrast, FortiManager reduced update times from 48 hours to less than one hour, which enabled the firm to avoid downtime or performance degradation during production hours as well improved operational productivity.

Navigating an Intense POC

Fortinet's POC went very well from the bank's perspective. When testing for integration with Ansible, the engineering teams were very impressed with the Fortinet robust representational state transfer (REST) API. While one other vendor had a visually appealing Ansible integration, that integration proved to be shallow compared with what could be built with the Fortinet REST API. Specifically, the firm found that the Fortinet REST API was both robust and flexible, enabling Ansible and a variety of the company's other applications to be integrated deeply and seamlessly.

FortiGate next-generation firewalls (NGFWs) also passed the company's scalability tests. In addition, their performance was so superior that some of the planned performance testing was canceled because everyone—including the other vendors—acknowledged that Fortinet would prevail in that area.

The institution's impression of Fortinet as a company was also positive. Fortinet engineers were very responsive during the POCs, delivering quickly on support requests—and on more than 15 requested new features. Additionally, in meetings with Fortinet leaders, the company found that Fortinet's vision for evolving its solution offerings and mapping to where security requirements are heading placed Fortinet ahead of other security providers.

- Ability to configure next-generation firewalls (NGFWs) in three- and four-node clusters improves efficiency and reduces risk
- Passed all scalability tests for one of the world's largest connected networks
- Reduced risk by ensuring that all security updates can be completed within change windows

Solutions

- FortiGate
- FortiManager
- FortiAnalyzer
- FortiCare Global First Service
- Fortinet Professional Services
- Fortinet Network Security Academy

An internal analysis projects cost savings of $100 million over five years.

Completing Certification and Testing

The POC process for all vendors was completed two years ago, and the firm soon notified Fortinet that it was the preferred provider upon completion of pricing negotiations. Once the deal was signed, the Fortinet solution would also need to go through an architectural certification process that is required of all hardware and software added to the company's network.

The initial order included hardware and software to complete the lab testing for the architectural certification. The firm also secured the services to optimize the deployment and provide for ongoing maintenance of the new network security infrastructure. Five engineers from Fortinet Professional Services now work onsite at several of the company's facilities around the world and are currently working on the deployment. As part of this process, the company has been able to offload tedious certification testing, quality assurance (QA) testing code releases, and automation tasks to Fortinet Resident Engineers from Professional Services. Other timesaving tasks include but are not limited to training, documentation creation, and management and conversion of vendor configurations from legacy solutions to Fortinet-enabled environments.

Preparing for the Rollout

A year later, the firm placed another order for its electronic trading group. The purchase included FortiGate NGFWs, along with FortiManager and FortiAnalyzer to assist with management and analytics and a FortiCare Global First contract for support. The Global First contract includes six dedicated technical account managers (TAMs)—covering every region—who help diagnose problems and route them to the best resources for resolution according to aggressive service-level agreements (SLAs).

The bank also invested heavily in training its staff on the Fortinet solution. The Fortinet Network Security Academy conducted onsite classroom training for 93 staff members at seven locations around the world. Separately, an additional 13 staff completed NSE training at the Fortinet Accelerate 2018 user conference. Training opportunities will be ongoing for these staff members, and management expects that many will choose to participate in Fortinet's eight-level Network Security Expert (NSE) certification program.

Fortinet's robust REST API enables a deep integration with Red Hat Ansible.

The company increased hardware-based firewall resiliency without adding any staff.

Expecting Big Benefits

As the company went through the selection process, return on investment was a constant consideration, and the company's finance team made detailed calculations on each potential solution. Their conclusion was that the firm would realize $100 million in cost savings and productivity gains over five years with the Fortinet solution. On the cost side, the team found that the Fortinet architecture was significantly less expensive while delivering superior performance. On the operational side, the team identified numerous savings including:

- **Reduced time to market.** Automated server provisioning and updates, which can be done without downtime with FortiGate NGFWs, will speed the time from PO to production when new resources are deployed.
- **Reduced server provisioning costs.** Automated provisioning means that the firm will no longer have to pay for a service provider to "stage" provisioned hardware in various regions so that it can be deployed relatively quickly.
- **Improved employee productivity.** The ability to architect the firewalls in three- or four-node clusters rather than two-node clusters will improve operational efficiency and reduce risk. And while this will significantly increase the number of NGFWs, the firm will not need to add more staff to manage the solution due to the ease of use of the FortiGate NGFWs.

Beyond these significant financial benefits, the firm's security posture is much improved as well. For one thing, the company will now be able to complete all security updates during the weekend time window when all offices are closed, eliminating missed or delayed updates. And as the company moves forward with its automation initiative—and any future digital innovation projects—automated server provisioning and updates will speed the time from PO to production. And these updates can be done without downtime with FortiGate NGFWs.

After a lengthy but productive vetting process, the networking team at the global financial services firm is excited to move forward with its FortiGate deployment—and the larger automation project that it will support. While the public thinks of this company as a financial services provider, internal employees see themselves as a technology company—rolling out comprehensive, automated solutions that transform the company's business.

September21,201910:59AM

322982-0-0-EN

D:\Fortinet\Work\2019\September\092119\cs-supporting-automation