516.281.2200
www.vandis.com
1 Albertson Avenue
Albertson, NY 11507

UPGRADING FIREWALLS FOR BETTER VISIBILITY, CONTROL & MANAGEMENT

Challenges

When Vandis first approached this company they were using Juniper firewalls, Bluecoat Web Filtering, and Tipping Point IPS to protect their network infrastructure at four different locations around the world. They were never able to reach a stable configuration and had to constantly tweak and adjust their web filters to have them function as needed. At the time, this company was managing 13 devices and wanted to drastically decrease that number to 4. The deadlines and site priorities for this project were dictated by the support that was expiring on their existing appliances.

Selection Criteria

This company stated to Vandis that they wanted to upgrade their legacy security which had become complex to manage and costly to maintain. They were hoping to implement one solution that would migrate them away from their multiple platforms. The major goals in undertaking this project were to simplify their environment, provide an easy to use management platform, reduce costs, and enable more visibility and control.

Solution

Vandis suggested Juniper Networks and Palo Alto Networks as the top options that should be considered for this project. In order to observe what technology would best fit their environment, a proof of concept (POC) was executed to allow the company to see what type of traffic was traversing their firewalls. The POC lasted approximately 2 weeks and, once completed, the company decided to purchase the Palo Alto Networks solution. This solution was ultimately chosen by the company as they believed it better aligned with the goals of their project. They believed that the Palo Alto Networks solution gave them better visibility into their environment and more control in their responses to network and security incidents. The company purchased PA5000, PA3000, and PA500 series firewalls with threat prevention and URL filtering. Vandis then performed the implementation of the solution over a 2-3 month period, starting with the major datacenters located inside and outside the United States that had appliances expiring soonest as to avoid having the company pay additional renewal costs. One of the complexities that Vandis faced during implementation was that each major data

center's firewall was responsible for controlling the communication between numerous subsidiary sites around the world. To minimize user disruption, Vandis suggested installing the routed firewalls in parallel with the old equipment. During service migration, the old firewalls were disabled and the new ones would be brought online. This minimized the need for routing changes and provided a simple rollback scenario. While Vandis' engineers were performing the implementation there was always a member of the company's IT team present to learn what was happening and ask any questions he or she may have had.

Results

With the Palo Alto Networks solution deployed and fully operational, the company had achieved the goals it had set before the start of the project. Their environment has become easier to manage, there are not as many single points of failure, and they have visibility that they didn't have before. In addition, compromised endpoints are detected earlier and are automatically prevented from making callbacks. Their service desk is now able to follow remediation plans with more confidence that the incident will be contained. This centralized console condensed 27 different independent firewalls into one that allowed the organization to create a global team working under a single pane of glass. Due to the success of this project, Vandis is now working with the company's network and security teams to execute a worldwide technology rollout.