IMPLEMENTING A MULTI-VENDOR SECURITY ENVIRONMENT

Challenges

This credit union was looking to replace their existing firewalls which were becoming legacy and unable to perform at a level that was being required by this organization.

Selection Criteria

This organization made it very clear to Vandis that they wanted a technology that had the ability to simplify their environment. At the time they were managing 15 devices on a daily basis and were looking to drastically decrease that number while still maintaining a next generation firewall. In addition, they were also looking to implement a layered security approach in order to better protect their network.

Solution

Taking into account their existing environment, Vandis recommended the technology that would best fit their needs for a simplified & converged network with better visibility and management would be Palo Alto Networks. During this project, Vandis was responsible for the sizing and configuration of the new firewall solution. Vandis suggested PA-3020s based upon the organization's existing bandwidth and future growth needs. Before deploying this new solution, Vandis performed the conversion from their existing Cisco ASAs to Palo Alto Networks. In addition, Vandis performed the deployment of the solution and had one of Vandis' certified Palo Alto Networks engineers perform a half day transfer of knowledge with the company's network and security team. This session allowed Vandis to fully explain the configuration, teach how to perform ongoing maintenance, and implement troubleshooting techniques.

With the new configuration running correctly and the client satisfied, they began gaining interest in adding additional layers of security. The credit union was looking for a layered security approach with a best of breed technology to alert on any malicious content which might bypass the firewall. Vandis recommended FireEye for its malware detection, protection and narrowed focus/core competency. The credit union received a demo appliance to perform a proof of concept which was conducted in FireEye's active testing lab where they were able to test the solution in a virtual sandbox to test its effectiveness against zero-day malware. With the credit union impressed by the POC, they decided to purchase the FireEye 2400NX-HW WEB MPS appliance and deploy this solution directly in line behind the Palo Alto Networks firewall. In addition, this

organization purchased the FireEye Remote Installation Service which allowed FireEye to assist in the setup of the appliance and provide an in depth product overview for the customer.

Results

With both solutions implemented, this credit union now has a next generation security solution to protect their network. Before this project was completed, this organization had a single security appliance to protect themselves. Now they have a best of breed layered security approach to help protect against malware and APTs. On top of improving the security footprint within their organization, they were also able to drastically simplify their environment.