

ENSURING MAXIMUM SECURITY AND FLEXIBILITY IN A HIGH VOLUME ENVIRONMENT

Challenges

As security moves into the forefront for most IT decision makers, the ability to ensure that critical data is highly available and secure is at an all-time high. This is especially apparent for media companies who transfer large amounts of outbound and inbound data between networks. When a large media company in NYC approached Vandis with a need to replace their old firewalls at several locations, Vandis realized it was important to find a solution that would be able to handle massive amounts of traffic and was flexible enough to write necessary security rules to protect their sensitive data.

Selection Criteria

The organization was unhappy with their current firewalls and distinct lack of support they were receiving from their previous vendor. Specifically, the organization wanted a solution that would allow them to move to a single solution, reducing complexity, but increasing visibility and control among their networks. Vandis was then asked to prepare new security rules for the organization's entire network to help ensure maximum security and continuity throughout.

Solution

After several meetings with Vandis and our engineers, it was determined that Palo Alto Networks would be the best solution. As the project consisted of multistate deployments and a redesign of their disaster recovery site, Vandis Professional Services was called upon to do a majority of the leg work to migrate the network from their old solution to the new firewalls. The organization purchased several PA 5060, PA 5020, PA 3050, and threat prevention licenses on all devices. In addition, the organization purchased a block of Vandis Professional Services hours to install and configure the gear.

The first deployment began at their brand new West Coast office, which consisted of a pair of 3050 in a High Availability cluster configuration. Prior to shipment, the devices were configured in the New York City office and would then be handled by the organization's team, with Vandis supporting remotely. The clusters would be configured to support the west coast office with an aggregated throughput up to 2Gbps. Vandis also worked with the organization to standardize network objects, zones, groups and services as well as create a simple security rule base for the office to follow.

The next step was to migrate the organization's old firewalls to the new Palo Alto Networks devices in its East Coast environment. This deployment was the most important as it would determine if the organization would proceed with purchasing and migrating all of their old firewalls to the new Palo Alto platform. Vandis deployed an HA pair cluster that would be configured to support the topology of the old firewalls and sustain an aggregated throughput of up to 10Gbps. Once that was put into place, Vandis then translated the defined network objects, groups and services from the old network to the Palo Alto environment. A security rulebase was then created for this PA cluster that was similar to the old cluster it was replacement. This consisted of approximately 119 Security Rules and 33 Network Address Translation Rules. The organization was pleased on how the migration went and then had Vandis migrate their other sites, including a redesign of their DMZ.

Results

Due to our success with the first implementation and deep knowledge of Palo Alto Networks, the organization felt comfortable working with Vandis. From start to finish, the project took about six months. Throughout the entire process, Vandis worked with the organization to make sure the multi-site deployment went smoothly. The organization was very happy with the migration to the Palo Alto Networks firewalls and has worked with Vandis several more times over the past year expanding their security offerings.