

ENHANCING SECURITY & CONNECTIVITY WITHIN AWS FOR A LARGE MEDIA COMPANY

Challenges

A global media organization reached out to Vandis to ask if we could implement a solution that would increase connectivity and security while decreasing administrative overhead in their AWS environment. Already redundant and capable of processing a high rate of rich media traffic, their AWS environment proved untenable to manage and secure as its scale increased.

Originally leveraging a combination of VPC peer links, security groups, and network access control lists to enable connectivity between VPCs while policing traffic, this client was reaching both the administrative and technical constraints of these technologies at scale. In addition, the company was looking to increase their security controls within their AWS environment while also eliminating some of the manual overhead that was required to maintain it. Due to an internal business constraint, Vandis was under a strict 4 week timeline to get this project completed.

Solution

After a few architectural design meetings, Vandis suggested utilizing Aviatrix, Palo Alto Networks VM-Series VM-300, and AWS Transit Gateway in order to accomplish the organization's objectives. Vandis defined and provisioned this solution in a controlled manner using Terraform, which is a tool for building, changing, and versioning infrastructure safely and efficiently. After a successful POC was performed to validate the solution, the client gave the go ahead for Vandis professional services to start implementation.

Vandis provided a solution that:

- Removed the complexity introduced by a tangle of VPC peer links
 - Vandis implemented an AWS transit gateway with routing orchestrated by Aviatrix's TGW Orchestrator
- Reduced the overall quantity of security groups and network access control lists required and the number of rules within the remaining groups and lists
 - Vandis utilized multiple Palo Alto Network's VM-Series Next-Generation Firewalls and Aviatrix's Firewall Network to secure the environment and load balance the firewalls without the use of source NAT
- Deployed in a controlled and repeatable fashion

- Vandis leveraged HashiCorp's Terraform to ensure the entire solution was seamlessly transitioned from Vandis' lab to the client's production environment

Results

With the new solution in place, the client now has better visibility into traffic passing through their AWS environment and more granular abilities in controlling traffic between VPCs. Security of their cloud environment was improved and streamlined to better protect their environment while reducing required management overhead. With the client working closely alongside Vandis during the implementation, there was an organic transfer of knowledge that took place throughout the project to enhance the organization's ability to maintain the solution. With the successful completion of this project, there have been additional talks to further tighten and optimize their security controls using the tools they now have in place.