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

DEPLOYING A NGFW IN AWS FOR SECURITY CONTROL CONFIGURATION MONITORING

Challenges

Having reached the limitations of their existing firewall solution, this organization realized that their current technology didn't have the features and capabilities their business required that today's Next Generation Firewalls (NFGW) are equipped to handle. The organization had multiple AWS Accounts broken out by business unit (Development, Production, Test, Shared Services, etc.) however, traffic flowed unrestricted between environments without implementation of Security Groups or NACLs. Specifically, this organization requested Vandis to deploy a NGFW solution for their on-premise and branch locations in order to standardize policies across their entire organization. Vandis was engaged to understand the customer's past, current, and future roadmaps, advise on a recommended solution meeting their criteria, and architect and implement a solution that would meet their requirements now, and in the future.

The solution required the ability to:

a) Route via BGP through a centralized point all East-West VPC traffic, North-South Internet ingress/egress, customer SSL-VPNs as well as AWS Direct Connect for On-Prem and their MPLS cloud.
b) Inspect all traffic through a central security gateway by eliminating all existing:
    a. VPC Peering Connections between Spoke VPCs
    b. Site-to-Site VPNs between Spoke VPCs and On-Prem locations
    c. Internet Gateways in Spoke VPCs
c) Protect their AWS presence by utilizing security features of today's NGFWs, including: Anti-Virus, Web Filtering, Application Control, Intrusion Prevention, and SSL/SSH inspection.
d) Perform SSL and IPSec VPN encryption/decryption at scale to meet the business needs of customer-facing and internal networking requirements.
e) Endure service disruption by design and be a highly available and resilient solution by deployment in an Active-Standby model across multiple Availability Zones.
f) Maintain administration and monitoring through centralized configuration, management, and logging applications.

By deploying this new NGFW solution in their AWS environment, it would enhance this organization's visibility into traffic across the different VPCs and help police the traffic by providing granular control, configuration and monitoring.

Solution

Vandis rearchitected this organization's AWS environment and implemented an HA pair of FortiGate NGFWs in a multi-availability zone deployment in the transit VPC to police North-South and East-West traffic. The solution also included FortiManager and FortiAnalyzer for centralized configuration management and logging analytics.

The FortiGate solution was set up to provide routing and inspection of all inter-VPC, cloud to on-prem and Internet traffic. The Spoke VPCs and Direct Connect were set up with VPN tunnels to the FortiGates in the Transit VPC so all traffic flowing in and out of a VPC is inspected by the FortiGates.

BGP was implemented to ease routing table administration. Vandis also migrated the previous solution's Elastic IP, firewall rules, and VPN peer configurations eliminating the need to involve IT resources for VPN peer reconfiguration at the remote end.

Most of the work Vandis completed was done during working sessions with the client to give them a thorough understanding of the solution and ensure they were informed through each step. Vandis also set up knowledge transfer sessions to cover specific aspects of the Fortinet configuration and answer any questions the organization had.

Results

With the project successfully completed, this organization now has FortiGate NGFW protection of their AWS environment as well as centralized traffic flow, security, and monitoring. This has allowed the organization to continue their cloud migration as they move workloads and VPN connections by partners and clients to AWS. Working with the client on an ongoing basis we have now focused on implementing a proactive solution that monitors and auto-remediates misconfiguration in their AWS Accounts according to industry compliance standards.