



Palo Alto Networks Encryption Over Layer 2 Cloud Interconnect for AWS

Executive Summary:

As a result of this engagement, you will have a highly available, secure implementation of an IPSec tunnel over their existing AWS Direct Connect using Palo Alto Next-Generation Firewalls to terminate the tunnels cloud side. It will also set up a VPN failover. This project will allow for enforced end to end traffic encryption between sites in your hybrid cloud environment.

Offering Description:

Vandis will work with your network and security teams to integrate Palo Alto Next-Generation Firewalls as a highly available VPN endpoint in a single region of AWS. We will assist with the design and configuration of the subnets, gateways, NSGs, and Route Tables and deliver those in VPC.

Throughout the engagement, your organization will work with the Vandis Engineering team to understand your security needs and goals. Vandis will also make recommendations on other solutions that may help achieve your cloud goals.

Deliverables:

- Cloud Design Session
 - Discuss Cloud Goals
 - Discuss underline Cloud Governance
 - Discovery of existing environment
- Palo Alto Next-Generation Firewall Deployment:
 - VPC topology and address space allocation
 - Subnet and network segmentation
 - Gateway Objects
 - Route Tables
 - Network Security Groups/NACLs
 - Load Balancers
 - Integration of Palo Alto Next-Generation Firewalls into the VPC
 - Integration into existing Panorama (if applicable)
 - External VPN set up
- Cloud Connectivity Set Up
 - Cloud Connectivity Checklist Review
 - Cloud Connectivity Circuit (Direct Connect) Set Up (if applicable)
 - Encryption over the Cloud Connectivity Circuit
- Palo Alto Next-Generation Firewall Design
 - Cloud Templates
 - Architectural Design Document

For additional information, please reach out to 516-281-2200 or cloud@vandis.com