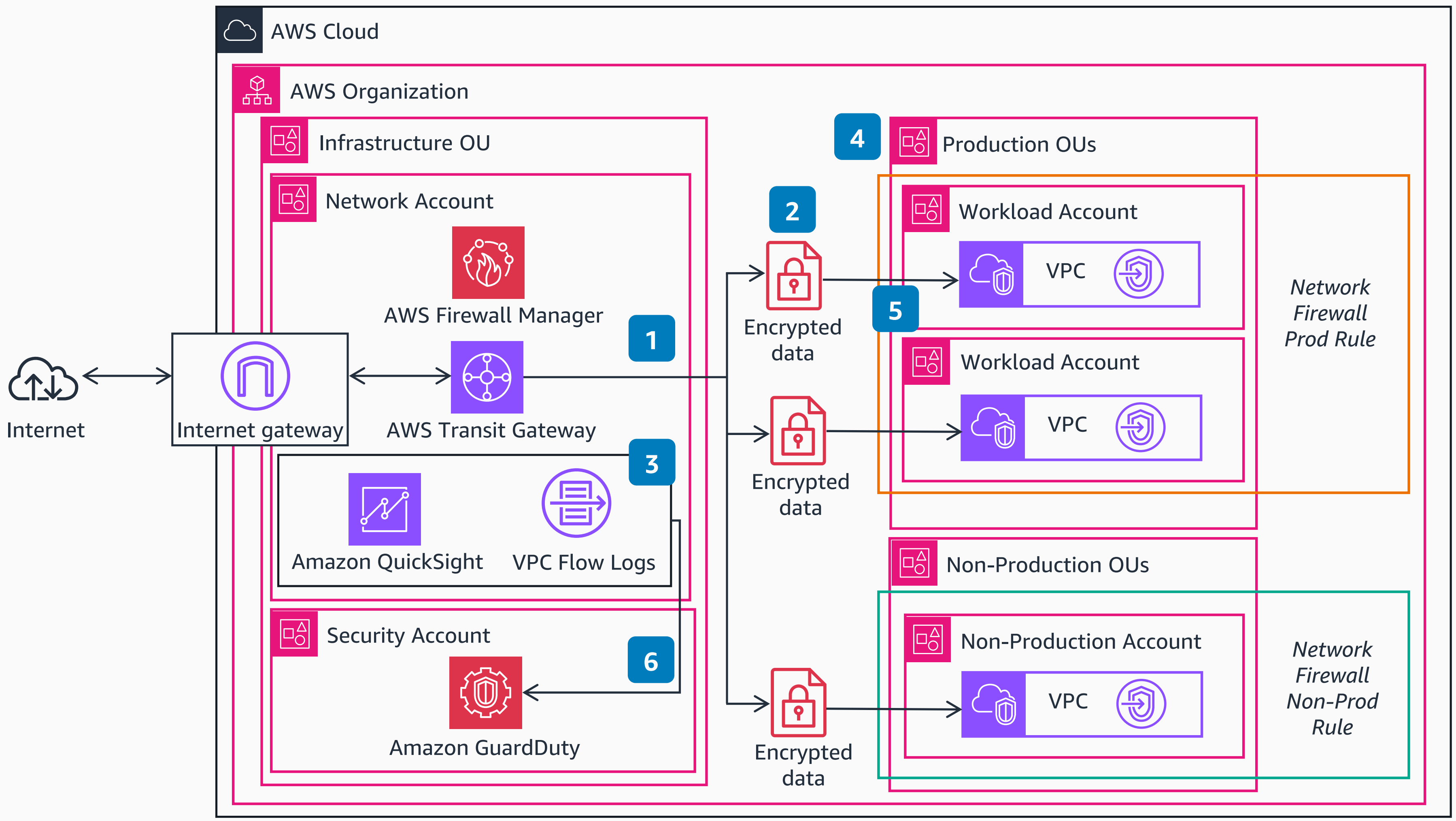
Guidance for Network Security on AWS

This architecture shows you how to set up your network security on AWS using AWS Organizations and organizational units (OUs) for infrastructure, production, and non-production workloads.



1. Expand your networks across AWS Regions and accounts that can be divided into isolated networks with segments. Each network segment will represent a routing domain, where you can provide additional security layers at the perimeter of each segment. External calls to the application destined for the web layer would come through the perimeter and must pass through a security device and access control list (ACL).

2. Enforce strong security policies to encrypt data and preserve its integrity, accountability, and authenticity across your entire network.

3. Inspect north (ingress)-south (egress) traffic, such as internet connectivity. You may also require inspection of east-west traffic, such as internal cross application or location. Visualize and analyze traffic with **Amazon QuickSight** dashboards.

4. Set up **AWS Firewall Manager** rules for different environments to filter traffic at the perimeter using a Layer 3/4 firewall appliance.

5. Protect access to your **Amazon Virtual Private Clouds (Amazon VPCs)** by creating **VPC** endpoints. These endpoints allow you to apply identity-based controls to your network resources and allow connectivity between workloads and networks. You can send your request and data through the internet without leaving the AWS network.

6. **Amazon GuardDuty** analyzes your network logs through intelligent threat detection.

Reviewed for technical accuracy August 14, 2023

AWS Reference Architecture