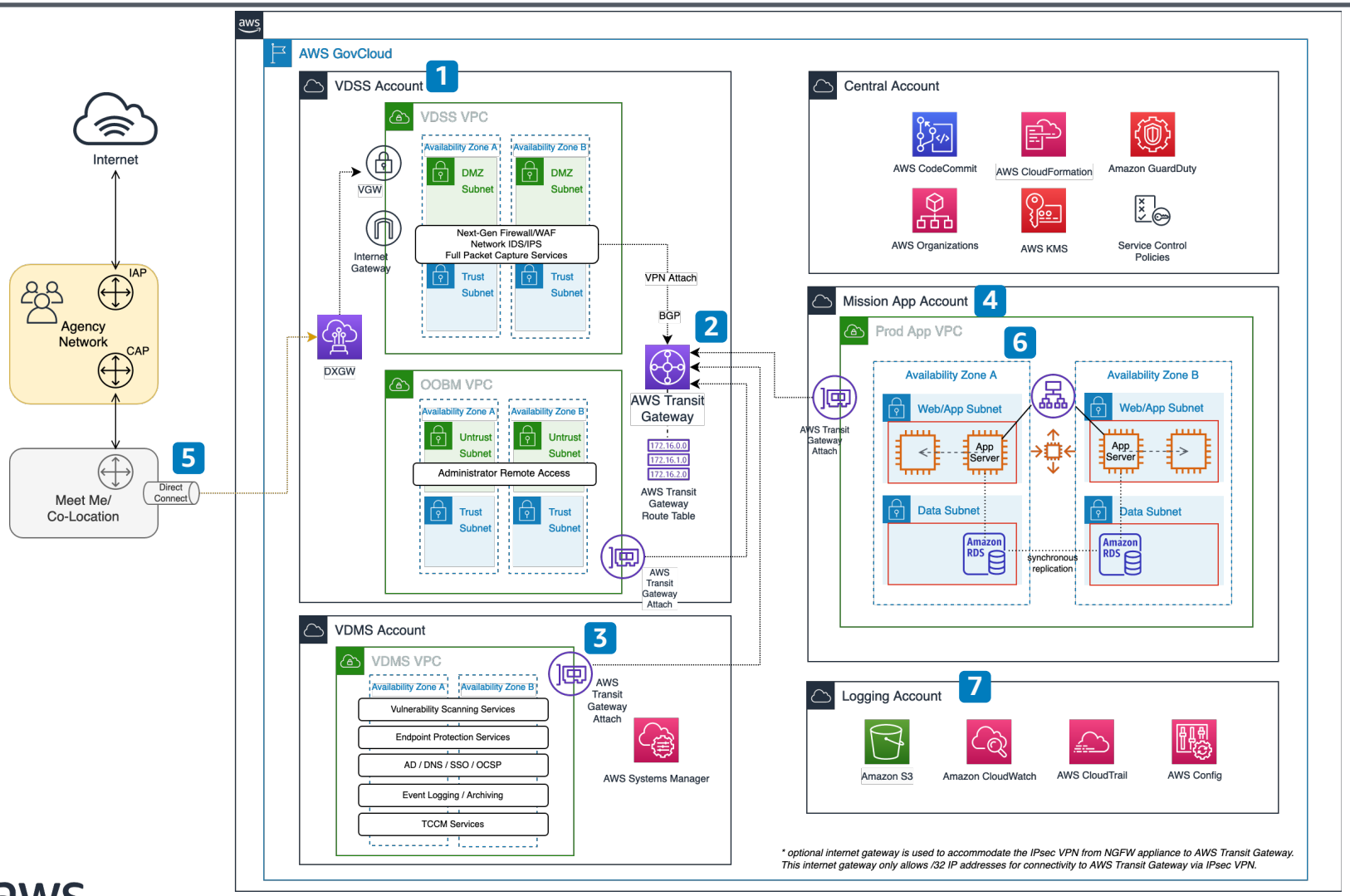
Secure Cloud Computing Architecture (SCCA) on AWS GovCloud (US)

Build a Defense Information Systems Agency (DISA) Compliant Landing Zone on AWS

This architecture provides the prerequisite framework for securely running U.S. Department of Defense workloads and storing Impact Level 4 and 5 data on AWS GovCloud (US) Regions, according to DISA standards.



1. Virtual Data Center Security Stack (VDSS) Account acts as boundary used for protection of mission owner applications.
2. **AWS Transit Gateway** acts as a hub that controls how traffic is routed among all the connected networks which act like spokes.
3. Virtual Data Center Management Stack (VDMS) Account includes capabilities such as Host Based Security System (HBSS), Assured Compliance Assessment Solution (ACAS), authentication systems, and other common services.
4. Mission App Account is where core workloads are deployed. All communications to and from the Mission App VPC transit the VDSS and consume shared services from the VDMS.
5. Connectivity to the Department of Defense Information Network (or other agency networks) is achieved through a Virtual Private Gateway (VGW).
6. Typical multi-tier mission workloads use **Elastic Load Balancing**, **AWS Auto Scaling Groups** and multiple **Availability Zones** for high availability and scalability.
7. The Logging Account represents the immutable location where logs are aggregated and stored.

AWS Reference Architecture