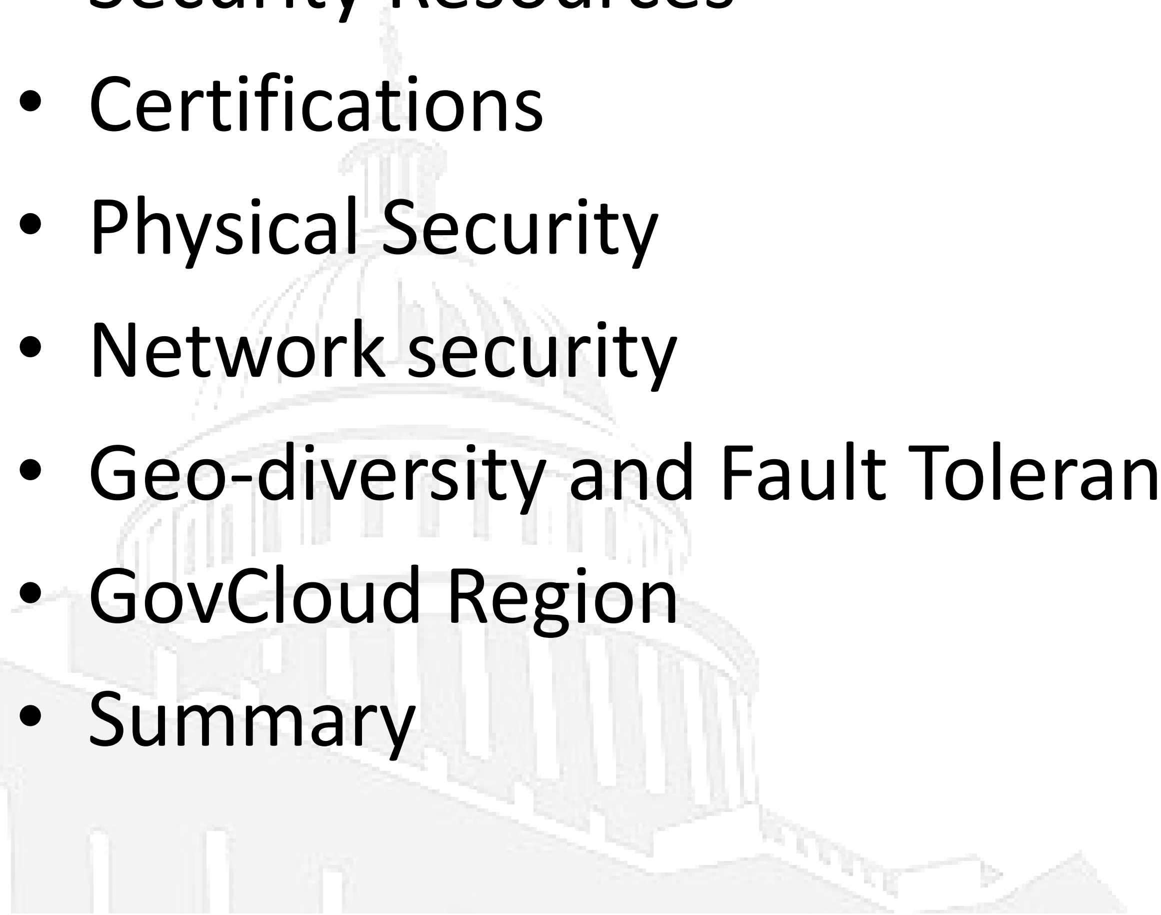
AWS Security

CJ Moses

Deputy Chief Information Security Officer

Security is Job Zero!

Overview

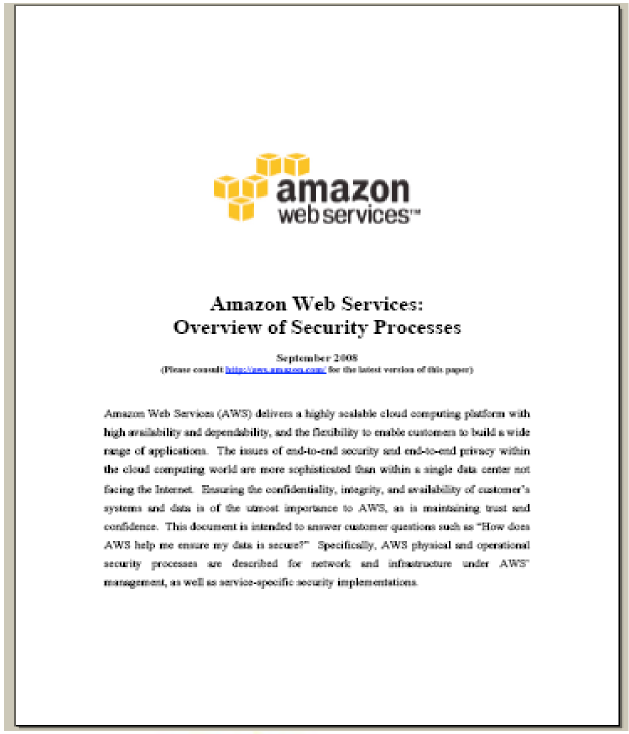


- Security Resources
- Certifications
- Physical Security
- Network security
- Geo-diversity and Fault Tolerance
- GovCloud Region
- Summary

AWS Security Resources

AWS Security Center

- http://aws.amazon.com/security/
- Security Whitepaper
- Risk and Compliance Whitepaper
- Latest Versions May 2011
- Regularly Updated
- Feedback is welcome



amazon web services™

Amazon Web Services:
Overview of Security Processes

September 2008
(Please consult http://aws.amazon.com/ for the latest version of this paper)

Amazon Web Services (AWS) delivers a highly scalable cloud computing platform with high availability and dependability, and the flexibility to enable customers to build a wide range of applications. The issues of end-to-end security and end-to-end privacy within the cloud computing world are more sophisticated than within a single data center not facing the Internet. Ensuring the confidentiality, integrity, and availability of customer's systems and data is of the utmost importance to AWS, as is maintaining trust and confidence. This document is intended to answer customer questions such as "How does AWS help me ensure my data is secure?" Specifically, AWS physical and operational security processes are described for network and infrastructure under AWS' management, as well as service-specific security implementations.

AWS Certifications

- Shared Responsibility Model
- Sarbanes-Oxley (SOX)
- ISO 27001 Certification
- Payment Card Industry Data Security Standard (PCI DSS) Level 1 Compliant
- SAS70 Type II (SOC1 coming soon) Audit
- FISMA A&As
  - Multiple NIST Low Approvals to Operate (ATO)
  - NIST Moderate – GSA ATO
  - FedRAMP
- DIACAP MAC III Sensitive IATO
- Customers have deployed various compliant applications such as HIPAA (healthcare)

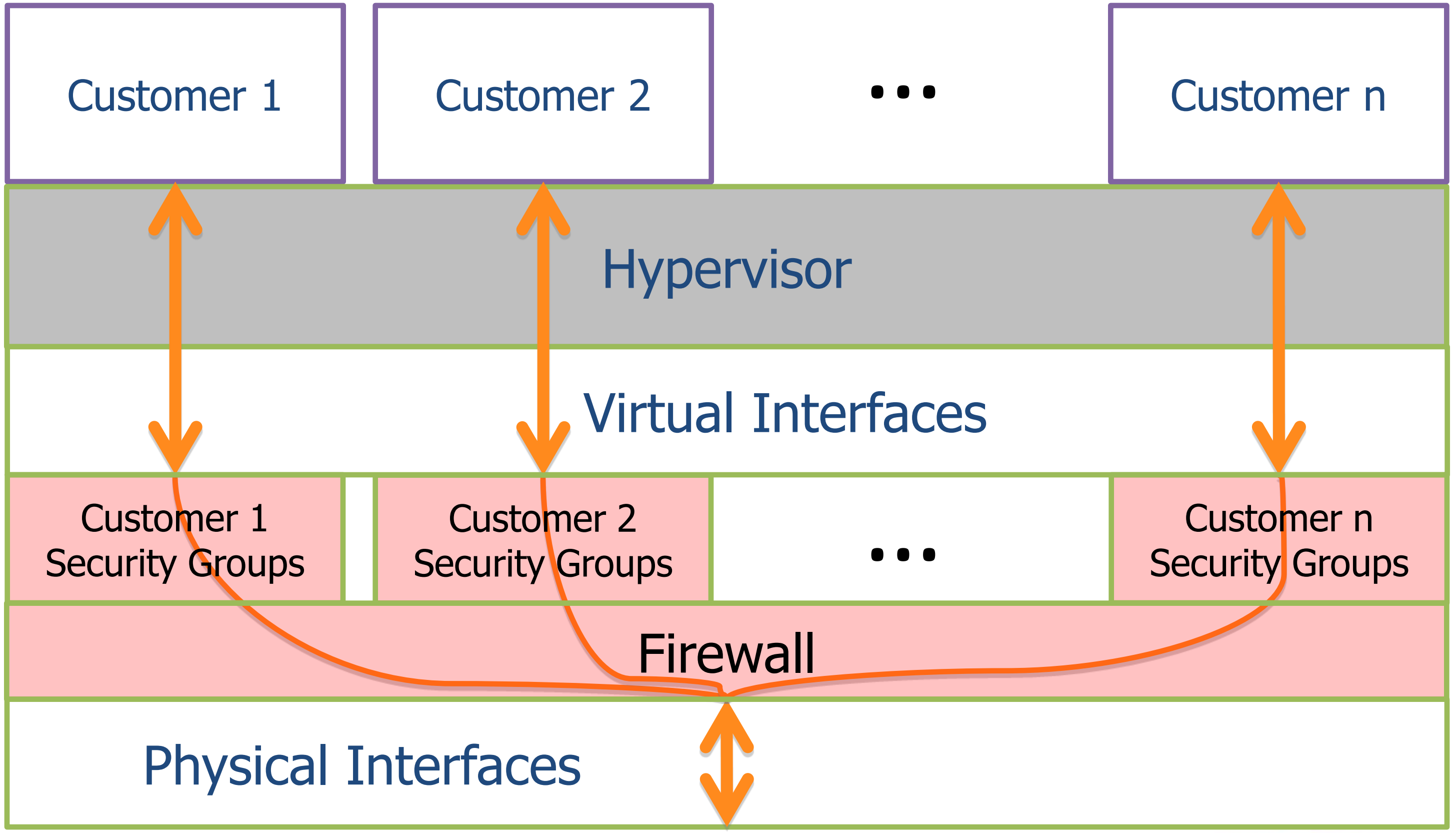
Physical Security

- Amazon has been building large-scale data centers for many years
- Important attributes:
  - Non-descript facilities
  - Robust perimeter controls
  - Strictly controlled physical access
  - 2 or more levels of two-factor auth
- Controlled, need-based access for AWS employees (least privilege)
- All access is logged and reviewed

Amazon S3 Data Protection

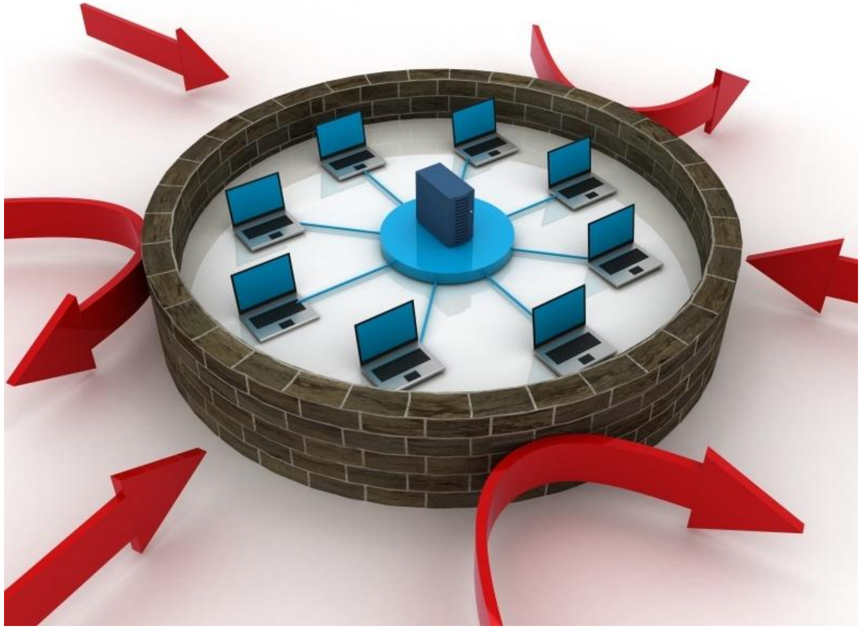
- Data in Transit
  - Supports Upload and Download data using secure HTTP (HTTPS) protocol
- Data Stored at Rest
  - Supports Amazon S3 Server Side Encryption (SSE) and Client Encryption libraries
- Access Control for Stored Data
  - Support for Access Control Lists (ACLs), Bucket Policies, and Identity and Access Management (IAM) policies

Amazon EC2 Instance Isolation

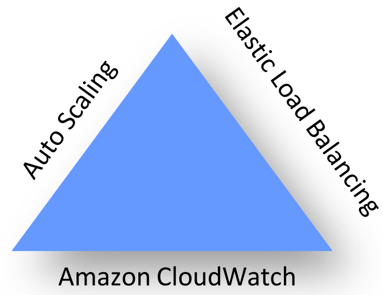


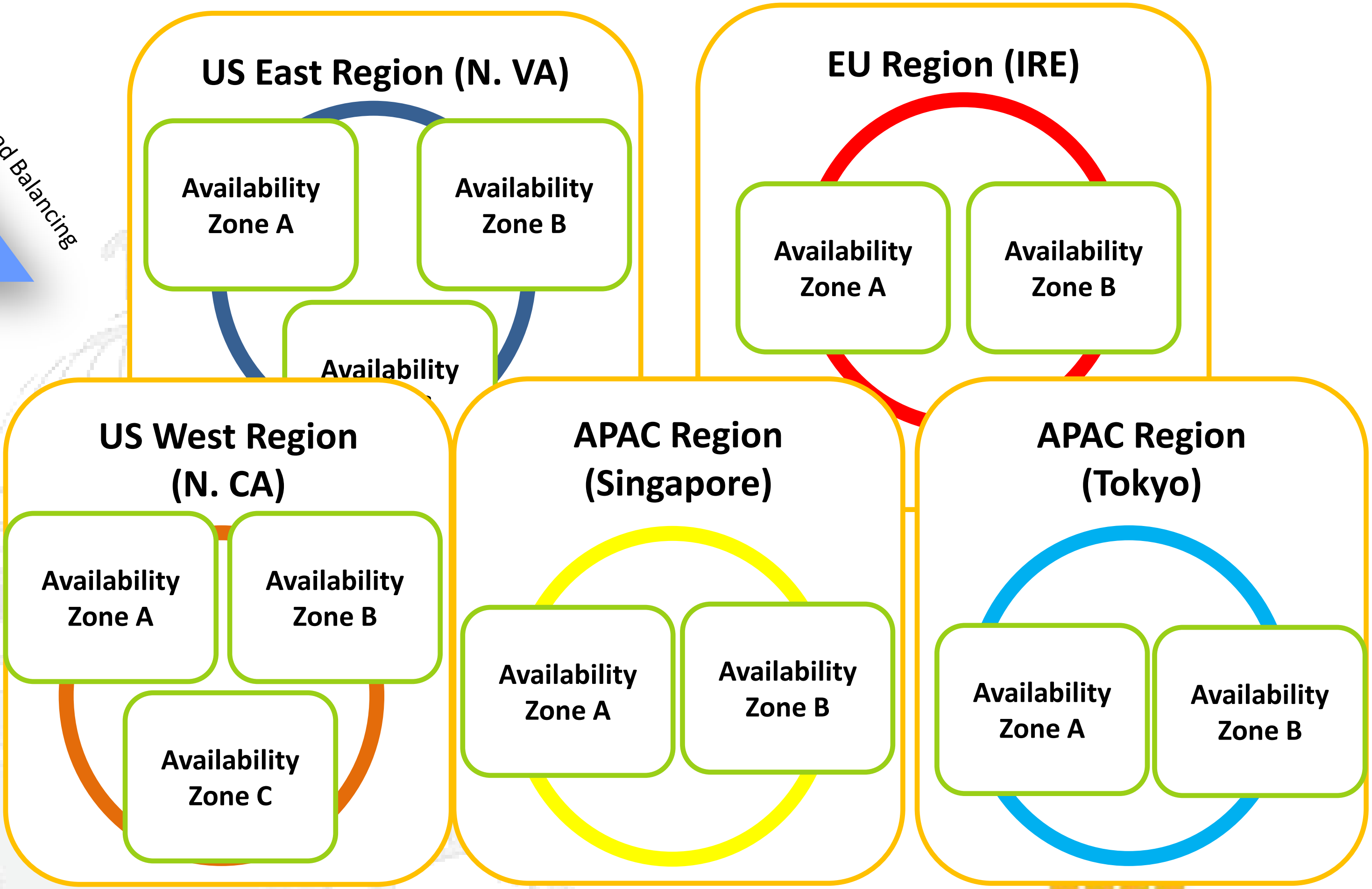
Network Security Considerations

- DDoS (Distributed Denial of Service):
  - Standard mitigation techniques in effect
- MITM (Man in the Middle):
  - All endpoints protected by SSL
  - Fresh EC2 host keys generated at boot
- IP Spoofing:
  - Prohibited at host OS level
- Unauthorized Port Scanning:
  - Violation of AWS TOS
  - Detected, stopped, and blocked
  - Ineffective anyway since inbound ports blocked by default
- Packet Sniffing:
  - Promiscuous mode is ineffective
  - Protection at hypervisor level
- Configuration Management:
  - Configuration changes are authorized, logged, tested, approved, and documented. Most updates are done in such a manner that they will not impact the customer. AWS will communicate with customers, either via email, or through the AWS Service Health Dashboard (http://status.aws.amazon.com/) when there is a chance that their Service use may be affected.



Fault Separation and Geographic Diversity

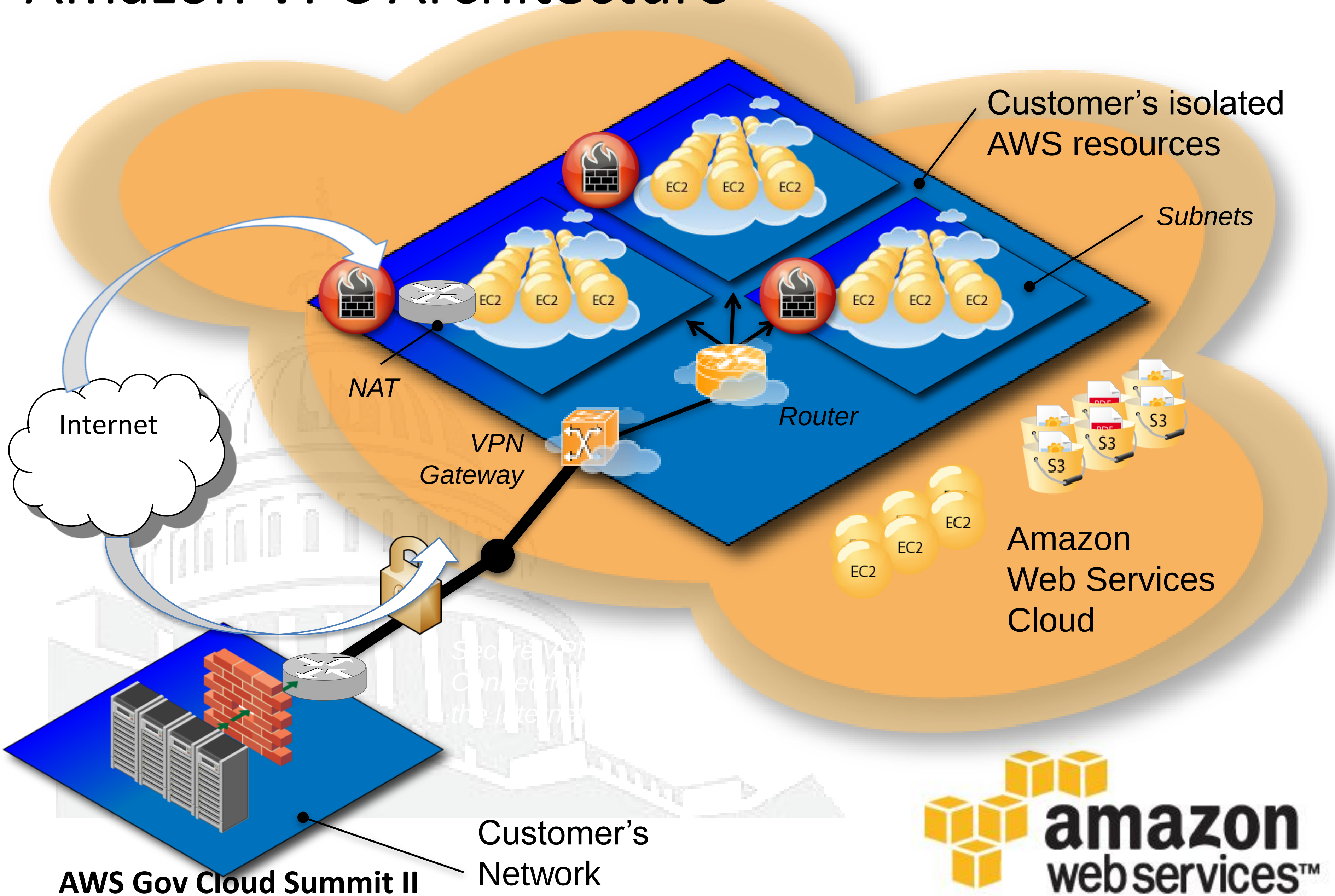




Note: Conceptual drawing only. The number of Availability Zones may vary

AWS Gov Cloud Summit II

Amazon VPC Architecture



Customer's isolated AWS resources

Subnets

NAT

Router

VPN Gateway

Internet

Amazon Web Services Cloud

Customer's Network

a new region…

AWS GovCloud (US)

Designed for US Government Customers

AWS will screen customers prior to providing access to the AWS GovCloud (US). Customers must be:

- U.S. Persons;
- not subject to export restrictions; and
- comply with U.S. export control laws and regulations, including the International Traffic In Arms Regulations.

- FISMA Moderate Compliant Controls
- US Persons-Only access (Physical & Logical)
- Data Isolation (Service & IAM Controls)
- Network Isolation (VPC required, FIPS 140-2 Compliant endpoints, AWS Direct Connect Optional)
- Machine Isolation (Dedicated instances optional)

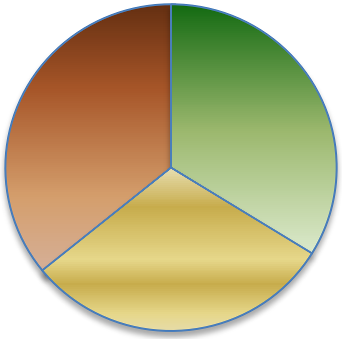
Summary of AWS Deployment Models

	Logical Server and Application Isolation	Granular Information Access Policy	Logical Network Isolation	Physical server Isolation	Government Only Physical Network and Facility Isolation	ITAR Compliant (US Persons Only)	Sample Workloads
Commercial Cloud	✓	✓					Public facing apps. Web sites, Dev test , FISMA low and Mod
Amazon Virtual Private Cloud (VPC)	✓	✓	✓	✓			Data Center extension, TIC environment, email, FISMA low and Mod.
AWS GovCloud	✓	✓	✓	✓	✓	✓	USP Compliant and Government Specific Aps.

AWS Cloud Security Model Overview

Certifications & Accreditations

- Sarbanes-Oxley (SOX) compliance
- ISO 27001 Certification
- PCI DSS Level I Certification
- HIPAA compliant architecture
- SAS 70 Type II Audit
- FISMA Low and Moderate ATOs
    - FedRAMP
- DIACAP MAC III –Sensitive IATO
- Service Health Dashboard



Shared Responsibility Model

- Customer/SI Partner/ISV controls guest OS-level security, including patching and maintenance
- Application level security, including password and role based access
- Host-based firewalls, including Intrusion Detection/Prevention Systems
- Encryption/Decryption of data. Hardware Security Modules
- Separation of Access

Physical Security

- Multi-level, multi-factor controlled access environment
- Controlled, need-based access for AWS employees (least privilege)

Management Plane Administrative Access

- Multi-factor, controlled, need-based access to administrative host
- All access logged, monitored, reviewed
- AWS Administrators DO NOT have access inside a customer's VMs, including applications and data

VM Security

- Multi-factor access to Amazon Account
- Instance Isolation
    - Customer-controlled per-VM firewall
    - Neighboring instances prevented access
    - Virtualized disk management layer ensure only account owners can access storage disks (EBS)
- Support for SSL end point encryption for API calls

Network Security

- Instance-level hypervisor-enforced firewalls can be configured across instances via security groups;
- The traffic may be restricted by protocol, by service port, as well as by source IP address (individual IP or CIDR)block).
- Virtual Private Cloud (VPC) provides IPSec VPN access from existing enterprise data center to a set of logically isolated AWS resources

AWS Gov Cloud Summit II

amazon web services™

Thank You!

aws.amazon.com/security

cmoses@amazon.com