AWS Architecture Training - IAM

Identity & Access Management and Security Overview

Module 3

Overview

- Identity & Access Management
- Key Security Concepts
- Certifications

Identity & Access Management

Two Types of Access

AWS APIs

- Launch, Start, Stop, Terminate EC2 instances
- Create, attach, delete storage
- Configure hypervisor firewall (Security Groups)
- Configure AWS infrastructure changes
- Things you can do through the AWS Console

AWS Identities
(e.g. AWS IAM)

Customer Instances (VMs)

- Operating System
- Application
- Security Groups
- OS Firewalls
- Network Configuration
- Account Management

Corporate
Identities
(e.g. AD)

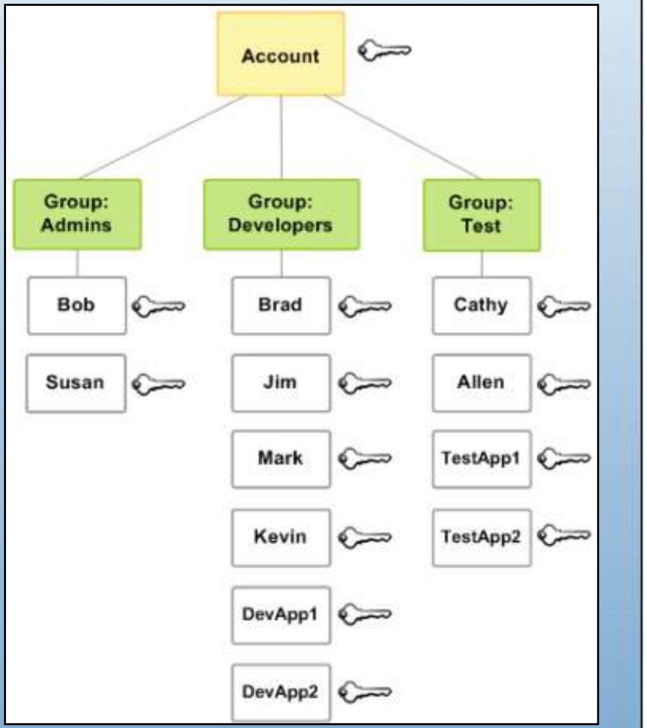
AWS Identities

- Account Owner ID
  - Access to all subscribed services
  - Access to billing reports
  - Access to console, REST and SOAP APIs

- IAM Users/Groups
  - Access to specific services
  - Access to console and/or REST APIs and/or SOAP APIs

AWS Identity and Access Management (IAM)

- Users and Groups within Accounts
- Unique security credentials
  - Access keys
  - Login/Password
  - optional MFA device
- Policies control access to AWS APIs
- API calls must be signed by either:
  - X.509 certificate
  - secret key
- Deep integration into some Services
  - S3: policies on objects and buckets
  - Simple DB: domains
- AWS Management Console supports User log on
- Not for Operating Systems or Applications
  - use LDAP, Active Directory/ADFS, etc...



Account

Group: Admins

Group: Developers

Group: Test

Bob

Susan

Brad

Jim

Mark

Kevin

DevApp1

DevApp2

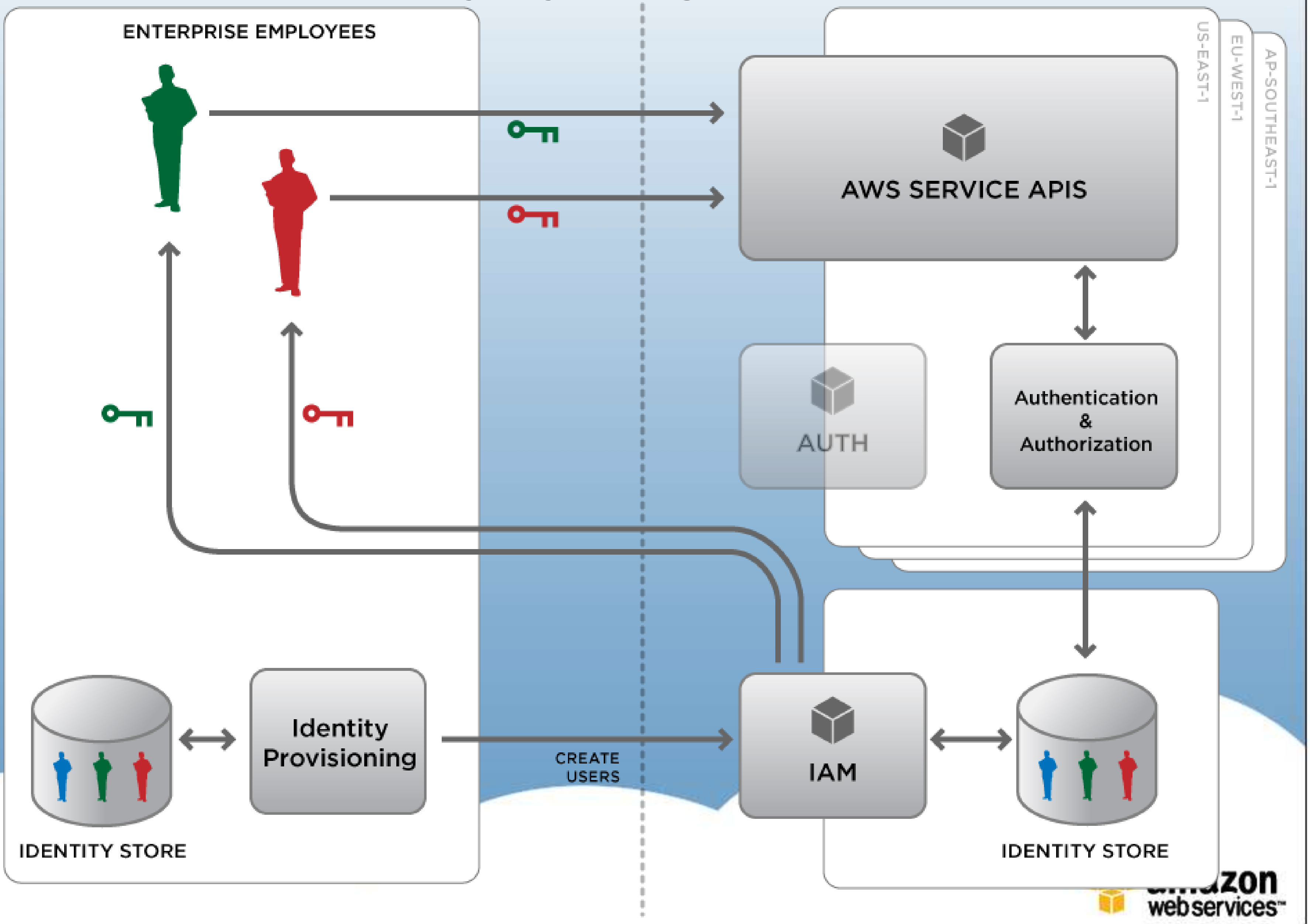
Cathy

Allen

TestApp1

TestApp2

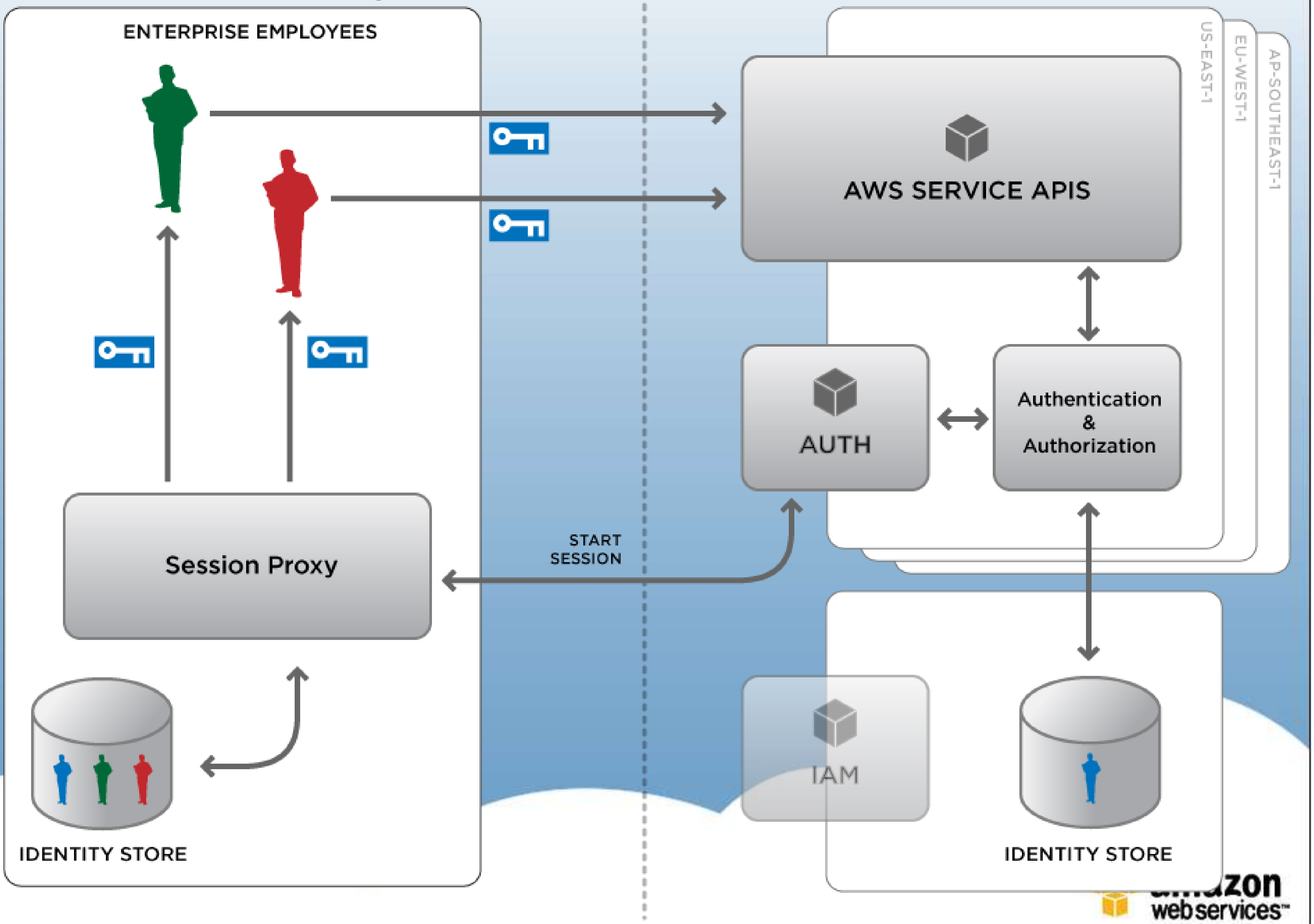
Identity Syncing with IAM



Temporary Security Credentials (sessions)

- Temporary security credentials containing
  - Identity for authentication
  - Access Policy to control permissions
  - Configurable Expiration (1 – 36 hours)
- Supports
  - AWS Identities (including IAM Users)
  - Federated Identities (users customers authenticate)
- Scales to millions of users
  - No need to create an IAM identity for every user
- Use Cases
  - Identity Federation to AWS APIs
  - Mobile and browser-based applications
  - Consumer applications with unlimited users

Identity Federation → AWS APIs



ENTERPRISE EMPLOYEES

AWS SERVICE APIS

US-EAST-1

EU-WEST-1

AP-SOUTHEAST-1

AUTH

Authentication
&
Authorization

START
SESSION

Session Proxy

IDENTITY STORE

IAM

IDENTITY STORE

AWS Multi-Factor Authentication

- Helps prevent anyone with unauthorized knowledge of your e-mail address and password from impersonating you
- Additional protection for account information
- Works with
  - Master Account
  - IAM Users
- Integrated into
  - AWS Management Console
  - Key pages on the AWS Portal
  - S3 (Secure Delete)

A recommended opt-in security feature!

Key Security Concepts

AWS Security and Compliance Center

(http://aws.amazon.com/security/)

- Answers to many security & privacy questions
  - Security whitepaper
  - Risk and Compliance whitepaper
- Security bulletins
- Customer penetration testing
- Security best practices
- More information on:
  - AWS Identity & Access Management (AWS IAM)
  - AWS Multi-Factor Authentication (AWS MFA)

Amazon Web Services:
Overview of Security Processes

[illegible]

Shared Responsibility Model

AWS

- Facilities
- Physical Security
- Physical Infrastructure
- Network Infrastructure
- Virtualization Infrastructure

Customer

- Operating System
- Application
- Security Groups
- OS Firewalls
- Network Configuration
- Account Management

Physical Security of Data Centers

- 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
- All access is logged and reviewed
- Separation of Duties
  - employees with physical access don’t have logical privileges
- Maps to an Availability Zone

AWS is Built for “Continuous Availability”

- Scalable, fault tolerant services
- All Datacenters (AZs) are always on
  - No “Disaster Recovery Datacenter”
  - Managed to the same standards
- Robust Internet connectivity
  - Each AZ has redundant, Tier 1 ISP Service Providers
  - Resilient network infrastructure

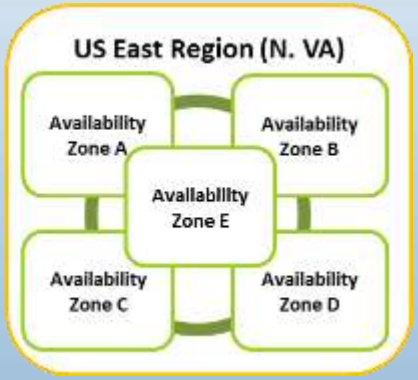
AWS Configuration Management

- Most updates are done in such a manner that they will not impact the customer
- Changes are authorized, logged, tested, approved, and documented
- 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 they may be affected

Customers are responsible for change control in their Instances!

Data Backups & Replication

- AWS favors replication over traditional backup
  - Equivalent to more traditional backup solutions
  - Higher data availability and throughput
- Makes data available in multiple edge locations
  - CloudFront, Route 53
- Data replicated to multiple Availability Zones within a single Region
  - S3, S3 RRS, SimpleDB, SQS, RDS Multi-AZ, EBS Snapshots
- Data replicated to multiple physical locations within a single Availability Zone
  - EBS, RDS
- Data NOT automatically replicated
  - EC2 ephemeral drives (a.k.a. instance store)



Storage Device Decommissioning

- All storage devices go through process
- Uses techniques from
  - DoD 5220.22-M (“National Industrial Security Program Operating Manual “)
  - NIST 800-88 (“Guidelines for Media Sanitization”)
- Ultimately
  - degaussed
  - physically destroyed

Certifications

AWS Certifications

- Based on the Shared Responsibility model
- AWS Environment
  - SSAE 16/SOC 1 Type II Audit
  - ISO 27001 Certification
  - Payment Card Industry Data Security Standard (PCI DSS) Level 1 Service Provider
  - FedRAMP (FISMA)
- Customers have deployed various compliant applications:
  - Sarbanes-Oxley (SOX)
  - HIPAA (healthcare)
  - FISMA Moderate (US Federal Government)
  - DIACAP MAC III Sensitive IATO

SOC 1 Type II (SSAE 16)

- Covers Access, Change Management and Operations of EC2 and S3
  - Control Objective 1: Security Organization
  - Control Objective 2: Amazon Employee Lifecycle
  - Control Objective 3: Logical Security
  - Control Objective 4: Secure Data Handling
  - Control Objective 5: Physical Security
  - Control Objective 6: Environmental Safeguards
  - Control Objective 7: Change Management
  - Control Objective 8: Data Integrity, Availability and Redundancy
  - Control Objective 9: Incident Handling
- Includes all Regions
- Audited by an independent accounting firm and updated every 6 months
- Report available under NDA
- Converted SAS 70 to Statement on Standards for Attestation Engagements (SSAE) 16 format (equivalent to the International Standard on Assurance Engagements [ISAE] 3402)

ISO 27001 Certification

- ISO 27001/27002 certification achieved 11/2010
- Follows ISO 27002 best practice guidance
- Covers the AWS Information Security Management System (ISMS)
- Covers EC2, S3, and VPC
- Includes all Regions
- ISO certifying agent: EY CertifyPoint

PCI DSS Level 1 Service Provider

- PCI DSS 2.0 compliant
- Covers core infrastructure & services
  - EC2, EBS, S3, VPC, ELB, and RDS
- Use normally, no special configuration
- Leverage the work of our QSA
- AWS will work with merchants and designated Qualified Incident Response Assessors (QIRA)
  - can support forensic investigations
- Certified in all regions

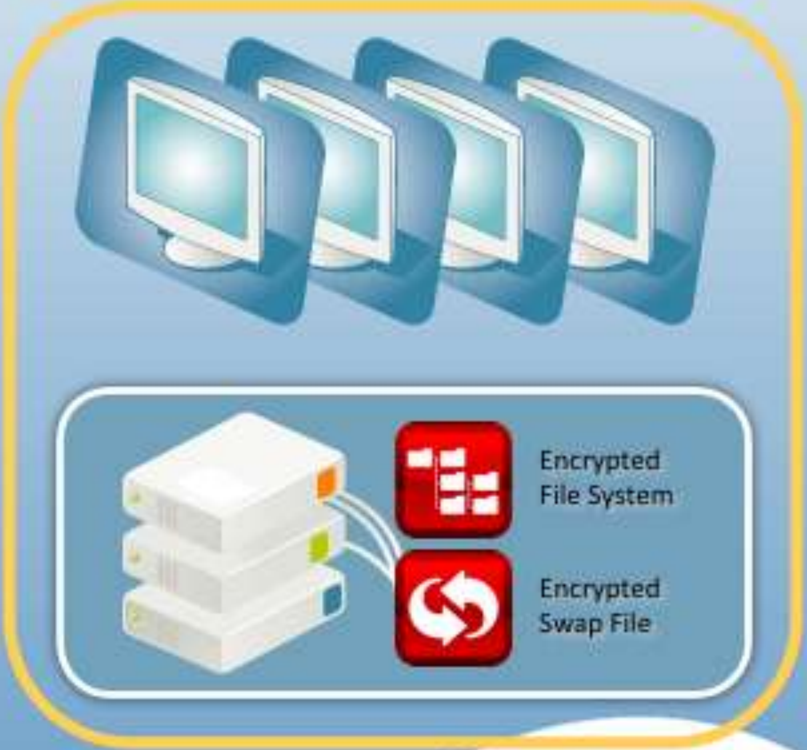
Security Features

EC2 (Virtual Machine) Security

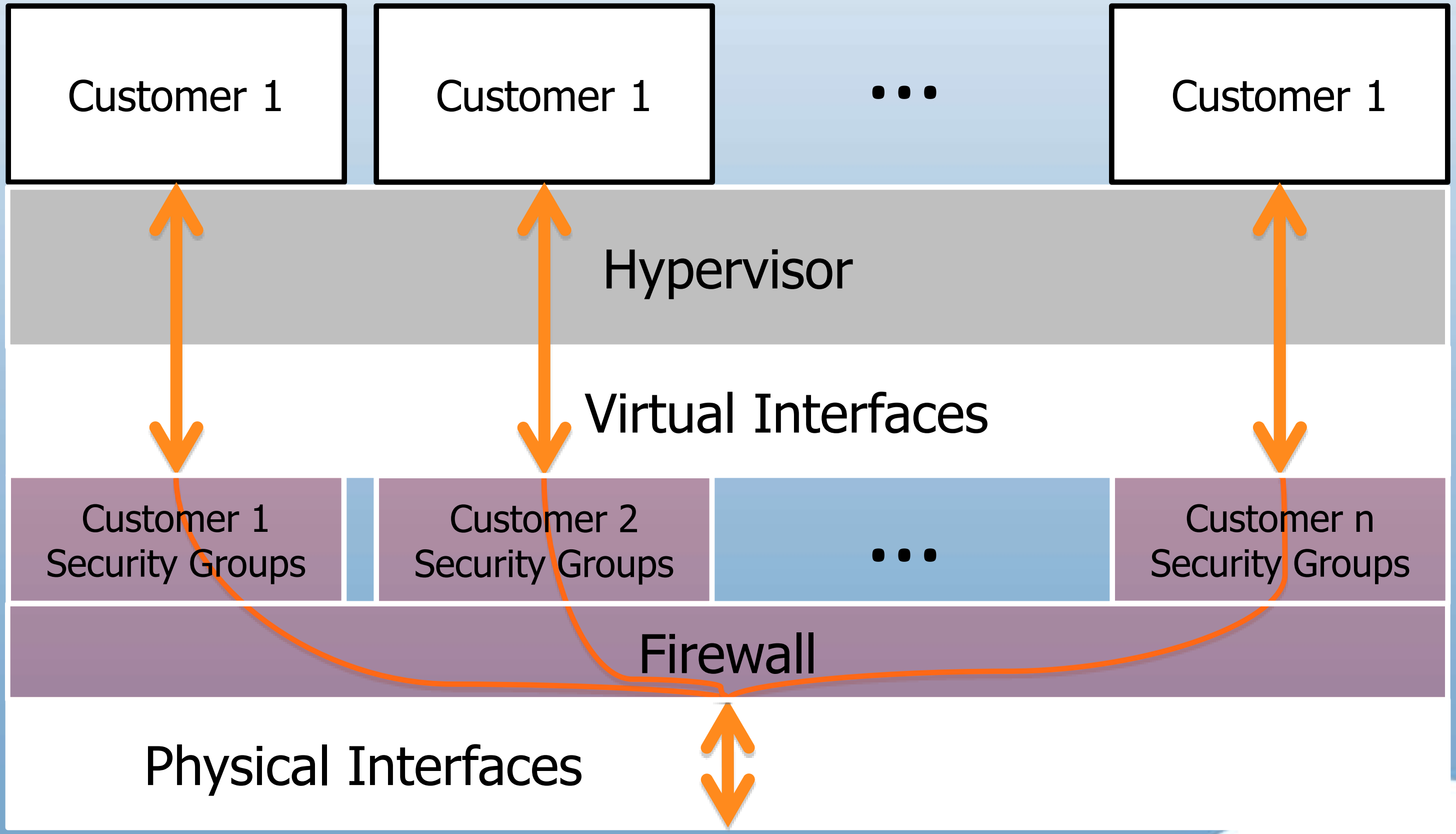
- Host operating system
  - Individual SSH keyed logins via bastion host for AWS admins
  - All accesses logged and audited
- Guest (a.k.a. Instance) operating system
  - Customer controlled (customer owns root/admin)
  - AWS admins cannot log in
  - Customer-generated keypairs
- Stateful firewall
  - Mandatory inbound firewall, default deny mode
  - Customer controls configuration via Security Groups
- Signed API calls
  - Require X.509 certificate or customer’s secret AWS key

Virtual Memory & Local Disk

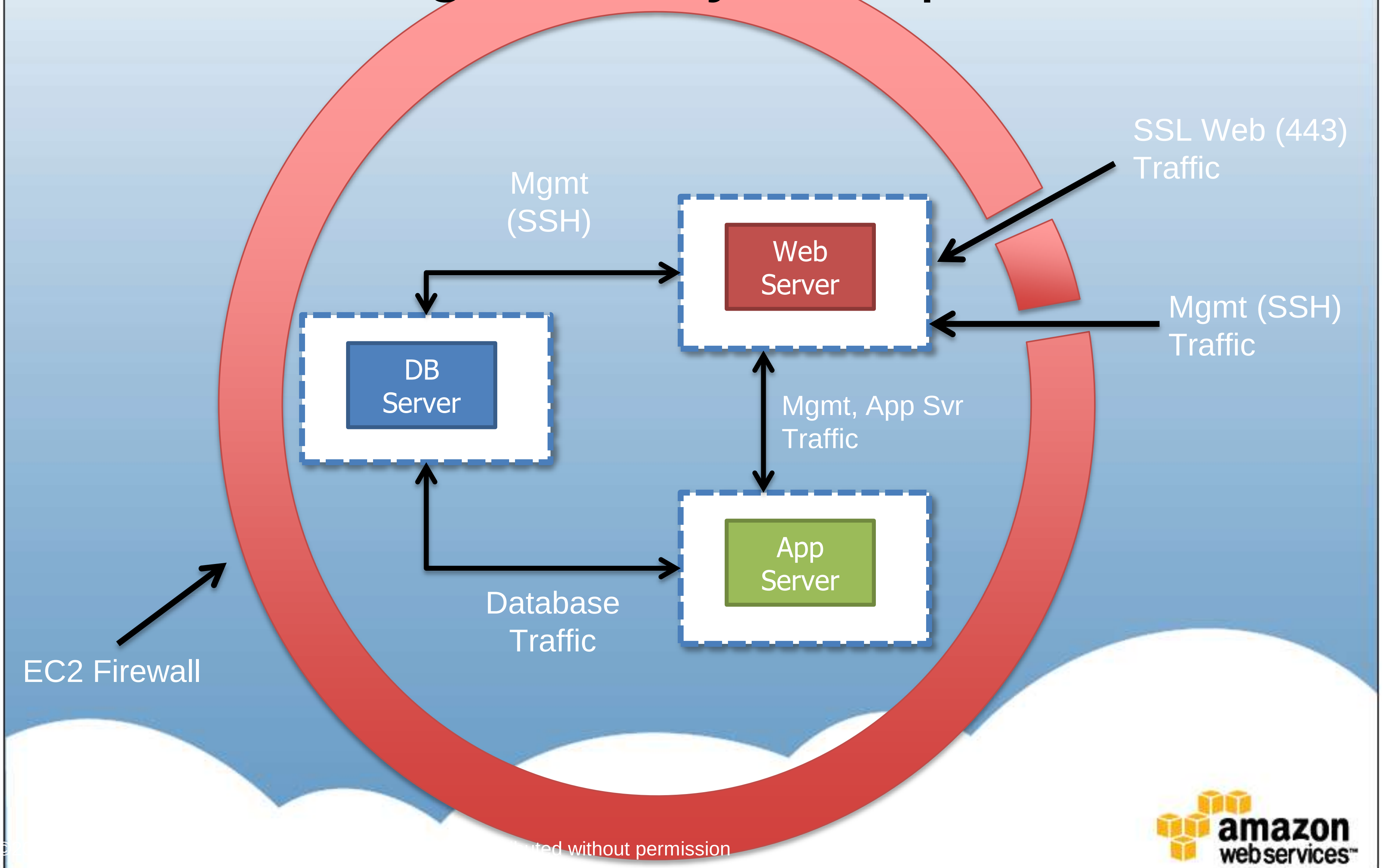
- Proprietary disk management prevents one Instance from reading the disk contents of another
- Disk is wiped upon creation
- Disks can be encrypted by the customer for an added layer of security



Amazon EC2 Virtualization



Tiering Security Groups



Mgmt (SSH)

Web Server

SSL Web (443) Traffic

Mgmt (SSH) Traffic

DB Server

Mgmt, App Svr Traffic

App Server

Database Traffic

EC2 Firewall

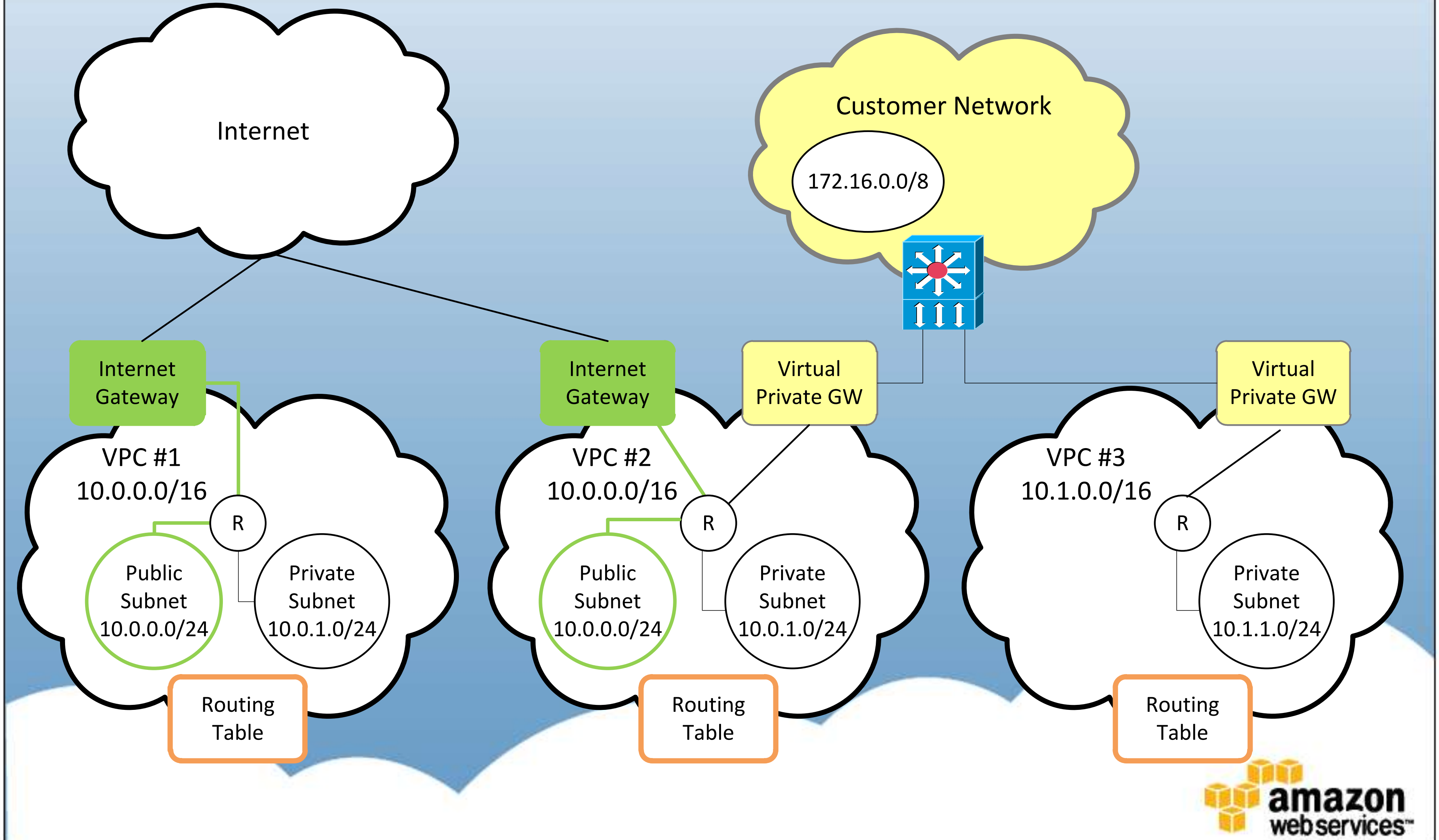
Network Security Considerations

- IP Spoofing/ARP Poisoning:
  - Prohibited at host OS level
- Packet Sniffing:
  - Promiscuous mode is ineffective
  - Protection at hypervisor level
- Unauthorized Port Scanning:
  - Violation of AWS TOS
  - Detected, stopped, and blocked
  - Ineffective anyway since inbound ports blocked by default
- MITM (Man in the Middle):
  - All endpoints protected by SSL
  - Fresh EC2 host keys generated at boot

Amazon Virtual Private Cloud (VPC)

- Create a **logically isolated** environment in Amazon’s highly scalable infrastructure
- Specify your **private IP** address range into one or more public or private subnets
- Control inbound and outbound access to and from individual subnets using stateless **Network Access Control Lists**
- Protect your Instances with stateful filters for inbound and outbound traffic using **Security Groups**
- Attach an Elastic IP address to any instance in your VPC so it can be reached **directly from the Internet**
- Bridge your VPC and your onsite IT infrastructure with an industry standard encrypted **VPN connection**
- Use a **wizard** to easily create your VPC in 4 different topologies

Multiple VPC Scenarios


Internet
Customer Network
172.16.0.0/8
Internet Gateway
Internet Gateway
Virtual Private GW
Virtual Private GW
VPC #1
10.0.0.0/16
R
Public Subnet 10.0.0.0/24
Private Subnet 10.0.1.0/24
Routing Table
VPC #2
10.0.0.0/16
R
Public Subnet 10.0.0.0/24
Private Subnet 10.0.1.0/24
Routing Table
VPC #3
10.1.0.0/16
R
Private Subnet 10.1.1.0/24
Routing Table
amazon webservices™