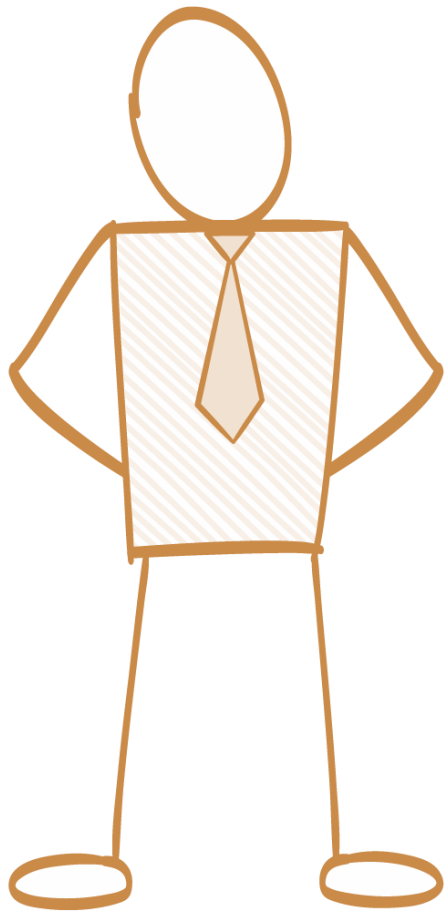




Architecting on AWS Student Guide

Version 3.1

100-ARC-31-EN-SG



Module 3: Security and Compliance

Before we start....

- Identify the correct statements:

Security and patching of the operating system and the application is the responsibility of the customer.	Penetration testing is a violation of the AWS Terms of Service.	Data on block storage devices (ephemeral storage and EBS) is encrypted by default.
Port scanning is performed by AWS to check for vulnerabilities in your application.	AWS is PCI DSS Level 1 certified, but customers are responsible for managing PCI compliance and certification for their own applications.	Each AWS Region has at least one Disaster Recovery Availability Zone.

Topics

- The shared responsibility security model
- AWS role in security
- Your role in security
- Securing networks with Security Groups

Topics

- **The shared responsibility security model**
- AWS role in security
- Your role in security
- Securing networks with Security Groups

The shared responsibility security model



The shared responsibility security model



Topics

- The shared responsibility security model
- **AWS role in security**
- Your role in security
- Securing networks with Security Groups

AWS role in Shared Responsibility Security Model

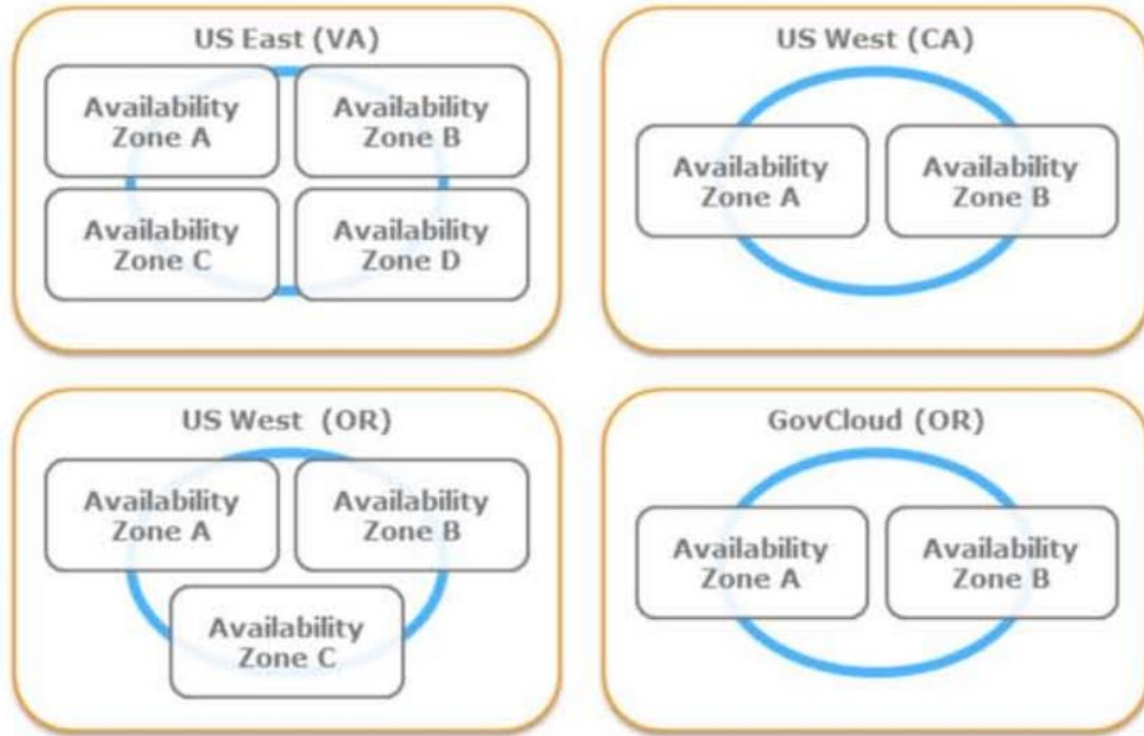
•AWS

- Facilities
- Physical Security
 - Physical infrastructure
 - Network infrastructure
- Virtualization infrastructure
- Third-Party Attestations, Reports, and Certifications for the above

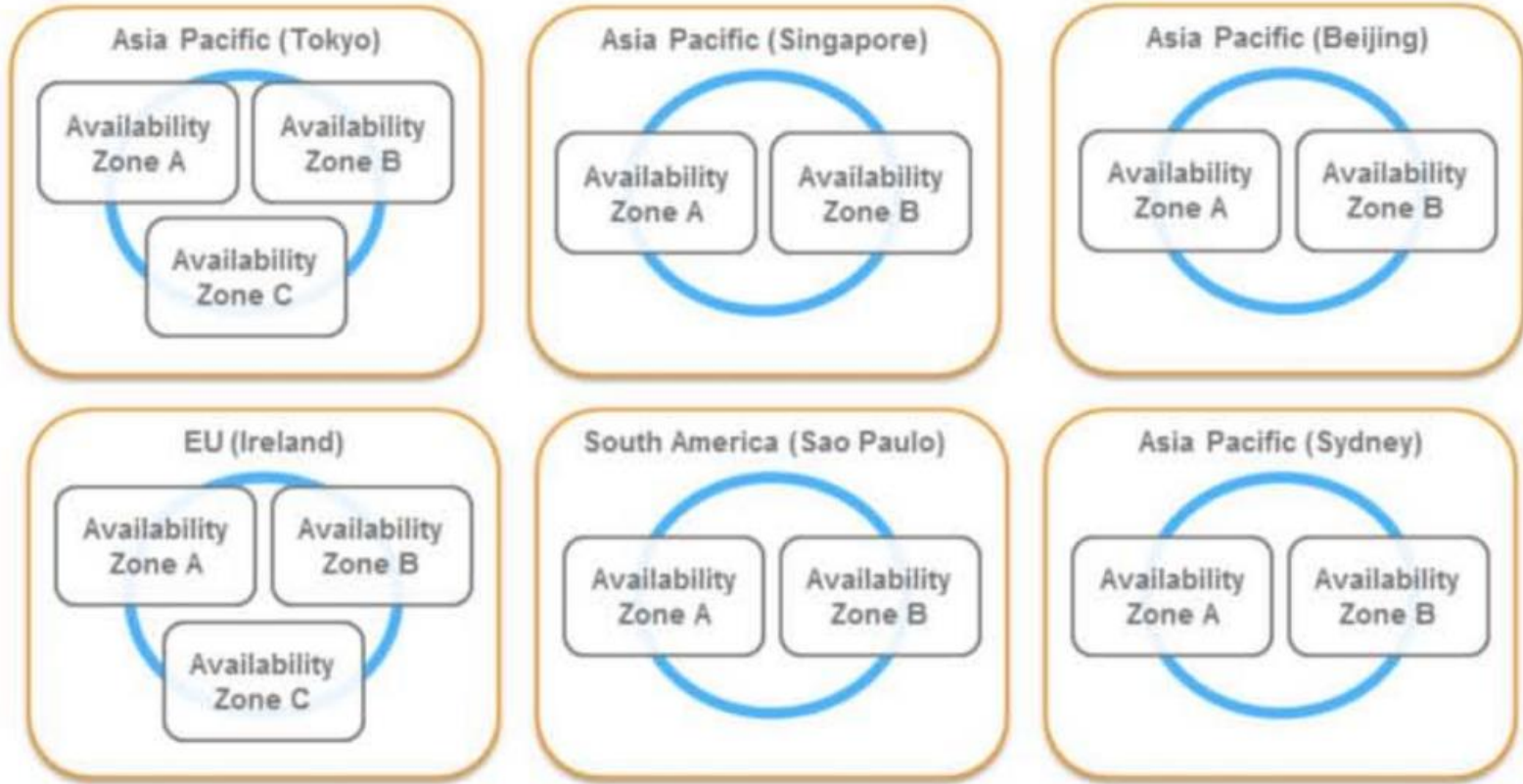
•Customer

- Operating system
- Application
- Security groups
- OS Firewalls
- Network configuration
- Account Management
- Certifying your applications

AWS US Regions



AWS Global Regions



Physical Security

- Controlled, need-based access
 - All access is logged and reviewed
 - Multi-factor authentication
- Separation of Duties
 - Employees with physical access do not have logical access
- 24 x 7 security guards

Network Security

- Distributed Denial of Service (DDoS)
 - Standard mitigation techniques in effect
- Man in the Middle (MITM)
 - All API endpoints protected by SSL
- IP Spoofing
 - Prohibited at host OS level
- Unauthorized Port Scanning
 - Violation of TOS
 - Detected, stopped, and blocked
- Packet Sniffing
 - Promiscuous mode ineffective
 - Protection at hypervisor level

Storage Device Decommissioning

- Uses techniques from:
 - DoD 5220.22-M (*“National Industrial Security Program Operating Manual”*)
 - NIST 800-88 (*“Guidelines for Media Sanitization”*)
- Ultimately, all devices are:
 - Degaussed
 - Physically destroyed

Virtual Memory and Local Disk Space

- Proprietary disk management prevents one instance from reading disk contents of another
- Disk is wiped upon creation
- Disks can be encrypted by customer

AWS Third-Party Attestations, Report, and Certifications

- AWS Environment

- Service Organization Controls(SOC) Reports
 - SOC 1 Type II (SSAE 16/ISAE 3402/formerly SAS70)
 - SOC 2 Type II
 - SOC 3
- Payment Card Industry Data Security Standard (PCI DSS) Level 1 Certification
- ISO 27001 Certification
- FedRAMP
- DIACAP and FISMA
- ITAR
- FIPS 140-2

AWS Third-Party Attestations, Report, and Certifications(continue)

- Customers have deployed various compliant applications:

- Sarbanes-Oxley (SOX)
- HIPAA (healthcare)
- FedRAMPSM (US Public Sector)
- FISMA (US Public Sector)
- ITAR (US Public Sector)
- DIACAP MAC III Sensitive IATO

Topics

- The shared responsibility security model
- AWS role in security
- Your role in security
- Securing networks with Security Groups

Your role in Shared Responsibility Security Model

•AWS

- Facilities
- Physical Security
 - Physical infrastructure
 - Network infrastructure
- Virtualization infrastructure
- Third-Party Attestations, Reports, and Certifications for the above

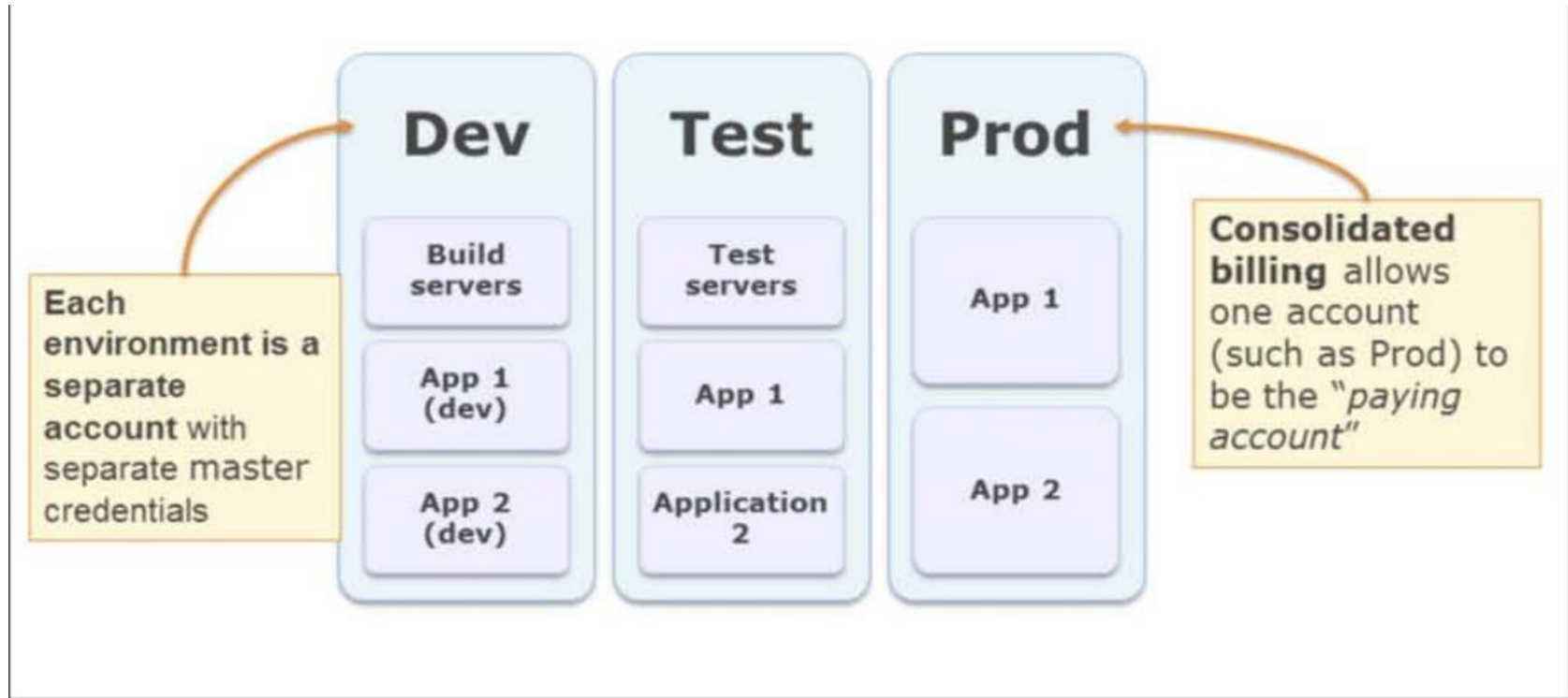
•Customer

- Operating system
- Application
- Security groups
- OS Firewalls
- Network configuration
- Account Management
- Certifying your applications

Account Management

- Master (root) account has root/admin-level access
- Multiple accounts may be created to isolate resources
- Account may be isolated by:
 - Environment (dev, test, prod)
 - Major System
 - Line of business/function
 - Customer
 - Risk level

AWS account management by enviroment



Identity and Access Management



Operating system security

- Guest (instance) operating system
 - Customer controlled (customer owns root/admin)
 - AWS admins cannot log in ← Why not?
- EC2 Key Pairs
 - You (and only you) have the private half of the key
 - You (and only you) can:
 - SSH to the instance (Linux)
 - Decrypt the Administrator password (Windows)

Operating system security

- You still need to patch

- Most traditional tools will work

- Emerging options

- Chef(www.opscode.com/chef)

- Puppet(www.puppetlabs.com)

- Fabric/Cuisine(www.fabfile.org)

- Capistrano(<https://github.com/capistrano/capistrano/wiki>)

- Amazon OpsWorks(<https://aws.amazon.com/opsworks>)

Your Data

- Protect privacy and enforce your policies with data encryption
- Encrypt data in transit
 - (SSL/TLS)
- Encrypt data at rest
 - Consider encrypted file systems for sensitive data
 - Encrypt objects before storing them
 - Encrypt records before writing in database
- EBS and Ephemeral volumes can be encrypted
- Variety of options
 - EncFS, Loop-AES, dm-Crypt, TrueCrypt, etc....

Encryption: File Systems

- Managing encryption keys

- Study key management capabilities of encryption product(s) you choose
- Establish a procedure that minimizes possibility of losing keys
- AWS CloudHSM
 - Securely generate, store and manage cryptographic keys used for data encryption
 - Dedicated SafeNet Luna SA

Use Multiple Security Layers

- Security Groups (EC2, VPC, RDS, ElastiCache, Redshift)
- Bastion Host
- Host-based Firewalls*
- IDS*

Topics

- The shared responsibility security model
- AWS role in security
- Your role in security
- Securing networks with Security Groups

Network Security: Security Groups

- Control inbound traffic
 - VPC groups can also control outbound
- Apply many Security Group to one instance
- Default group: no access
- Several services use Security Groups
 - EC2
 - VPC(more advanced features)
 - RDS
 - ElastiCache
 - Redshift

Network Security: Security Groups(continue)

- When defining inbound rules, specify source by:
 - CIDR address
 - 0.0.0.0/0 for Internet, 10.0.0.0/16 for EC2 private, and so on
 - Security Group Name
 - Restrict access to other EC2 instances in the specified security group

CIDR Notation: An Overview

- CIDR notation is useful for expressing a range of IP address
- Consider this IP(v4) address:

216.173.122.34

- Each number can be between 0 to 255
- Each number is a single byte(8 bits)

CIDR Notation: An Overview

- What if you wanted to express a firewall rule that allowed traffic from any address in the last octet?

—Specify the first valid value in the last octet, the first allowable value is 0

216.173.122.* 

We want to allow all values

—In this case, we want 216.173.122.0 

bits: 3 octets == 3 bytes == 24 bits. Therefore → 216.173.122.0/24

CIDR Notation: A few more examples

- Match an exact address

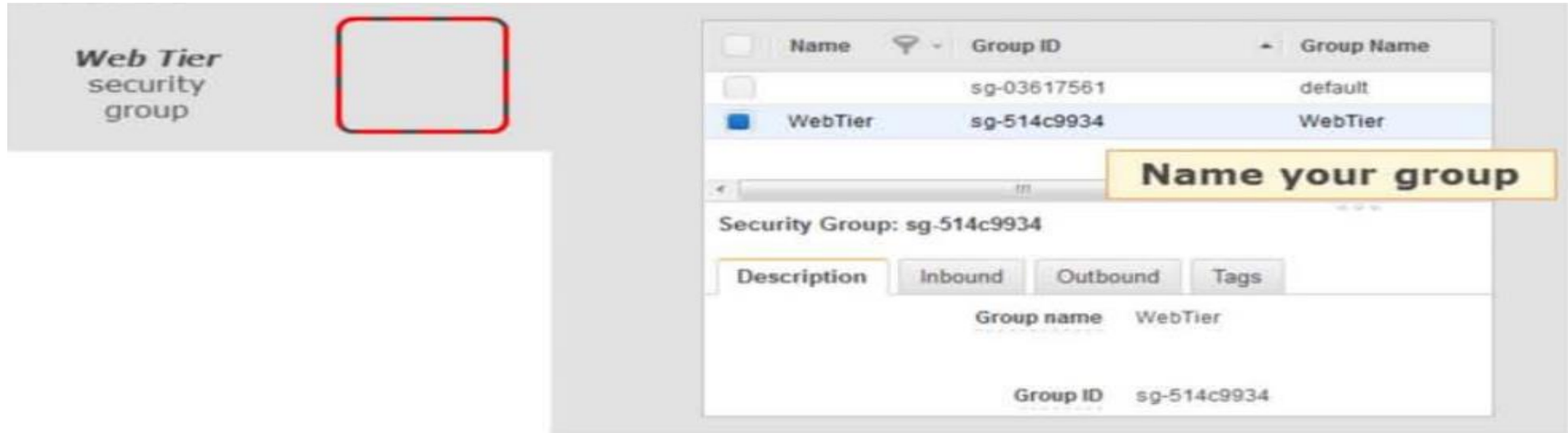
–216.173.122.34  216.173.122.34/32

- Match any address

–*. *.*.*.*  0.0.0.0/0


Security Groups Example: Web Server Instance(1 of 3)

- Design a security group for Apache web servers in your application's web tier



Security Groups Example: Web Server Instance (2 of 3)

Web Tier
security
group



Specify allowed port, protocol and source

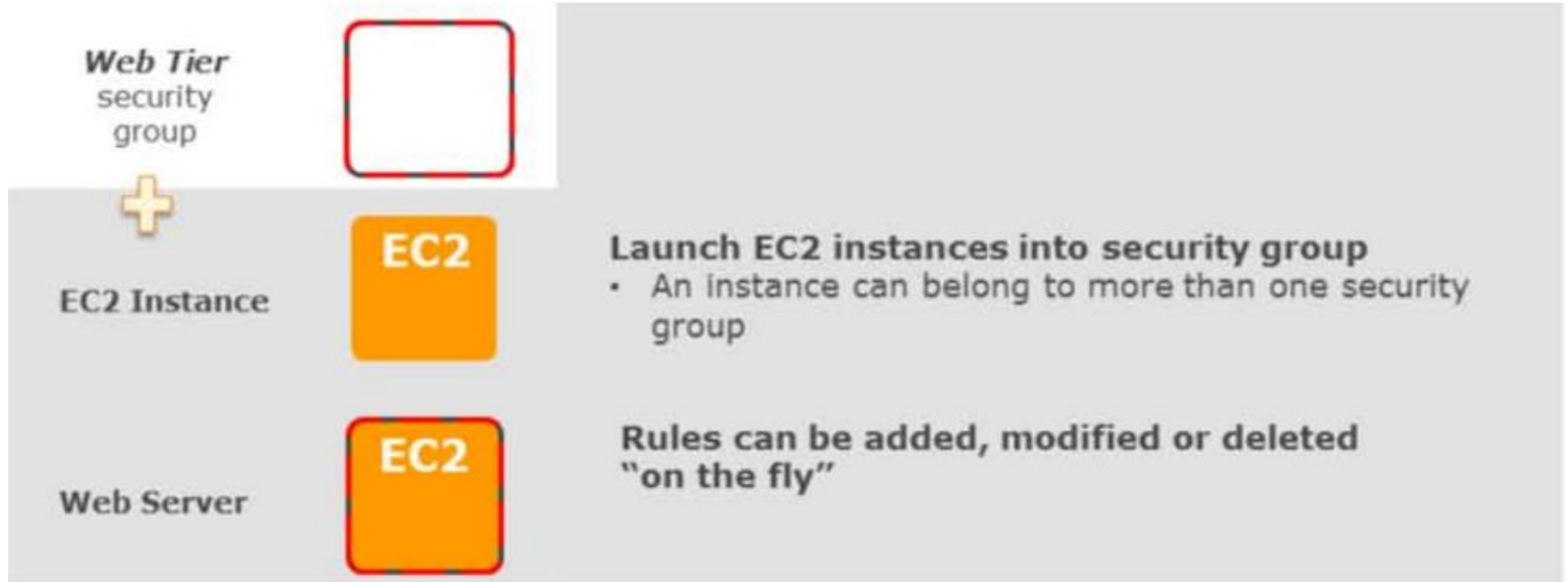
Security Group: sg-514c9934

Description Inbound Outbound Tags

Edit

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
HTTP	TCP	80	0.0.0.0/0

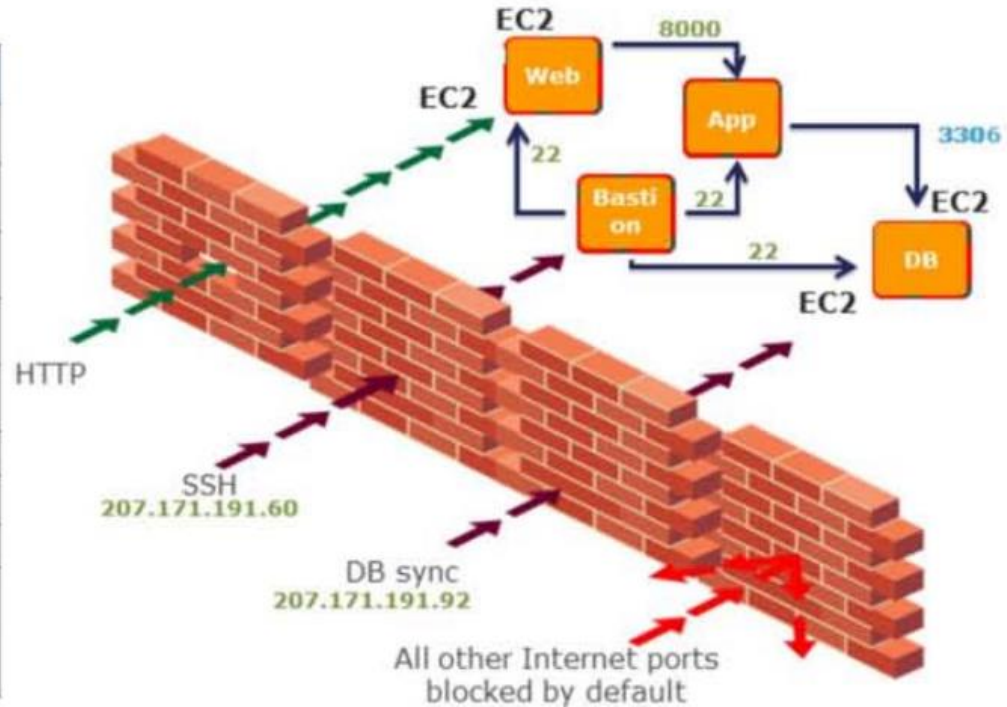
Security Groups Example: Web Server Instance (3 of 3)



Security Groups Example: Multi-tier Security Group Activity

Define the Groups

Tier	Port	Source
Web	80	0.0.0.0/0
	443	0.0.0.0/0
	22	Bastion
App	22	Bastion
	8000	Web
DB	3306	207.171.191.92/32
	3306	App
	22	Bastion
Bastion	22	207.171.191.60/32



Most security best practices still apply in the Cloud

- Secure coding standards
- Perform penetration testing
 - <http://aws.amazon.com/security/penetration-testing>
- Antivirus where appropriate
- Intrusion Detection
 - Host-based Intrusion Detection (such as OSSEC)
- Log events
- Role-based access control
 - AWS Identity & Access Management
 - LDAP and/or Active Directory for Operating System & Applications

Module review

- What are the five main layers of security for cloud architecture?
- What security model is used with AWS services
- What areas of security is AWS responsible for?
- What areas of security are you, the customer, responsible for?

Copyright © 2014 Amazon Web Services, Inc. or its affiliates. All rights reserved.

This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited.

Errors or corrections? Email us at aws-course-feedback@amazon.com.
Other questions? Email us at aws-training-info@amazon.com.

All trademarks are the property of their owners.

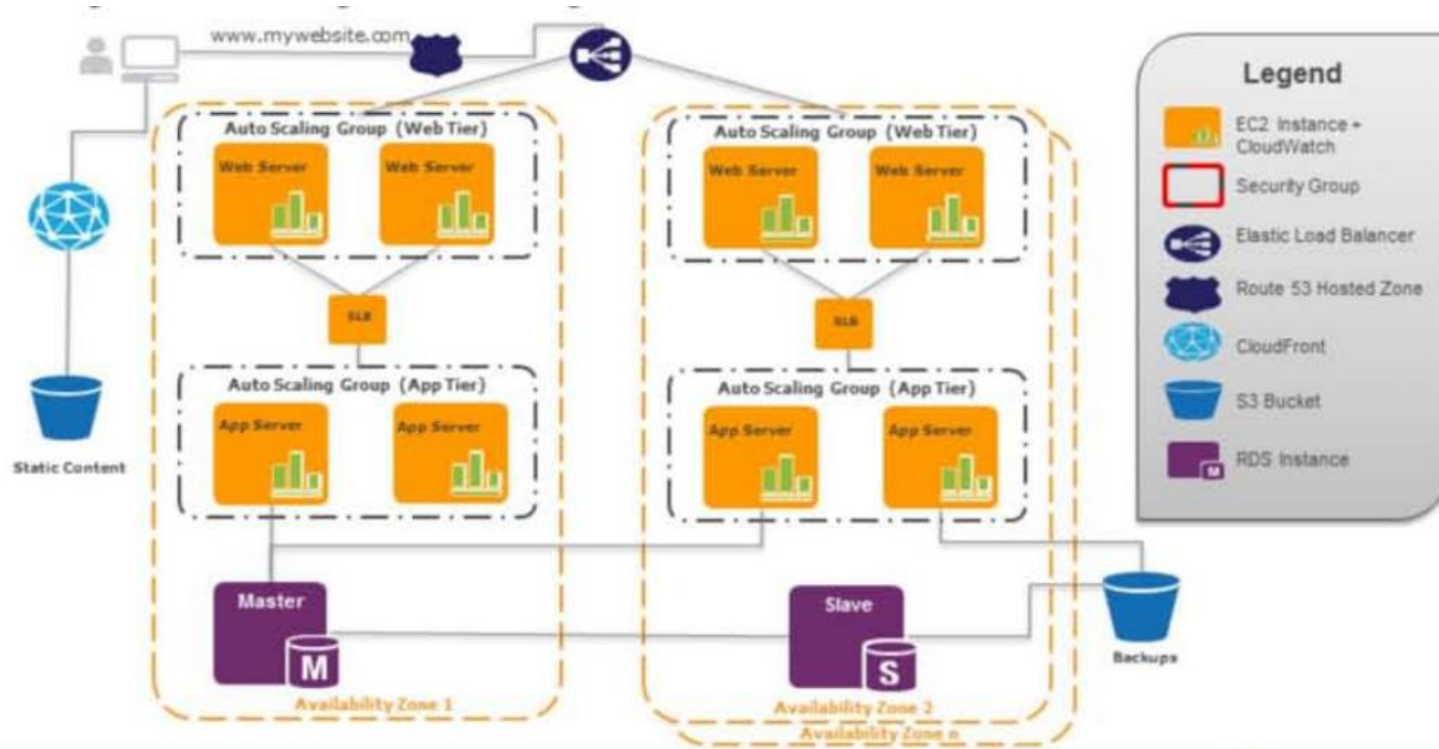
Appendix

Activity---Identify Security Mechanisms

- Consider the architecture for a scalable web application. How do you secure it? Address the following aspects of security:

- Physical
- Network
- Data(in transit and at rest)
- Operating system
- Security credential management
- Logging

Activity --- Identify Security Mechanisms



Activity --- Identify Security Mechanisms

