Copyright © 2013 Amazon Web Services, Inc. and 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.

Architecting on AWS

Security and Compliance

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

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 (i.e., 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.

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security and Compliance | What we'll cover

1

The shared responsibility security model

2

AWS role in security

3

Your role in security

4

Securing networks with Security Groups

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

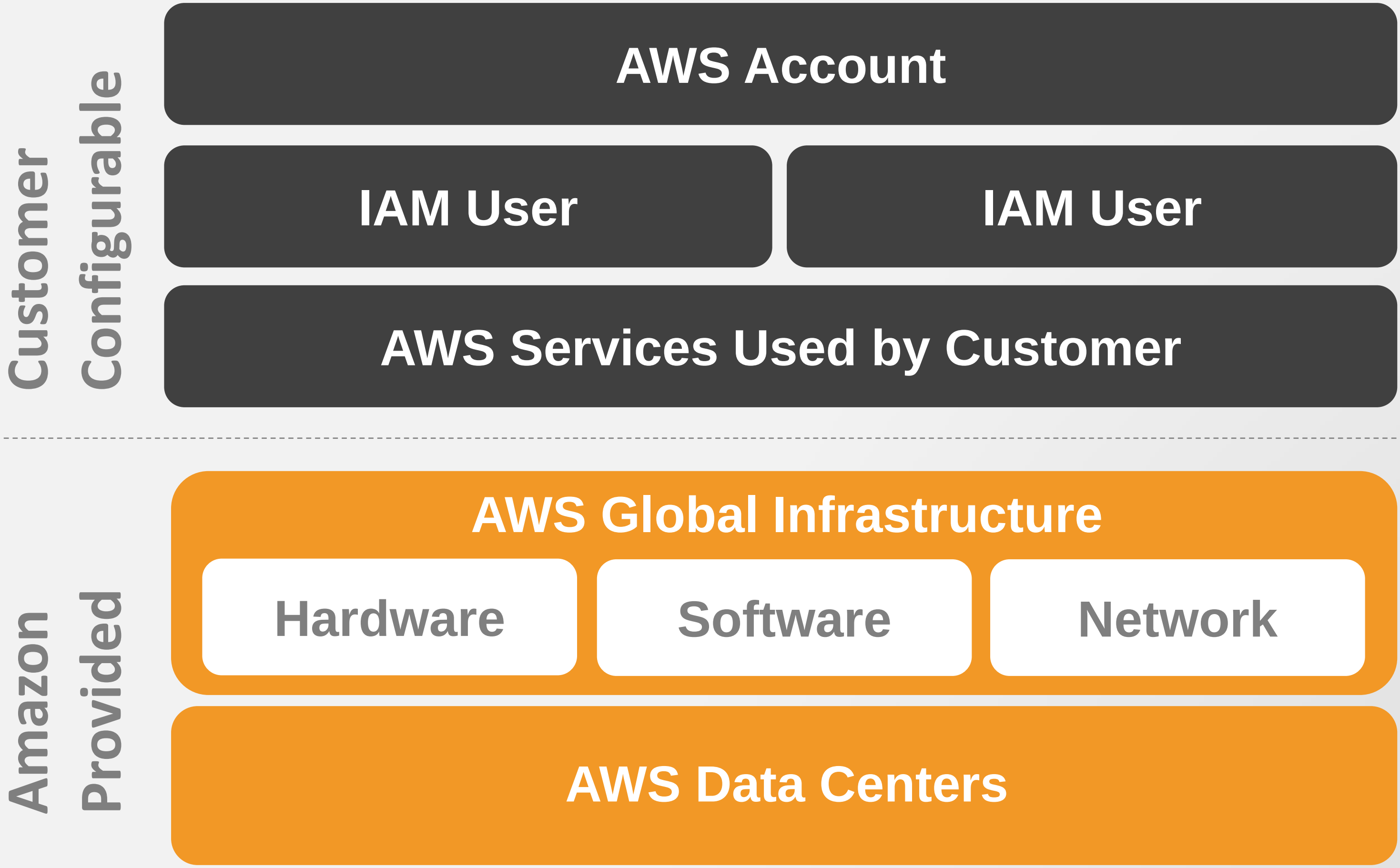
Security and Compliance | The shared responsibility security model

1

The shared responsibility security model

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security and Compliance | The shared responsibility security model



Customer Configurable

AWS Account

IAM User

IAM User

AWS Services Used by Customer

Amazon Provided

AWS Global Infrastructure

Hardware

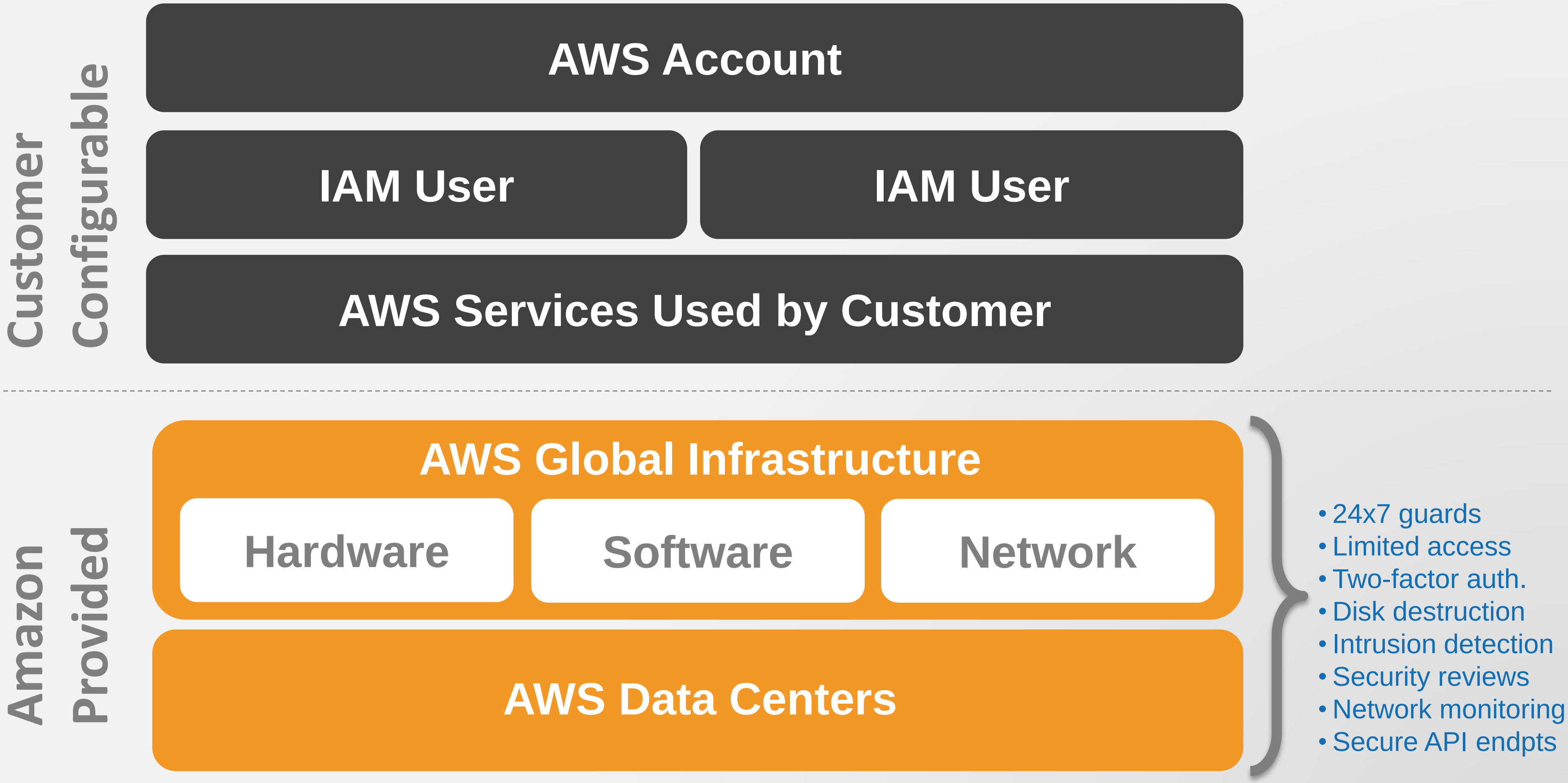
Software

Network

AWS Data Centers

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security and Compliance | The shared responsibility security model



Customer Configurable

AWS Account

IAM User

IAM User

AWS Services Used by Customer

Amazon Provided

AWS Global Infrastructure

Hardware

Software

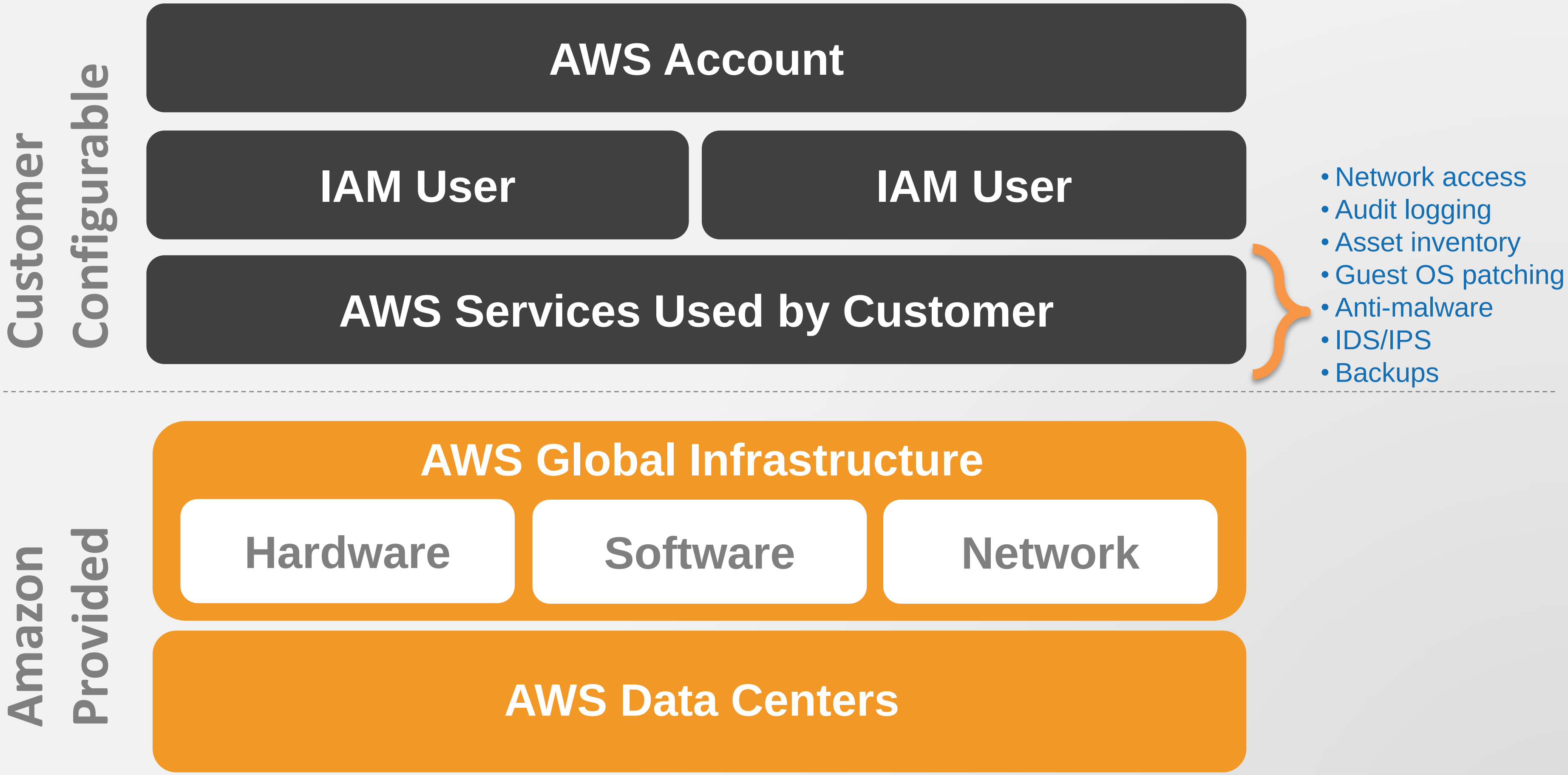
Network

AWS Data Centers

- 24x7 guards
- Limited access
- Two-factor auth.
- Disk destruction
- Intrusion detection
- Security reviews
- Network monitoring
- Secure API endpts

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security and Compliance | The shared responsibility security model



Customer Configurable

AWS Account

IAM User

IAM User

AWS Services Used by Customer

- Network access
- Audit logging
- Asset inventory
- Guest OS patching
- Anti-malware
- IDS/IPS
- Backups

Amazon Provided

AWS Global Infrastructure

Hardware

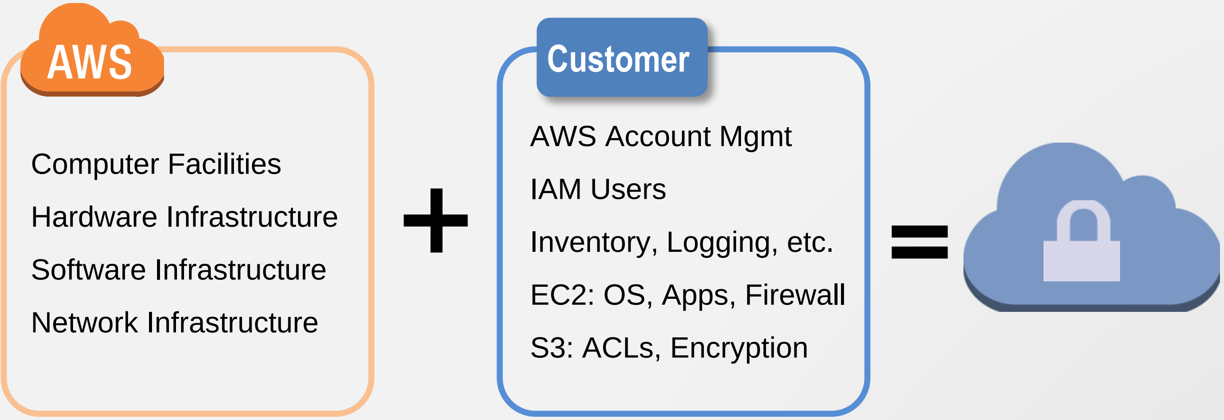
Software

Network

AWS Data Centers

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security and Compliance | The shared responsibility security model



AWS

Computer Facilities

Hardware Infrastructure

Software Infrastructure

Network Infrastructure

+

Customer

AWS Account Mgmt

IAM Users

Inventory, Logging, etc.

EC2: OS, Apps, Firewall

S3: ACLs, Encryption

=

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security and Compliance | AWS Role in Security

2

AWS role in security

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shared Responsibility Security Model

AWS

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

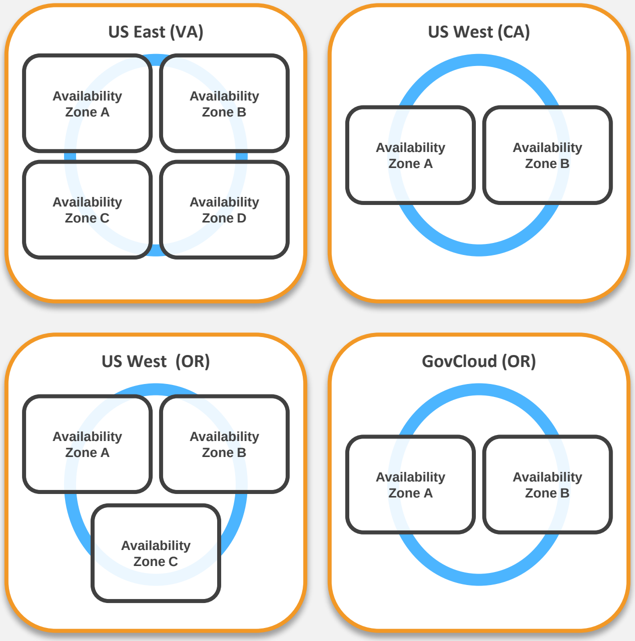
Customer

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

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security and Compliance | AWS Role in Security

US Regions



US East (VA)

Availability Zone A
Availability Zone B
Availability Zone C
Availability Zone D

US West (CA)

Availability Zone A
Availability Zone B

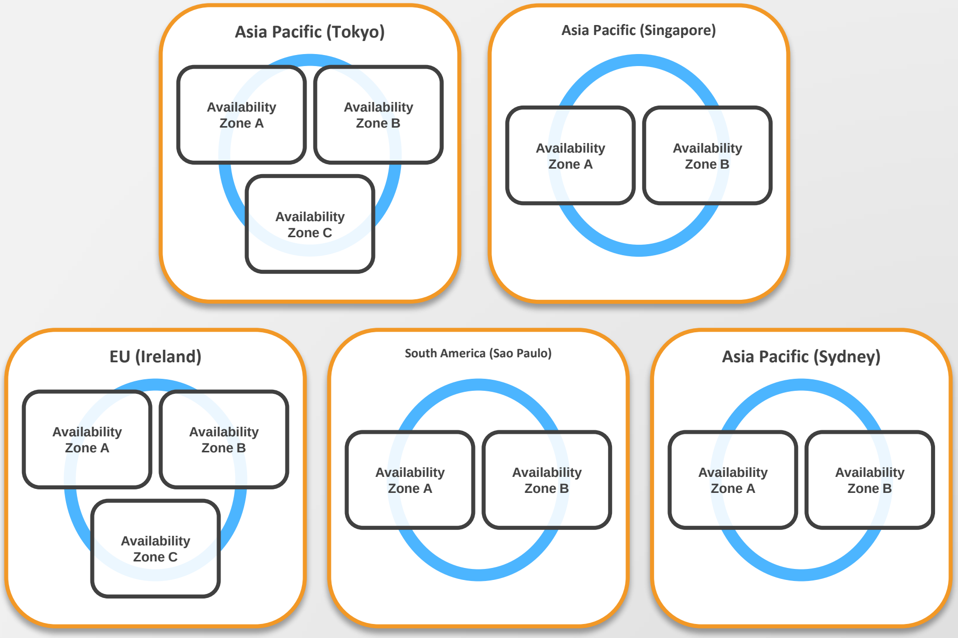
US West (OR)

Availability Zone A
Availability Zone B
Availability Zone C

GovCloud (OR)

Availability Zone A
Availability Zone B

Global Regions



Asia Pacific (Tokyo)

Availability Zone A
Availability Zone B
Availability Zone C

Asia Pacific (Singapore)

Availability Zone A
Availability Zone B

EU (Ireland)

Availability Zone A
Availability Zone B
Availability Zone C

South America (Sao Paulo)

Availability Zone A
Availability Zone B

Asia Pacific (Sydney)

Availability Zone A
Availability Zone B

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Physical Security of Data Centers

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

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

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

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network Security

- Unauthorized Port Scanning
  - Violation of TOS
  - Detected, stopped and blocked
- Packet Sniffing
  - Promiscuous mode ineffective
  - Protection at hypervisor level

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Storage Device Decommissioning

- Uses techniques from:
  - DoD 5220.22-M (“National Industrial Security Program Operating Manual “)
  - NIST 800-88 (“Guidelines for Media Sanitization”)

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

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

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Virtual Memory and Local Disk

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

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Third-Party Attestations, Reports, 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^{SM}
  - DIACAP and FISMA
  - ITAR
  - FIPS 140-2

Additional information available at https://aws.amazon.com/compliance/.

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Third-Party Attestations, Reports and Certifications

- Customers have deployed various compliant applications:
  - Sarbanes-Oxley (SOX)
  - HIPAA (healthcare)
  - FedRAMP^{SM} (US Public Sector)
  - FISMA (US Public Sector)
  - ITAR (US Public Sector)
  - DIACAP MAC III Sensitive IATO

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shared Responsibility: Half Way There

- Any questions about the AWS half?

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Shared Responsibility: Half Way There

- Any questions about the AWS half?
- Now, let’s talk about…

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security and Compliance | Your Role in Security

3

Your role in security

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

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

$\left.\begin{array}{l}\text{Operating system}\\\text{Application}\\\text{Security groups}\\\text{OS Firewalls}\end{array}\right\}$ EC2

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Account Management

- Master (i.e., root) account has root/admin-level access

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Account Management

- Multiple accounts may be created to isolate resources
- Accounts may be isolated by:
  - Environment (e.g., dev, test, prod)
  - Major System
  - Line of business / function
  - Customer
  - Risk level

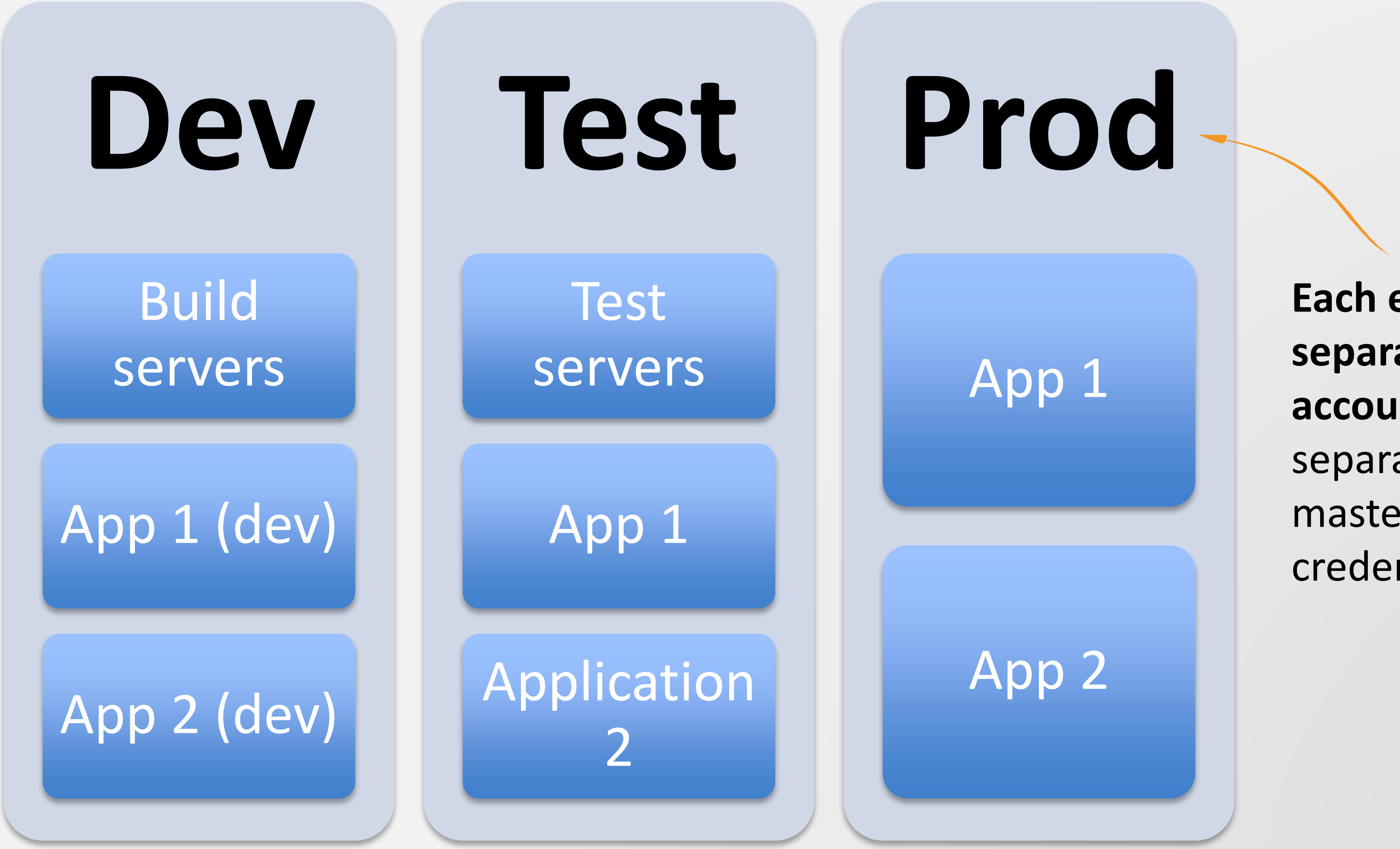
© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Account Management

- Multiple accounts may be created to isolate resources
- Accounts may be isolated by:
  - **Environment (e.g., dev, test, prod)**
  - Major System
  - Line of business / function
  - Customer
  - Risk level

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Account Management – By Environment



Dev

Build servers

App 1 (dev)

App 2 (dev)

Test

Test servers

App 1

Application 2

Prod

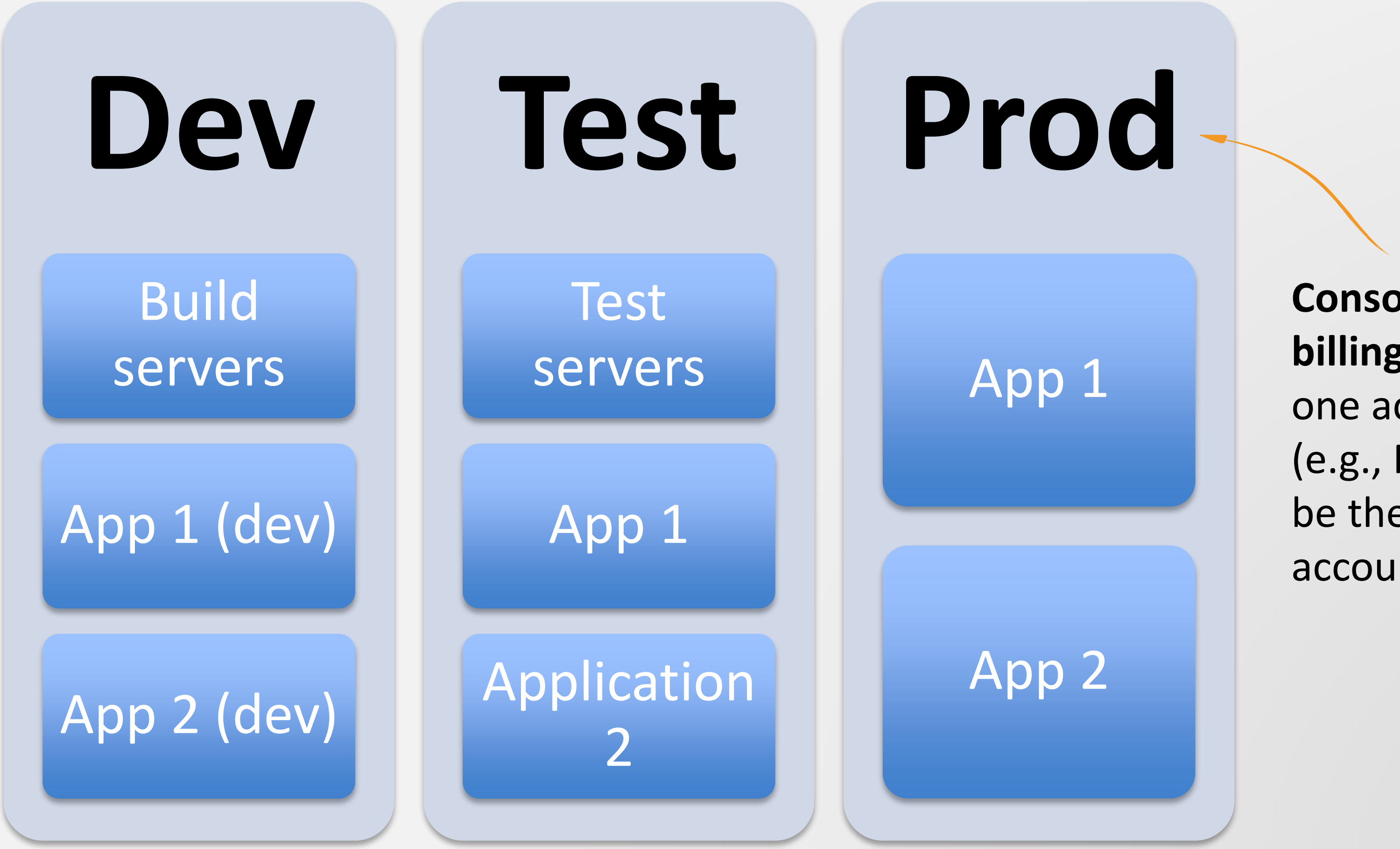
App 1

App 2

Each env is a separate account with separate master credentials

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

AWS Account Management – By Environment



Dev

- Build servers
- App 1 (dev)
- App 2 (dev)

Test

- Test servers
- App 1
- Application 2

Prod

- App 1
- App 2

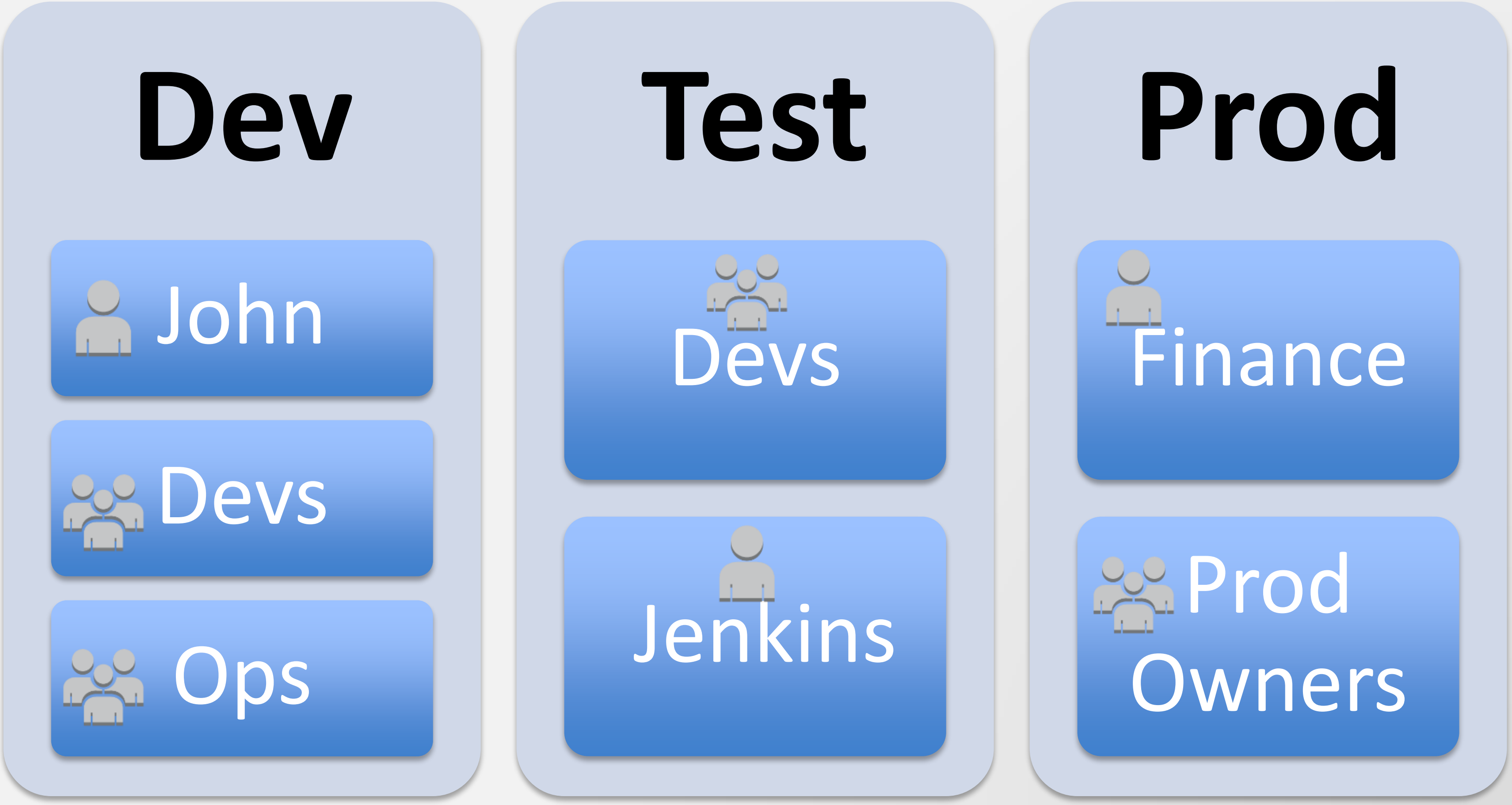
Consolidated billing allows one account (e.g., Prod) to be the ‘paying account’

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Identity and Access Management

- Create Users and Groups within a master account

Identity and Access Management



Dev

John

Devs

Ops

Test

Devs

Jenkins

Prod

Finance

Prod Owners

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Operating system security

- Guest (i.e., Instance) operating system
  - Customer controlled (customer owns root/admin)
  - AWS admins cannot log in

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Operating system security

- Guest (i.e., Instance) operating system
  - Customer controlled (customer owns root/admin)
  - AWS admins cannot log in ← **Why not?**

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Operating system security

- Guest (i.e., Instance) operating system
  - Customer controlled (customer owns root/admin)
  - AWS admins cannot log in ← **Why not?**
- EC2 Key Pairs

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Operating system security

- Guest (i.e., 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)

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

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)

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

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

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security and Compliance | Your Role in Security

Your Data

- EBS and Ephemeral volumes can be encrypted
- Variety of options
  - EncFS, Loop-AES, dm-Crypt, TrueCrypt, etc…

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

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

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Encryption: File Systems

Managing encryption keys

- AWS CloudHSM
  - Securely generate, store and manage cryptographic keys used for data encryption
  - Dedicated SafeNet Luna SA

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use Multiple Layers of Defense

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use Multiple Layers of Defense

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

* Third-Party tools/solutions

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Use Multiple Layers of Defense

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

* Third-Party tools/solutions

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security and Compliance | Securing Networks with Security Groups

4

Securing networks with Security Groups

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security and Compliance

Network Security: **Security Groups**

- Control **inbound** traffic
- Apply many Security Groups to 1 instance
- Default group: no access

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network Security: **Security Groups**

Several services use Security Groups

- EC2
- VPC (more advanced features)
- RDS
- ElastiCache

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network Security: **Security Groups**

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

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network Security: **Security Groups**

Let’s take a brief detour to explain CIDR notation…

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Brief Detour: CIDR Notation

- Useful for expressing a range of IP addresses
- Consider this IP(v4) address:

216.173.122.34

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

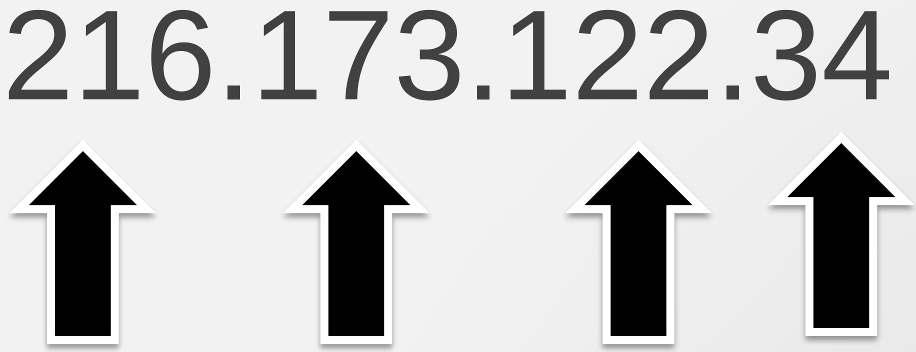
Brief Detour: CIDR Notation

216.173.122.34

Each number can have a decimal value between 0 and 255.

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Brief Detour: CIDR Notation



216.173.122.34

Each number is a single byte (8 bits).

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Brief Detour: CIDR Notation

216.173.122.*

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

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Brief Detour: CIDR Notation

216.173.122.0

Specify the first valid number in the range. If we want to allow all values in the last octet, the first allowable value is 0.

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Brief Detour: CIDR Notation

216.173.122.0

Now specify a mask that indicates how many bits (starting from the left) are “frozen”.

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Brief Detour: CIDR Notation

216.173.122.0

Now specify a mask that indicates how many bits (starting from the left) are “frozen”.

In this case, we want to freeze the first 3 octets.
3 octets == 3 bytes == 24 bits.

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Brief Detour: CIDR Notation

216.173.122.0/24

Now specify a mask that indicates how many bits (starting from the left) are “frozen”.

In this case, we want to freeze the first 3 octets.
3 octets == 3 bytes == 24 bits.

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Brief Detour: CIDR Notation

A few more examples…

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Brief Detour: CIDR Notation

Match an exact address: 216.173.122.34

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Brief Detour: CIDR Notation

Match an exact address: 216.173.122.34

216.173.122.34/32

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Brief Detour: CIDR Notation

Match any address: *.*.*.*

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Brief Detour: CIDR Notation

Match any address: *.*.*.*

0.0.0.0/0

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network Security: **Security Groups**

Example: Web Server Instance

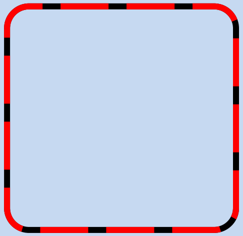
- Design a security group for Apache web servers in your application's web tier

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

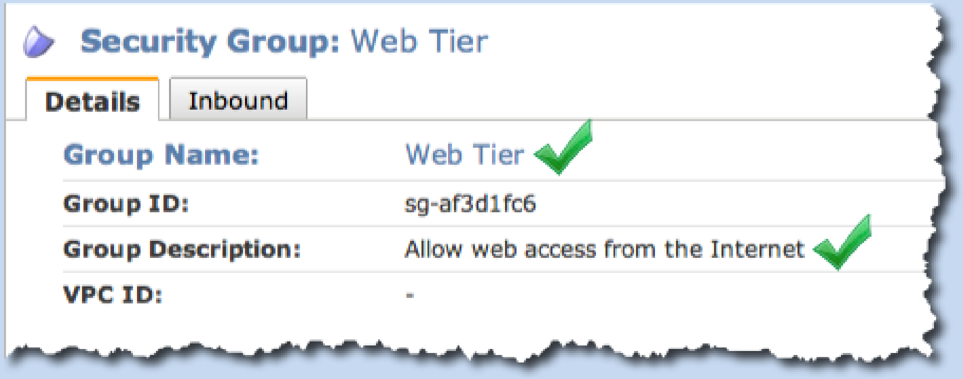
Network Security: **Security Groups**

Example: Web Server Instance

Web Tier security group



Name Your Group



Security Group: Web Tier

Details | Inbound

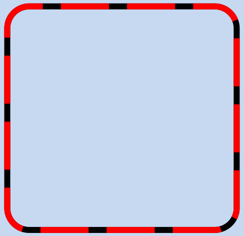
Group Name:	Web Tier ✓
Group ID:	sg-af3d1fc6
Group Description:	Allow web access from the Internet ✓
VPC ID:	-

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

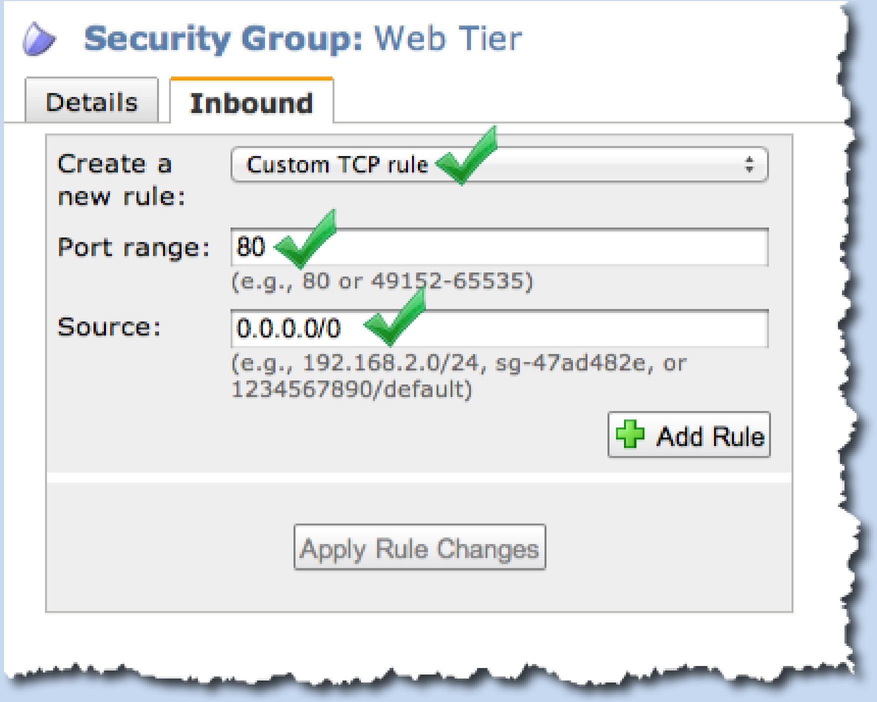
Network Security: **Security Groups**

Example: Web Server Instance

Web Tier security group



Specify allowed port, protocol, and source



Security Group: Web Tier

Create a new rule: Custom TCP rule ✓

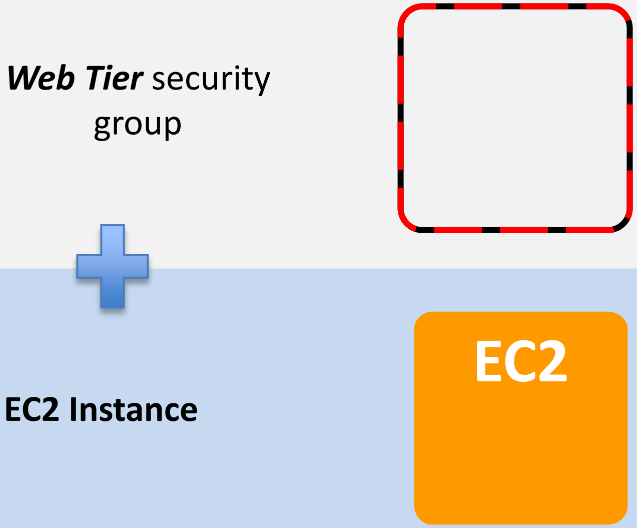
Port range: 80 ✓
(e.g., 80 or 49152-65535)

Source: 0.0.0.0/0 ✓
(e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network Security: **Security Groups**

Example: Web Server Instance



Web Tier security group

EC2 Instance

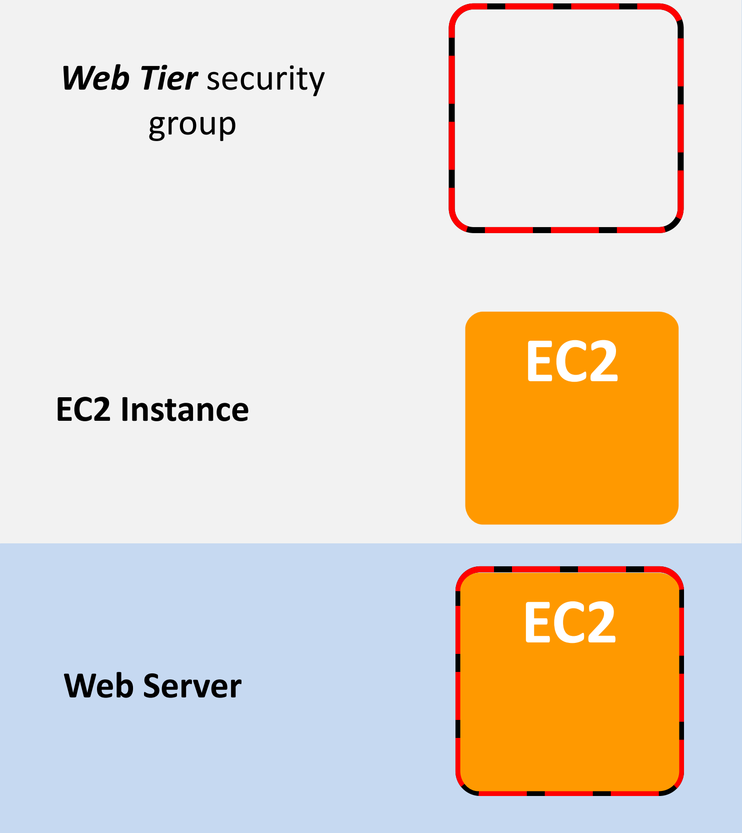
Launch EC2 instances into security group

- An instance can belong to more than one security group

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Network Security: **Security Groups**

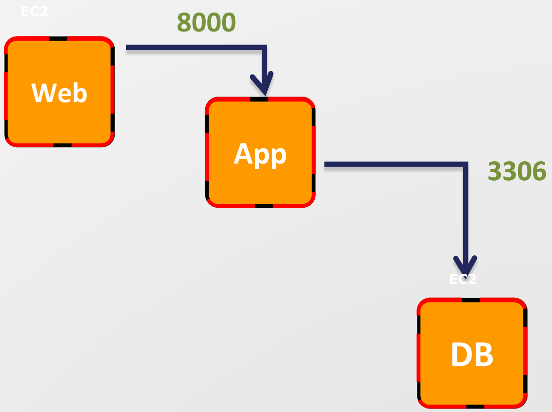
Example: Web Server Instance



Rules can be added, modified or deleted "on the fly"

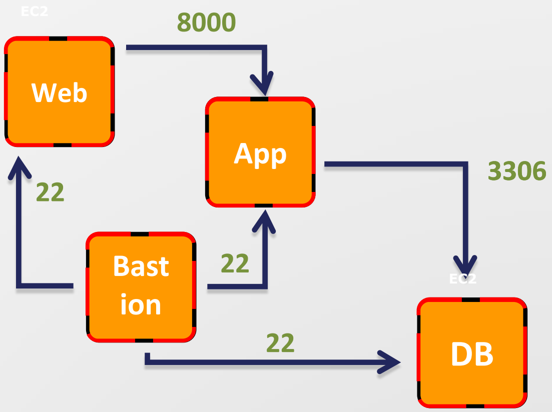
© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multi-tier Security Group Activity



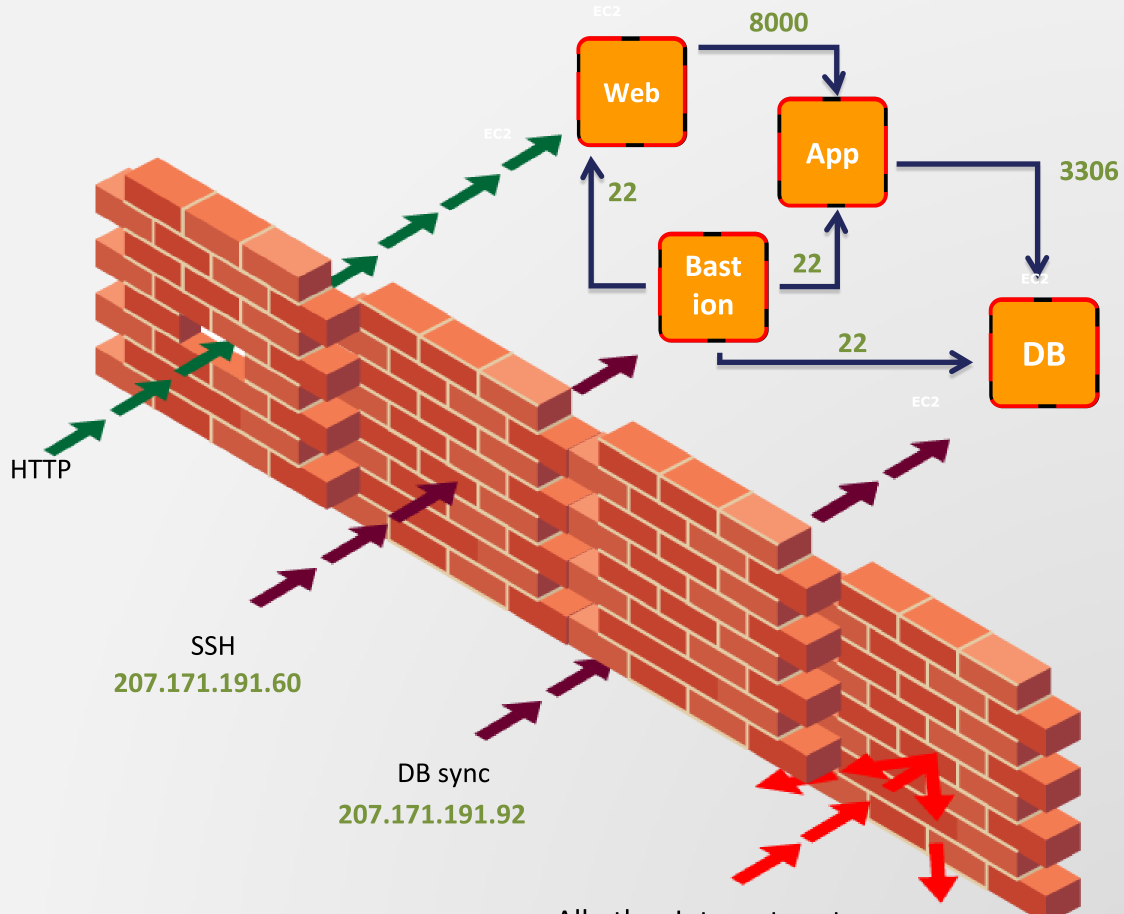
© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multi-tier Security Group Activity



© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Multi-tier Security Group Activity



EC2

Web

8000

EC2

App

3306

22

Bast
ion

22

EC2

22

DB

EC2

HTTP

SSH

207.171.191.60

DB sync

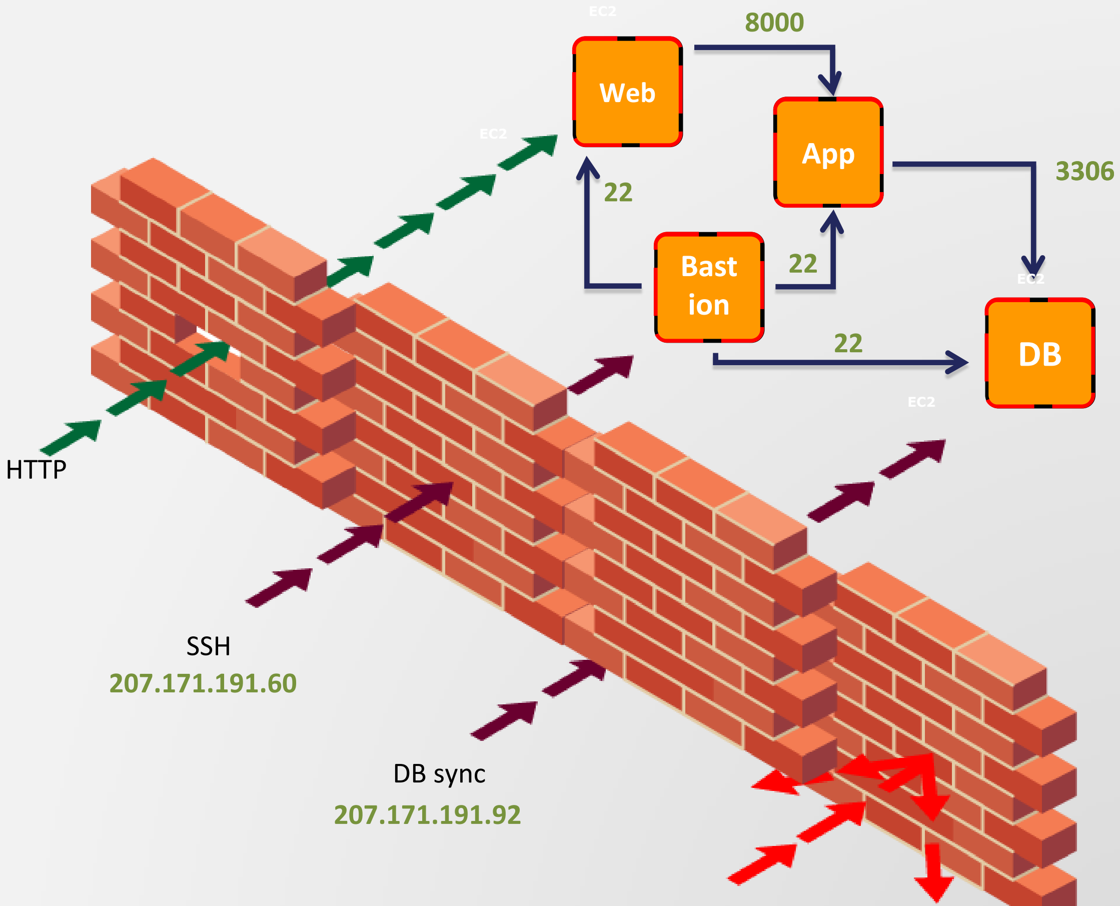
207.171.191.92

All other Internet ports
blocked by default

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Define the Groups

Tier	Port	Source
Web		
App		
DB		
Bast ion		



SSH
207.171.191.60

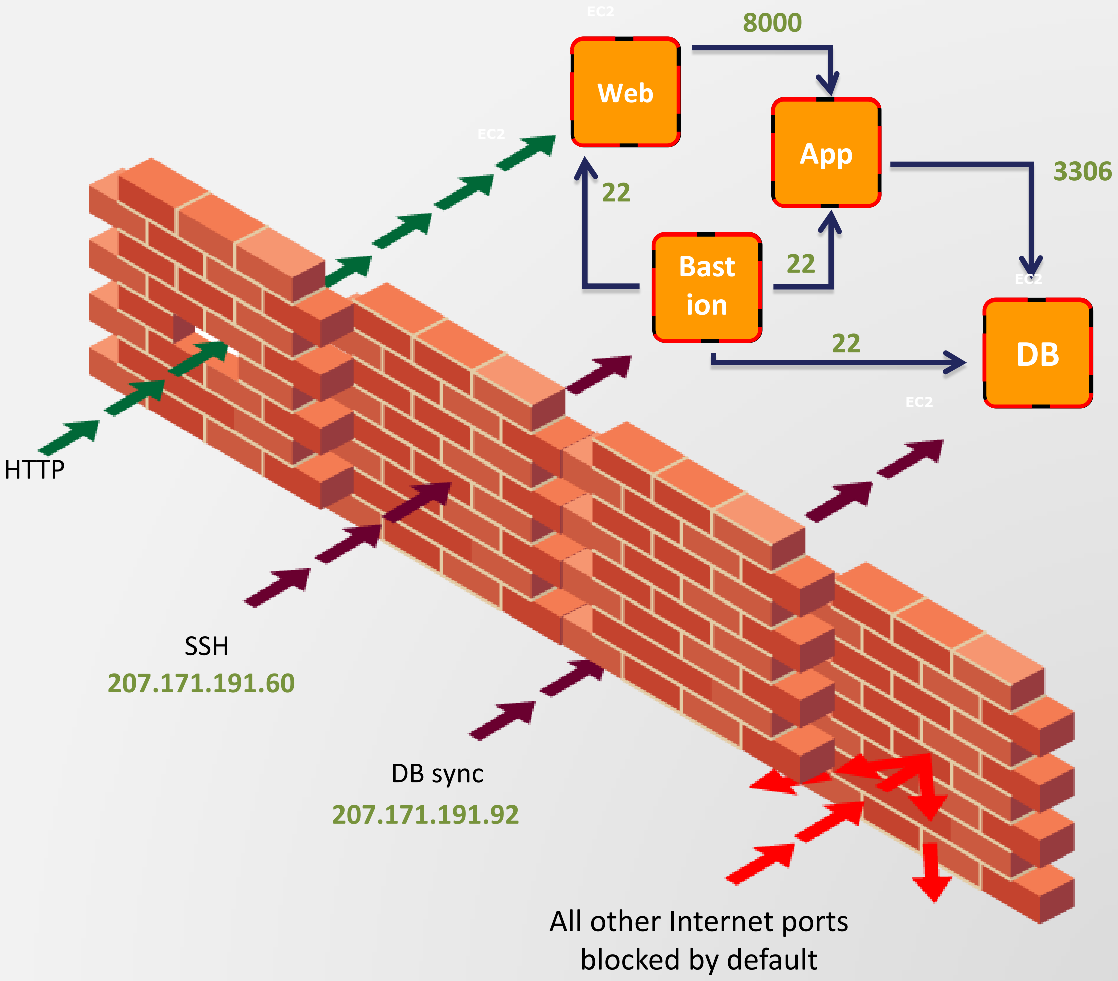
DB sync
207.171.191.92

All other Internet ports
blocked by default

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Define the Groups

Tier	Port	Source
Web		
App		
DB		
Bastion	22	207.171.191.60/32

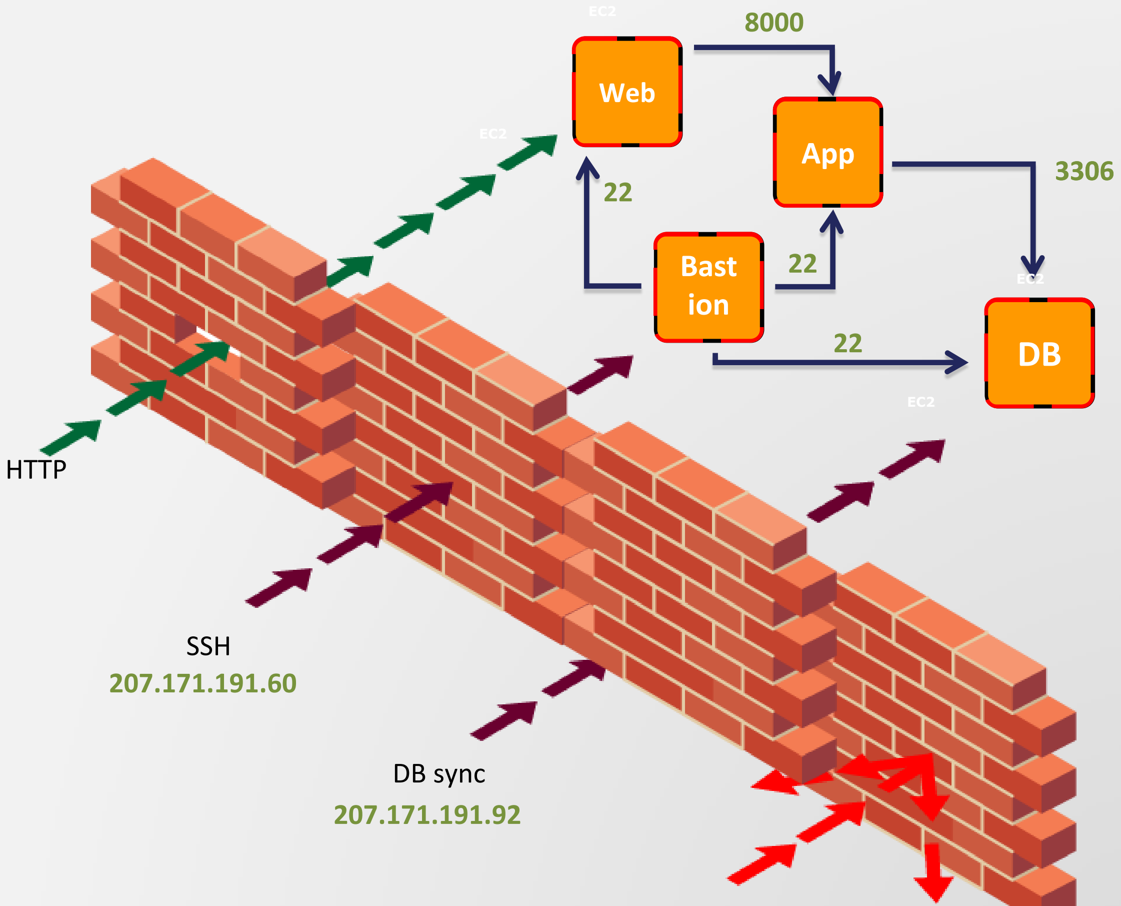


All other Internet ports blocked by default

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Define the Groups

Tier	Port	Source
Web		
App		
DB	3306	207.171.191.92/32
	3306	App
	22	Bastion
Bastion	22	207.171.191.60/32

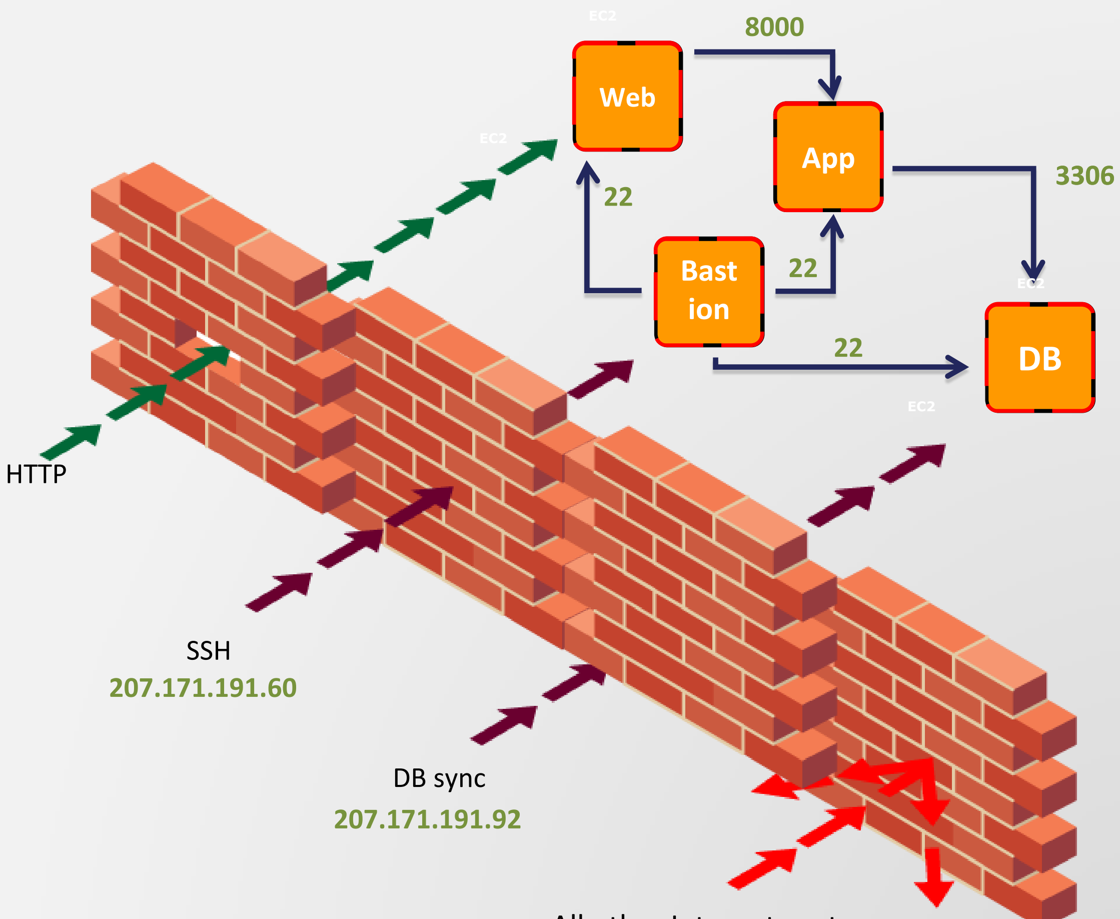


All other Internet ports blocked by default

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Define the Groups

Tier	Port	Source
Web		
App	22	Bastion
	8000	Web
DB	3306	207.171.191.92/32
	3306	App
	22	Bastion
Bastion	22	207.171.191.60/32



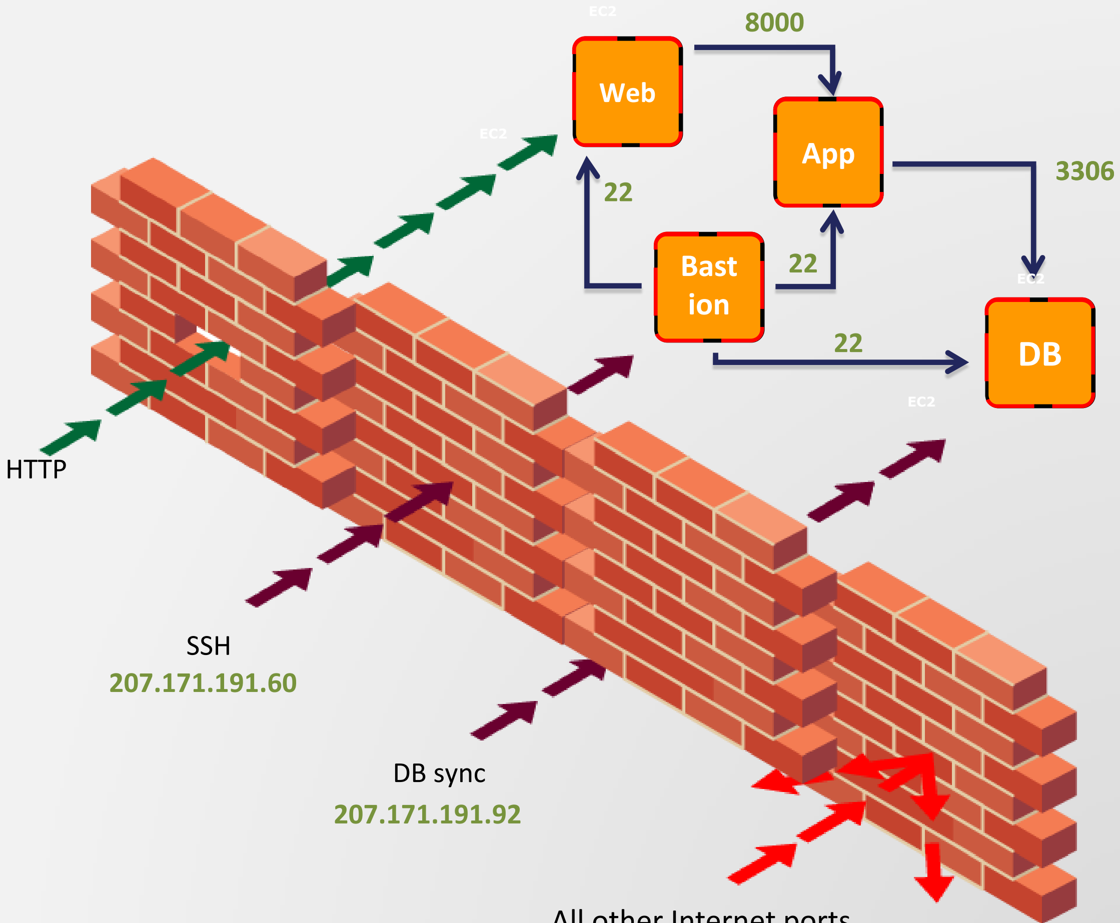
All other Internet ports blocked by default

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security and Compliance | Securing Networks with Security Groups

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



SSH
207.171.191.60

DB sync
207.171.191.92

All other Internet ports blocked by default

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security and Compliance | Conclusion

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

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Most security best practices **still apply** in the Cloud

- Intrusion Detection
  - Host-based Intrusion Detection (e.g., OSSEC)
- Log events
- Role-based access control
  - AWS Identity & Access Management
  - LDAP and/or Active Directory for Operating Systems & Applications

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

For 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?

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Appendix

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

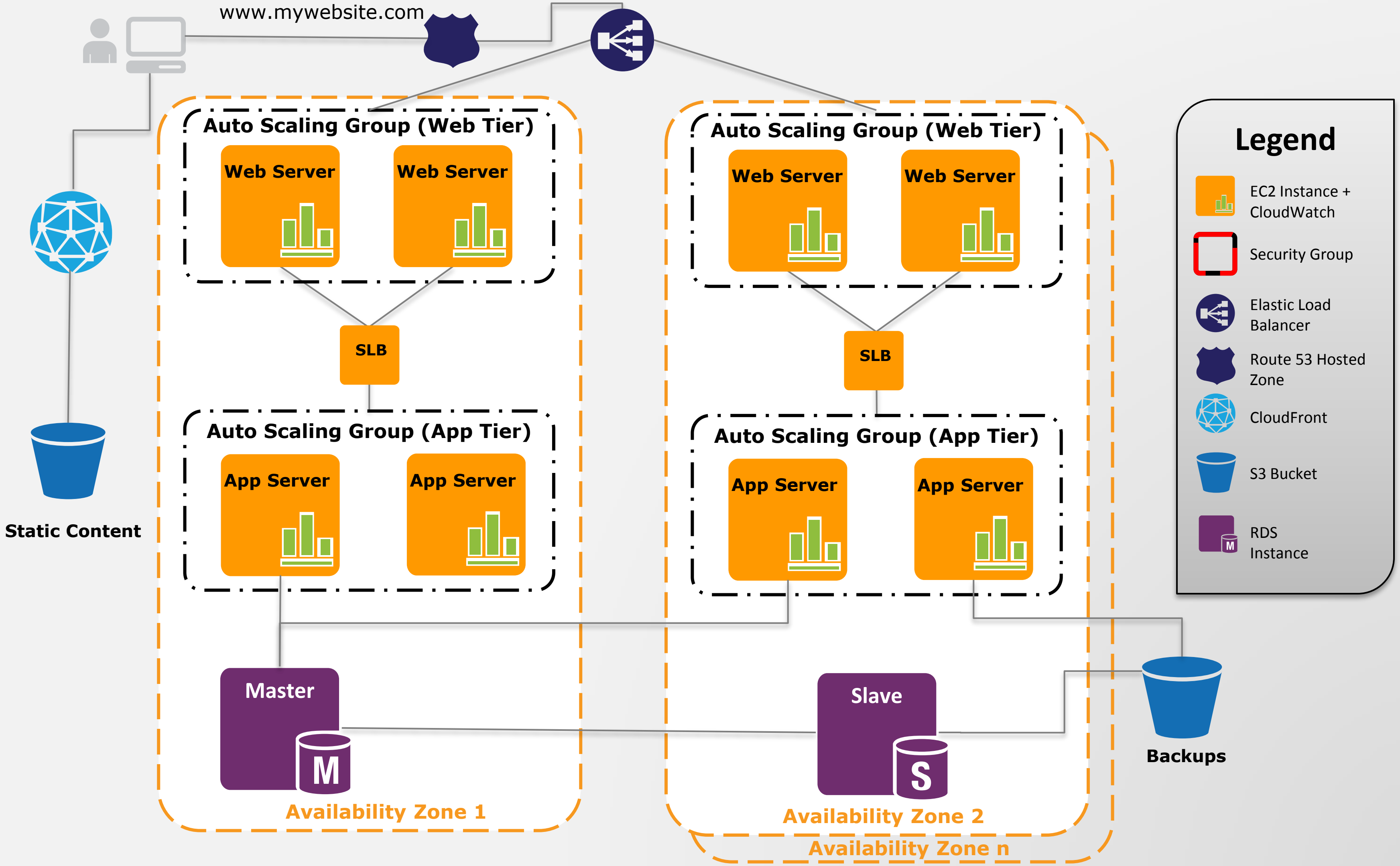
Activity: Identify Security Mechanisms

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

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

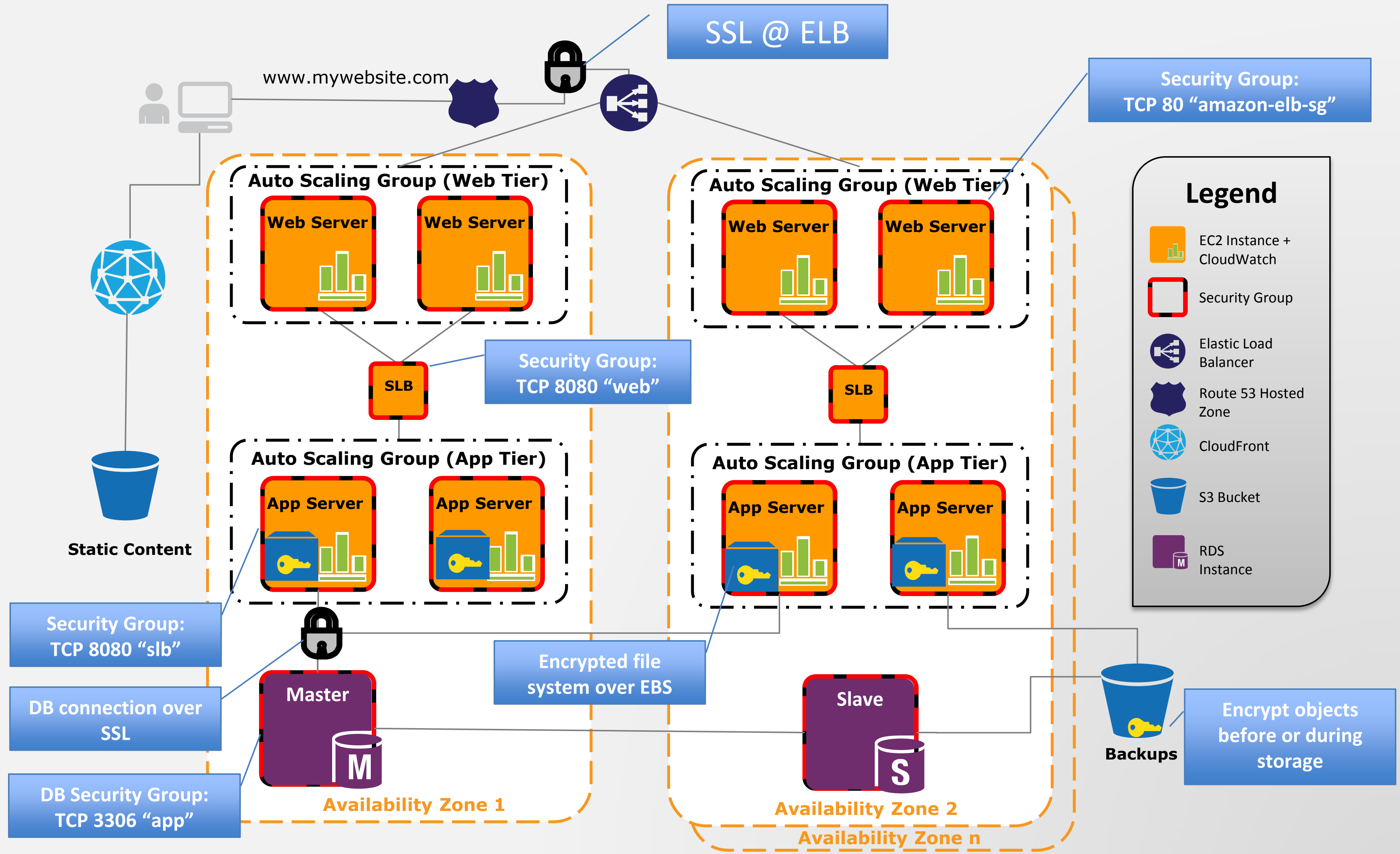
Build security in every layer



© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Architecting With AWS

Security and Compliance | Activity—Identify Security Mechanisms



SSL @ ELB

Security Group: TCP 80 “amazon-elb-sg”

Security Group: TCP 8080 “web”

Security Group: TCP 8080 “slb”

Encrypted file system over EBS

DB connection over SSL

DB Security Group: TCP 3306 “app”

Encrypt objects before or during storage

© 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.