Cloud Security Operations for CCSP®

Operating and Maintaining Physical and Logical Cloud Security Part 1 Components

Dr. Lyron H. Andrews
CISSP/CCSP/SSCP/CRISC/CISM/CCSK

https://www.profabula.com/whyprofabula

CCSP Certification Examination

Domains	Weights
1. Cloud Concepts, Architecture and Design	17%
2. Cloud Data Security	20%
3. Cloud Platform and Infrastructure Security	17%
4. Cloud Application Security	17%
5. Cloud Security Operations	16%
6. Legal, Risk and Compliance 13%	13%

Overview

Enumerate the major components that provide physical and logical security

Review the configuration options of the components

Demonstrate use-cases for implementation

Service Provider Hypervisor Security

Two Types of Hypervisor

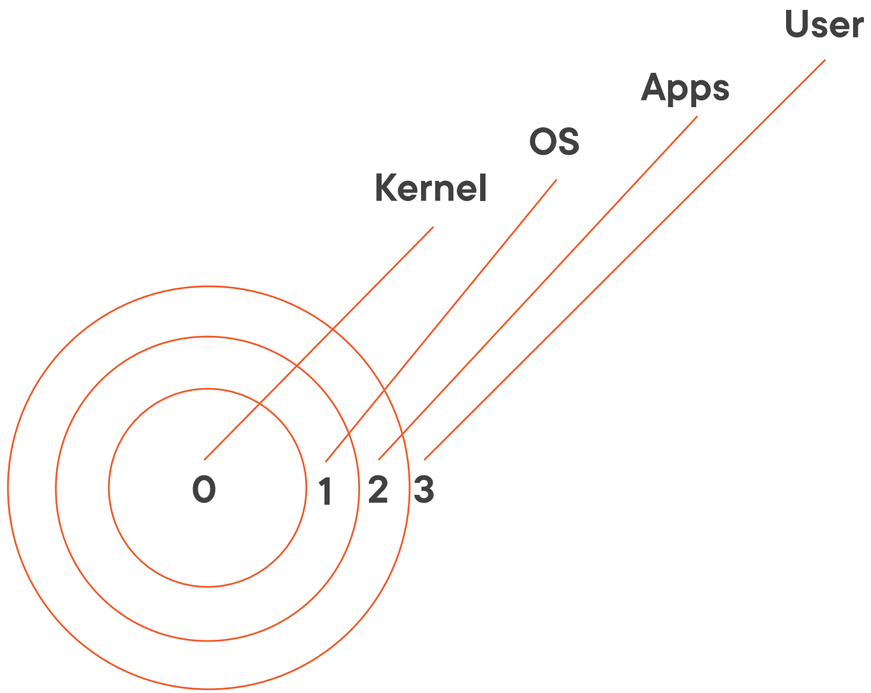
Type II

OS or hosted application hypervisor

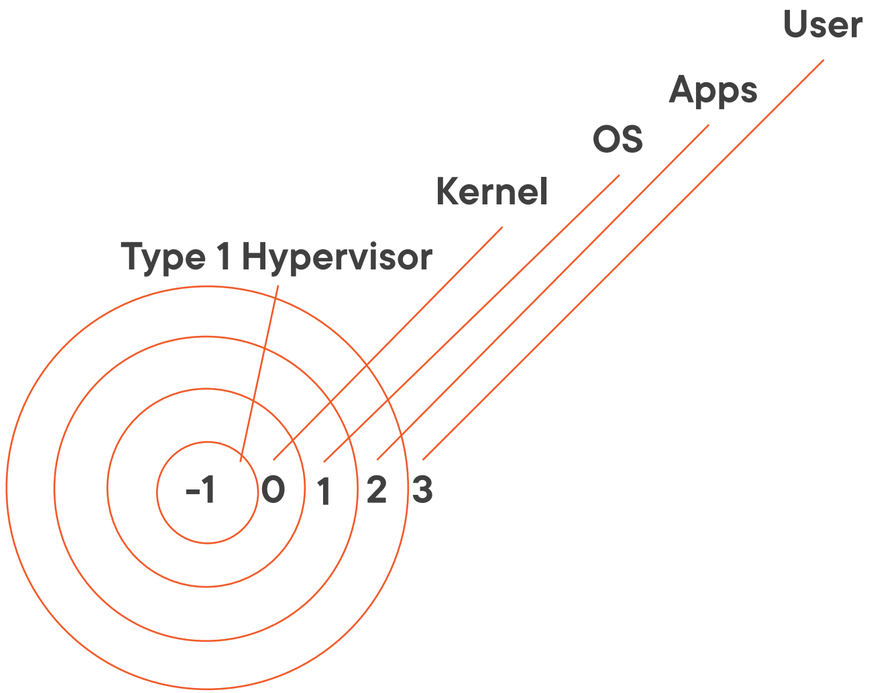
Type I

Modern cloud hypervisor

Type I Hypervisor (Continued)



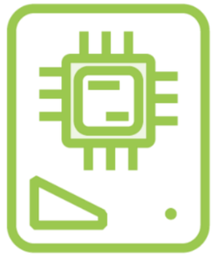
Traditional OS



Type I Hypervisor

Type I Hypervisor

Bare-metal, embedded, or native



Work directly on hardware

Small form factor; few hundred megabytes

Major Cloud Provider's Hypervisors

Amazon Web Service

Xen and Nitro

Google Cloud Platform

KVM

Azure

Windows Hyper-V

Amazon Web Services Nitro Security

Nitro Enclaves

NitroTPM

Secure cryptography

Security Governance

Google Cloud KVM Security

Vulnerability search	**Non-QEMU**	**Cryptographic communication**
Code provenance	**Rapid response**	**Policy-based releases**

Azure Hyper-V Security

Isolation

Host-based

Virtualization-based

Integrity of user/kernel mode

Exploit mitigation

ASLR and DEP

Automation

Stack variable

Zero-initialize

Block injections

Trusted Platform Module

TPM Use-Cases

Storing secrets

Confirming integrity

Tampering resistance

TPM Services

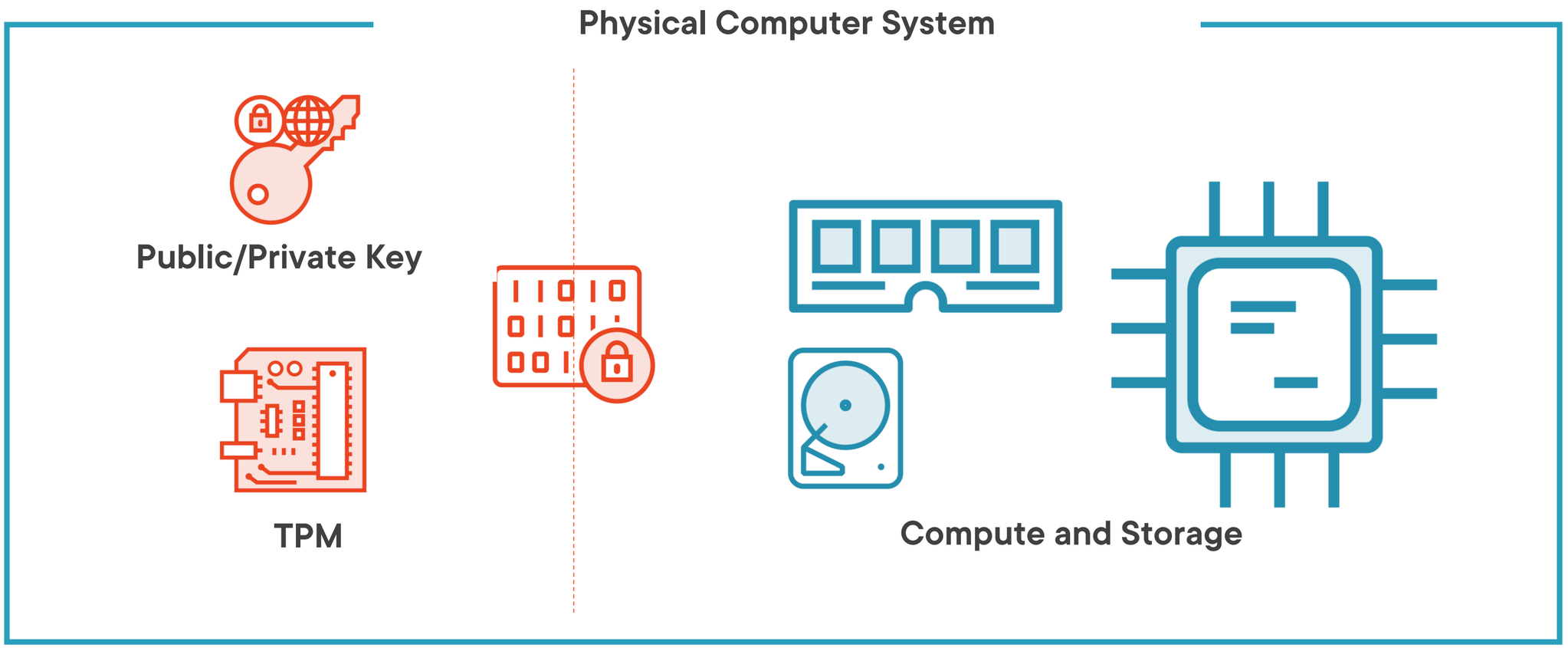
Random number generation

Hashing

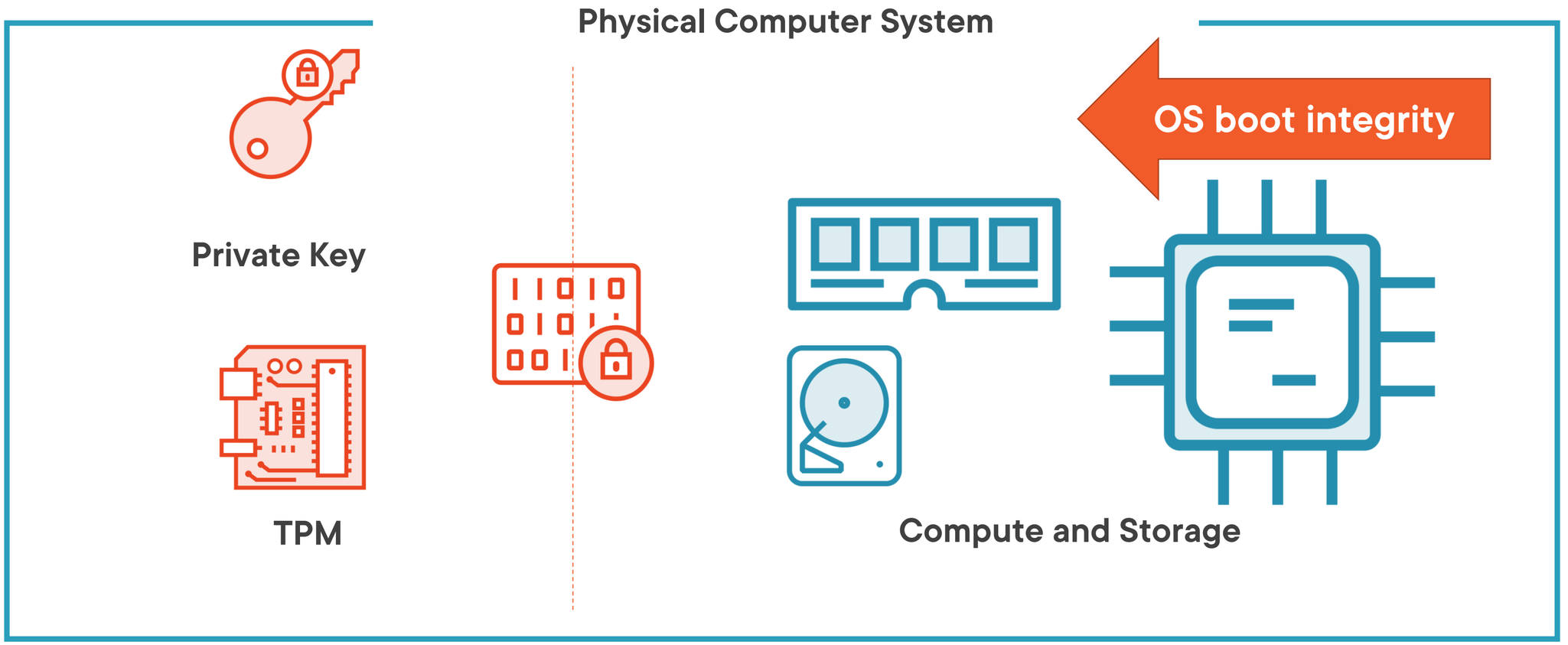
Asymmetric and symmetric keys

Code signing

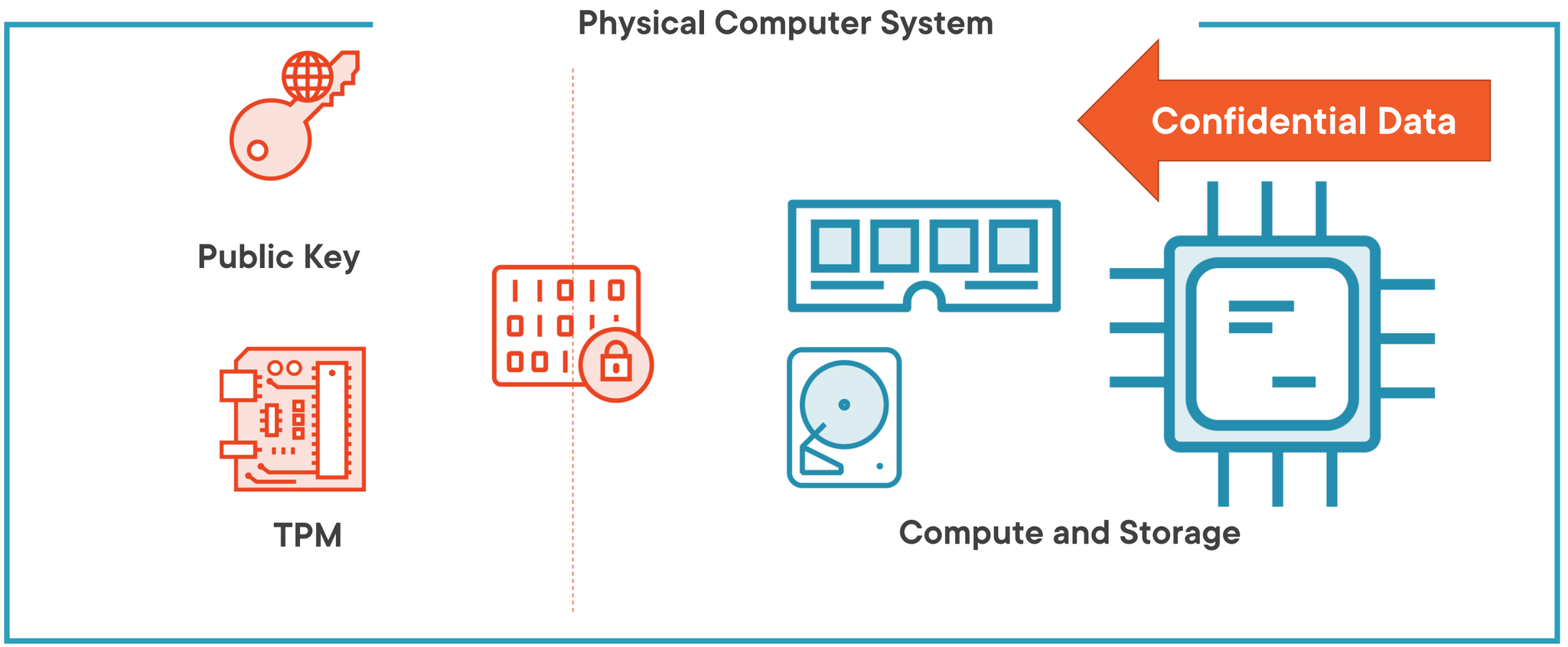
TPM Service Within Computer



TPM Service Within Computer



TPM Service Within Computer



Hardware Security Module (HSM)

HSM Services

Random number generation

Hashing

Asymmetric and symmetric keys

Code signing

FIPS 140-2 Specification Levels

Justification for HSM

Bad Actor

Private key stored locally

Justification for HSM

Bad Actor

Compromise of server exposes private key

Private key stored locally

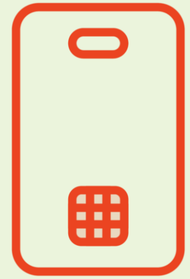
Stolen private key

Justification for HSM

Bad Actor

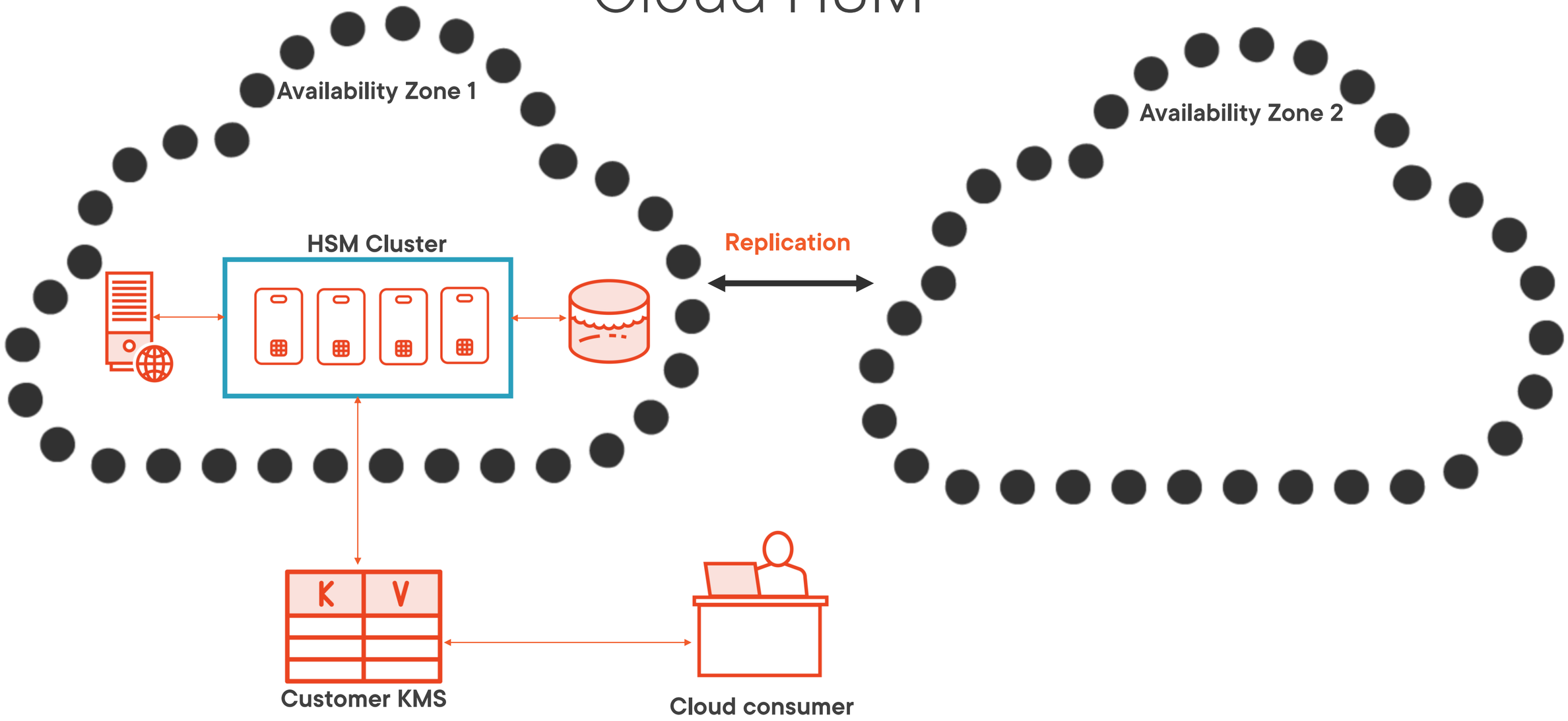
Compromise of server doesn't expose private key

Data stored locally

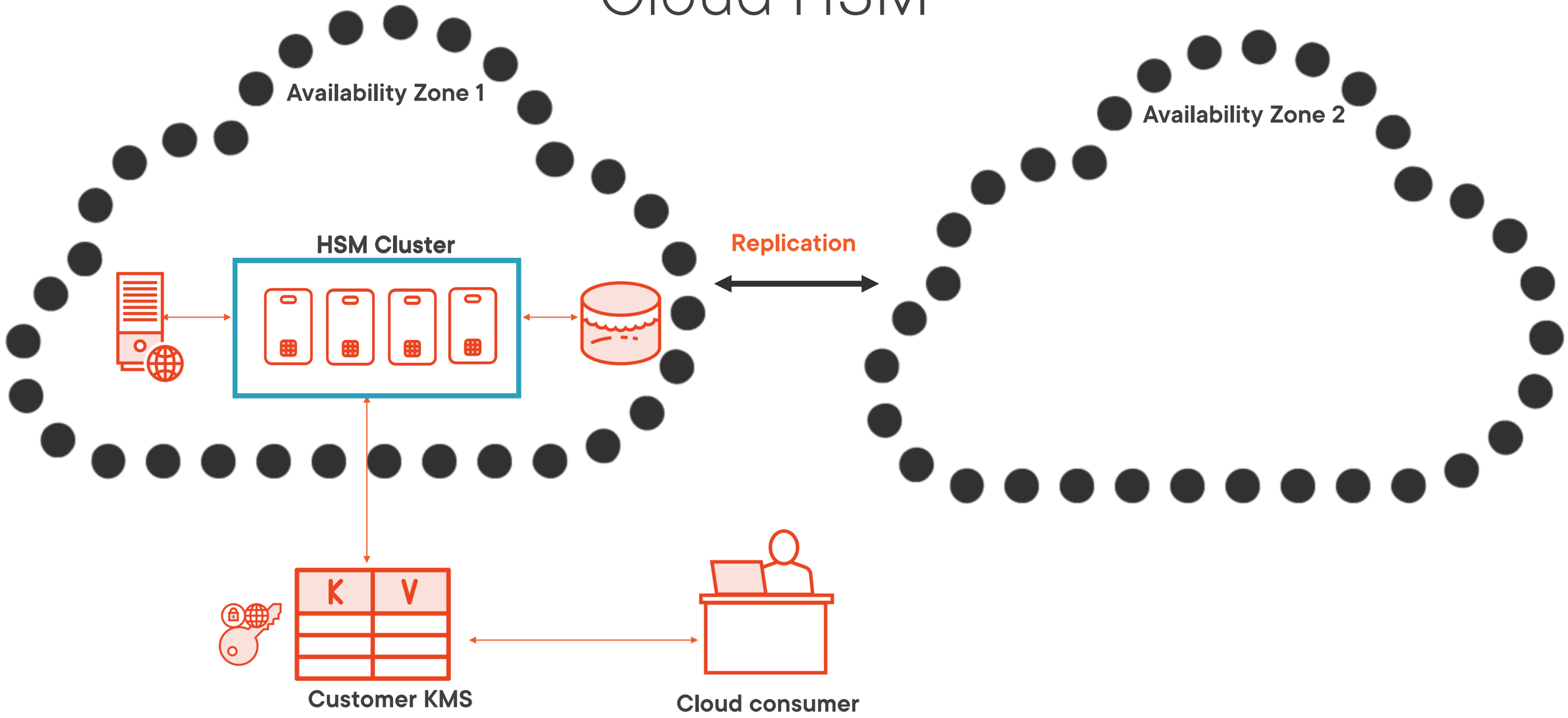


HSM stores private key

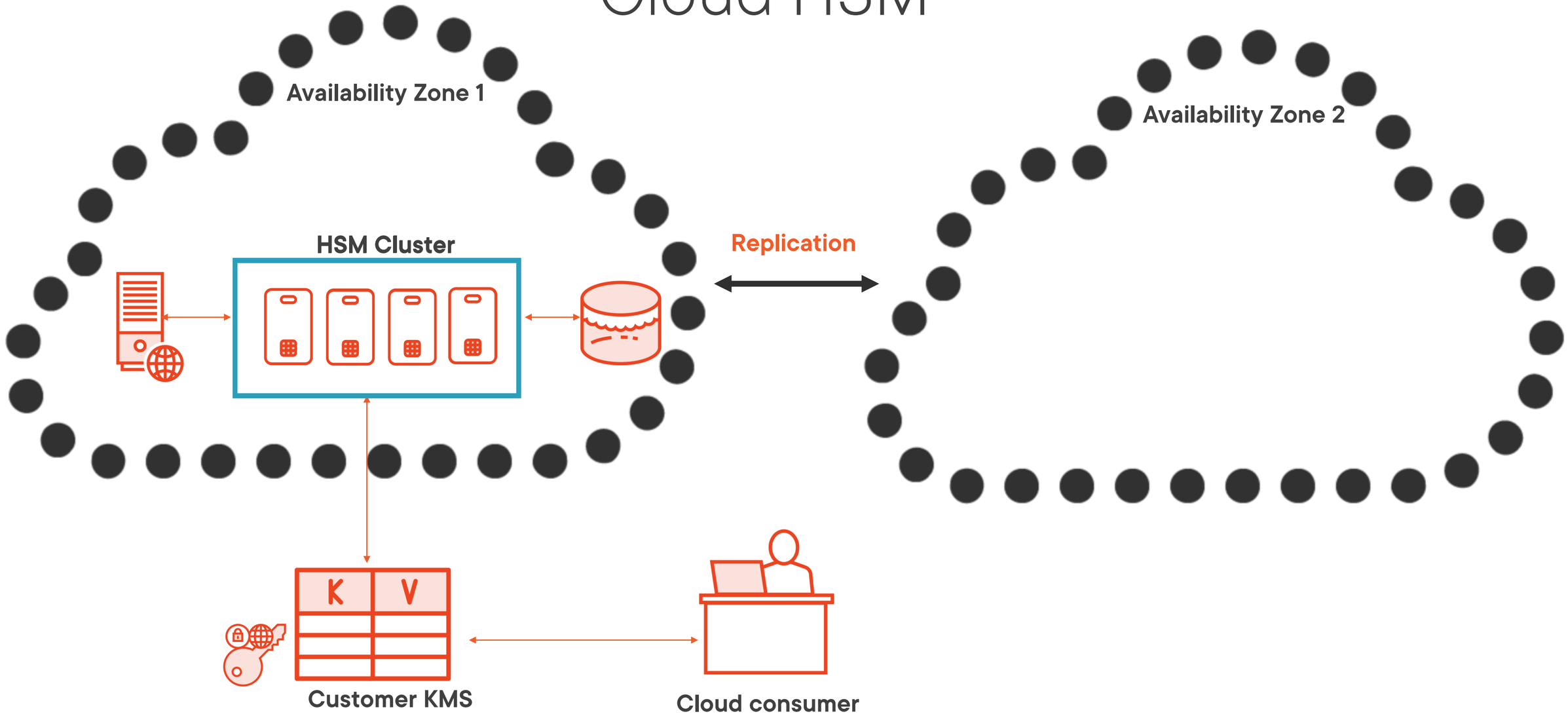
Cloud HSM


Availability Zone 1
Availability Zone 2
HSM Cluster
Replication
K
V
Customer KMS
Cloud consumer

Cloud HSM

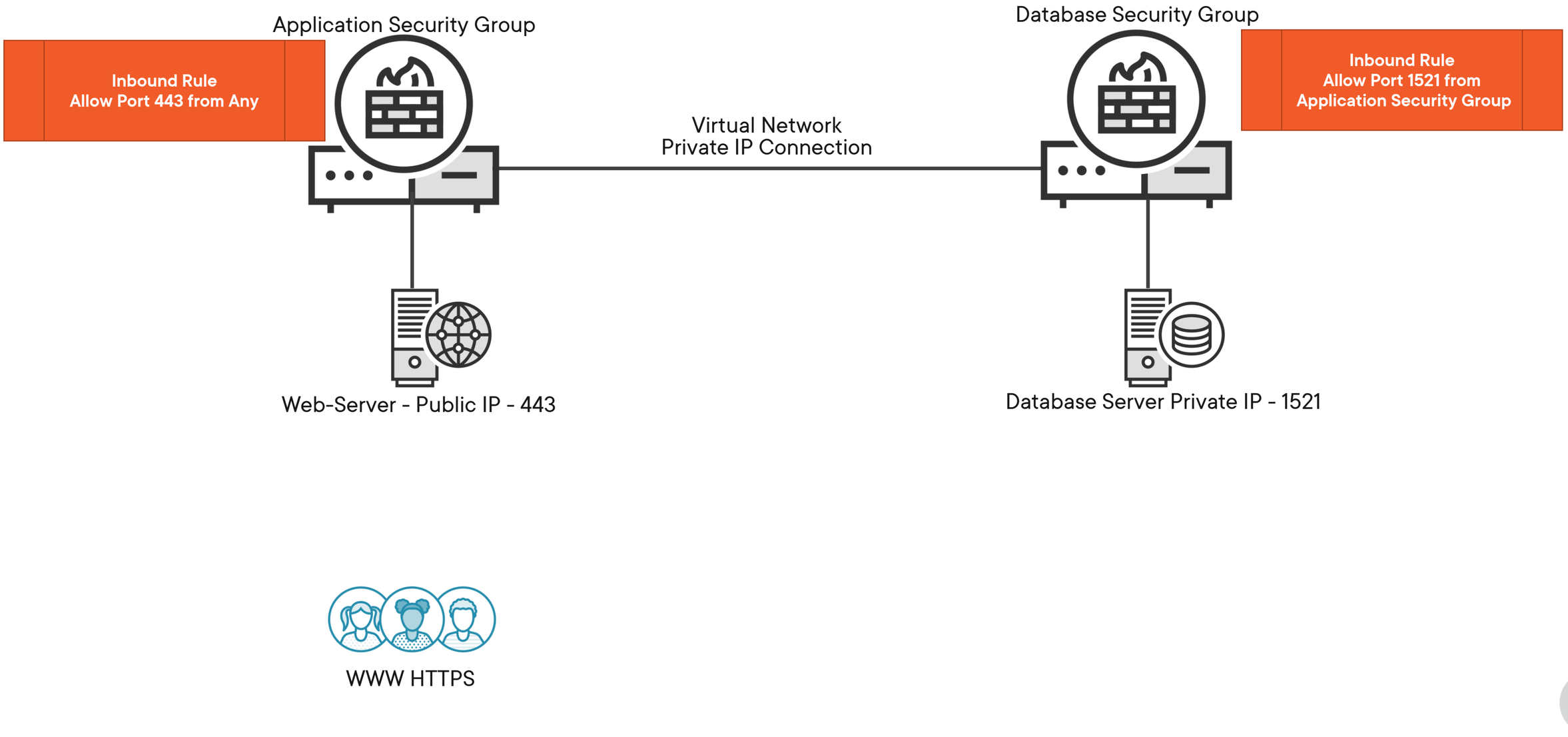

Availability Zone 1
Availability Zone 2
HSM Cluster
Replication
K
V
Customer KMS
Cloud consumer

Cloud HSM

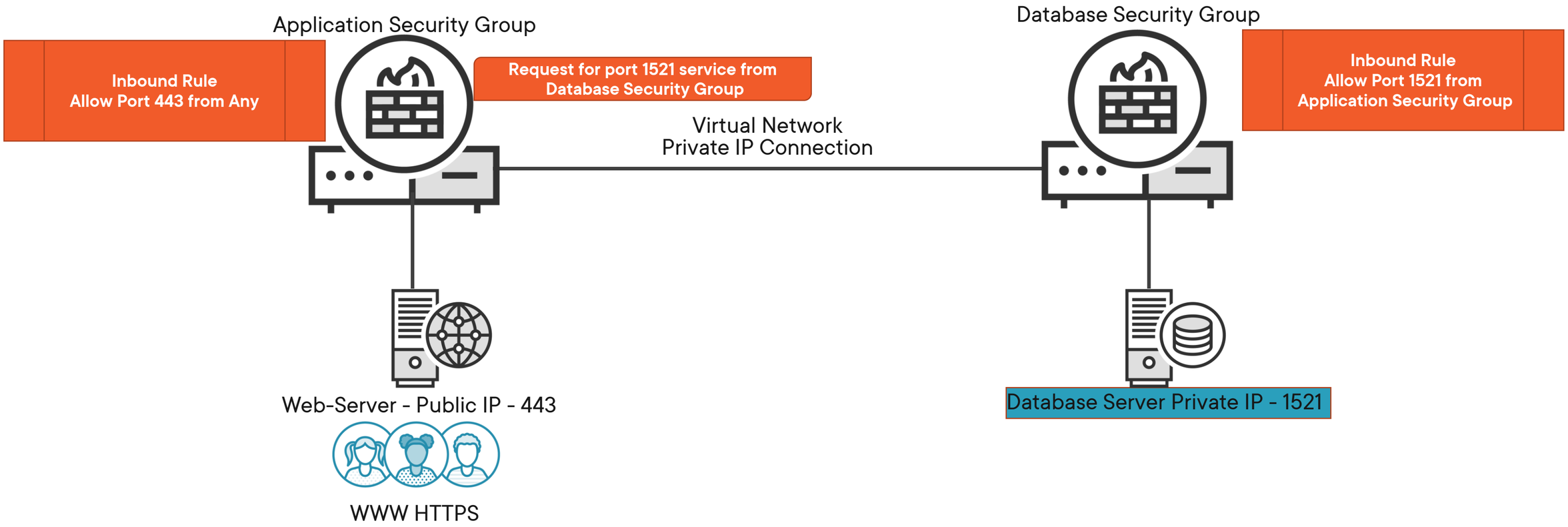

Availability Zone 1
Availability Zone 2
HSM Cluster
Replication
K
V
Customer KMS
Cloud consumer

Security Group and Jumpbox Configuration

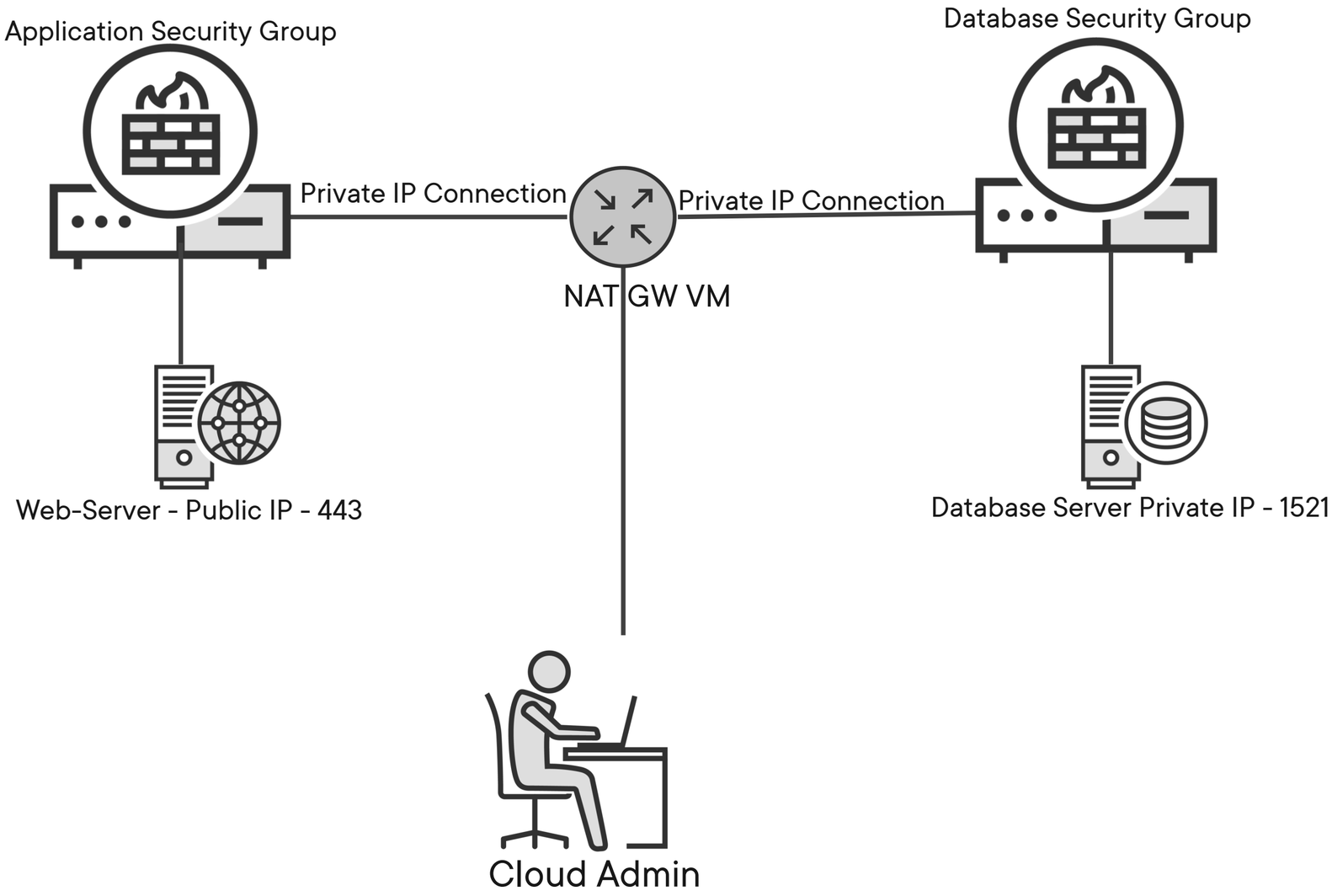
Security Group Fundamentals



Security Group Fundamentals



Cloud Jumpbox Configuration



Demo

Create a security group for a web application and another for a database

Security groups allow explicit access to services

- The security group will enable only specific service access
- We will login to the AWS console to manage the VPC

Additional Network Security Controls

The Primary Firewall Types

Static

Ingress and egress rules with ports and IP addresses

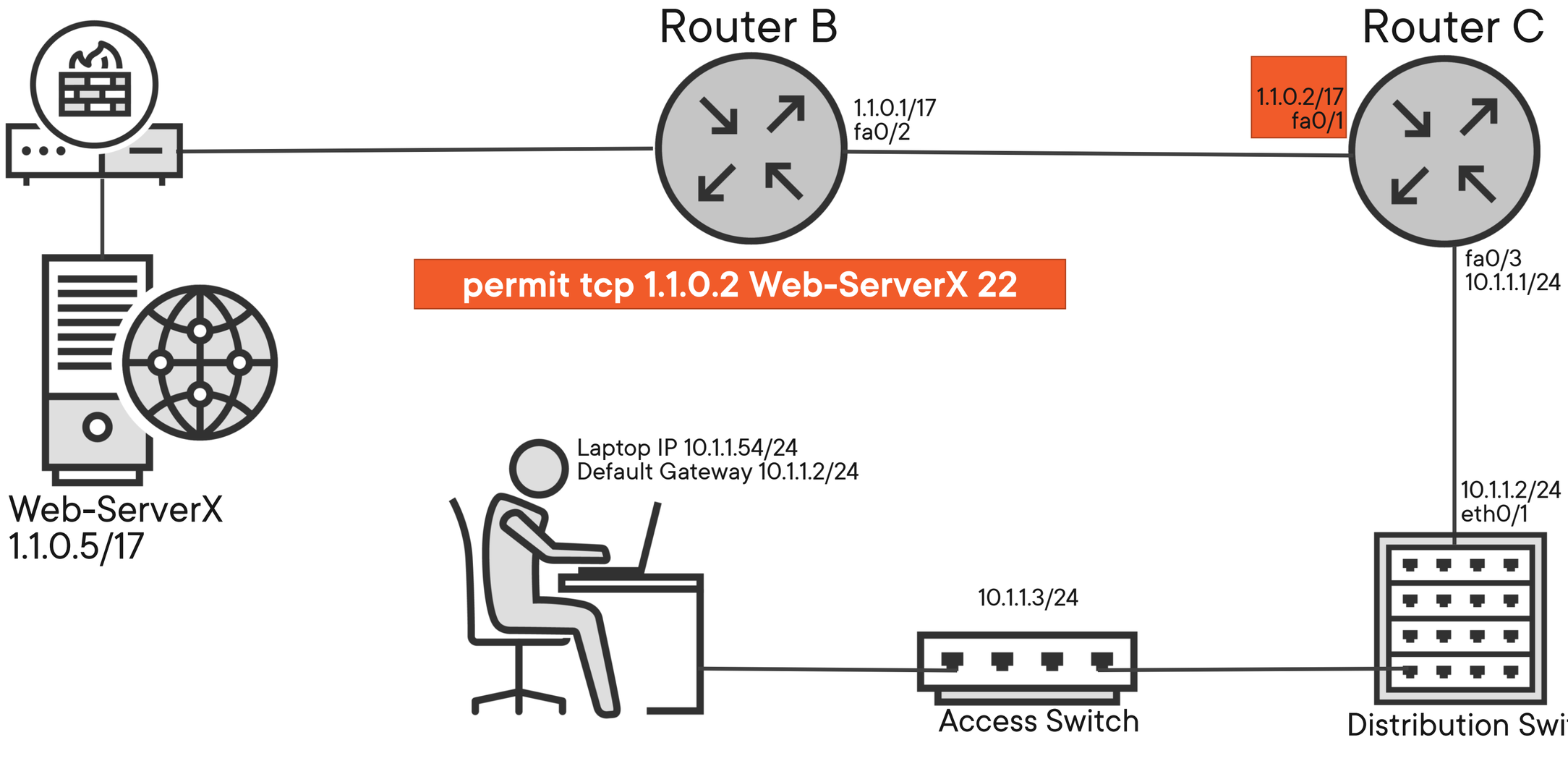
Dynamic

Stateful, signature, anomaly, and heuristics

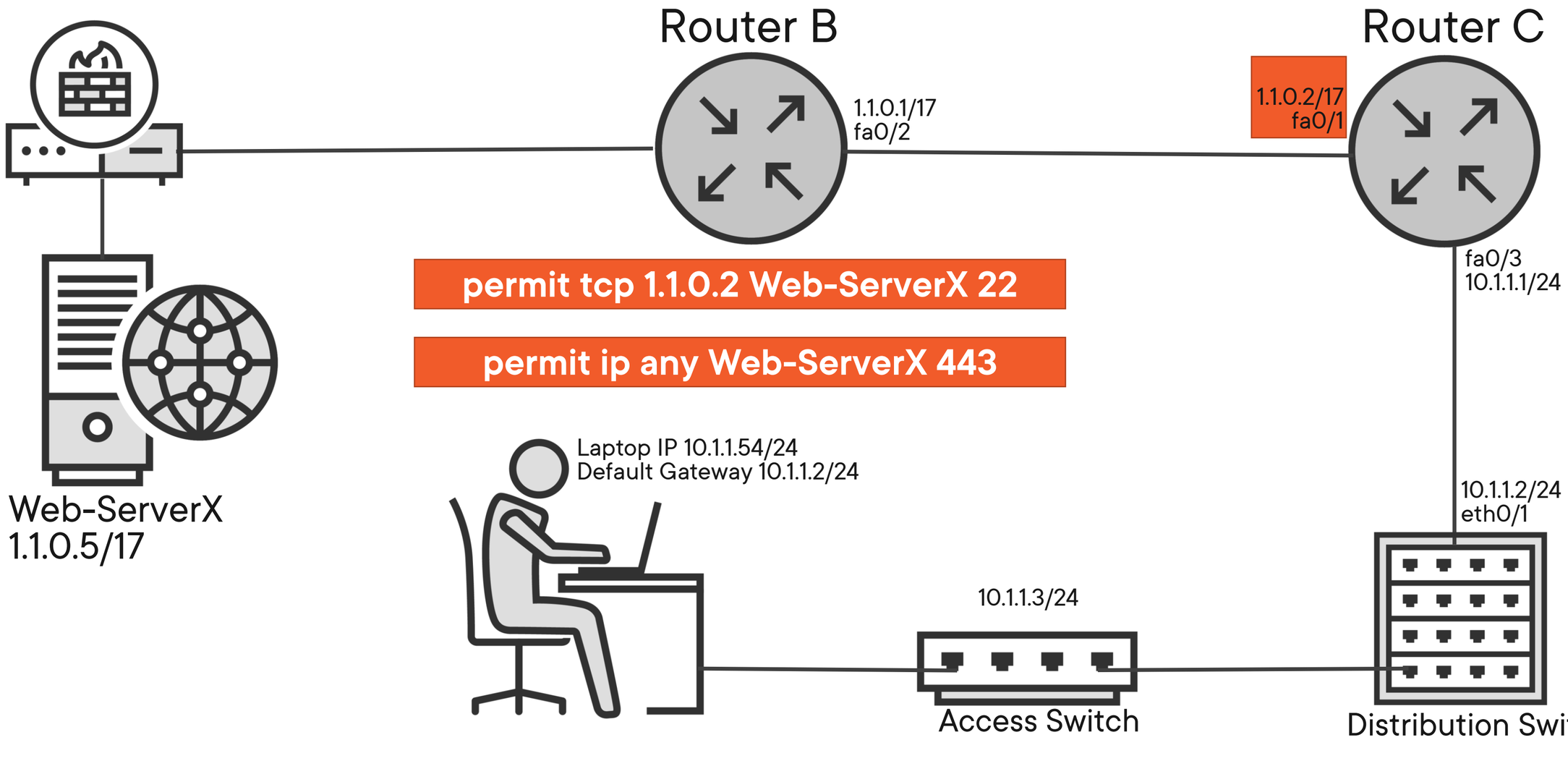
Next Generation

Application control, IPS integration, threat intelligence

Static Firewall Example



Static Firewall Example



Stateful packet inspection

Anomaly-based

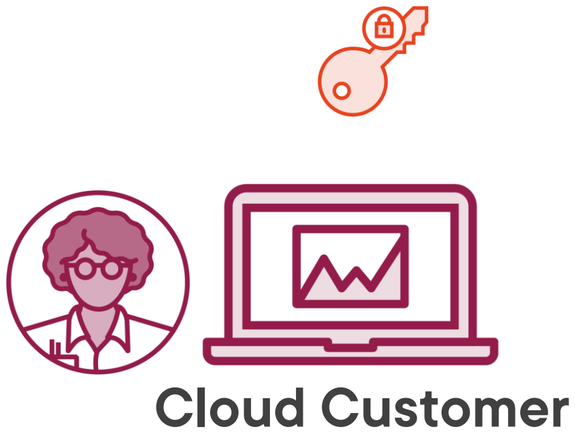
Heuristic scanners

Signature-based

Dynamic Firewalls and IPS

Data Encryption Key (DEK) for Storage Services

Server-Side vs. Client-Side Encryption

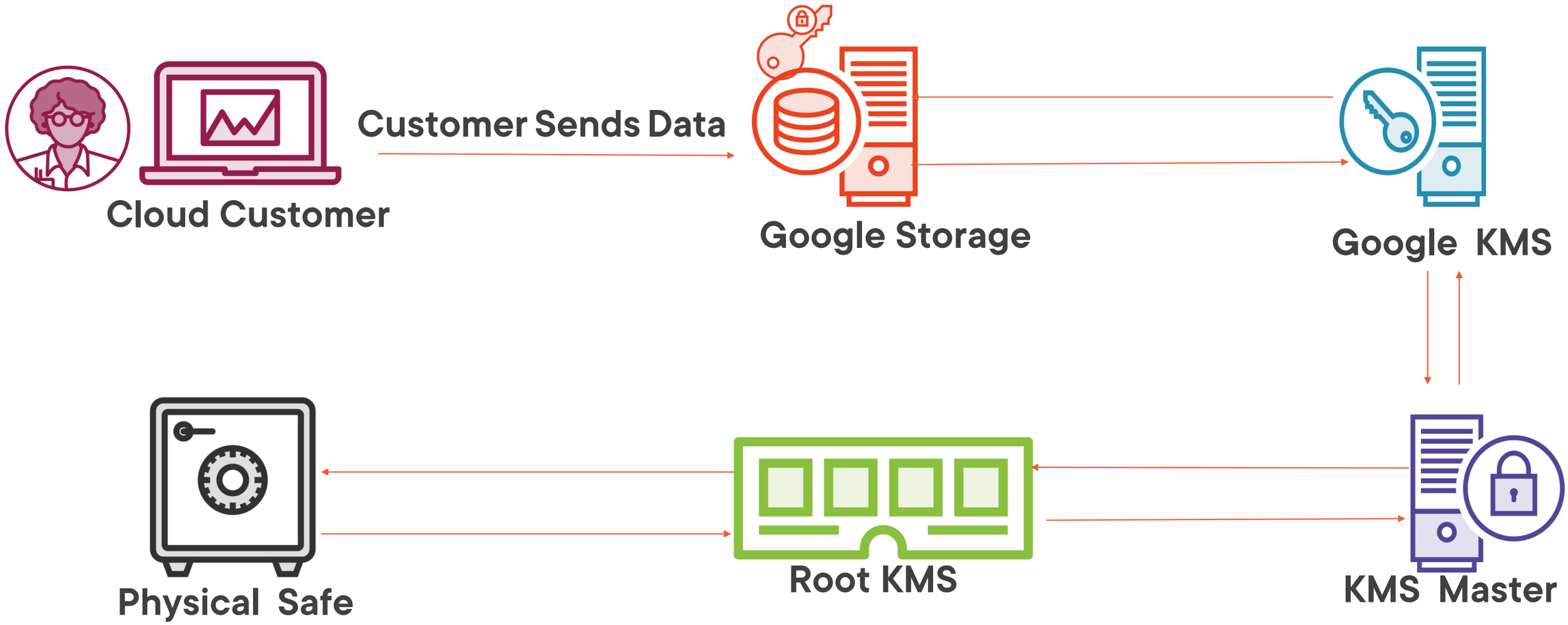


Server-Side vs. Client-Side Encryption

Cloud Customer

Cloud Storage

GCP Data Encryption at Rest



Summary

What major components of physical and logical security are engaged in your cloud?

How does the shared responsibility model affect your control of those components?

What can be done to enhance the security of those components?

Up Next:

Operating and Maintaining Physical and Logical Cloud Security - Part 2 Systems