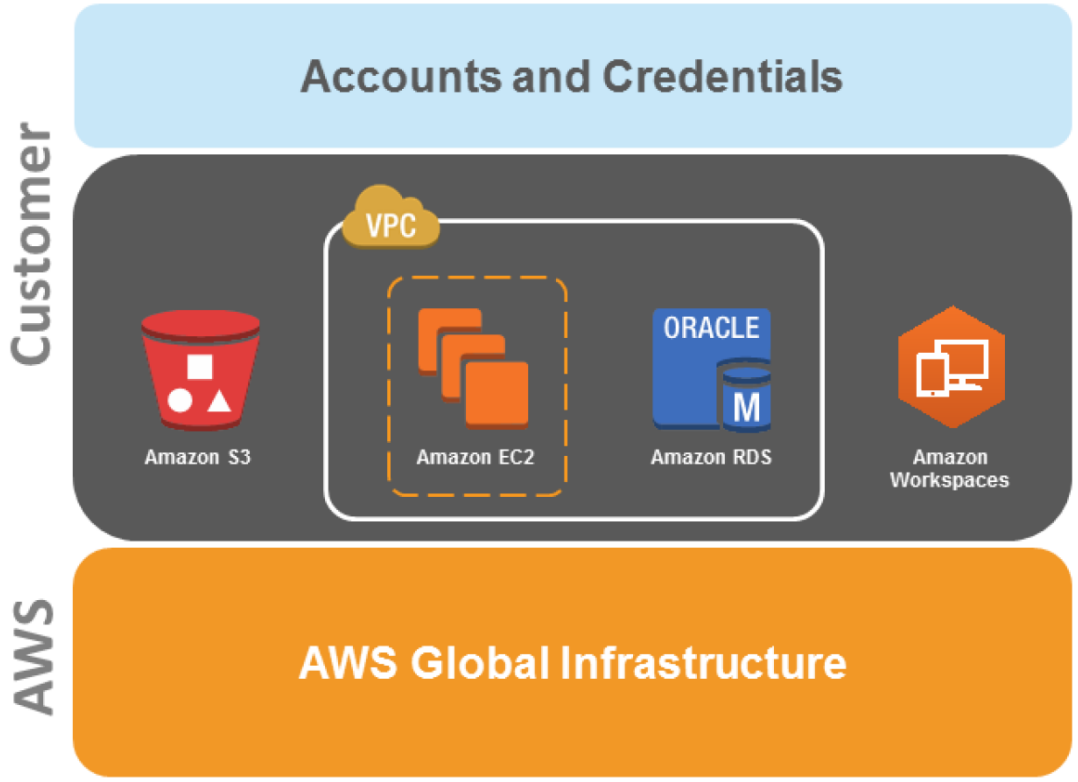
Security

Shared Security Responsibility Model

- AWS is responsible for securing the underlying infrastructure that supports the cloud, and you're responsible for anything you put on the cloud or connect to the cloud.



Shared Security Model

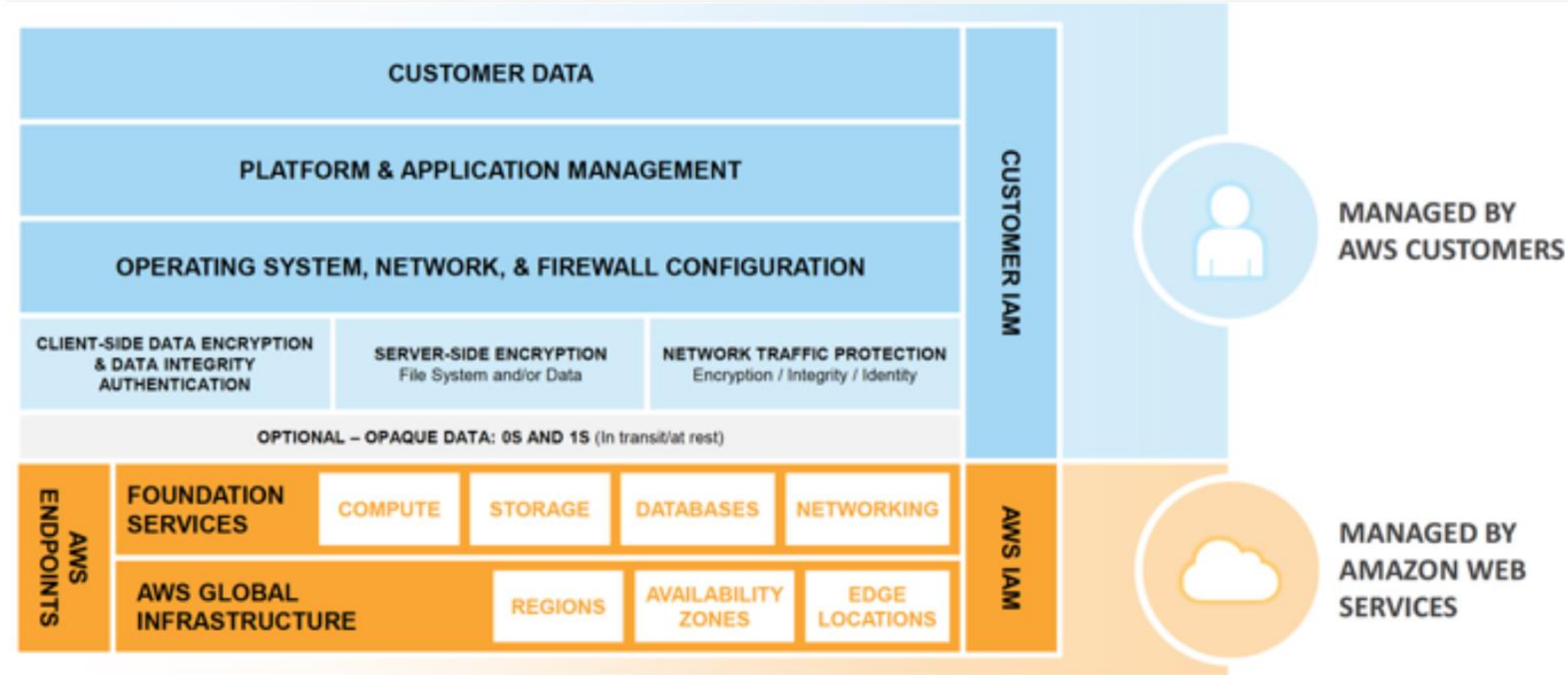
- Shared Responsibility
  - Let AWS do the heavy lifting
  - Focus on what's most valuable to your business

- AWS
  - Facility operations
  - Physical Security
  - Physical Infrastructure
  - Network Infrastructure
  - Virtualisation Infrastructure
  - Hardware lifecycle management

- Customer
  - Choice of Guest OS
  - Application Configuration Options
  - Account Management flexibility
  - Security Groups
  - ACLs
  - Identity Management

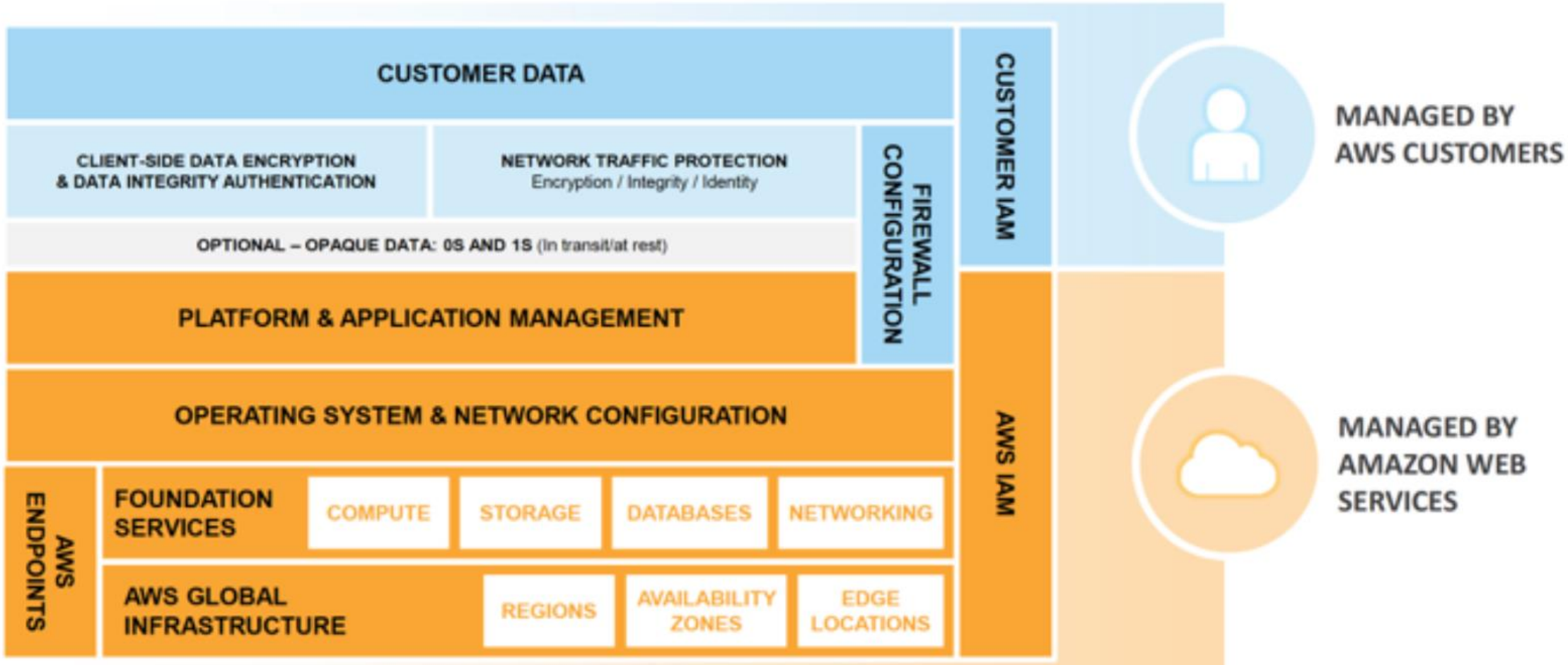
Shared Security Model: Infrastructure Services

Such as Amazon EC2, Amazon EBS, and Amazon VPC



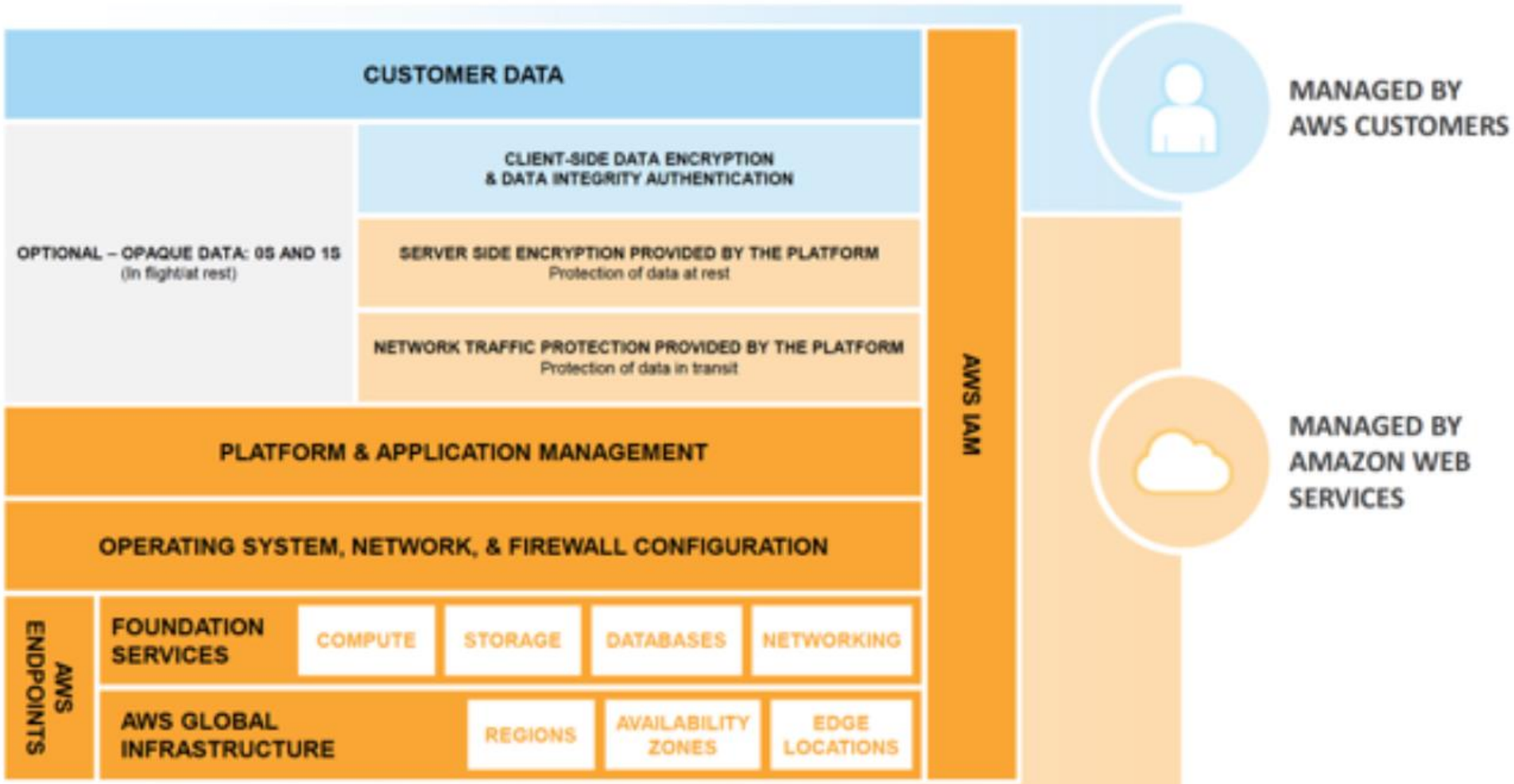
Shared Security Model: Container Services

Such as Amazon RDS and Amazon EMR



Shared Security Model: Abstracted Services

Such as Amazon S3 and Amazon DynamoDB



AWS Security Compliance

AWS complies with:

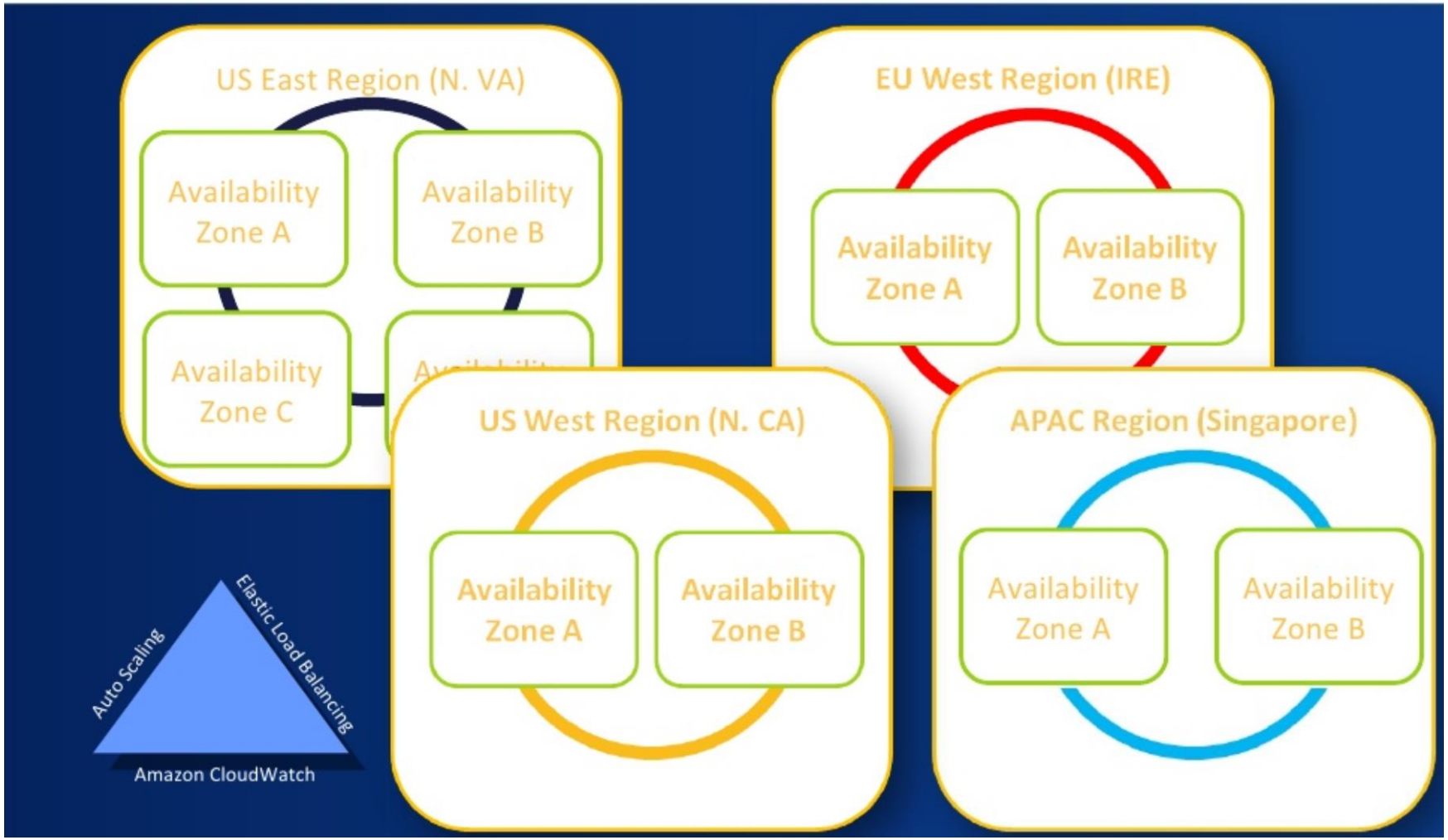
- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70)
- SOC 2
- SOC 3
- FISMA, DIACAP, and FedRAMP
- DOD CSM Levels 1-5
- PCI DSS Level 1
- ISO 9001 / ISO 27001
- ITAR
- FIPS 140-2
- MTCS Level 3

- AWS platform provides capabilities that allows customers to deploy solutions that meet several industry-specific standards, including:
  - Criminal Justice Information Services (CJIS)
  - Cloud Security Alliance (CSA)
  - Family Educational Rights and Privacy Act (FERPA)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Motion Picture Association of America (MPAA)

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

FAULT SEPARATION AND GEOGRAPHIC DIVERSITY

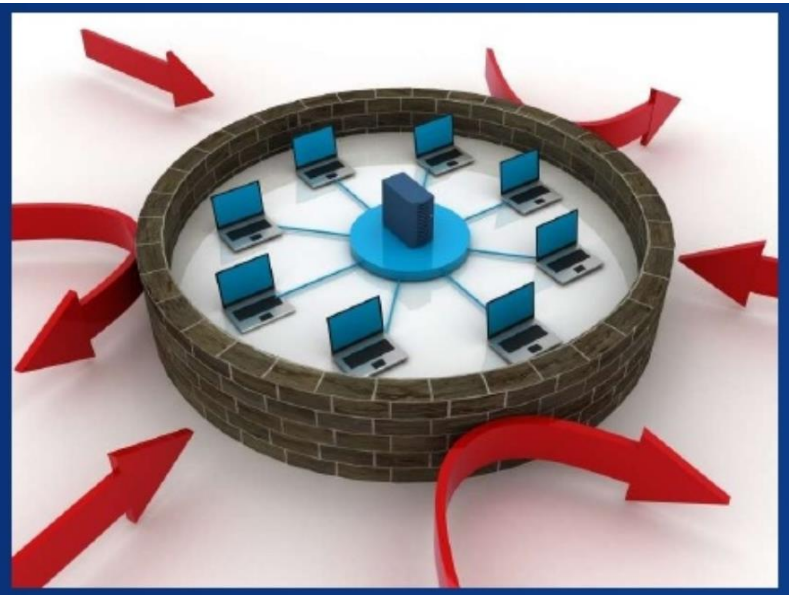


DATA BACKUPS

- Data stored in Amazon S3, Amazon SimpleDB, and Amazon EBS is stored redundantly in multiple physical locations
- Amazon EBS redundancy remains within a single Availability Zone
- Amazon S3 and Amazon SimpleDB replicate customer objects across storage systems in multiple Availability Zones to ensure durability
  - Equivalent to more traditional backup solutions, but offers much higher data availability and throughput
- Data stored on Amazon EC2 local disks must be proactively copied to Amazon EBS and/or Amazon S3 for redundancy

Network Protection

- 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.



AWS Security Capabilities: Overview

- Infrastructure Security
  - Network firewalls built into Amazon VPC, and web application firewall capabilities in AWS WAF let you create private networks, and control access to your instances and applications
  - Encryption in transit with TLS across all services
  - Connectivity options that enable private, or dedicated, connections from your office or on-premises environment

AWS Security Capabilities: Overview

- Data Encryption

- Data encryption capabilities available in AWS storage and database services, such as EBS, S3, Glacier, Oracle RDS, SQL Server RDS, and Redshift
- Flexible key management options, including AWS Key Management Service, allowing you to choose whether to have AWS manage the encryption keys or enable you to keep complete control over your keys
- Encrypted message queues for the transmission of sensitive data using server-side encryption (SSE) for Amazon SQS
- Dedicated, hardware-based cryptographic key storage using AWS CloudHSM, allowing you to satisfy compliance requirements

AWS Security Capabilities: Overview

- Monitoring and Logging

- Deep visibility into API calls through AWS CloudTrail, including who, what, who, and from where calls were made
- Log aggregation options, streamlining investigations and compliance reporting
- Alert notifications through Amazon CloudWatch when specific events occur or thresholds are exceeded

AWS Security Capabilities: Overview

- Identity and Access Control

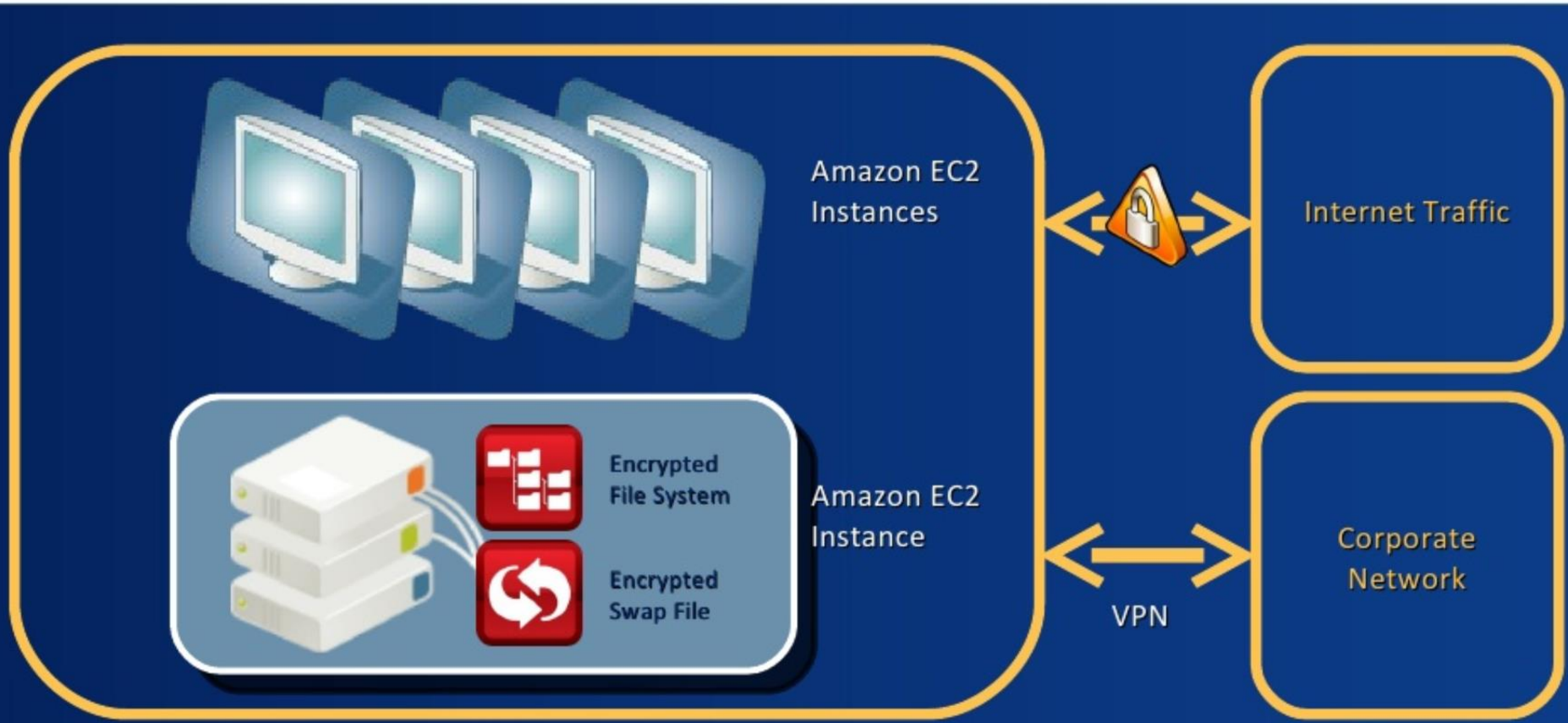
- AWS Identity and Access Management (IAM) lets you define individual user accounts with permissions across AWS resources
- AWS Multi-Factor Authentication for privileged accounts, including options for hardware-based authenticators
- AWS Directory Service allows you to integrate and federate with corporate directories to reduce administrative overhead and improve end-user experience

AWS Security Capabilities: Overview

- Penetration and Testing

- Permission is required for all penetration tests.
- To request permission, you must be logged into the AWS portal using the root credentials associated with the instances you wish to test, otherwise the form will not pre-populate correctly.
- Our policy only permits testing of EC2 and RDS instances that you own.
- At this time, our policy does not permit testing small or micro RDS instance types. Testing of m1.small or t1.micro EC2 instance types is not permitted.

NETWORK TRAFFIC CONFIDENTIALITY



- All traffic should be cryptographically controlled
- Inbound and outbound traffic to corporate networks should be wrapped within industry standard VPN tunnels (option to use Amazon

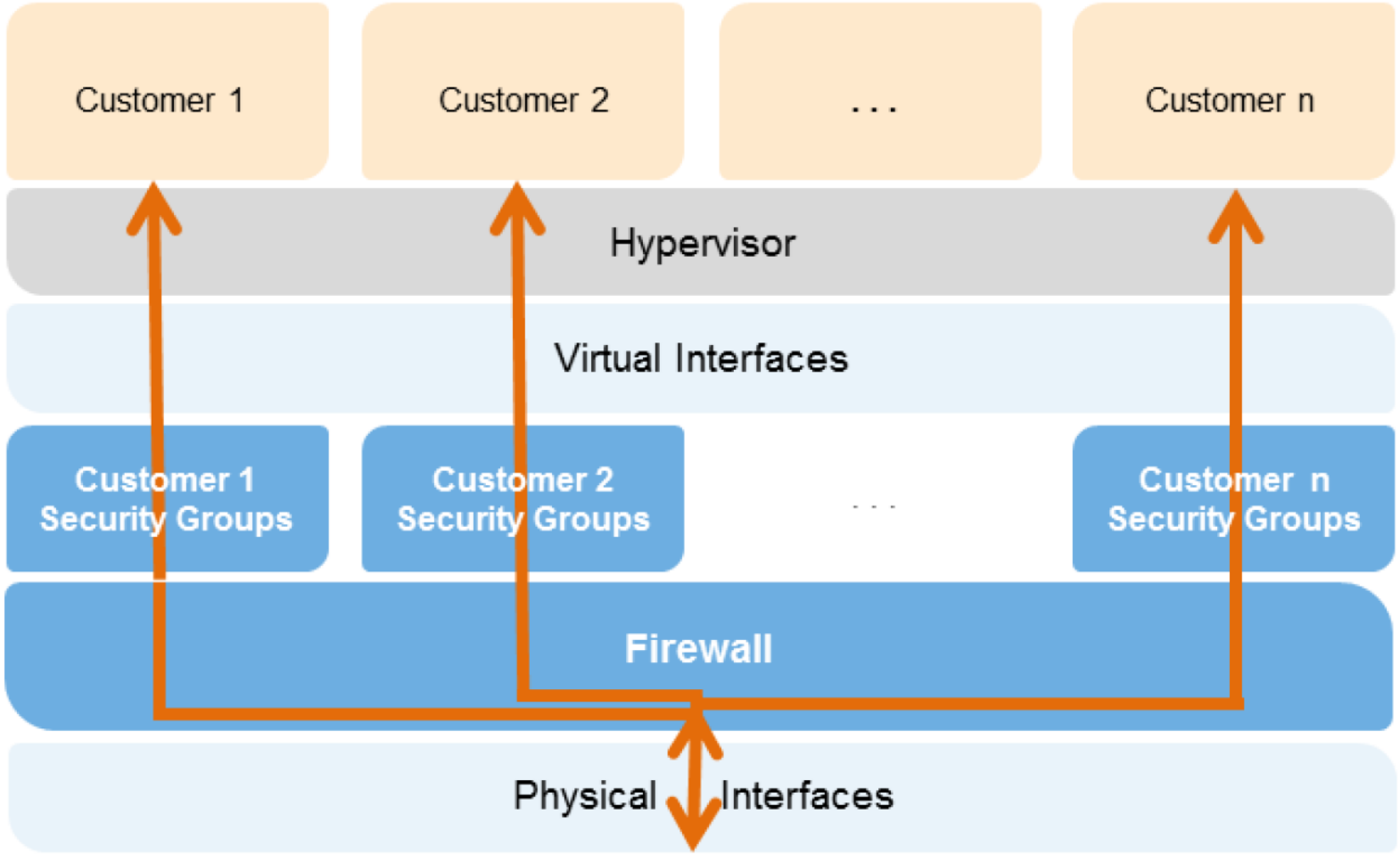
AWS Account Security Features

Credential Type	Use	Description
Passwords	AWS root account or IAM user account login to the AWS Management Console	A string of characters used to log into your AWS account or IAM account. AWS passwords must be a minimum of 6 characters and may be up to 128 characters.
Multi-Factor Authentication (MFA)	AWS root account or IAM user account login to the AWS Management Console	A six-digit single-use code that is required in addition to your password to log in to your AWS Account or IAM user account.
Access Keys	Digitally signed requests to AWS APIs (using the AWS SDK, CLI, or REST/Query APIs)	Includes an access key ID and a secret access key. You use access keys to digitally sign programmatic requests that you make to AWS.
Key Pairs	• SSH login to EC2 instances • CloudFront signed URLs	A key pair is required to connect to an EC2 instance launched from a public AMI. The keys that Amazon EC2 uses are 1024-bit SSH-2 RSA keys. You can have a key pair generated automatically for you when you launch the instance or you can upload your own.
X.509 Certificates	• Digitally signed SOAP requests to AWS APIs • SSL server certificates for HTTPS	X.509 certificates are only used to sign SOAP-based requests (currently used only with Amazon S3). You can have AWS create an X.509 certificate and private key that you can download, or you can upload your own certificate by using the Security Credentials page.

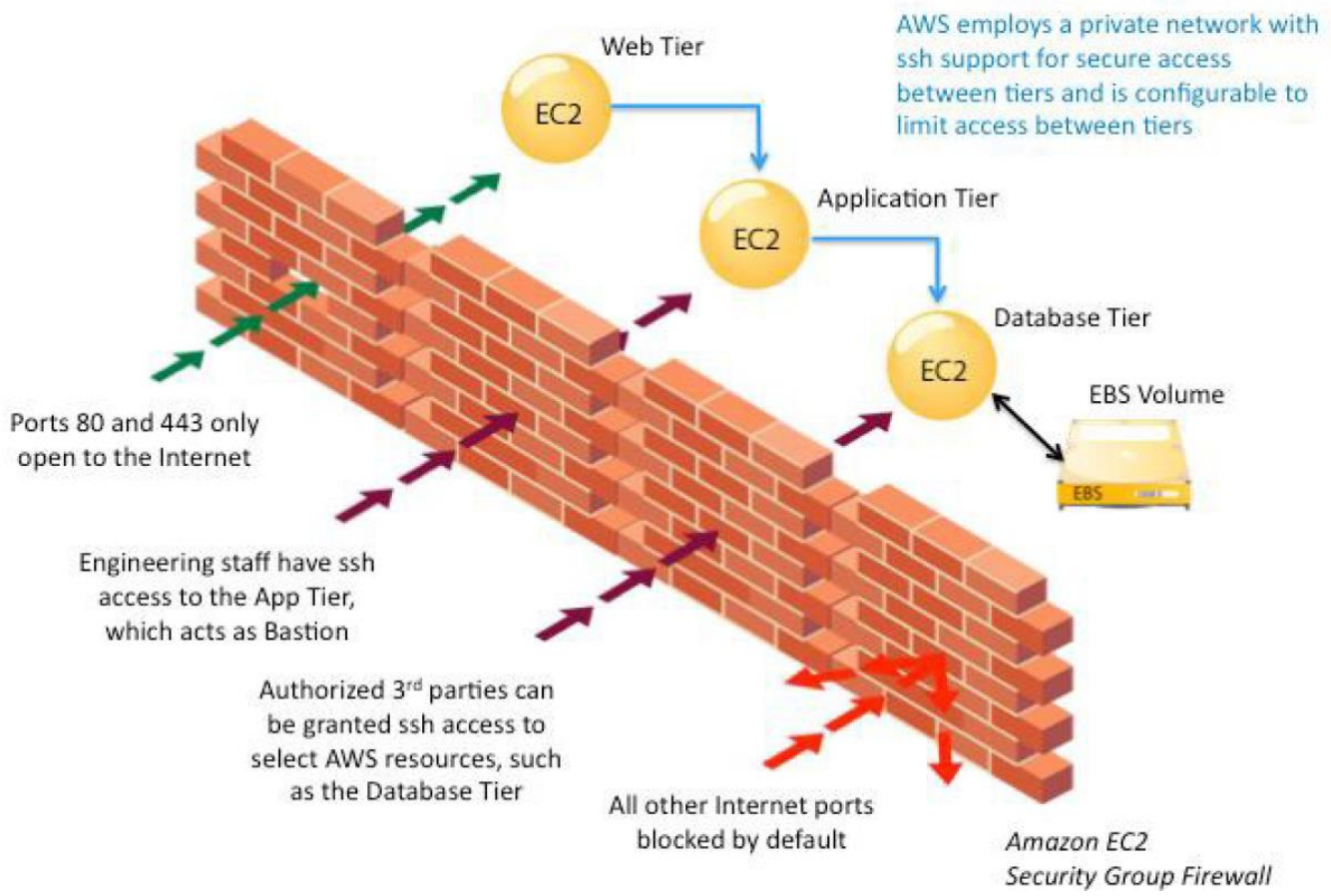
EC2 Security

- Host operating system
  - Individual SSH keyed logins via bastion host for AWS admins
  - All accesses logged and audited
- Guest operating system
  - Customer controlled at root level
  - AWS admins cannot log in
  - Customer-generated keypairs
- Stateful firewall
  - Mandatory inbound firewall, default deny mode
- Signed API calls
  - Require X.509 certificate or customer's secret AWS key

EC2: Multi level of security

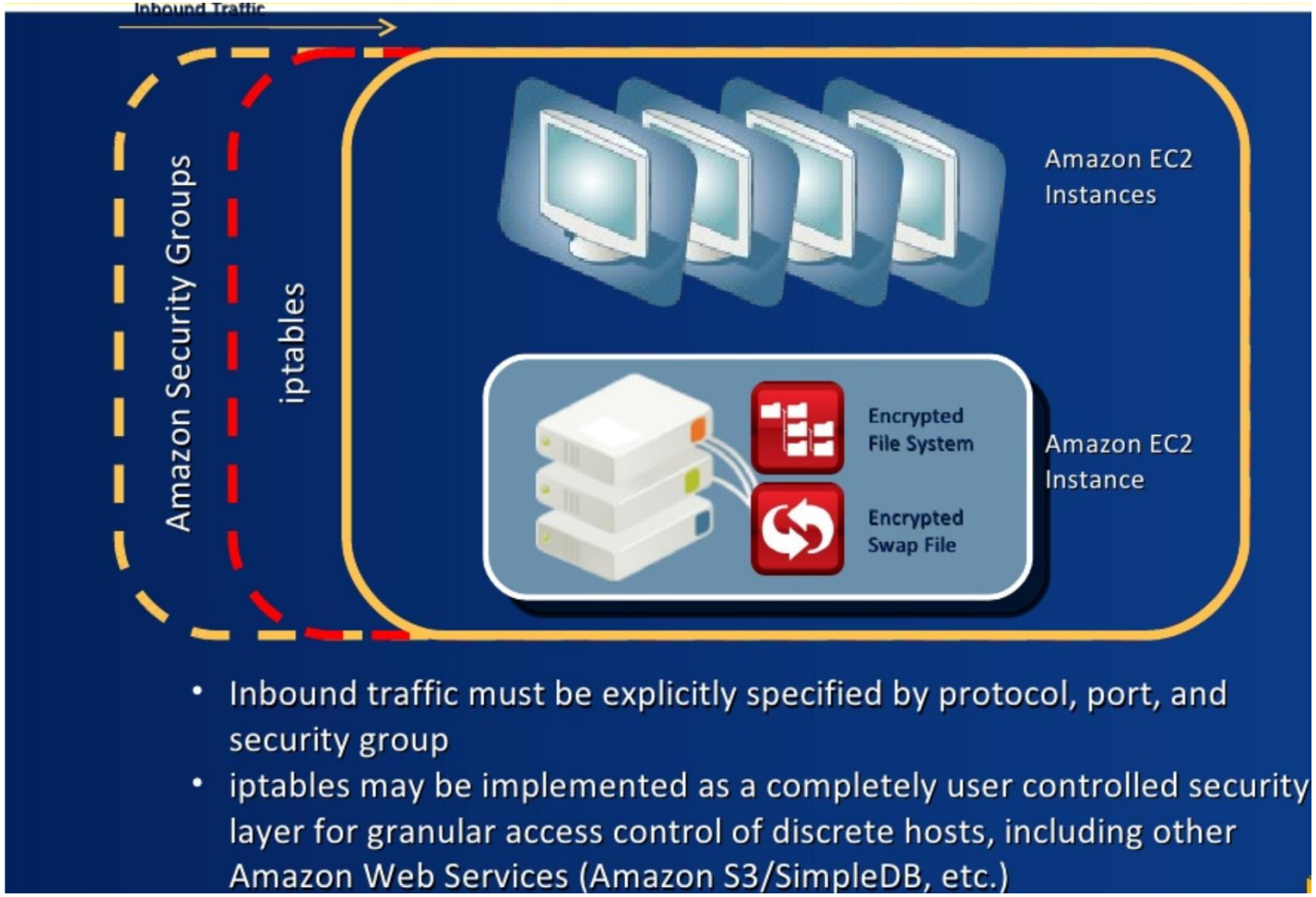


EC2: Firewall



EC2 Virtual Memory and Local Disk

Network Traffic Flow Security



EBS

- EBS allows you to create storage volumes from 1 GB to 16 TB that can be mounted as devices by EC2 instances
- AWS provides the ability to encrypt EBS volumes and their snapshots with AES-256.
  - The encryption occurs on the servers that host the EC2 instances, providing encryption of data as it moves between EC2 instances and EBS storage.
- EBS are wiped before made available for use
- Custom wiping procedures can be implemented before EBS are deleted by AWS
  - DoD 5220.22-M (“National Industrial Security Program Operating Manual “) or
  - NIST 800-88 (“Guidelines for Media Sanitization”),

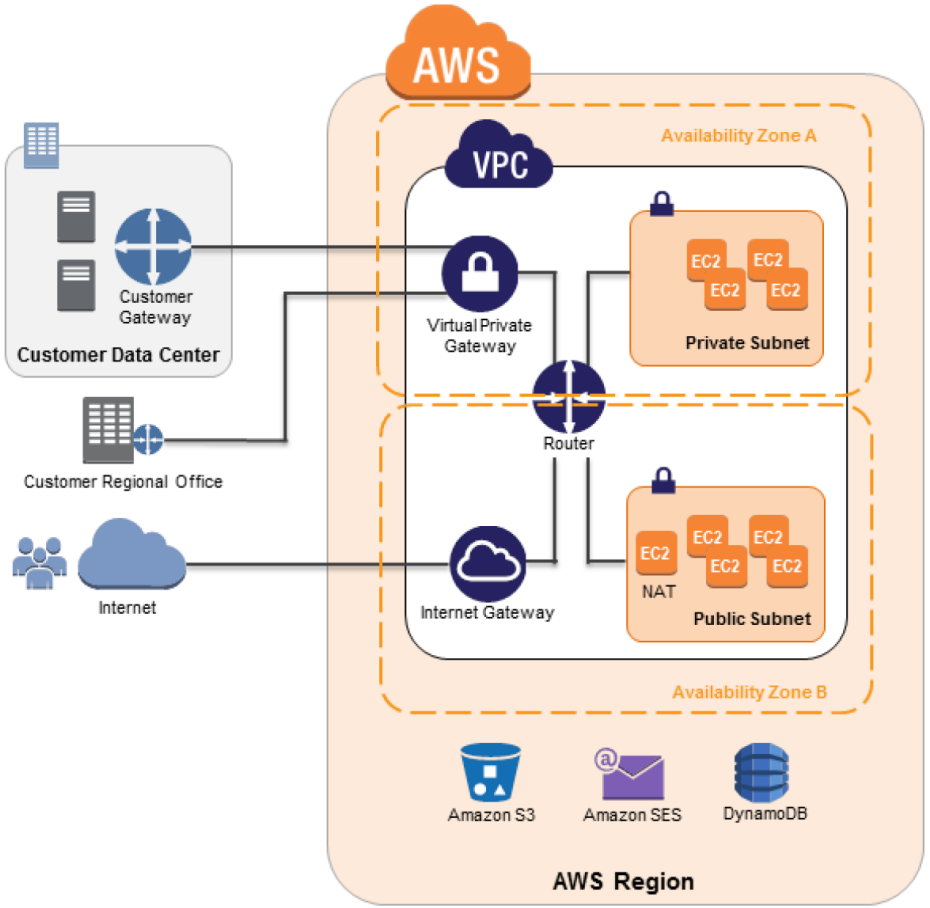
Network Services

- ELB
  - Takes over the encryption and decryption work from the Amazon EC2 instances and manages it centrally on the load balancer
  - Offers clients a single point of contact, and can also serve as the first line of defense against attacks on your network
  - When used in an Amazon VPC, supports creation and management of security groups associated with your Elastic Load Balancing to provide additional networking and security options
  - Supports end-to-end traffic encryption using TLS (previously SSL) on those networks that use secure HTTP (HTTPS) connections. When TLS is used, the TLS server certificate used to terminate client connections can be managed centrally on the load balancer, rather than on every individual instance.

- VPC (Default Configuration)
  - VPC with a single public subnet only.
  - VPC with public and private subnets
    - Outbound connections to the Internet via the public subnet using Network Address Translation (NAT).
  - VPC with public and private subnets and hardware VPN access..
  - VPC with private subnet only and hardware VPN access.

VPC Security Services

- API Access with SSL
- Subnets and Route Tables
- Firewall (Security Groups)
- Network Control Access List
- Virtual Private Gateway
- Internet Gateway
- Dedicated EC2 instances
- Elastic Network Interfaces (max 2 per EC2 instance)



S3 Security

- IAM Policies
- Access Control List (ACLs)
- Bucket Policies
- In Fly
  - SSL encrypted endpoints for Data Transfer
- At Rest
  - S3 Server Side Encryption (SSE)
  - 256-bit Advanced Encryption Standard (AES-256).
- Availability
  - 99.999999999% durability and 99.99% availability of objects over a given year
- Access Logs
  - Contains details about each access request including request type, the requested resource, the requestor's IP, and the time and date of the request.
- Cross-Origin Resource Sharing (CORS)
  - Amazon S3 bucket can be configured to explicitly enable cross-origin requests.
  - Modern browsers use the Same Origin policy to block JavaScript or HTML5 from allowing requests to load content from another site or domain as a way to help ensure that malicious content is not loaded from a less reputable source (such as during cross-site scripting attacks).

Cloud Front

- Uses the SSLv3 or TLSv1 protocols and a selection of cipher suites that includes the Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) protocol on connections to both viewers and the origin.
- ECDHE allows SSL/TLS clients to provide Perfect Forward Secrecy, which uses session keys that are ephemeral and not stored anywhere. This helps prevent the decoding of captured data by unauthorized third parties, even if the secret long-term key itself is compromised

- CloudFront control API is only accessible via SSL-enabled endpoints.
- “Origin Access Identities” is used to control access to the original copies of objects in Amazon S3
  - Amazon S3’s ACL feature, which limits access to that Origin Access Identity so the original copy of the object is not publicly readable.

AWS Security Services

Amazon Cloud Directory
Create flexible cloud-native directories

AWS Identity & Access Management
Manage User Access and Encryption Keys

Amazon Inspector
Analyze Application Security

Amazon Macie
Discover, Classify, and Protect Your Data

AWS Certificate Manager
Provision, Manage, and Deploy SSL/TLS Certificates

AWS CloudHSM
Hardware-based Key Storage for Regulatory Compliance

AWS Directory Service
Host and Manage Active Directory

AWS Key Management Service
Managed Creation and Control of Encryption Keys

AWS Organizations
Policy-based management for multiple AWS accounts

AWS Shield
DDoS Protection

AWS WAF
Filter Malicious Web Traffic

AWS CloudHSM

- AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to generate and use your own encryption keys on the AWS Cloud.
- Support encryption keys using FIPS 140-2 Level 3 validated HSMs.
- Integrate with industry-standard APIs, such as PKCS#11, Java Cryptography Extensions (JCE), and Microsoft CryptoNG (CNG) libraries.