Amazon Web Services: Security Overview

amazon
web services™

RESOURCES

amazon web services™

Amazon Web Services: Overview of Security Processes

November 2009

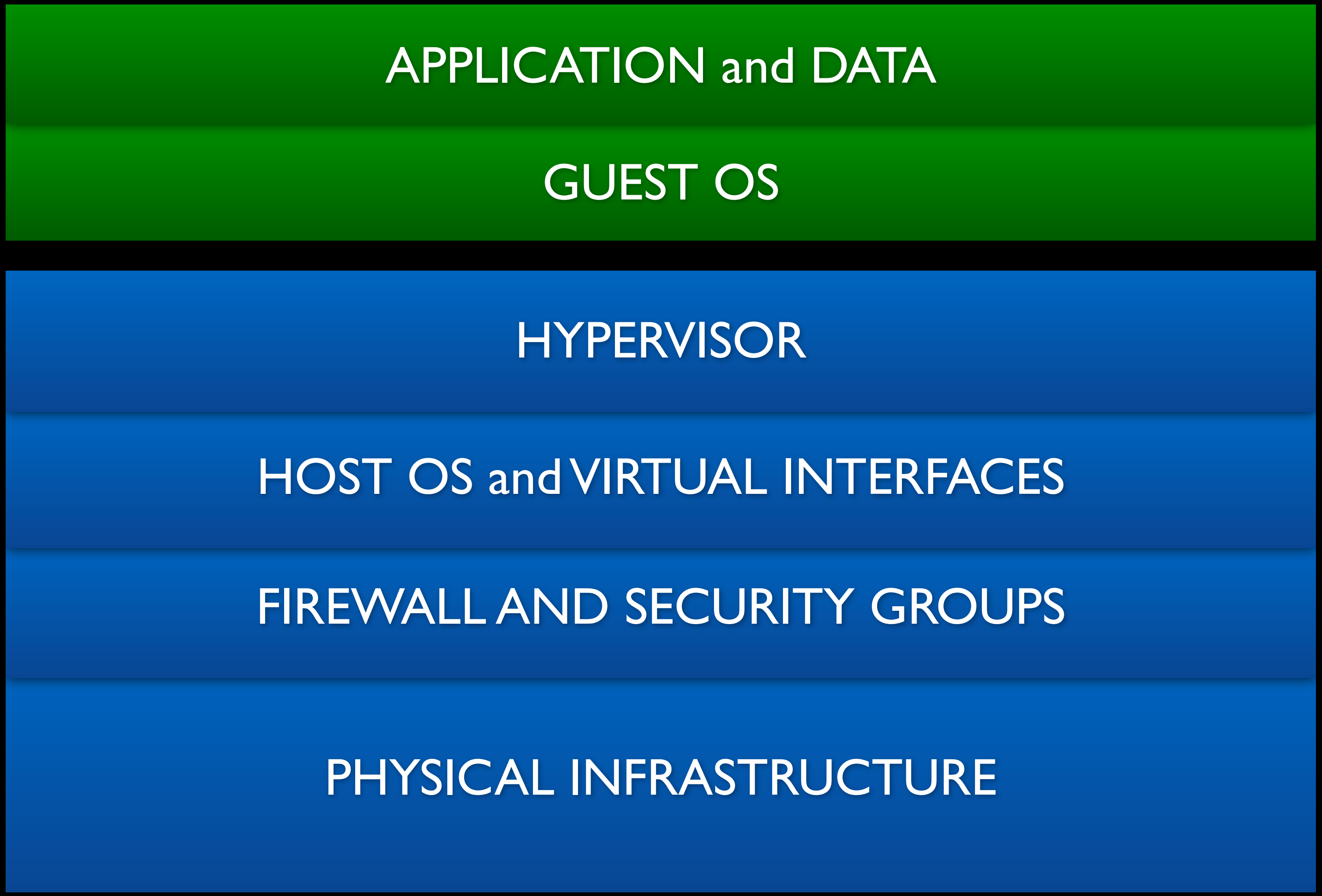
(Please consult http://aws.amazon.com/security for the latest version of this paper)

Security White Paper

aws.amazon.com/security

Updated twice a year - Feedback welcome

Shared responsibility model



APPLICATION and DATA

GUEST OS

HYPERVISOR

HOST OS and VIRTUAL INTERFACES

FIREWALL AND SECURITY GROUPS

PHYSICAL INFRASTRUCTURE

CERTIFICATION

Certified:

Sarbanes-Oxley (SOX)

SAS70 Type II Audit

Pursuing:

FISMA (NIST) C&A

ISO 27001

CERTIFICATION

Deployed:

HIPAA (health care)

DSS (credit card)

PHYSICAL SECURITY

Many years of experience in building large-scale, secure facilities.

Non-descript buildings

Robust perimeter controls

Strictly controlled physical access

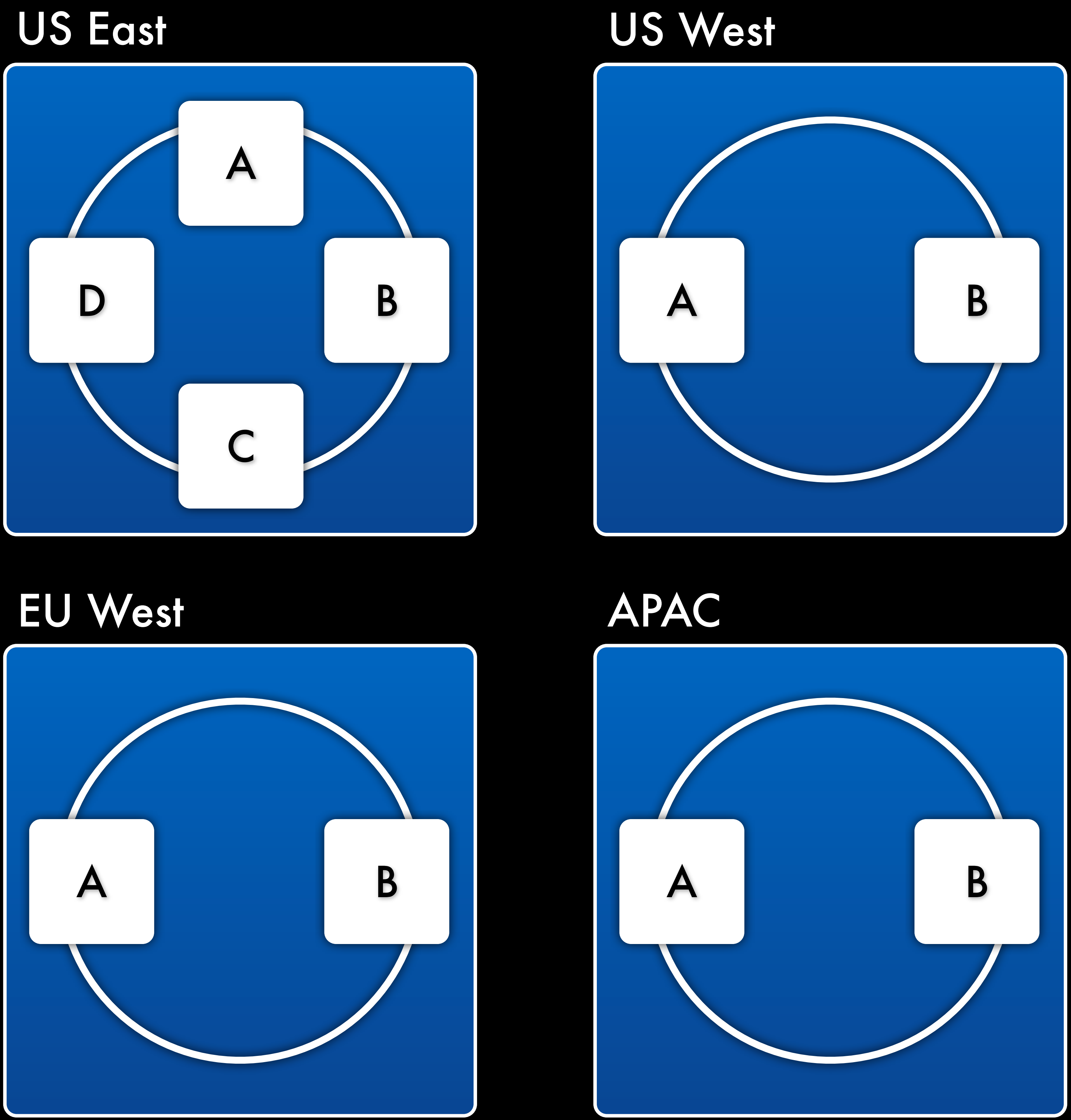
2 or more levels of two-factor authentication

PHYSICAL SECURITY

Controlled, need-based access

All access is logged and reviewed

FAULT SEPARATION



CloudWatch

Autoscaling

Monitoring

Load balancing

Redundant storage

Multiple physical locations

EBS redundancy remains in single Availability Zone

S3 and SimpleDB objects replicated across multiple Availability Zones

EC2 local data must be copied to EBS or S3 for redundancy

MULTI FACTOR

Multifactor authentication
to protect credentials

Recommended. Opt in.

Access controls for buckets and objects

Read, write, full

Owner has full control

Owner should encrypt when stored

Time limited URLs

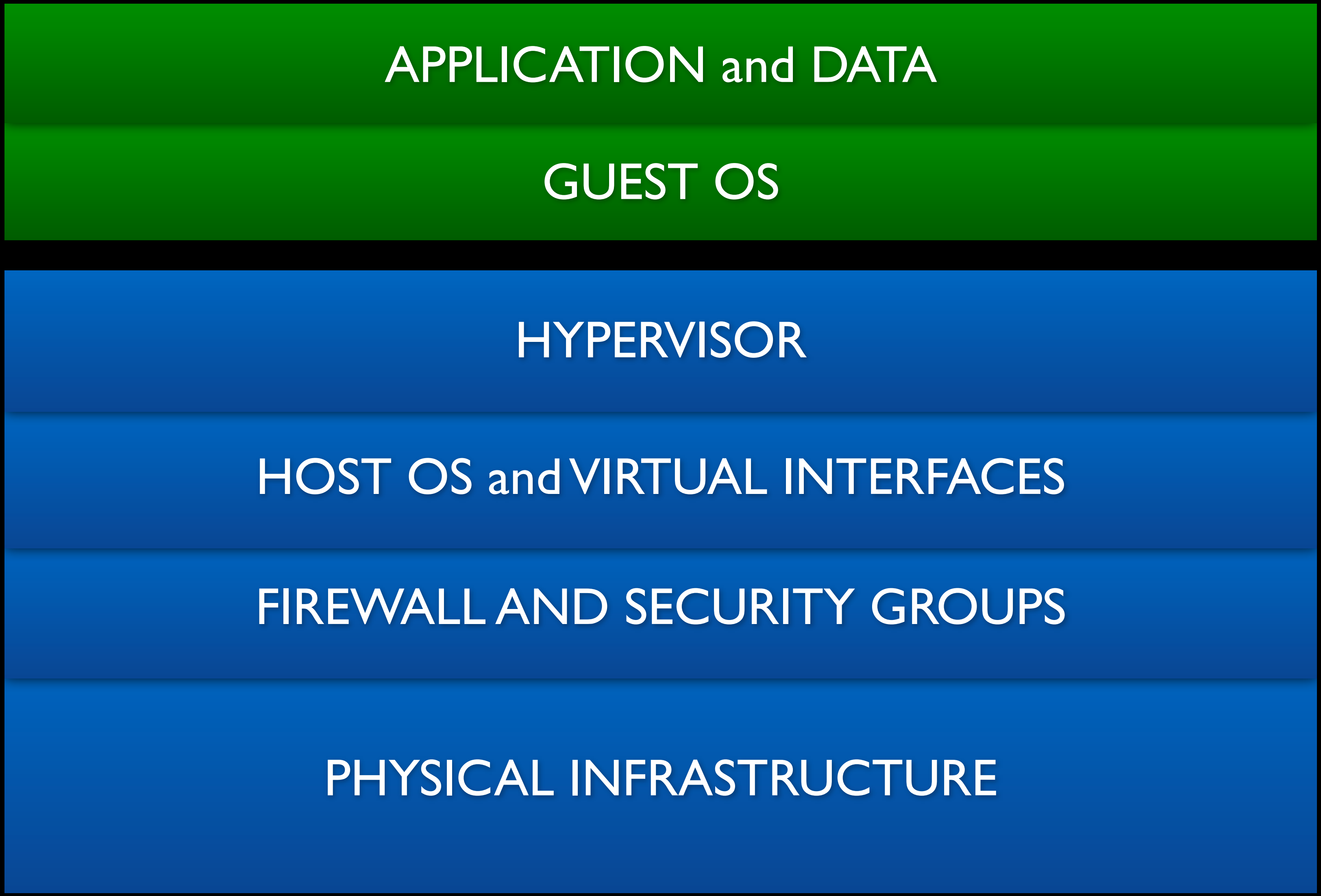
Versioning (with MFA delete)

Detailed access logging

Storage Drive Decommissioning

Military grade data destruction
DoD 5220.22-M/NIST 800-88

Security at every level



APPLICATION and DATA

GUEST OS

HYPERVISOR

HOST OS and VIRTUAL INTERFACES

FIREWALL AND SECURITY GROUPS

PHYSICAL INFRASTRUCTURE

EC2 SECURITY

Guest OS - Customer controlled

Certificate based root login

Customer generated keypairs

No access for AWS admins

Host OS - AWS controlled

SSH keyed logins via Bastion host

All access logged and reviewed

EC2 SECURITY

Security groups

Customer controlled

Fine grained access control

Stateful firewall

Mandatory inbound firewall

Default deny

Signed API calls

Requires X.509 certificate or secret key

Distributed Denial of Service

Standard mitigation techniques in effect

Man in the Middle

All endpoints protected by SSL

Fresh EC2 host keys generated at boot

IP spoofing

Prohibited at Host OS level

Unauthorised port scanning

Terms of Service violation

Actively monitored

Detected, stopped and blocked

Ineffective since inbound ports blocked by default

Packet sniffing

Promiscuous mode is ineffective

Protection at hypervisor level

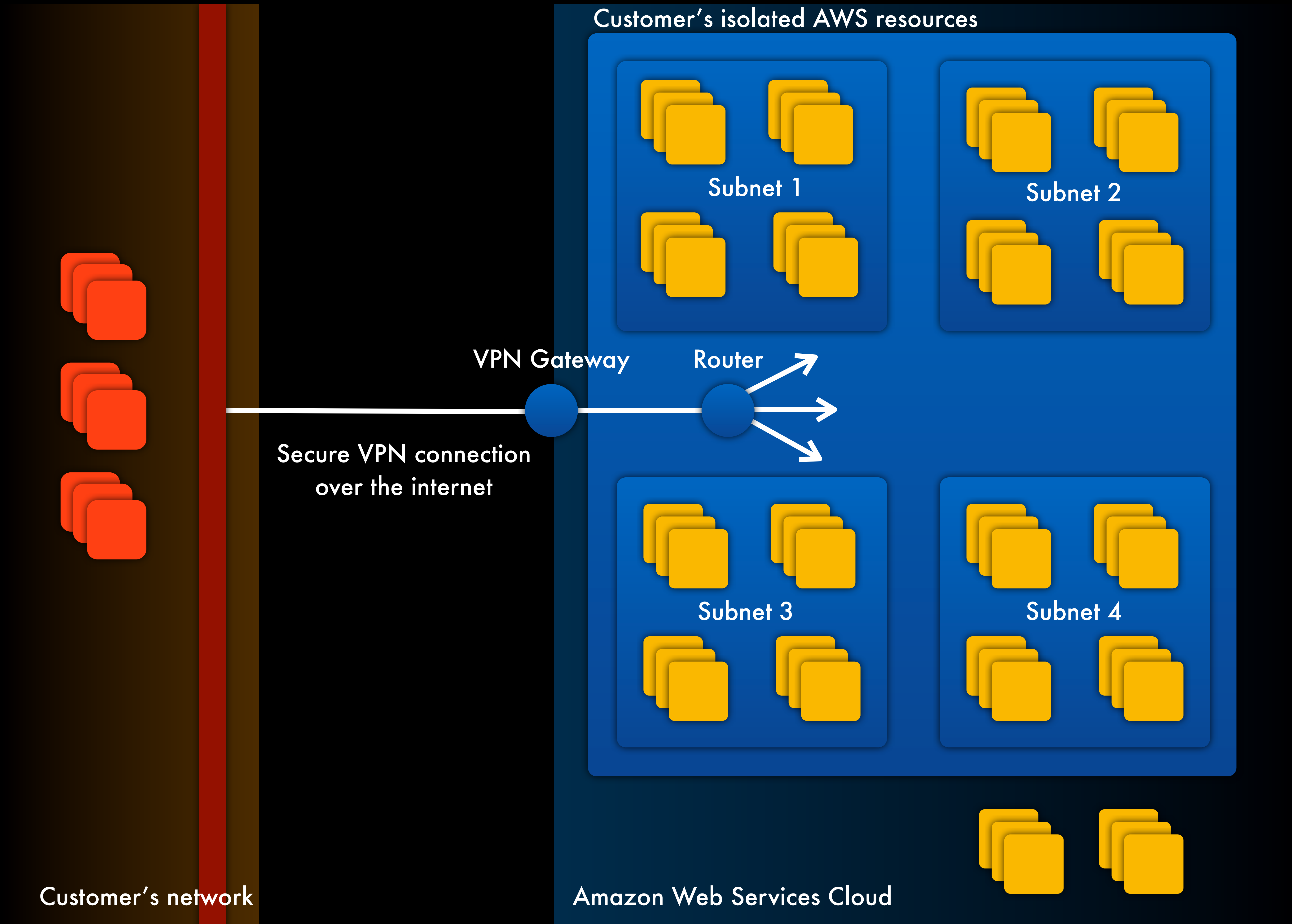
Configuration management

Configuration changes are:
authorised, logged, tested approved and documented

Most updates are done without affecting customers

Communication via email and
Service Health Dashboard

VIRTUAL PRIVATE CLOUD



VIRTUAL PRIVATE CLOUD

Create isolate environment within AWS

Establish subnets for access control

Connect your isolated AWS resources and IT infrastructure via a VPN

Launch AWS resources within the isolated network

VIRTUAL PRIVATE CLOUD

Extend existing security and networking technologies to examine traffic to and from your isolated resources

Extend existing security and management policies within you IT infrastructure to your isolated AWS resources as if they were running within your own infrastructure

Thank you

mawood@amazon.com

aws.amazon.com