CLOUD SECURITY 101

It's a shared responsibility

Sanjeev Kumar Jaiswal

What we will cover

- Quick recap of Cloud Computing - 5 mins.
- Service model and Deployment model - 5 mins.
- Why we need Cloud Security - 5 mins.
- Cloud Security Fundamentals - 40 mins.
- What’s Next - 5 mins.
- References & Credits - 2 min.

> Cloud Computing is the use of computing services like servers, storage, databases, networking, software, analytics, intelligence and many more over the Internet (“the cloud”)

What is Cloud Computing

Why we need cloud computing at all?

- Better Availability
- Higher durability
- Secured?
- Economical
- Compliant
- Go live in a minute

Advantages of Cloud Computing

- Pay as you go
- Resilient
- Scalable
- Economical
- Enhance Productivity, Performance and
- Security

Cloud Computing Deployment Model

Public Cloud

- Elasticity
- Utility Pricing
- Leverage Expertise

Private Cloud

- Total Control
- Regulation
- Flexibility

Community Cloud

- Meets shared concerns

Cloud Computing Service Model

- IaaS - Digital Ocean, Rackspace, GCE, Amazon EC2
- PaaS - Beanstalk, Heroku, Google App Engine
- SaaS - Gmail, Facebook, Dropbox, Wordpress, Office365
- XaaS - Database as a Service, Security as a Service, Malware as a Service (VMware AppDefense)

CLOUD SECURITY BASICS

Why we need cloud security

✳Cloud computing is being used for more than two decades. Still, several businesses find **security** as a challenge to handle.

- Everyone is in Cloud now a days
- It's shared responsibility
- Still new, so more to explore
- Multi tenancy make things more attack prone
- Service Providers are not macho man
- Data Security is a big concern
- and many more …

ID	Date	Type	Subject
AWS-2018-020	December 4, 2018	Important	Kubernetes Security Issue (CVE-2018-1002105)
AWS-2018-019	August 14, 2018	Important	L1 Terminal Fault Speculative Execution Issue
AWS-2018-018	August 6, 2018	Important	Linux Kernel Updates to address SegmentSmack & FragmentSmack
AWS-2018-017	June 13, 2018	Important	Xen Security Advisory 267
AWS-2018-016	June 13, 2018	Informational	Redis Security Advisory
AWS-2018-015	May 21, 2018	Important	Additional Processor Speculative Execution Research Disclosures
AWS-2018-014	May 8, 2018	Informational	Xen Security Advisories 260-262 (XSA-260, XSA-261, XSA-262)
AWS-2018-013	January 3, 2018	Important	Processor Speculative Execution Research Disclosure

Exploited Vulnerabilities Are Prevalent

When it comes to exploits, 45% reported experiencing one or more attacks from an exploit of known vulnerabilities of unpatched applications, known vulnerabilities of unpatched operating system vulnerabilities, and/or new and unknown zero-day vulnerabilities.

45%

have experienced one or more of these three types of exploits

Zero-day exploits that take advantage of OS/app vulnerabilities unknown to the victim

Exploits that take advantage of known vulnerabilities in unpatched applications

Exploits that take advantage of known vulnerabilities in unpatched operating system versions

Meltdown Performance Impact: MongoDB, AWS, Azure

	Meltdown	Spectre
Allows kernel memory read	Yes	No
Was patched with KAISER/KPTI	Yes	No
Leaks arbitrary user memory	Yes	Yes
Could be executed remotely	Sometimes	Definitely
Most likely to impact	Kernel integrity	Browser memory
Practical attacks against	Intel	Intel, AMD, ARM

Most Crucial aspects of Cloud Security

Security in the cloud consists of 4 areas:

- Data Protection
- Infrastructure Protection
- Privilege Management
- Detective Controls

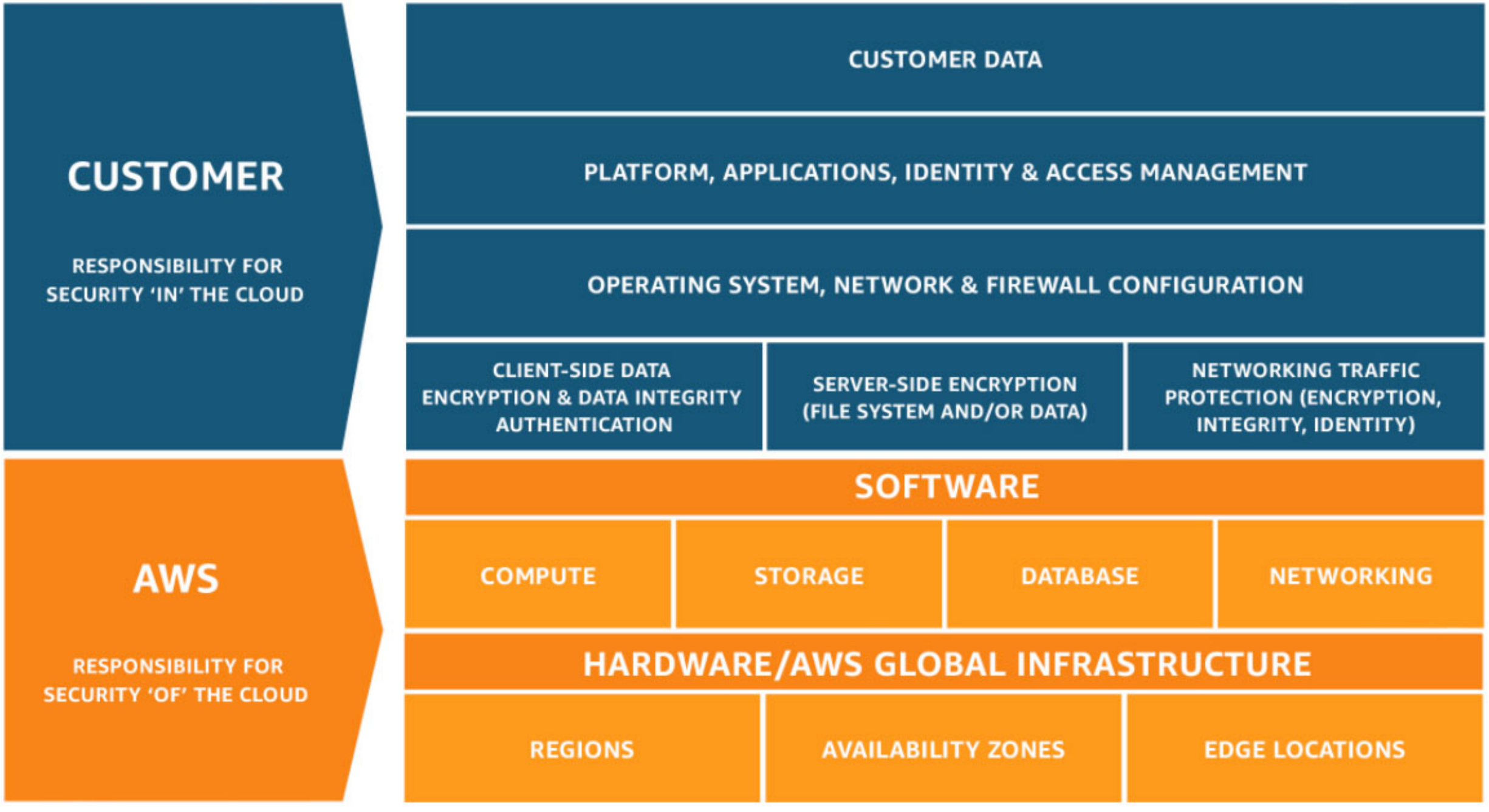
Cloud Security Dissection

- It's a shared responsibility
- IAM: Principle of Least Privilege
- Network Security
- Application Security
- Data Security
- Logging and Monitoring
- Cloud Security Automation

Cloud-Native Security vs Hybrid Cloud Security

- Door with built-in lock
- CCTV camera
- You need both for better security

Shared Responsibility



AWS Identity and Access Management (IAM)

AWS Identify and Access Management

User | User | User

Groups

Roles

Temporary Credentials

Policies

Multi-factor authentication

Hardware

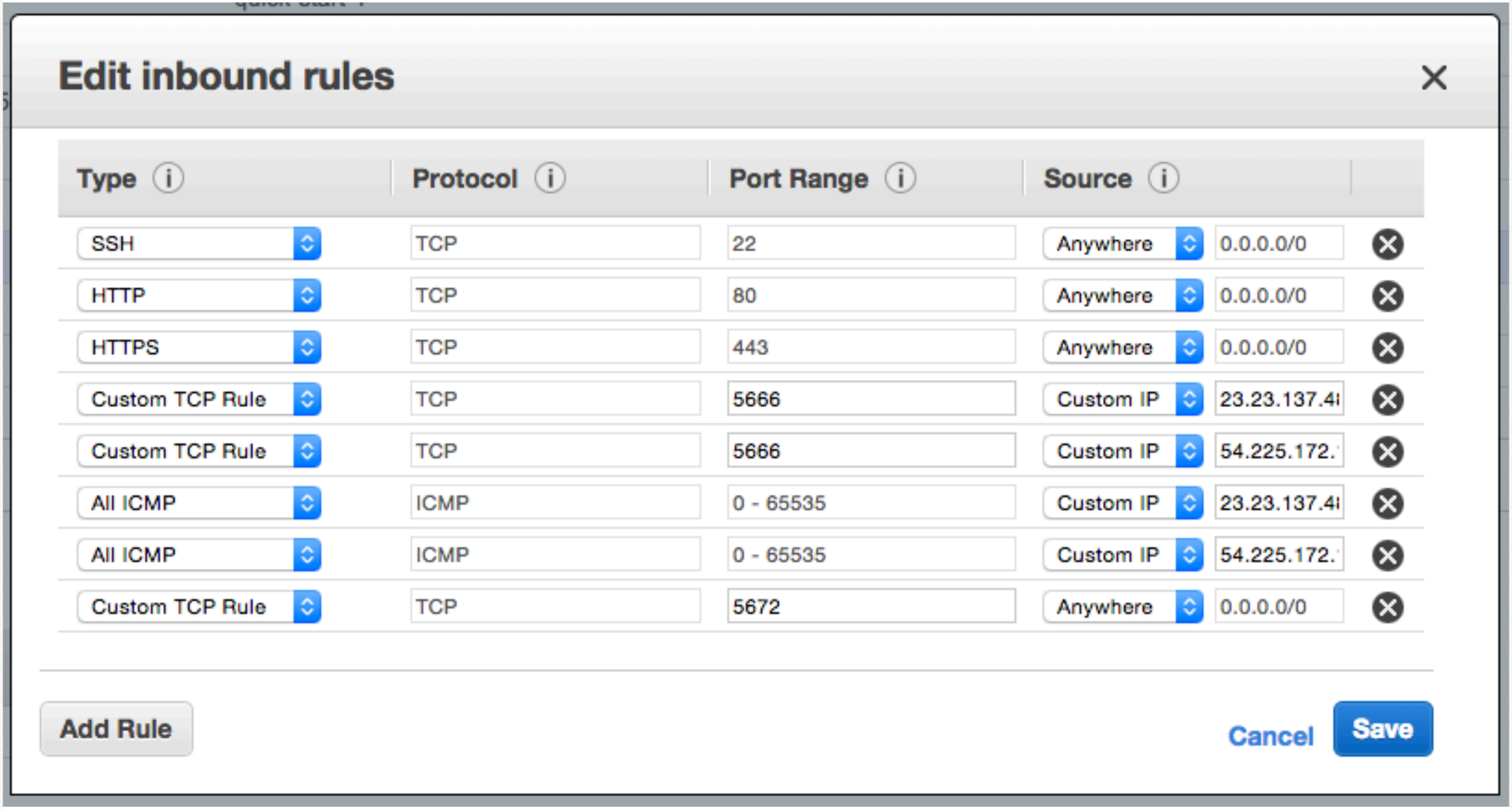
Software

IAM AWS administrative users

Root account

Enforce the principle of least privilege

A *security group* acts as a virtual firewall that controls the traffic for one or more instances.



Inbound						
Rule #	**Type**	**Protocol**	**Port Range**	**Source**	**Allow/Deny**	**Comments**
100	HTTP	TCP	80	0.0.0.0/0	ALLOW	Allows inbound HTTP traffic from any IPv4 address.
110	HTTPS	TCP	443	0.0.0.0/0	ALLOW	Allows inbound HTTPS traffic from any IPv4 address.
120	SSH	TCP	22	192.0.2.0/24	ALLOW	Allows inbound SSH traffic from your home network's public IPv4 address range (over the Internet gateway).
130	RDP	TCP	3389	192.0.2.0/24	ALLOW	Allows inbound RDP traffic to the web servers from your home network's public IPv4 address range (over the Internet gateway).
140	Custom TCP	TCP	32768-65535	0.0.0.0/0	ALLOW	Allows inbound return IPv4 traffic from the Internet (that is, for requests that originate in the subnet). This range is an example only. For more information about how to select the appropriate ephemeral port range, see Ephemeral Ports.
*	All traffic	All	All	0.0.0.0/0	DENY	Denies all inbound IPv4 traffic not already handled by a preceding rule (not modifiable).

Data Protection

Protecting Data Using Encryption

Topics

- Protecting Data Using Server-Side Encryption
- Protecting Data Using Client-Side Encryption

Data protection refers to protecting data while in-transit (as it travels to and from Amazon S3) and at rest (while it is stored on disks in Amazon S3 data centers). You can protect data in transit by using SSL or by using client-side encryption. You have the following options of protecting data at rest in Amazon S3.

- **Use Server-Side Encryption** – You request Amazon S3 to encrypt your object before saving it on disks in its data centers and decrypt it when you download the objects.
- **Use Client-Side Encryption** – You can encrypt data client-side and upload the encrypted data to Amazon S3. In this case, you manage the encryption process, the encryption keys, and related tools.

Logging

- Whom to give log access
- What to Log
- Where to store
- Log Duration
- Secured Cloud Logging Service - sumologic, alertlogic
- Cloudtrail, Cloudwatch, VPC flow logs in AWS

Alert & Monitoring

- Trigger point
- What to monitor
- At what frequency
- How much possibility through Automation?
- Alert response mechanism
- IR Mechanism

AWS Security Resources/Tools Examples

- AWS IAM
- KMS
- AWS CloudTrail
- AWS Config
- AWS GuardDuty
- AWS Macie
- AWS Inspector
- AWS Shield
- AWS WAF
- Trusted Advisor
- Security Hub
- Pacu, Prowler, Cloud Custodian, Cloudcheckr, Tenable, and so on…

What's next?

- Advanced Network and Infra Security
- SIEM in Cloud
- CSPM vs CASB (also check CWPP)
- Cloud Security Threats
- CSA and NIST standards
- Data Governance and Compliance
- Security Automation :
  - Cloudformation, Terraform, Pulumi etc.
  - Security in CI/CD -> DevSecOps (Hotshot)

References & Credits

- Basics of Cloud Security
- Cloud Services Explained by IBM
- Awesome Cloud Security
- Cloud Computing Courses from Acloud.guru
- Oracle and KPMG Cloud Threat Report, 2018
- Cybersecurity in the Cloud Specialization (Coursera)