AWS Security Best Practice

CRS = Can't remember stuff

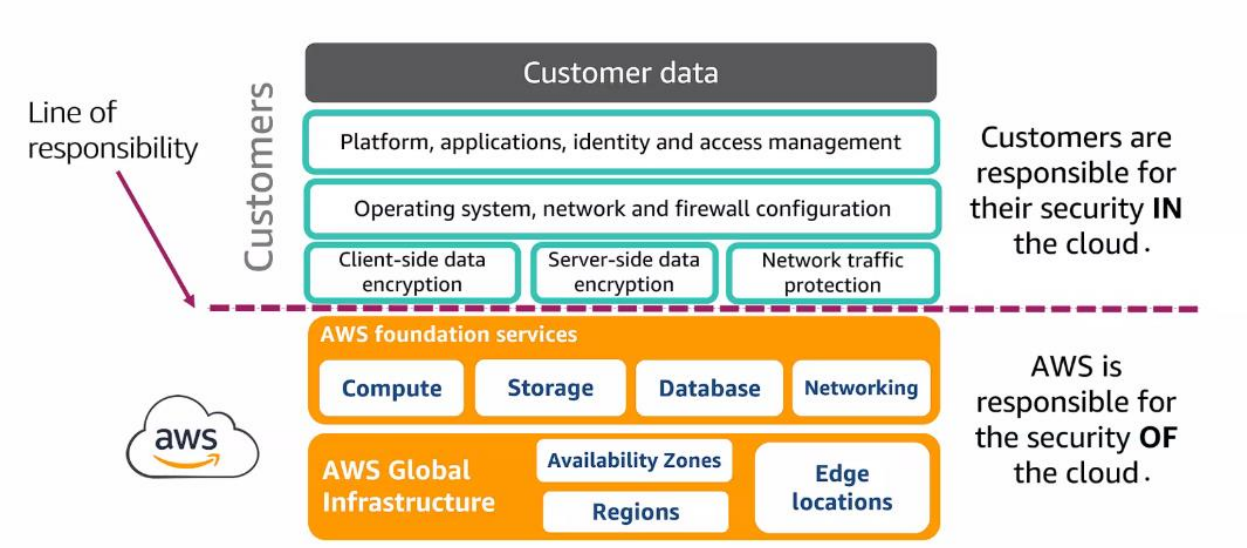
Objectives

Design and implement a secure network infrastructure, compute security, and logging solution

Shared Responsibility Model

Section 1 of 5

Module 1



Customers are basically responsible for what they put in the cloud = Security **IN** the cloud

AWS is responsible for physical security = Security **OF** the cloud

AWS is the home builder, and the customers is the home buyer. AWS has built the infrastructure and layers for governing bodies. But once the "home" is bought… The customer is responsible for anything adding into the home that is the customers responsibility

Customer Challenges

Section 2 of 5

To protect and safeguard data…

- Technology changes in size and complexity
    - This drives everything, something new comes out a lot
- Resources and workforce limitations
- Evolving threats and expanding threat surfaces
- Changes to legal and regulatory requirements

Vulnerability is a weakness

Threat is a possibility to exploit the vuln

Risk is the potential for loss, damage, or destruction of resources due to a threat

Threats in the cloud

- DDoS
- Malware infections
- Unathorized access or insider threats
- Misconfigs

Assessing Risk

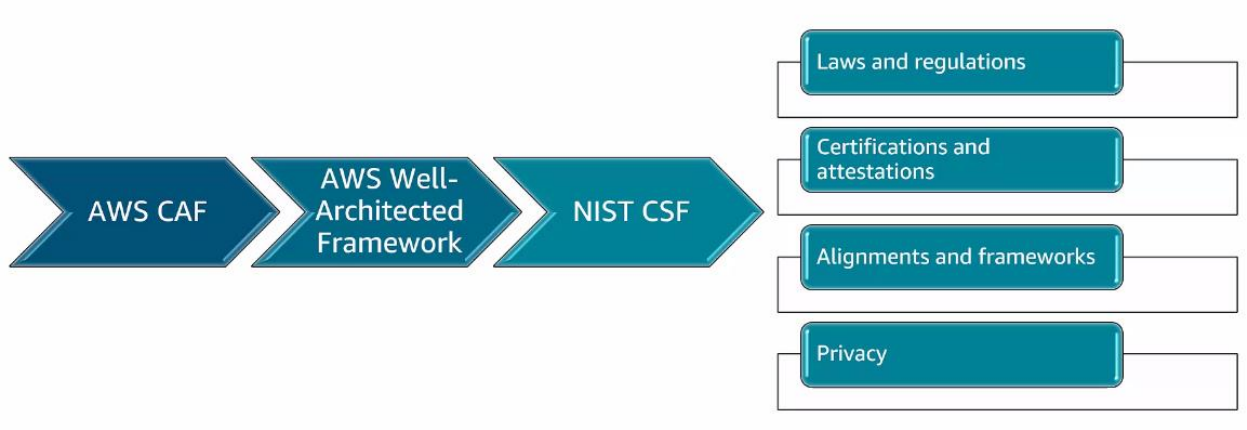
- Also known as risk analysis
- Use qualitive (Math) measurements or qualitive (Mental) measurements

Risk Management

Framework and standards

Section 3 of 5

Employ effective security controls to identify, protect, detect, respond, and recover from destructive events



- AWS CAF
  - Migrating from on-prem to AWS cloud
- AWS Well-Architected Framework
  - 6 pillars
- NIST CSF
  - Audit manager, looking at different frameworks that can help fit what that particular workload is

Establishing best practices

Section 4 of 5

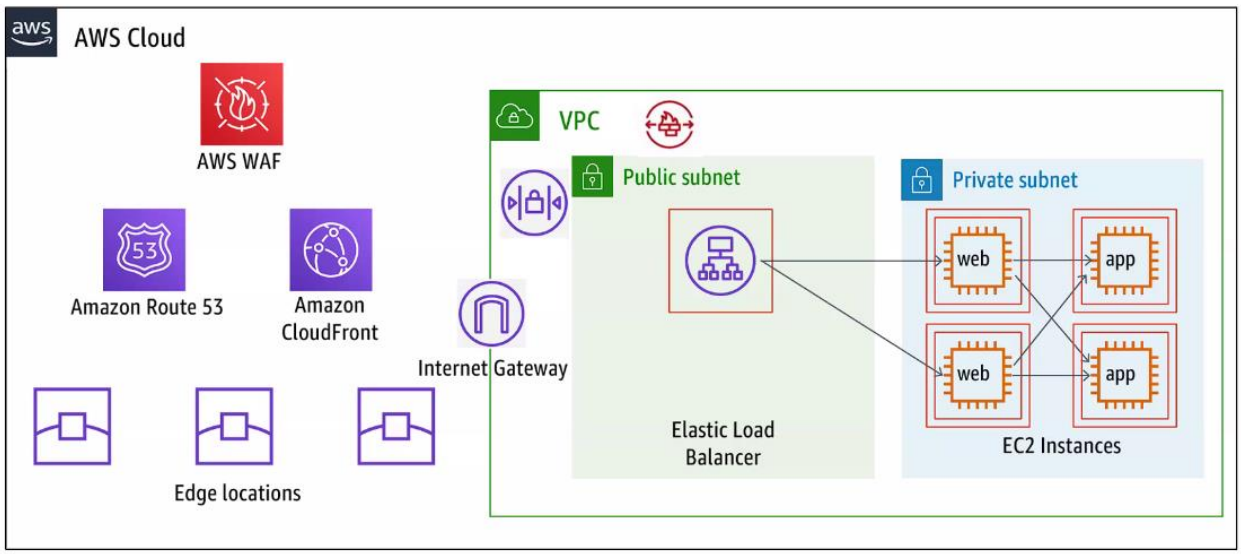
AWS Security Page https://aws.amazon.com/security/

AWS Security Documentation- https://docs.aws.amazon.com/security/

CIA Triad

- Confidentiality: Amazon Elastic Block Storage (EBS) encryption
- Integrity: AWS CloudTrail log file validation
  - Log file validation, if someone tries to change or manipulate the CloudTrail log you will know
- Availability: Elastic Load Balancing (ELB)
  - Multiple resources carrying the workload which spreads out, so if 1 goes down, something else is up and running
  - Another example is auto scaling

Layering Defense: Castle analogy



1. Amazon Route 53 geo routing
    a. Route based on origin location of domain name system
    b. Route to static or dynamic resources
2. CloudFront geo restriction
    a. Permit approved countries
    b. Block or deny banned countries
3. AWS WAF Rules
    a. Deny (based on IP source)
    b. SQL injection prevention
    c. Cross-site scripting prevention
    d. Bad bot blocking
    e. Content scraper blocking
4. Network Firewall
    a. Fine-grained control over network traffic
    b. Traffic inspection to ID & block vulnerability exploits
5. Network ACL
    a. Deny or block by IP
    b. Use port blocking
6. Security Groups
    a. Only allow required ports
    b. Only allow from required sources that you allow it from

All above is what an attacker must get through in order. Nothing is going to stop a professional, it will only slow them down. Which gives you time to react and act.

Compliance in AWS

Section 5 of 5

Customer Responsibilities

- Remember they are responsible what workloads must be regulated by which applicale standards

AWS Compliance programs

- IT standards that AWS complies
    - Certifications and attestations
    - Laws, regulations and privacy
    - Alignments and frameworks

AWS Artifact

- Reports on demand
- Global available
- Continuous monitoring
- Enhanced transparency
    - AWS isn't going to hide anything from you

AWS Artifact > Reports

Lets say you have to deal with a payment card industry you can search "PCI" remember the reporting period. This is what you inherited from AWS.

Another is "C5" that is expired. But you want to use what is in date. Just depends what you're working with.

Customer is responsible for what they put IN the cloud

Security Frameworks can help:

- AWS Well-Architected Framework
- AWS CAF
- NIST CSF

Securing the Network

AWS Security Best Practices

Module 2

Flexible and secure

Section 1 of 4

Starting with VPC

A sound strategy for designing, building, and maintain the network and architecture provides the best foundation for scaling and security

Best practices

- You define your own space. Use subnets to isolate the tiers of your application within a single VPC
    - Such as web, application and database tiers
- Avoid opening SSH or RDP between or within instances of the production environment whenever possible.

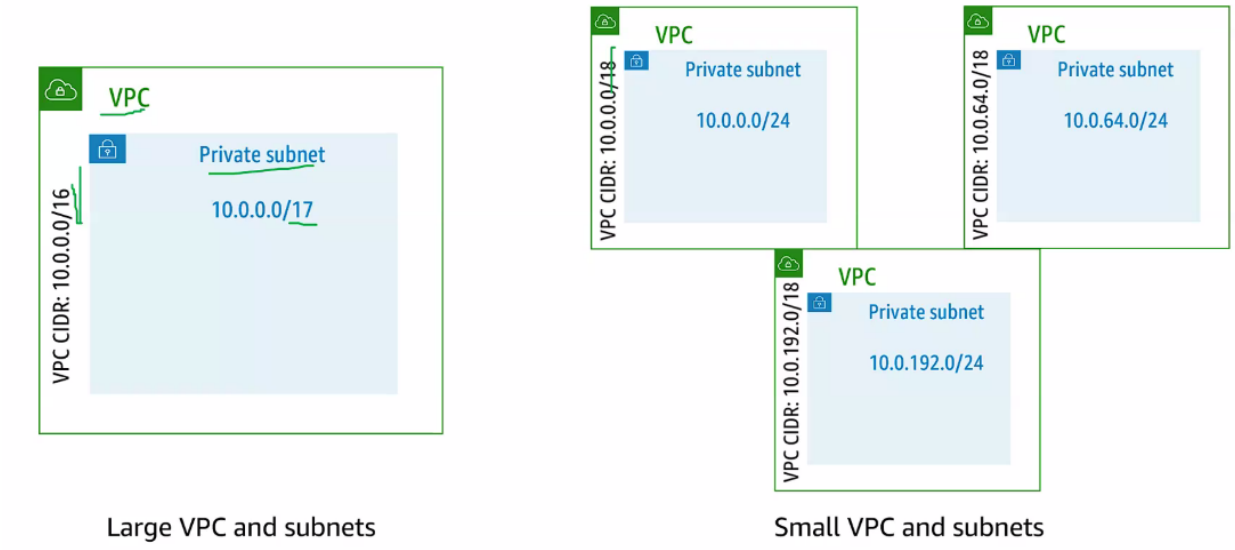
Designing a network

- Monitor at boundaries
    - Such as EC2 or ELB
- Subnet to create isolation
    - Database tier is different from your web tier
- Connect externally through protective devices
    - Only the ones you choose to setup

Network sementation

- Advantages of using subnets for network segmentation
    - D

VPC and subnet strategy



Large VPC and subnets

Small VPC and subnets

Amazon Route 53 using DNSSEC

Domain name security extensions helps prevent DNS attacks like DNS cache poisoning and DNS spoofing

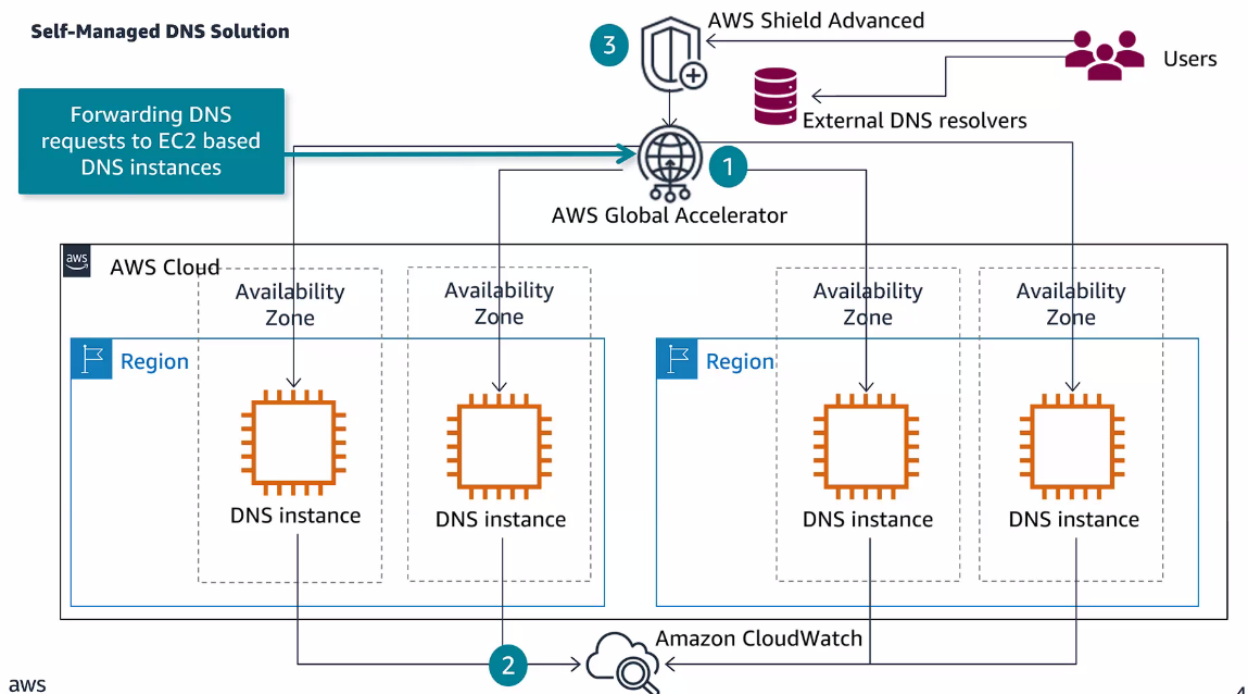
- Store private keys in AWS KMS

Sign public hosted zones or use DNSSEC validation. And also use a single key across multiple public hosted zones. (Beware of alias and tagging within KMS)

Route 53 Resolver DNS Firewall

- Protects outbound request
- Define domain name filtering rules to control access to sites and block DNS-level threats
- Centralize management with AWS Firewall manager
    - Network ACL you can't manage in the firewall manager
- Filters User Datagram Protocol DNS traffic (not HTTPS, TLS, SSH or, other protocols)

Self-Managed DNS solution



1. Global Accelerator – Provides static IP address, routes user traffic based on user performace, locations and policies you configure
    a. Then the GA will route it to an Instance
2. Amazon CloudWatch
    a. Be monitoring the DNS instance, and will let GA know that it can't send anymore traffic to that instance
3. D

Questions

What is the performance impact of DNSSEC signing?

May require some researching into benchmarks or performing benchmarks in the customers environment. The question comes down to how noticeable it is or not. AWS typically builds this into the SLA's and performance is considered part of the SLA of these managed services

Wouldn't having a single key to handle everything be more of a security issue?

Yes, it is a balance between managing keys and the impact of any of them being exploited. Goes back to C-I-A triad.

Security inside the VPC

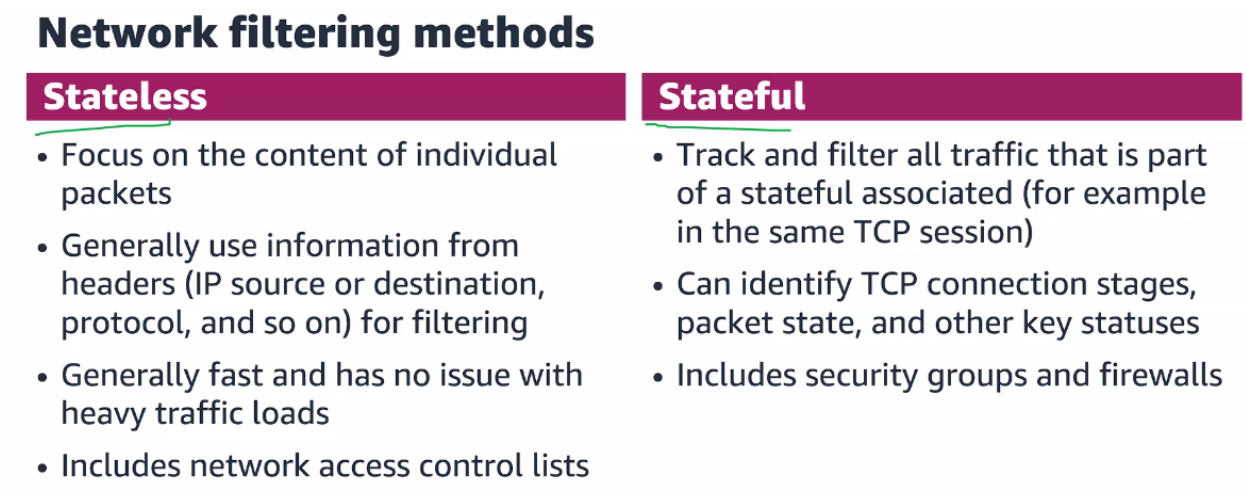
Section 2 of 4

VPC gives you different features and services

Best practices

- Layer security groups and network ACLs together
- Out-of-band management whenever possible
- Use Amazon CloudWatch to monitor your VPC components
- Use flow logs to capture information about traffic in your VPC
    - Only give people exactly what they need to do their job. Nothing extra
- Always use IAM to limit access to your resources, including the VPC

Network filtering methods



Network ACL review

DEFAULT MODE: Explicit deny and implicit allow

When you create a VPC a default NACL is automatically created for you. Nothing draws your attention to that NACL. But if you don't go in and manually do it… It will be applied to every subnet in that VPC

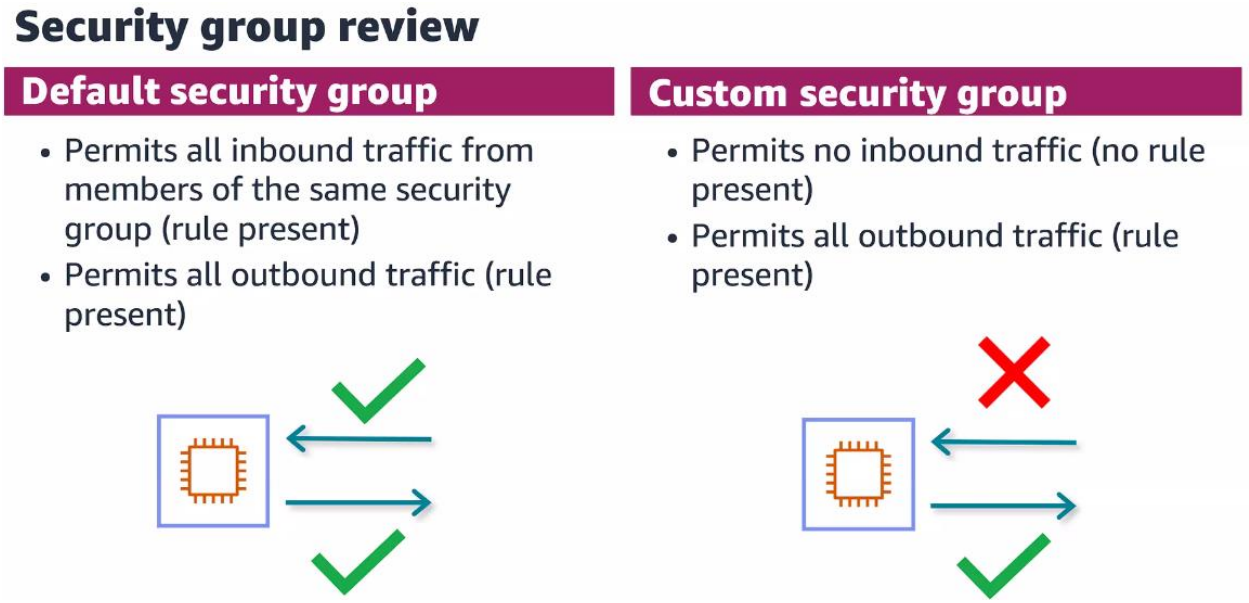
Basically, the default VPC is wide open. So, you must write rules on what traffic you want in and out. Or you can create a custom NACL. A custom NACL is not letting anything in nor out. Just about writing rules. Just comes down how many rules you want to write. For best practice, a custom rule sounds more secure even though it is more time consuming but since custom NACL doesn't let anything in or out sounds good to me (of course you can change).

Question in sequence, which comes first? NACL or Security Group?

Assuming using SG's with EC2. For traffic coming from the internet, NACL will be evaluated first before packet gets to the subnet. Once in the subnet, SH is next to secure the EC2 instance. But keep in mid that SG's can be assigned to other resources like ALB.

Best practices

- Remember the default network ACL
- Monitor and audit network ACLs for ineffective "deny" rules
    - Might be best to look at rules at the end of the week if changes were being made that week.
- Consider limitations
- Do not ignore outbound rules on network ACLs
    - Control what comes in and what is allowed in the subnet



* Security is like an onion. The deeper an attacker gets into it, the more they want to cry.

- App tier also has DB tier info of allowing and denying ports

    This is true, you can setup NACL's at various tiers, not just web tier

- Do we have to worry about ephermeral ports for outbound rules when using NACLs?
    - Yes you do

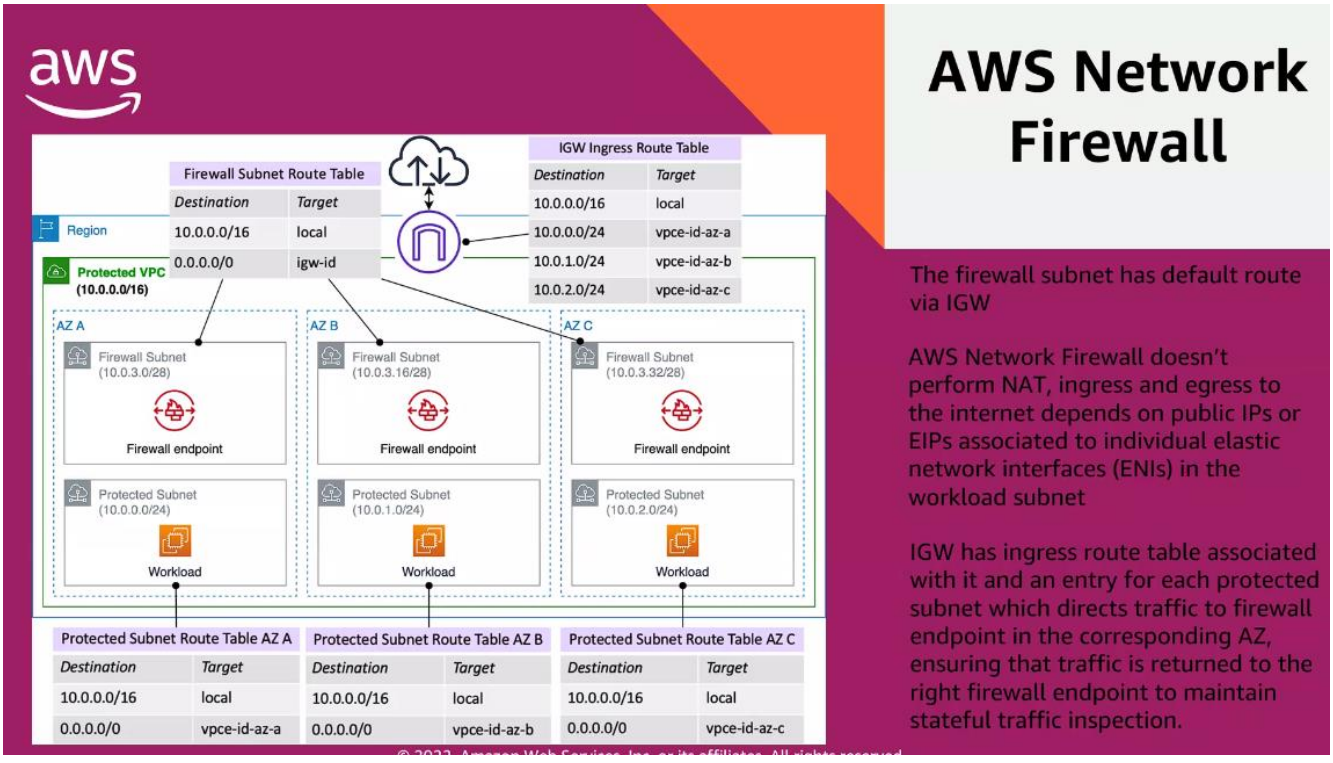
Best practices

- Never keep unattached security groups
    - If isn't attached…. Get rid of it
- Track rate of change in production environments
- Use ELB with security groups to restrict access to the internet
- Limit modifications to only certain IAM roles

- Principle of least privilege
- Do NOT ignore outbound rules of security groups
  - Control what you allow out

AWS Network Firewall is a managed network protection service that provides the following:

- Stateful firewall
- Web filtering
- Intrusion protection
- Central management and visibility
- Rule management and customization
- Partner integrations



On the Ingress route table the "vpce" the letter e stands for endpoint.

Network Firewall and other AWS security services

	Network Firewall	VPC security group	Network ACL	AWS WAF
Where is the protection applied?	Route level, based on VPC routes	Amazon EC2-instance level	Subnet level	Endpoint level (API Gateway, ALB, CloudFront)
Stateful or stateless	Both	Stateful	Stateless	Stateless
Which flows are protected?	All ingress/egress flows at perimeter of VPC (e.g., IGW, VGW, DX, VPN, VPC–VPC)	All ingress/egress flows at instance level (EC2–EC2, EC2–IGW, EC2–DX, etc.)	All ingress/egress flows at subnet level (subnet–subnet, subnet–IGW, subnet–DX, etc.)	Ingress only from internet to API Gateway, ALB, CloudFront
Which OSI layer?	L3-7	L4	L3	L7
Features	Stateless/ACL L3 rules, stateful/L4 rules, IPS–IDS/L7 rules, FQDN filtering, protocol detection, deep packet inspection, large IP block/allow lists	IP | port | protocol filtering	IP | port | protocol filtering	Deep application layer filtering, managed rules
Default behavior	Allow	Deny	Allow	Customer chooses

Building for availability

Availability is an important part of the C-I-A triad.

Global availability

- AWS Global infrastructure spans 99 AZs within 31 Geo regions around the world
- More regions coming
    - Israel, New Zealand, Canada and Thailand

VPC and AZ availability

Elastic Load Balancing (ELB)

- ELB distributes traffic over a group of resources in one or more Availability Zone.
- Deploy ELB with AWS Application Auto Scaling, AWS Auto Scaling, or Amazon EC2 Auto Scaling.
- Choose the type of load balancing device you need.
- **(Best practice)** Use security groups to protect ELB.

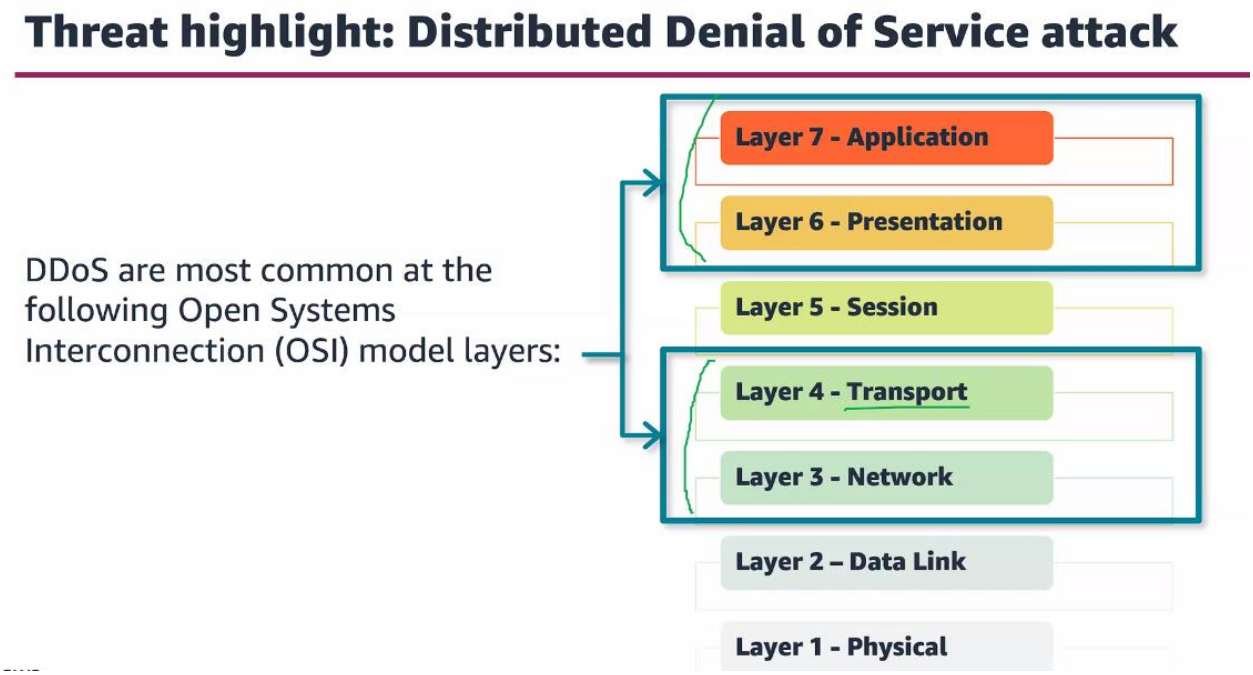
If you put all resources in 1 AZ and that 1 AZ goes down. You are dead in the water. It would be best to implement multiple AZ at least 3 AZ. So, if 1 AZ goes down, the customers will never know (But the customer may be logged out and would have to sign back in) Just depends.

Management best practices

Port 22 Linux machine SSH

Port 389 for RDP

Use additional security groups or network interfaces to control Amazon EC2 instance management traffic separately from regular application traffic. Implement special IAM polices for change control and auditing.



- NACL > Layer 4 and 3
- Which is the most common. AWS Shield helps with this. Shield advance helps with Layer 7 and 6

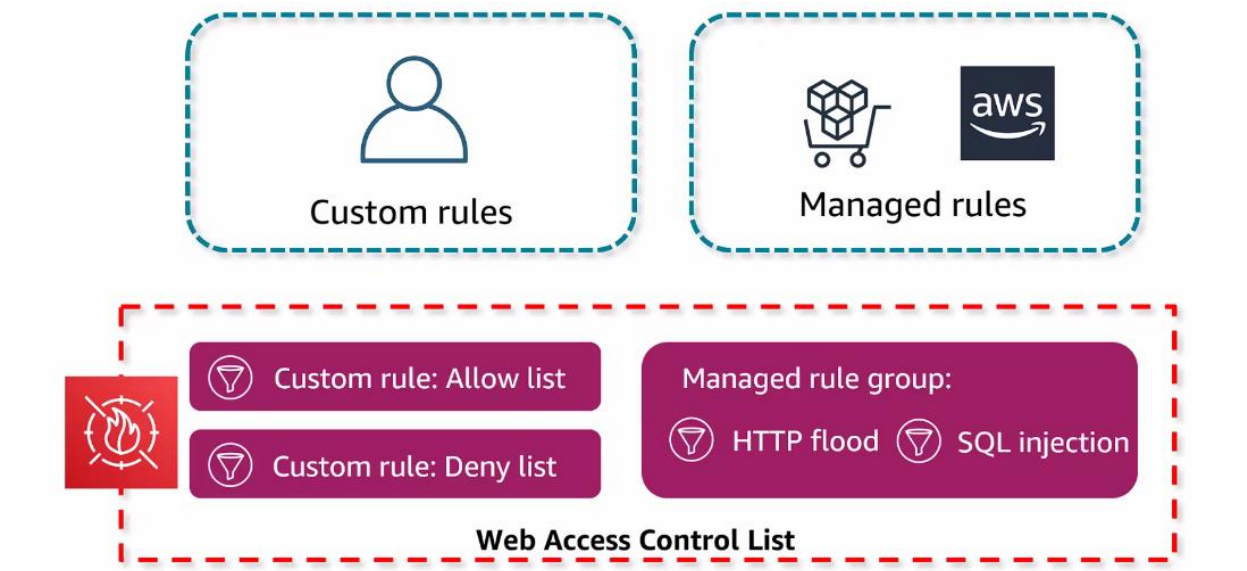
AWS WAF filters traffic for your web applications based on the following criteria:

- IP address origin of the request
- Country of origin of the request
- String match or regular expression (regex) match in a part of the request
- Size of a particular part of the request
- Malicious SQL code or scripting

This service is provided to customers using AWS Shield Advanced for no additional cost and adds additional DDoS protection

AWS Web Application Firewall

Lets say you see over 5000 request blocks within 5 mins. That is a good giveaway that there is a DDoS attack going on. Which you can set after a set number a attempt you can block that IP address.



The managed rules can go into the custom rules as well

AWS Shield

Remember this happens at layer 3 and 4. Most common attacks

Standard Protection	Advanced Protection
• Available to all AWS Customers at **no additional cost** • Automatic detection and mitigation • Protection from most common DDoS attacks (SYN/UDP Floods, Reflection Attacks, etc.)	• Paid service that provides additional protection, features, and benefits. • Includes Shield Response Team (SRT), AWS WAF for layer 7 DDoS attack mitigation, and AWS Firewall Manager

Standard is free, advanced (layer 7 and 6) is a paid service.

The Shield response team can walk you through or they can go into your account and change things to fight off the attack. But if I am paying for the service. Let the Shield Reponses team go into that account… You're paying for it so let them do it.

There will be some paper work involved with them going into the account. So while you're waiting for the paper work you're still getting attacked. Just be proactive and go ahead and give them the permissions in advanced. Because as mentioned… while you're getting attacked you're filling out that paper work.

Third-Party

Section 3 of 5

You can go into the AWS marketplace

So if you want a “ngfw” you can get Fortinet, Paloalto, anything (SaaS or cloud delivery network providers)

Module 2: Securing the network

Amazon EC2 Security

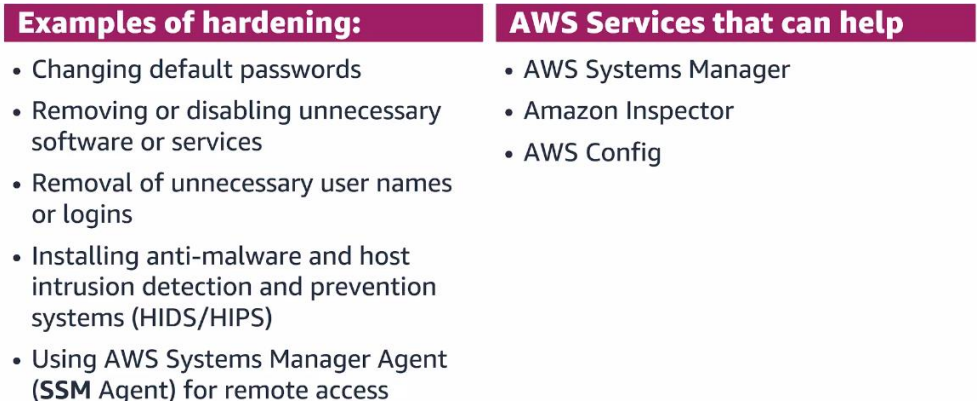
Compute hardening

Section 1 of 5

Common vulnerabilities

- Exposing EC2 instances to the

Hardening your systems



Hardening with benchmarks

- Create Amazon Machine Image (AMI) from your instance to save the configuration as a template for launching future instances.
- Or
- Use EC2 Image builder to create and maintain images
    - In the EC2 Image builder. There are other 3rd party “Harden images” that are set to certain standards. Or you can do it manually with AMI
- Use benchmarks (From CIS and others) to harden common vulnerabilities and help minimize the attack surface.

CIS Benchmarks purpose

Globally recognize for security best practices

- Using industry best practices
- Removing the guesswork in hardening

Which these align with or map to frameworks

- National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- PCI DSS
- HIPPA
- ISO/IEC 2700
- GDPR

Amazon EBS encryption

Section 2 of 5

- Use separate Amazon EBS volumes for the OS and your data
    - Like an external HD
- Encrypt EBS volumes and snapshots
- Understand the implications of the root device type for data persistence, backup and recovery

Encryption by default

By default is best practice to ensure security of data at rest

- Encryption by default is a region-specific setting
- Do NOT use encryption by default while using automated migration services.
    - Do not use this during migration, do it after migration is complete. May mess things up

AWS KMS

- Supports many of the security best practices

7-30 days for customer managed keys (KMS)

Secure management and maintance

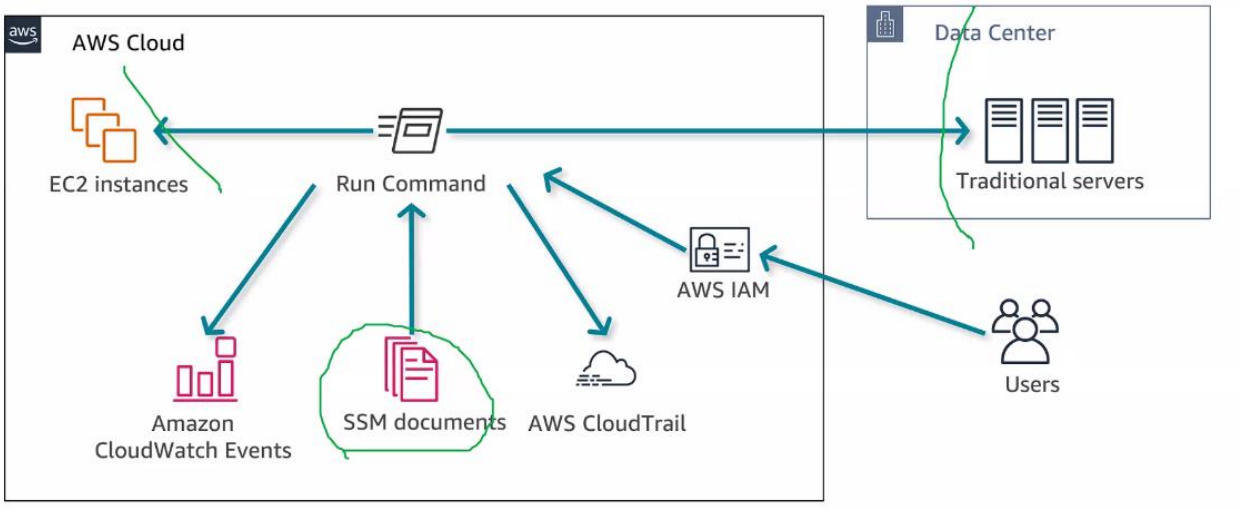
Section 3 of 5

Best practice

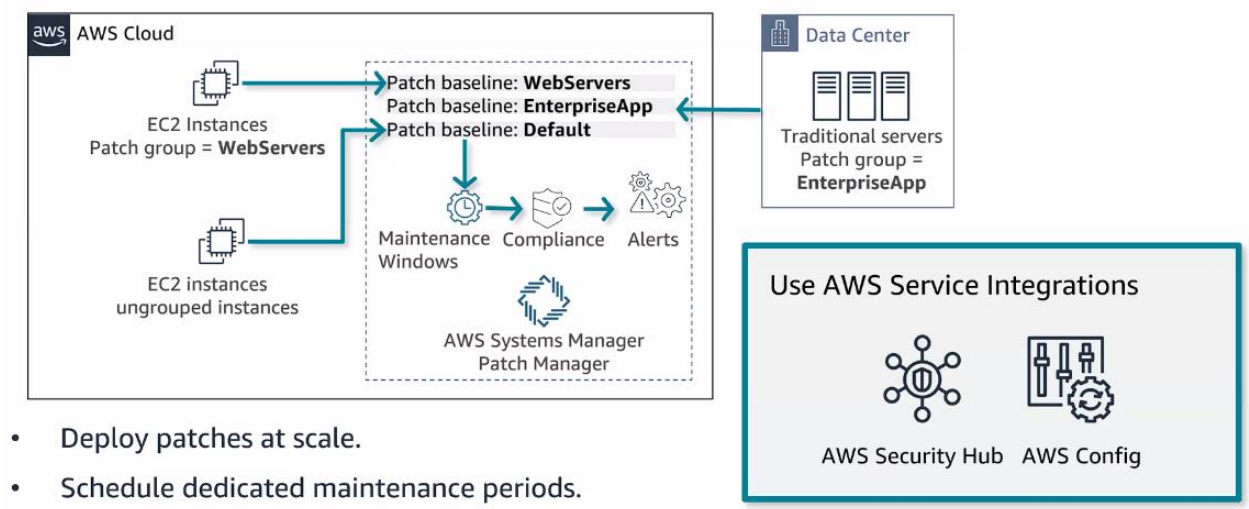
- Limit access and authorization for connecting to instances (Session Manager)
- Securely manage instances at scale (Using run command)
- Regularly patch and update with define maintenance windows (Patch manager)
- Automate monitoring and remediate of configuration drift (State Manager)
- Secure, monitor, and rotate secretes (Secrets manager or parameter store)

AWS Systems Manager (Agent based)

- Session Manager
    - Improves security posture in the EC2 instances
    - No need to have a jump box
    - No open inbound ports and no need to manage bastion hosts or SSH keys
    - Logging and auditing session activity
- Run Command
    - Connection has been made
    - Manage EC2 instance
    - Gives you the ability to apply an update to all the EC2 instances and servers to on-prem all at once
    - In SSM Documents you can specify what user can do what which is tracked in cloud trail
    - You can do multiple jobs



- State and patch Manager
    - Patch manager allows you to deploy patches at scale
    - Scheduled dedicated maintenance periods
    - Test patches in a non-prod environment



- Deploy patches at scale.
- Schedule dedicated maintenance periods.
- Test patches in a nonproduction environment.

    - State manager

State Manager

Usage

- Maintain visibility over system states.
- Apply configurations based on policies.
- Create and push alerts when configuration drifts are detected.
- Query statuses for on-demand visibility into compliance status.

Best practices

- Update SSM Agent using the preconfigured AWS-UpdateSSMAgent document.
- Use tags to create groups then target nodes using the targets parameter.
- Use a centralized configuration repository for your SSM documents, and share it across your organization.

Basically monitors changes for you

- Parameter Store and secrets manager

Parameter Store	Secrets Manager
• Can notify you of expiring secrets but cannot rotate them for you • Can be referenced from AWS CloudFormation templates • Supports storing values under a name or key, encryption of secrets, and versioning	In addition to the capabilities of Parameter Store: • Provides full key rotation integration with Amazon RDS • Randomly generates passwords in CloudFormation and stores the password in Secrets Manager • Shares secrets across different AWS accounts • Can exceed storage capacity of Parameter Store, but has costs associated to storage of secrets and API calls

Both services you can store both secrets in KMS to encrypt your values. CloudFormation works with both. Versioning allows you to view or restore a parameter, but the difference…. Parameter can notify but can't rotate secrets. Whereas secrets manager can do both. Secrets manager can randomly store passwords. Parameter has no additional cost, limit of 10,000, secrets doesn't have a limit.

- And much more

Detecting vulnerabilities

Section 4 of 5

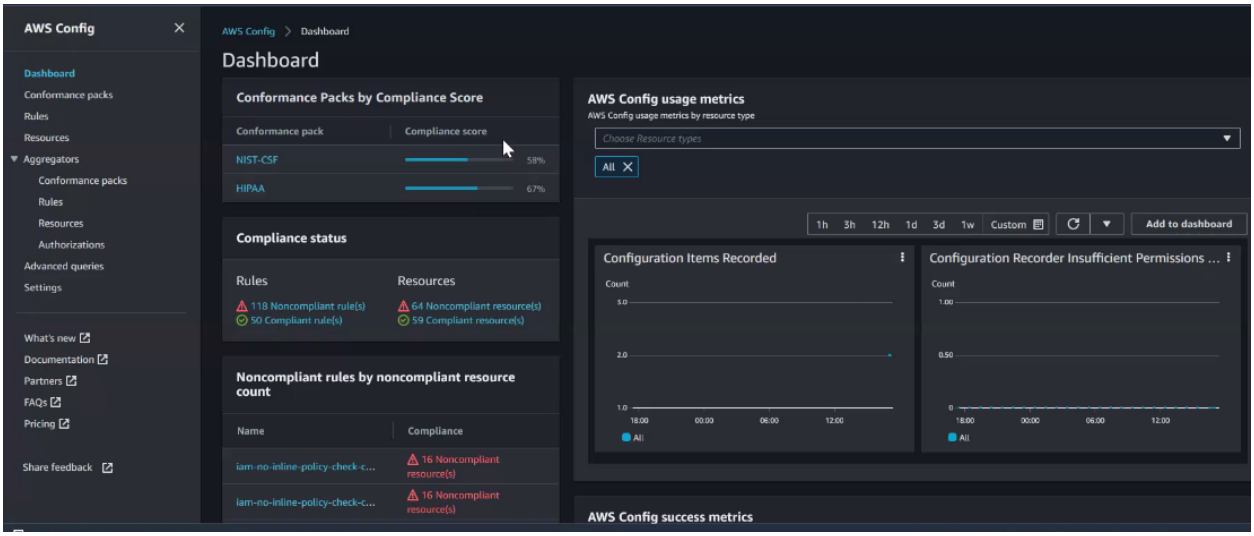
Amazon Inspector

- Scans your resources to help you meet compliance requirements, Identify zero-day vulnerabilities sooner, and prioritize patch remediation.

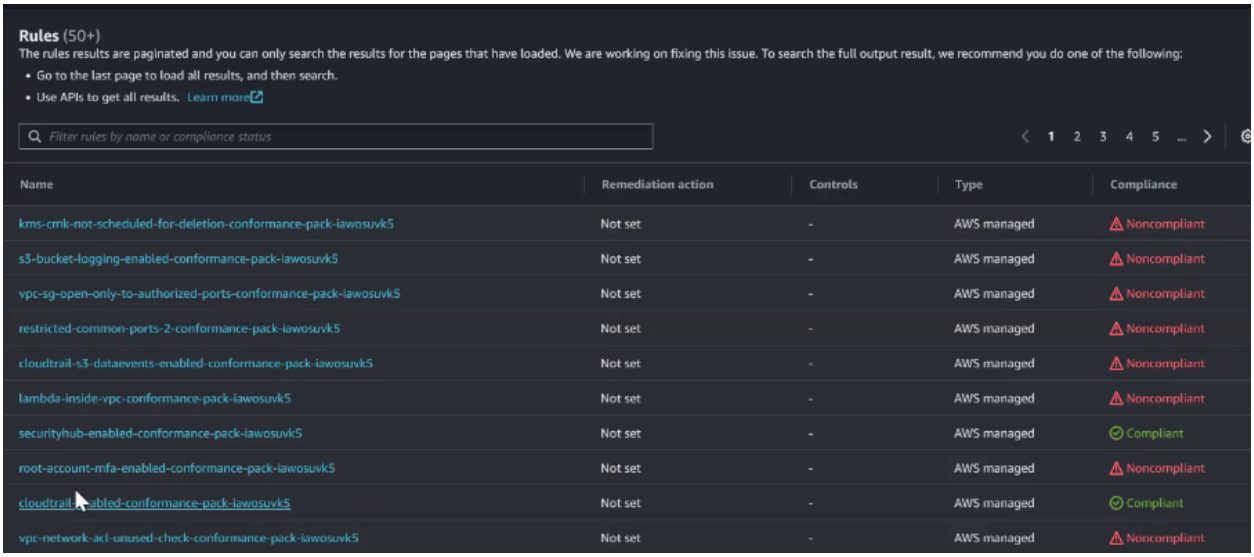
This integrates with AWS organizations, AWS Security Hub, and Amazon EventBridge which can trigger a Lambada function.

AWS Config

- Auto discover resources
- Record the state of a resource
- Track changes; collect historical record of changes
- Evaluate config changes against compliance polices
- Automate remediation activates
- Using SNS to notify you of compliance problems for being compliant or non-compliant



Click on conformance packs can give more so a graphical and rules that will show compliant and noncompliant



You can only have 2 conformance packs at a time. When creating a pack, there are templates you can find.

It may take a full day for deployment status to go to completed to look at everything

AMI Security requirements

AMI security requirements in AWS Marketplace

AWS Marketplace: AMI security requirements

- AMIs must not contain known vulnerabilities or malware.
- AMIs must use current OSs and software packages.
- AMIs must not request or use secret keys.
- Linux-based AMIs must not allow SSH password authentication.
- Instance access must be key pair based (no password-based authorization).

Module 3: Compute Security

Remember…

- Harden against compute vulnerabilities.
  - Hardening with benchmarks
  - AMIs or image security
- Protect data on your instances.
  - Encryption on Amazon EBS
  - AWS Systems Manager for management and maintenance
  - Secure secrets storage
- Detect vulnerabilities.
  - Amazon Inspector
  - AWS Config

Monitoring and Alerting

Module 4

Section 1 of 4

VPC Flow Logs

What they are

VPC Flow Log capture packet metadata like the source IP address, destination IP address, ports, protocol, packet size and other metadata.

- Flow Logs cannot monitor packet contents (payload or application layer data).
- They are not real-time, they use aggregation interval for capture.
- Some types of traffic traversing your network are **NOT** captured by Flow Logs.
- They have no affect on network throughput or latency.

Best practices

- **VPC flow logging should be enabled for packet rejects for all VPCs.**
- Flow logging is instrumental to network traffic investigations.
- AWS Config has a rule to check if a VPC has flow logging enabled.

You can send these logs to S3 or even CloudWatch.

- You can also send in Kiniesis firehose in the same or different account. But since we are thinking of security, the ones above stated would be good

CloudWatch logs would be good cause you can be alerted.

This doesn't help with packet sniffing cause it doesn't have all that detail. But

Traffic Mirroring

- Allows you to get that full packet info. Such as wireshark
- Detect network and security anomalies
    - Detect and respond to attacks more quickly

Logging user and API traffic

Section 2 of 5

CloudTrail Functions

- Simplify compliance audits by automatically recording and storing activity logs for an AWS account.
- Increase visibility into user and resource activity.
- Discover and troubleshoot security and operational issues by capturing a comprehensive history of changes that occurred in an AWS account.

AWS CloudTrail tracks the who, what, where, and when of activity that occurs in your AWS environment and records this activity in audit logs.

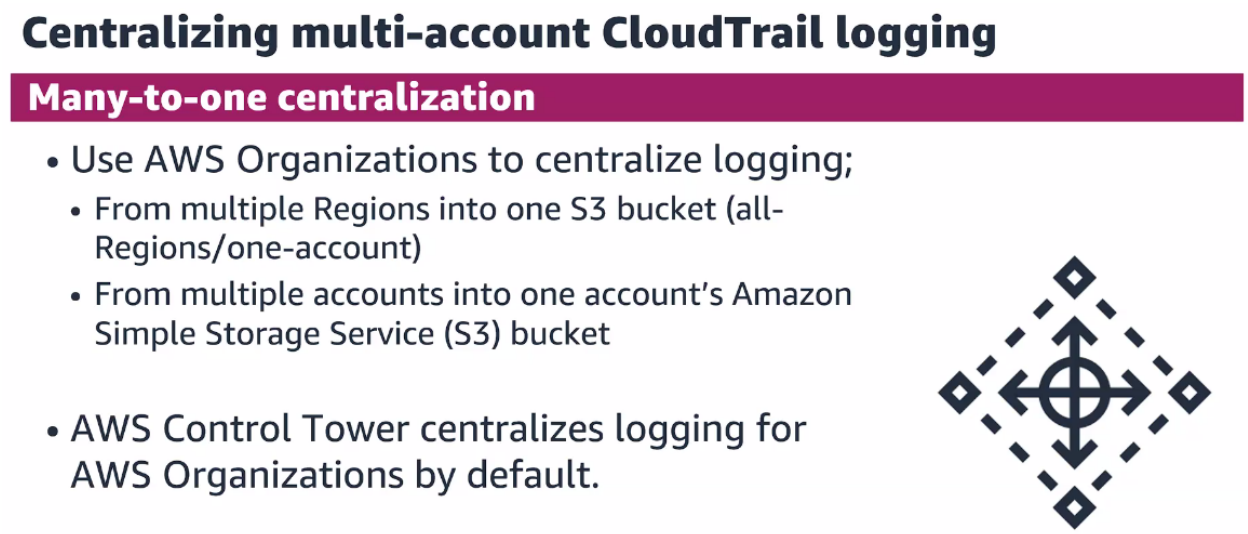
CloudTrail default setting gives you a 7 day window. So that may not be enough for your audit logs. So some cases could be kept for 6 months, maybe a year. So after the 8th day… The logs that were on Monday will be removed.

CloudTrail API call history into log management and analytics solutions

Detect malicious activities and integrate other AWS services to automate remediation. MFA authentication would be good to implement.

*Remember Flow logs will capture network activity

Best practice for CloudTrail



Instead of jumping around, but the cloud trail logs into a single S3 bucket. Just use a dedicated bucket for that.

- Implement least-privilege access to buckets where you store log files
- Enable MFA delete on the log storage bucket
- Limit access to the "AWSCloudTrail_FullAccess" policy
    - That means they can go in and do whatever they want… So limit it

CloudTrail: Lifecycle management

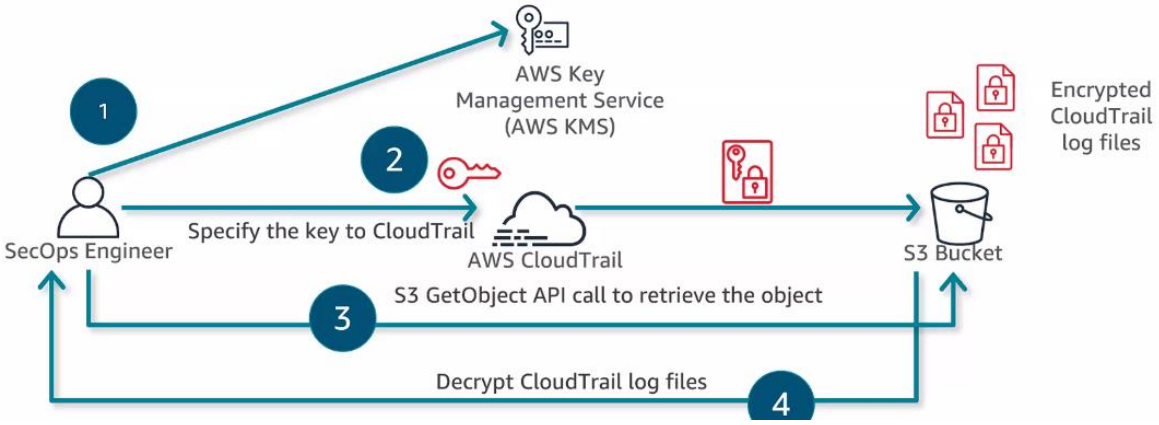
Best practices

- Configured through Amazon S3
- Available actions:
  - Transition to different storage tier
  - Expire (delete) object
  - Transition and expire

CloudTrail confidentiality: AWS KMS encryption

Best practice

- Create or use an existing AWS Key Management Service (KMS) key and apply key policy to allow CloudTrail to encrypt and SecOps engineers to decrypt.



Remember S3 bucket are encrypted by default, but you can go further and use KMS which you can give that key to only the people that actually need it.

https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucket-encryption.html

Enable log integrity validation

Best practice

Once you turn on log file integrity validation, CloudTrail will start delivering digest files on an hourly basis to the same S3 bucket where you receive your CloudTrail log files, but with a different prefix.

- CloudTrail log files are delivered to: /optional_prefix/AWSLogs/AccountID/CloudTrail/*
- CloudTrail digest files are delivered to: /optional_prefix/AWSLogs/AccountID/CloudTrail-Digest/*

Leave the integrity validation as is, make sure it is checked

CloudTrail is integrated with CloudWatch logs because you want to be alerted

Stopped at slide 15/8

You can call GuardDuty for intrusion detection tool. Which shows in detail. It tells you want it finds, but you can tie it with other services. Such as CloudTrail, CloudWatch logs, DNS Logs,