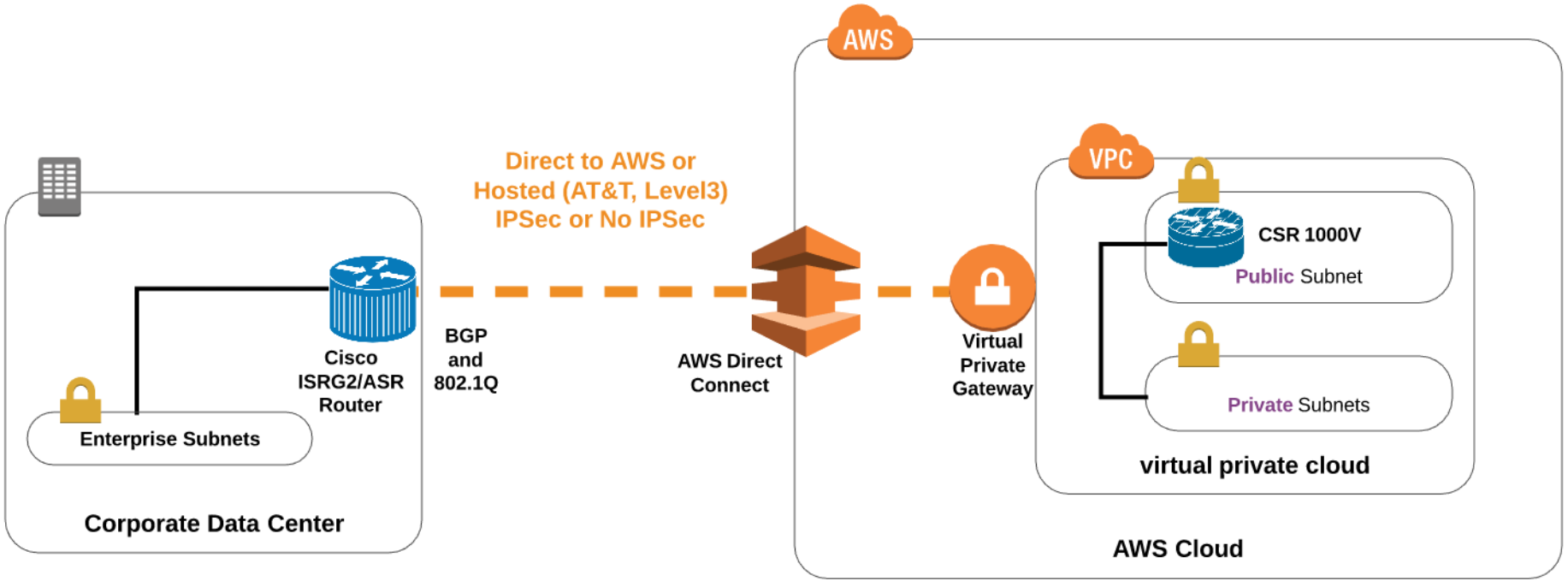
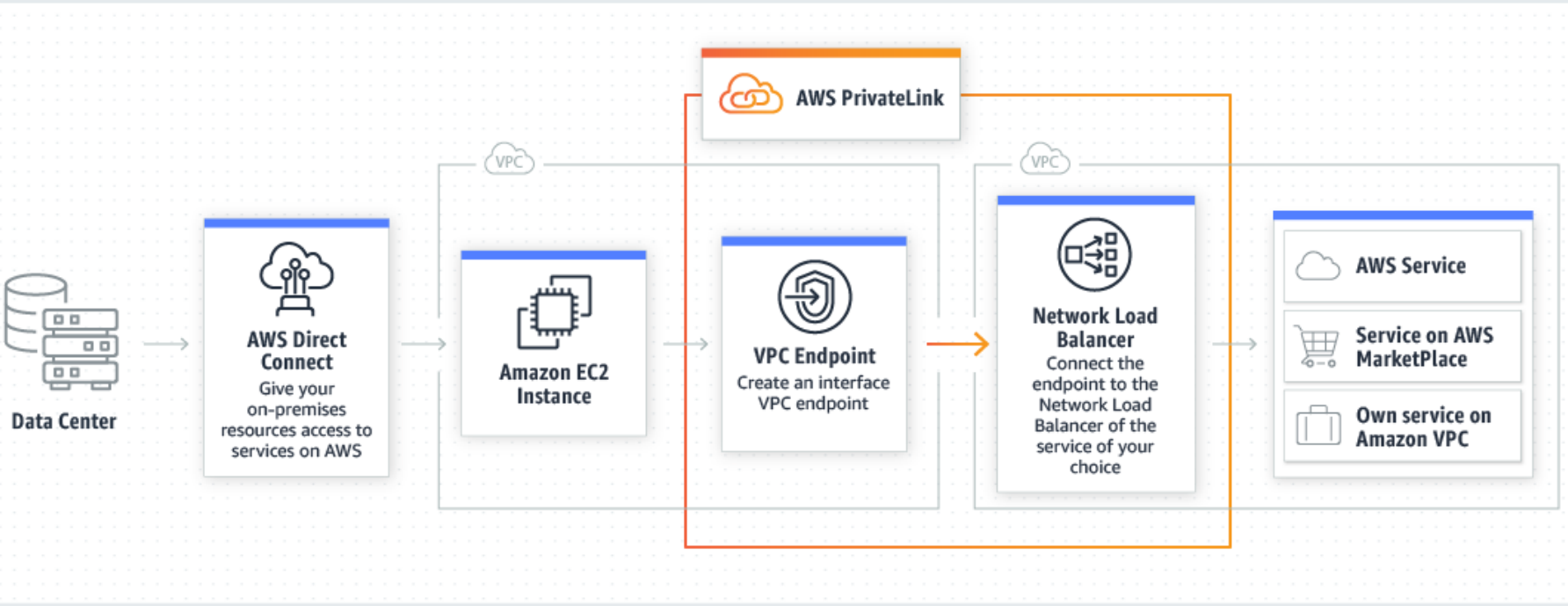
AWS Direct Connect



AWS PrivateLink

- AWS PrivateLink simplifies the security of data shared with cloud-based applications by removing the exposure of the public Internet
- PrivateLink offers isolated connectivity between VPCs, AWS services, and on-premises applications, securely on the Amazon network infrastructure
- PrivateLink makes it easy to connect services across different accounts and VPCs to considerably streamline the network architecture

AWS PrivateLink



@aws.amazon.com

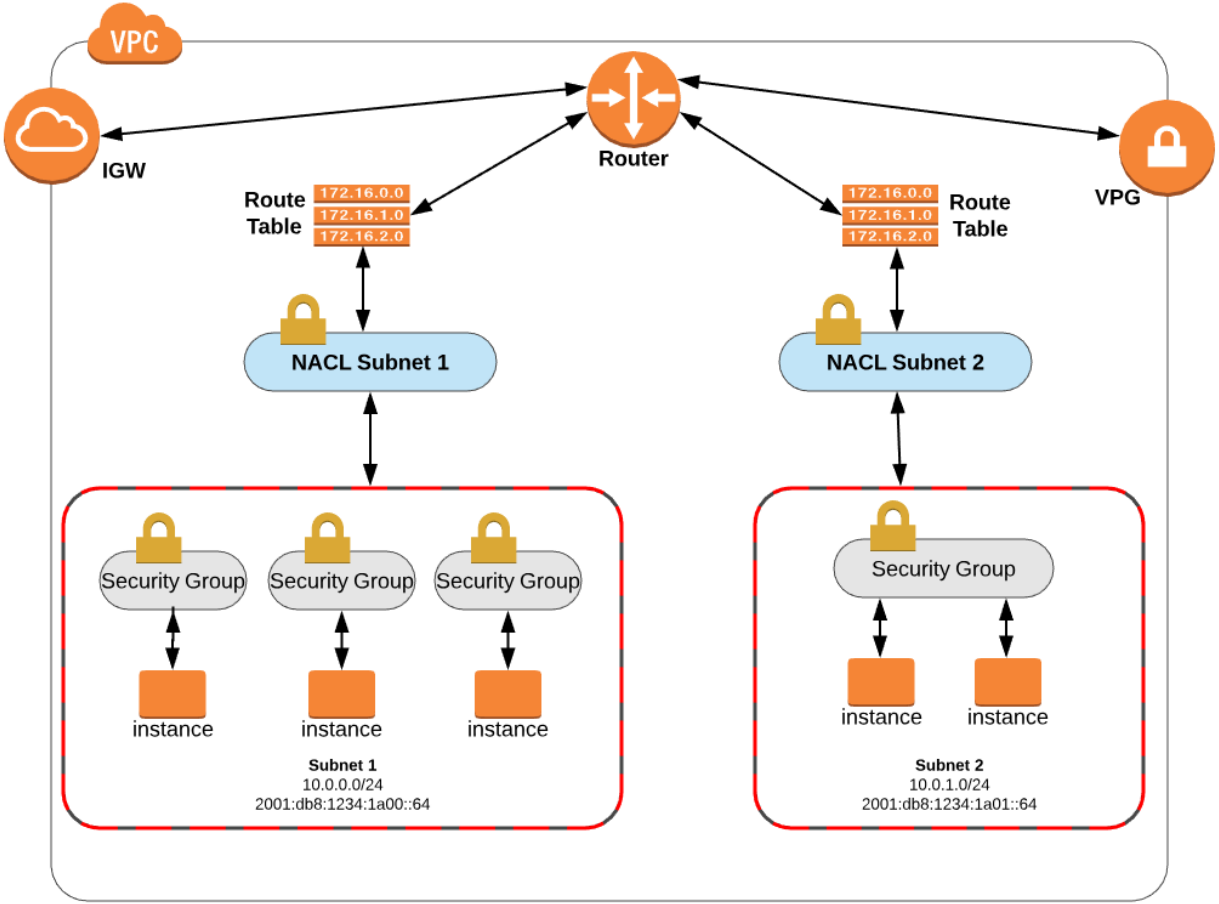
AWS Transit Gateway

- **AWS Transit Gateway** allows customers to connect their VPCs and their on-premises networks to a single gateway
- You can easily to scale your networks across multiple accounts and Amazon VPCs to keep up with growth
- You only need to create and manage a single connection (hub) from the central gateway to each VPC, on-premises data center, or remote office across your network
- Any new VPC is simply connected to the Transit Gateway and is then automatically available to every other network that is connected to the Gateway

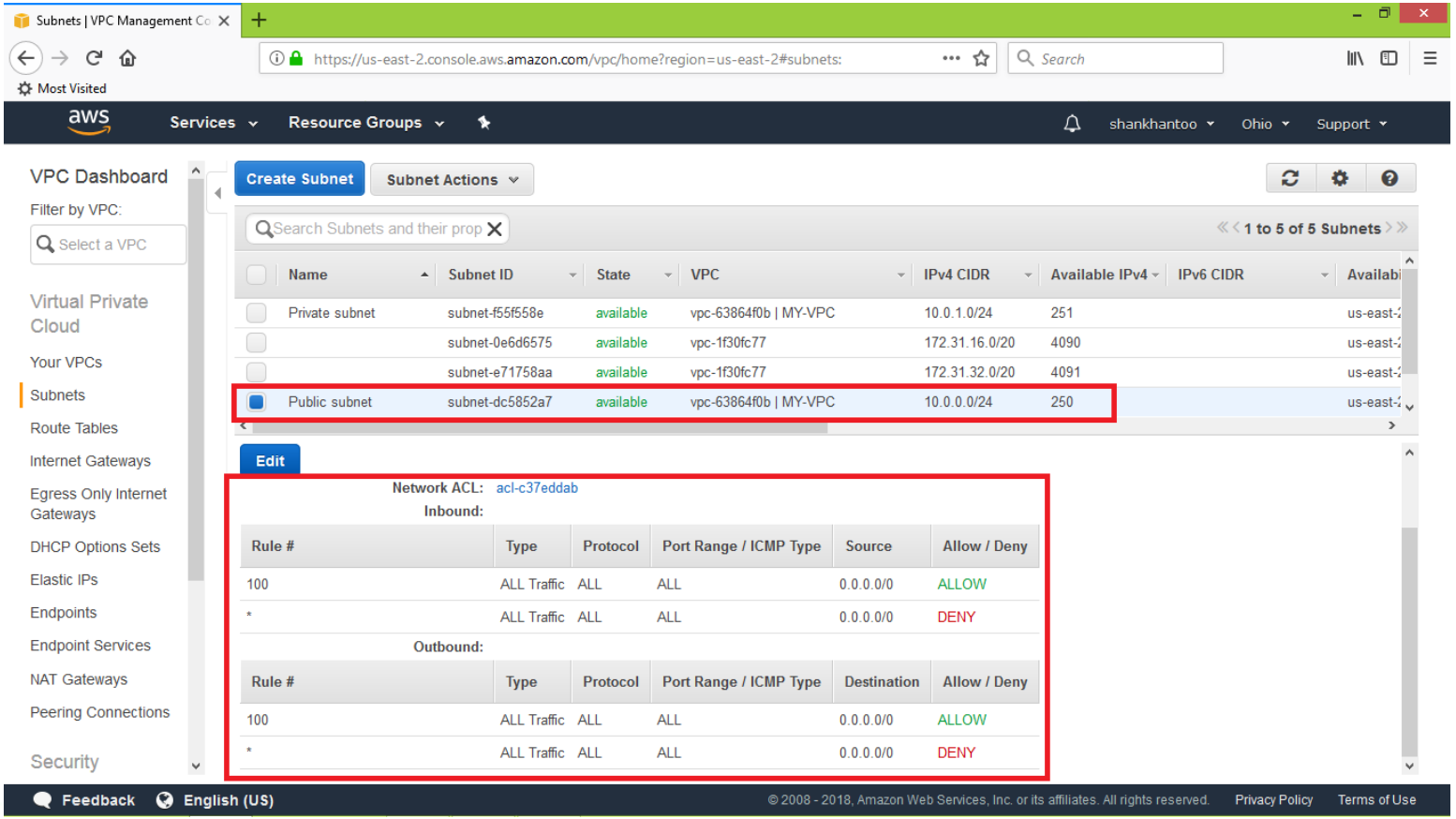
Network ACLs

- NACLs allow stateless traffic filtering and management of IPv4 and IPv6 traffic
- Applies to all inbound OR outbound traffic from a subnet within a VPC
- Can contain ordered rules (ACE's) to permit or deny based on IP protocol (for example GRE, IPSec ESP, ICMP), service port, and source/destination IP address
- NACLs are agnostic of TCP and UDP sessions
- NACLs work in conjunction with security groups and can permit or deny traffic before it reaches the security group

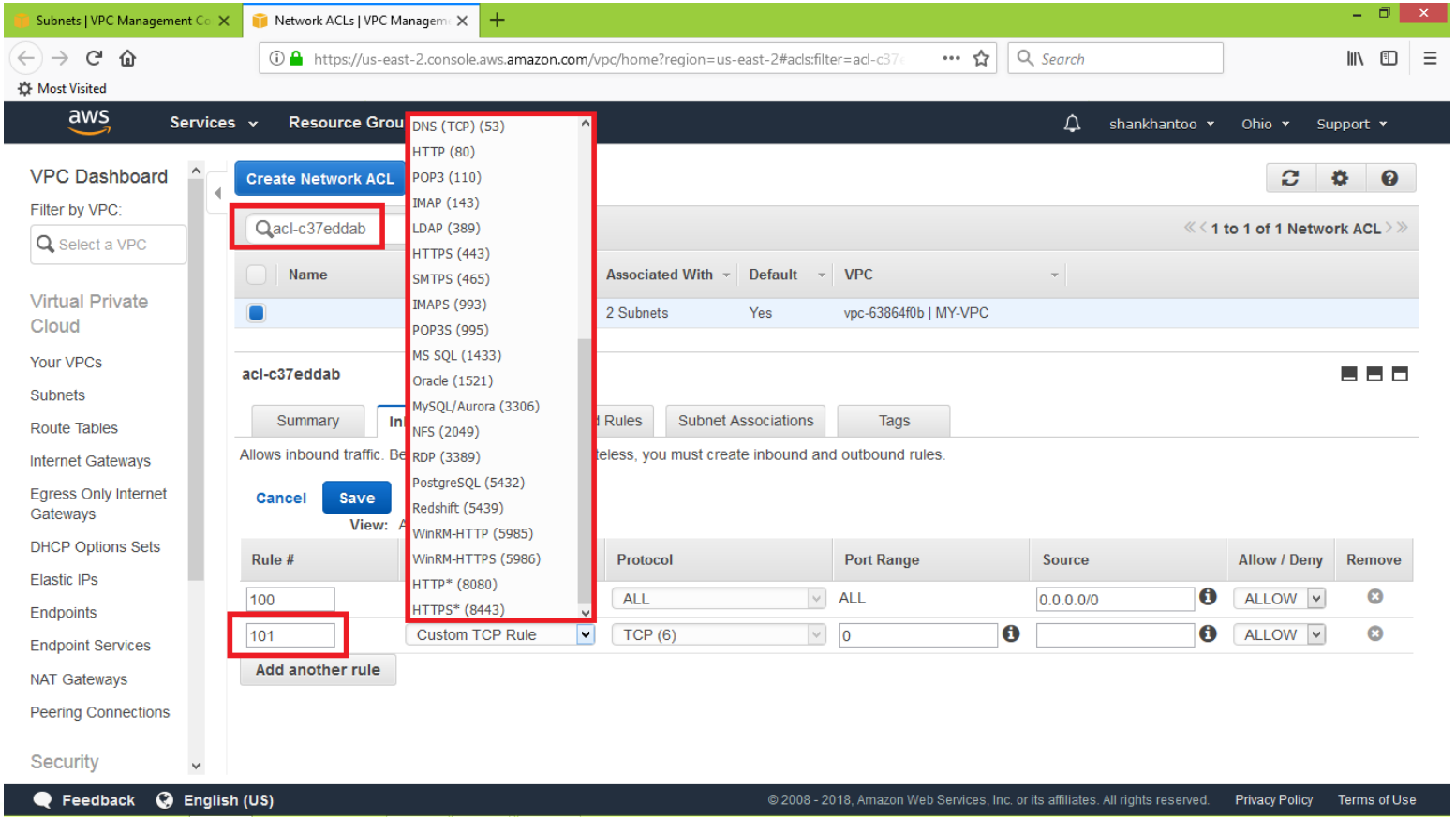
NACLs and Security Groups



NACLs

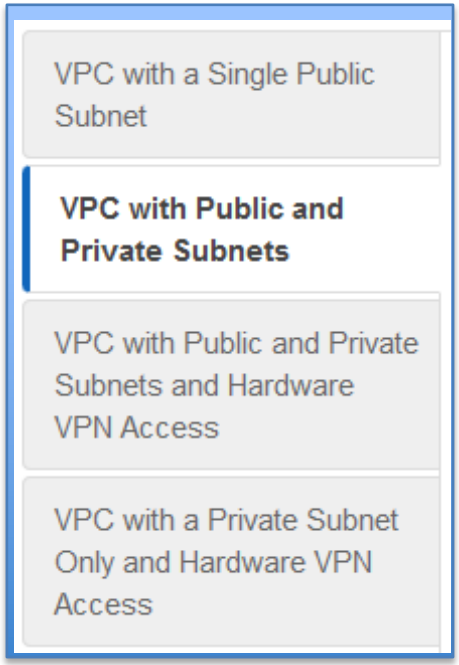

Subnets | VPC Management Co
https://us-east-2.console.aws.amazon.com/vpc/home?region=us-east-2#subnets:
Search
Most Visited
aws
Services
Resource Groups
shankhantoo
Ohio
Support
VPC Dashboard
Filter by VPC:
Select a VPC
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
Egress Only Internet Gateways
DHCP Options Sets
Elastic IPs
Endpoints
Endpoint Services
NAT Gateways
Peering Connections
Security
Create Subnet
Subnet Actions
Search Subnets and their prop
1 to 5 of 5 Subnets
Name
Subnet ID
State
VPC
IPv4 CIDR
Available IPv4
IPv6 CIDR
Private subnet subnet-f55f558e available vpc-63864f0b | MY-VPC 10.0.1.0/24 251
subnet-0e6d6575 available vpc-1f30fc77 172.31.16.0/20 4090
subnet-e71758aa available vpc-1f30fc77 172.31.32.0/20 4091
Public subnet subnet-dc5852a7 available vpc-63864f0b | MY-VPC 10.0.0.0/24 250
Edit
Network ACL: acl-c37eddab
Inbound:
Rule # Type Protocol Port Range / ICMP Type Source Allow / Deny
100 ALL Traffic ALL ALL 0.0.0.0/0 ALLOW
* ALL Traffic ALL ALL 0.0.0.0/0 DENY
Outbound:
Rule # Type Protocol Port Range / ICMP Type Destination Allow / Deny
100 ALL Traffic ALL ALL 0.0.0.0/0 ALLOW
* ALL Traffic ALL ALL 0.0.0.0/0 DENY
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

NACLs



NACL Recommendations

- AWS Documentation » **Amazon Virtual Private Cloud » User Guide** » Security » Recommended Network ACL Rules for Your VPC



ACL Rules for the Public Subnet

Inbound					
Rule #	**Source IP**	**Protocol**	**Port**	**Allow/Deny**	**Comments**
100	0.0.0.0/0	TCP	80	ALLOW	Allows inbound HTTP traffic from any IPv4 address.
110	0.0.0.0/0	TCP	443	ALLOW	Allows inbound HTTPS traffic from any IPv4 address.
120	Public IP address range of your home network	TCP	22	ALLOW	Allows inbound SSH traffic from your home network (over the Internet gateway).
130	Public IP address range of your home network	TCP	3389	ALLOW	Allows inbound RDP traffic from your home network (over the Internet gateway).
140	0.0.0.0/0	TCP	1024-65535	ALLOW	Allows inbound return traffic from hosts on the Internet that are responding to requests originating in the subnet. This range is an example only. For information about choosing the correct ephemeral ports for your configuration, see Ephemeral Ports.
*	0.0.0.0/0	all	all	DENY	Denies all inbound IPv4 traffic not already handled by a preceding rule (not modifiable).

Security Groups

- A security group is a virtual layer 3/4 **stateful** firewall that controls the (whitelisted only) traffic flow for its associated instances
- SGs operate at the hypervisor level for all EC2 instances and other VPC objects
- All EC2 instances are launched with the default SG unless a user-defined SG is specified when spun up
- An unchanged default SG will **permit** communication between all resources within the security group AND allows all outbound traffic
- All other traffic is implicitly denied

Security Groups

- Security groups are stateful—if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules
- IOW, Responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules
- You add the inbound rules to control incoming traffic to the instance and outbound rules to control the outgoing traffic from your instance
- Remember: You can specify allow rules, but not deny rules

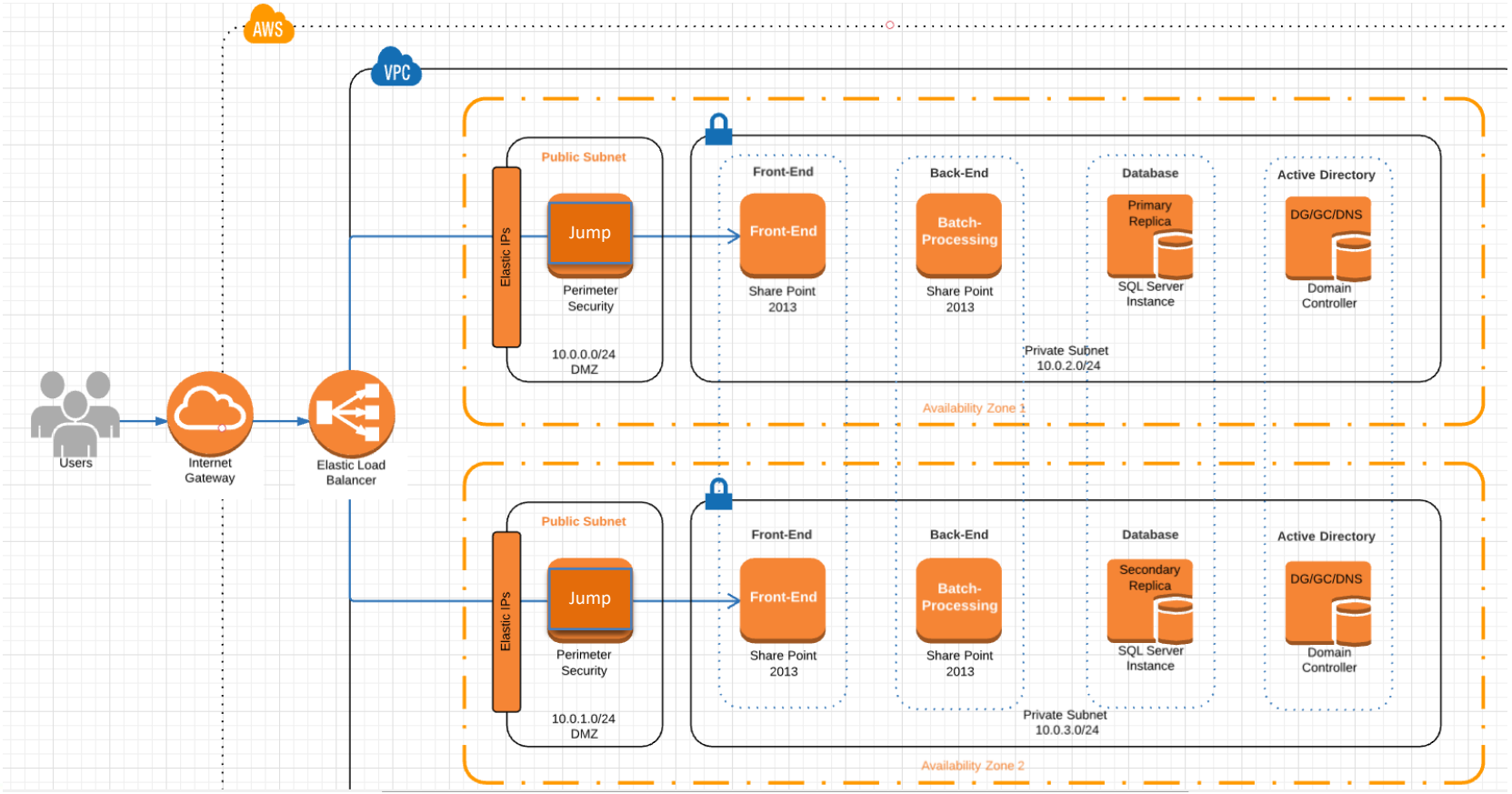
Security Groups

- To associate a security group with an instance, it is best practice to specify the security group when you launch the instance
- When **you** create a security group, it has no inbound rules. Therefore, no inbound traffic originating from another host to your instance is allowed until you add inbound rules to the security group
- By default, an SG includes an outbound rule that allows all outbound traffic but no inbound traffic is allowed until you add inbound rules to the security group

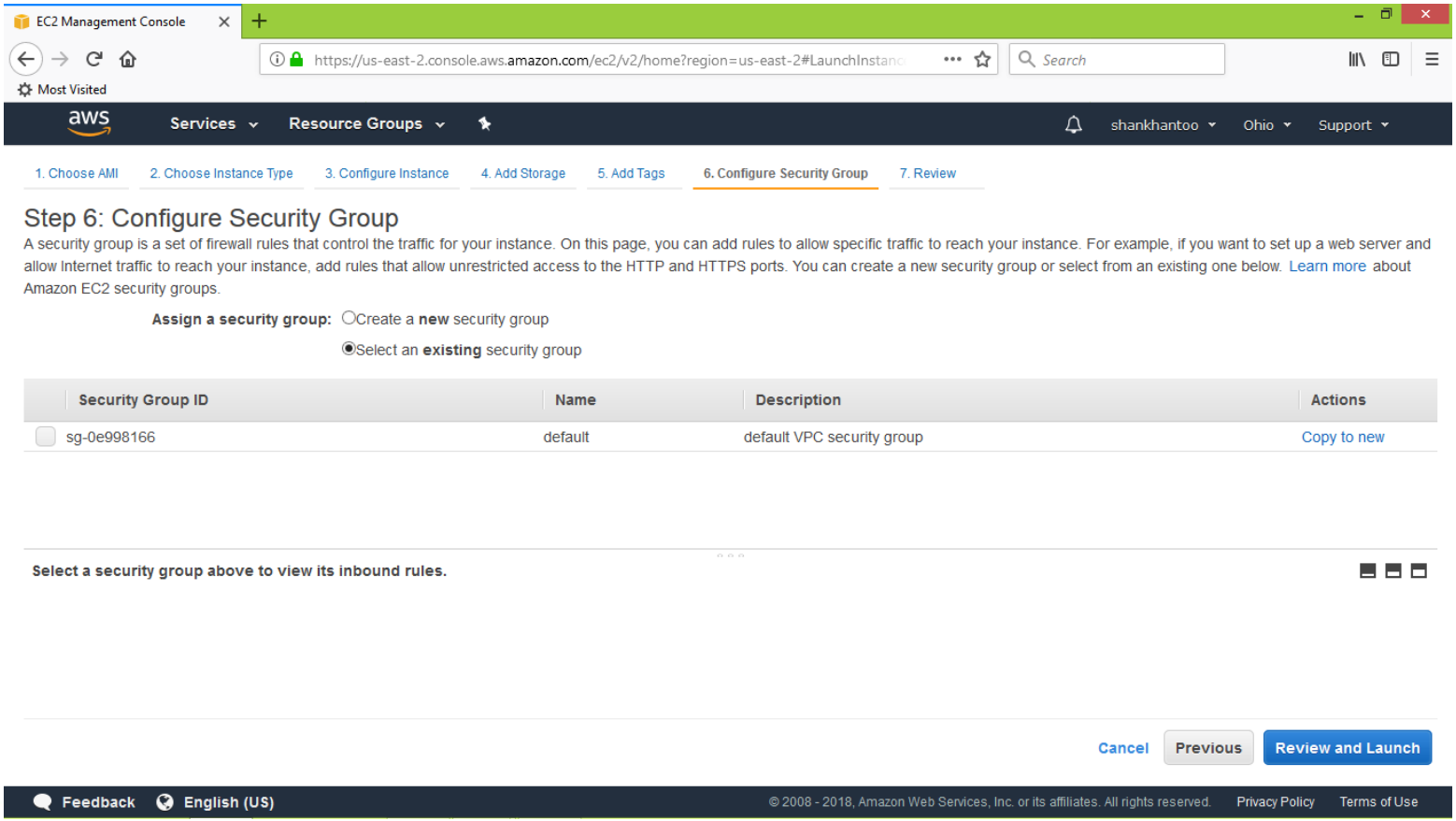
Comparing Security Groups and NACLs

Network ACL	Security Group
Functions at the network level	Functions at the instance level
Supports allow and deny rules	Supports allow rules only (whitelisting)
Stateless so return traffic must be explicitly allowed	Stateful so that return traffic is automatically allowed
Rules are processed in a numbered order	All rules are evaluated before deciding to allow traffic
Applies automatically to all of the instances in the associated subnet	Applies to the instance only

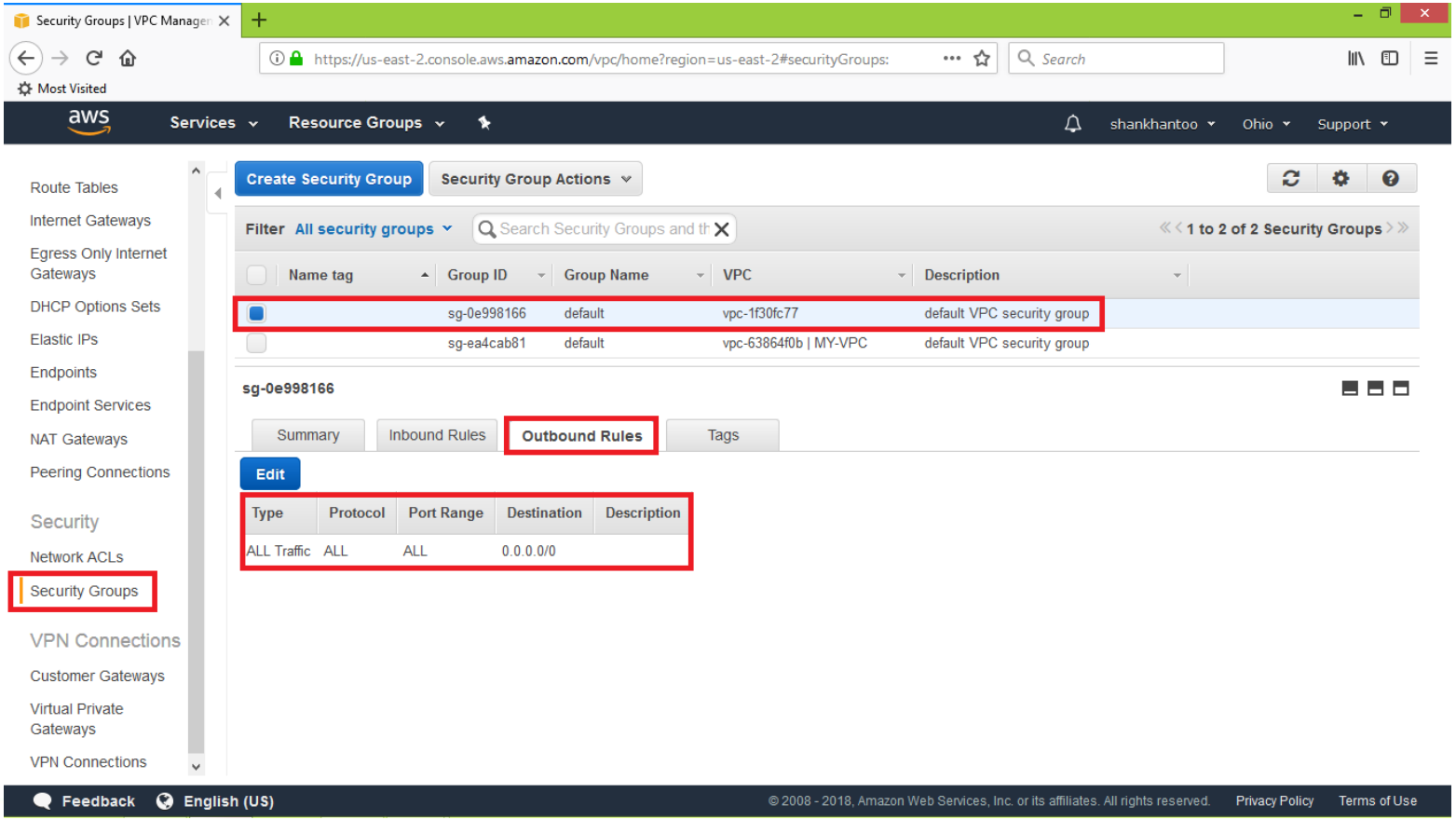
SG Defense-in-Depth



Assign a Security Group



Default Security Group

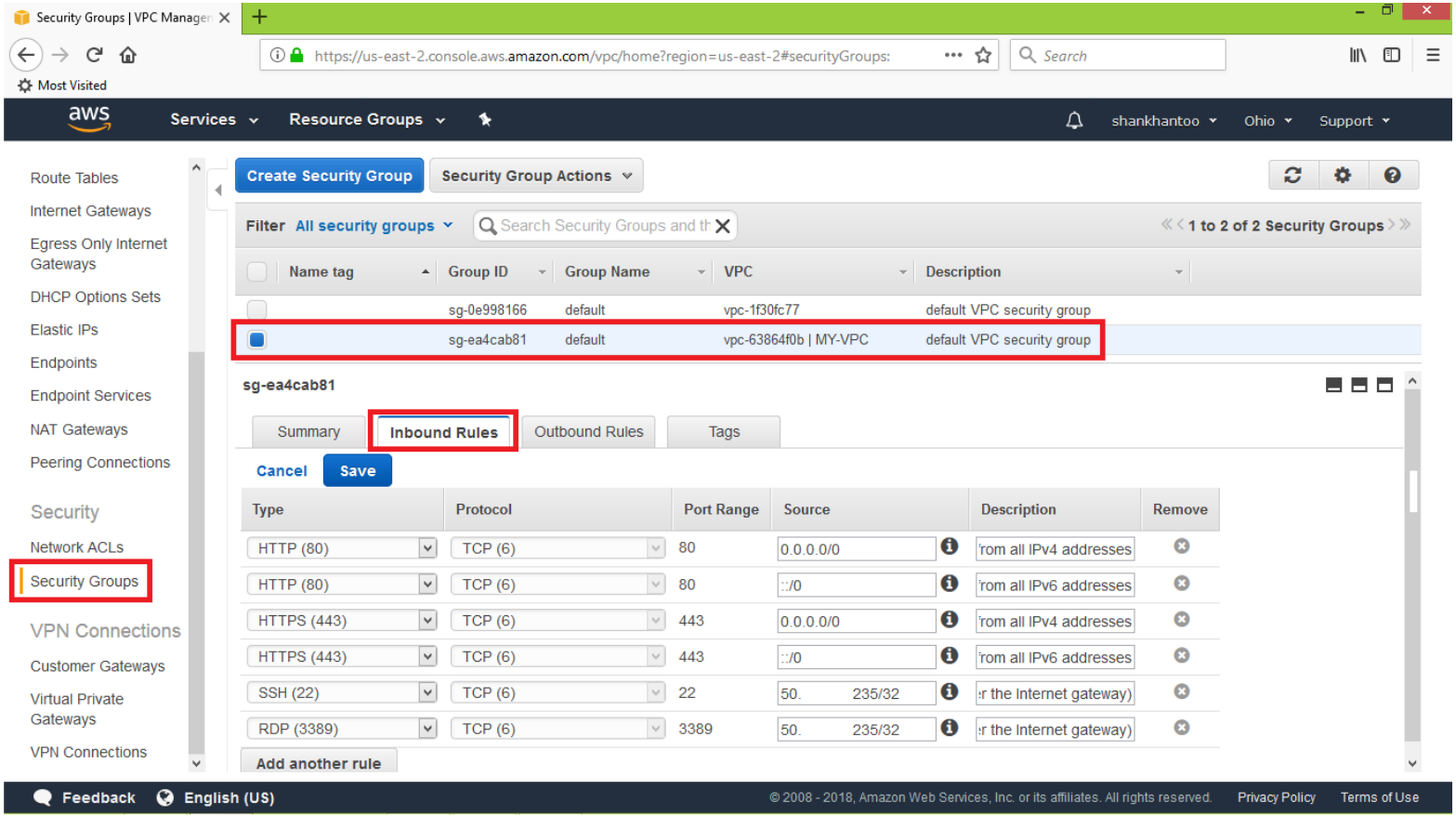


Pearson

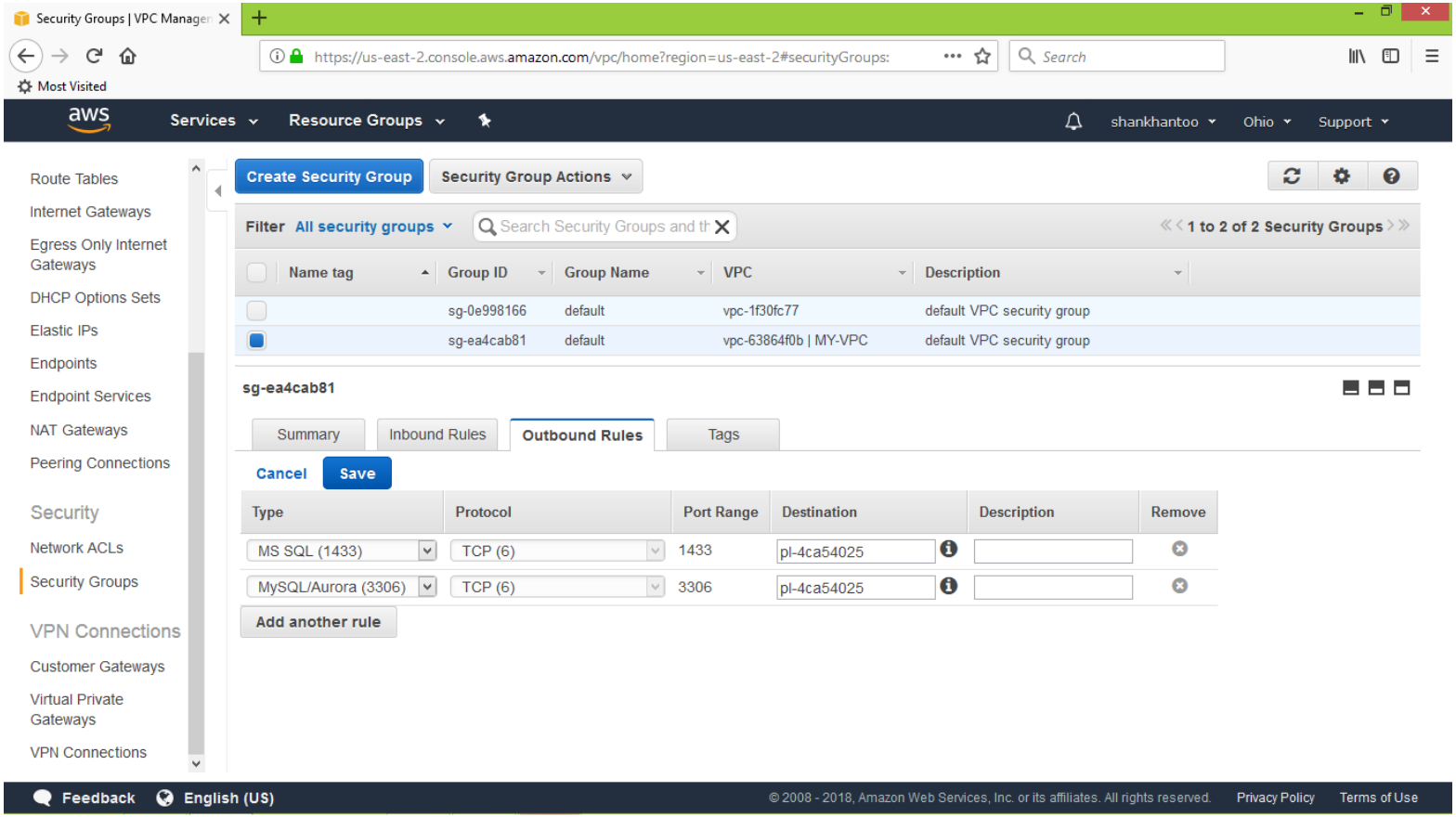
Default Security Group

Inbound			
Source	**Protocol**	**Port Range**	**Comments**
The security group ID (sg-*xxxxxxxx*)	All	All	Allow inbound traffic from instances assigned to the same security group.
Outbound			
Destination	**Protocol**	**Port Range**	**Comments**
0.0.0.0/0	All	All	Allow all outbound IPv4 traffic.
::/0	All	All	Allow all outbound IPv6 traffic. This rule is added by default if you create a VPC with an IPv6 CIDR block or if you associate an IPv6 CIDR block with your existing VPC.

Inbound Rules to Web Servers



Outbound Rules to Web Servers



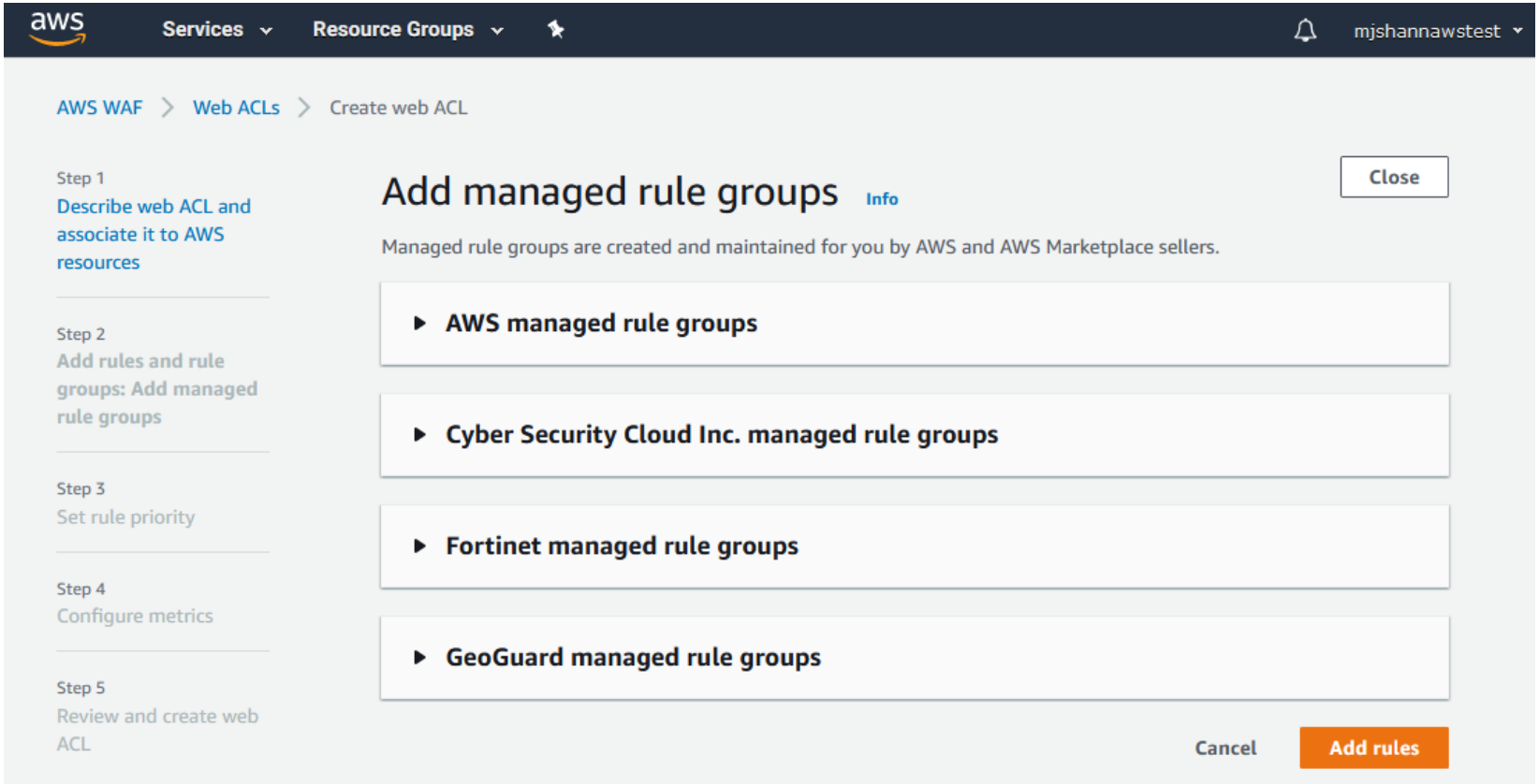
Segment 4: AWS WAF, Shield Advanced, and GuardDuty

AWS Web Application Firewall (WAF)

- AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests forwarded to Amazon CloudFront or an ELB Application Load Balancer

- At a basic level WAF can:
  - Allow all requests except for ones you designate (permissive)
  - Block all requests except for ones you designate (restrictive)
  - Count the requests that match the properties that you specify (monitor mode before deployment)

Using Managed Rule Groups



Using Managed Rule Groups

Name	Capacity	Action
Admin protection Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application.	100	Add to web ACL
Amazon IP reputation list This group contains rules that are based on Amazon threat intelligence. This is useful if you would like to block sources associated with bots or other threats.	25	Add to web ACL
Core rule set Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP publications and common Common Vulnerabilities and Exposures (CVE).	700	Add to web ACL
Known bad inputs Contains rules that allow you to block request patterns that are known to be invalid and are associated with exploitation or discovery of vulnerabilities. This can help reduce the risk of a malicious actor discovering a vulnerable application.	200	Add to web ACL
Linux operating system Contains rules that block request patterns associated with exploitation of vulnerabilities specific to Linux, including LFI attacks. This can help prevent attacks that expose file contents or execute code for which the attacker should not have had access.	200	Add to web ACL
PHP application		

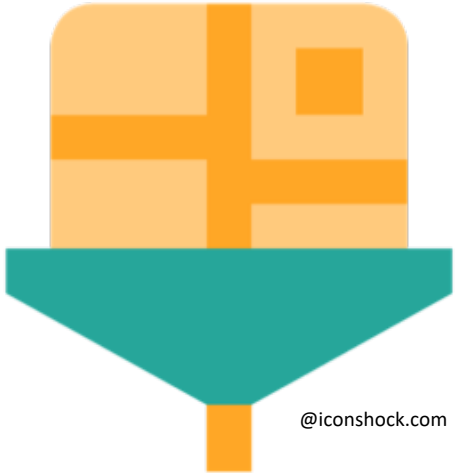
WAF Matching Attributes

- IP addresses of originating requests
- Country that requests originate from
- Values in request headers
  (e.g. User-Agent, Content-Type)
- Literal or regex string patterns that appear in requests (e.g. [cC][mM][dD].[eE][xX][eE])
- Length of requests (buffer overflows)
- Presence of SQL injection code that is likely to be malicious
- Presence of a malicious cross-site scripting attack

@iconshock.com

WAF Matching Attributes

- Rules that can allow, block, or count web requests that meet the specified conditions
- Rules can block or count web requests that meet or exceed a specified number of requests in any 5-minute period
- Rules that you can reuse for multiple web applications
- Real-time metrics and sampled web requests
- Automated administration using



WAF Rules

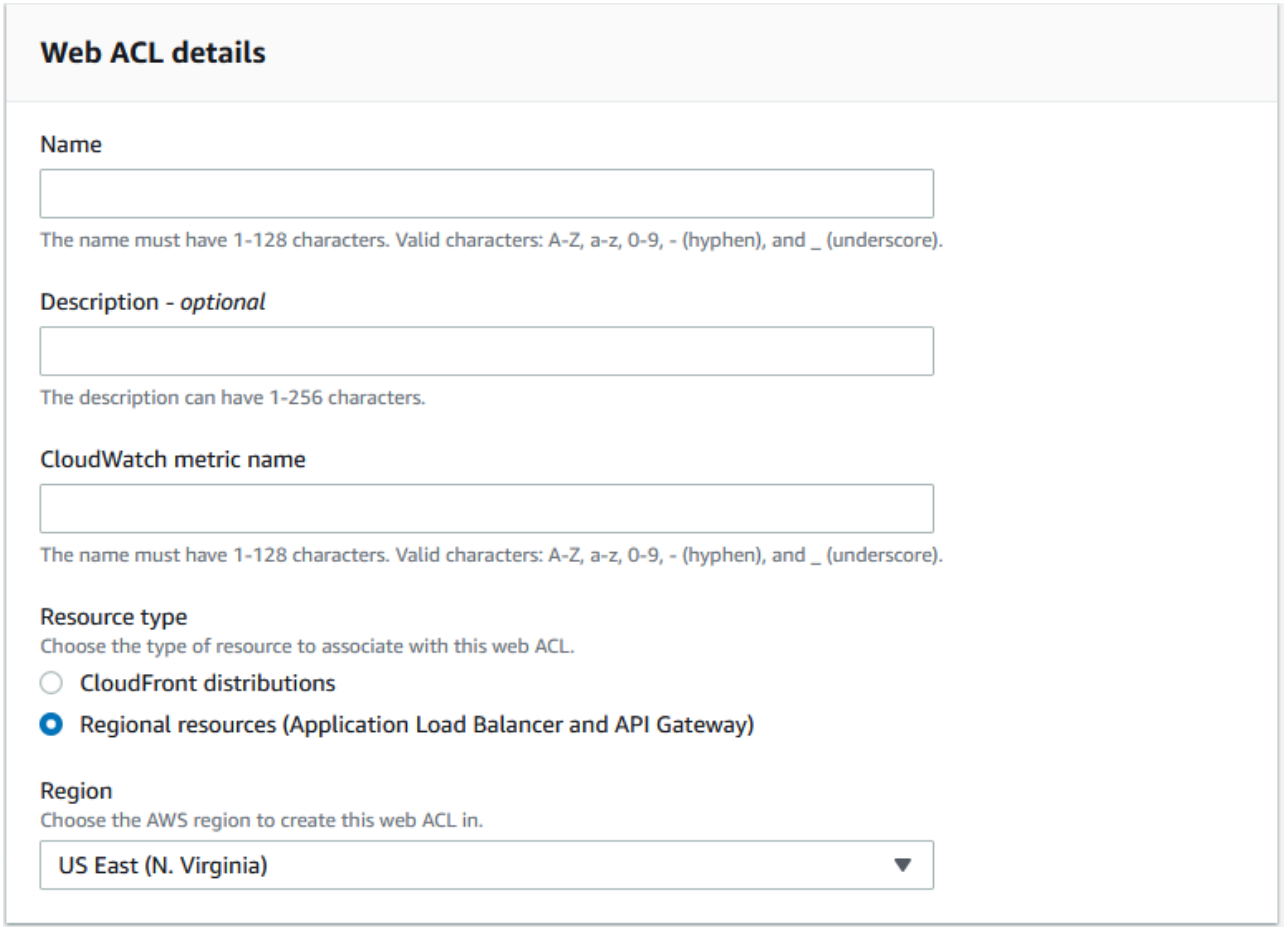
- **Regular rules** use only conditions to target specific requests
  - The requests come from 192.168.2.55
  - They contain the value EvilBot in the User-Agent header
  - They appear to include SQL-like code in the query string
- **Rate-based Rules** are similar to regular rules, with one addition: a rate limit
  - They count the requests that arrive from a specified IP address every five minutes
  - The rule can trigger an action if the number of requests exceed the rate limit

Web ACLs

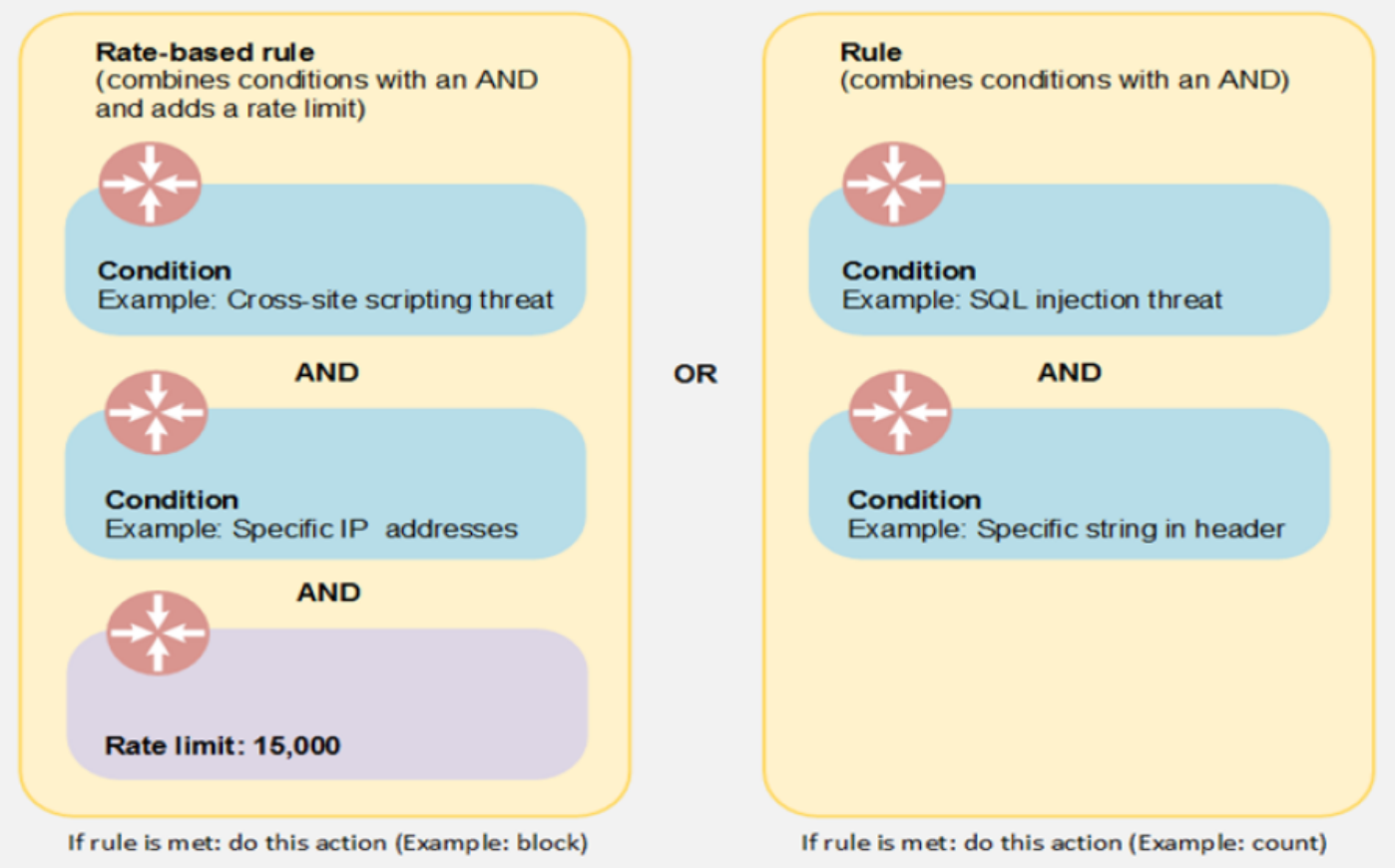
- After you combine your conditions into rules, you combine the rules into a web ACL
- This is where you define an action for each rule—allow, block, or count—**and a default action**

@iconshock.com

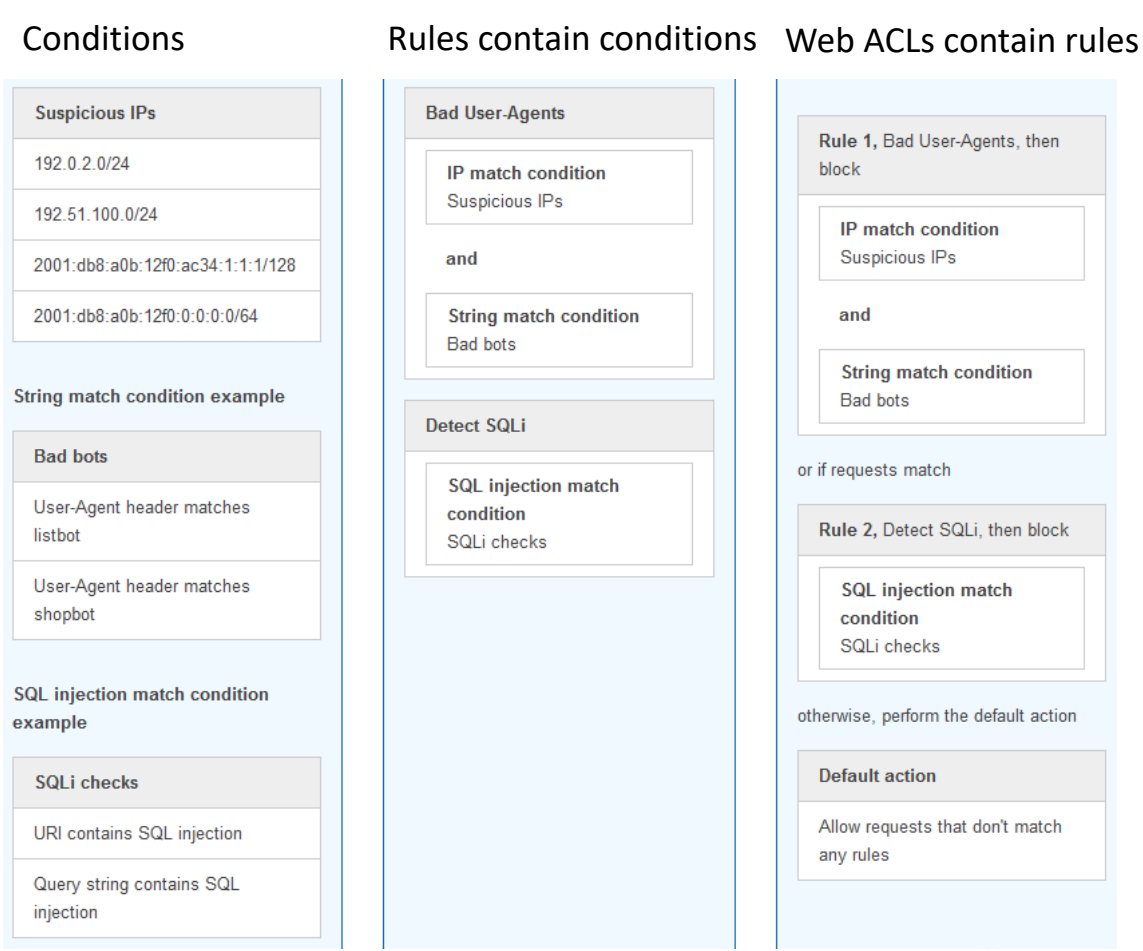
AWF WAF Configuration



Web ACL



WAF Configuration Basics



AWF WAF Configuration

Create conditions

Conditions specify the filters that you want to use to allow or block requests that are forwarded to AWS resources such as Amazon CloudFront distributions.

Cross-site scripting match conditions

Name	Create condition
You don't have any cross-site scripting match conditions. Choose **Create XSS match condition** to get started.	

A cross-site scripting match condition specifies the parts of a web request (such as a User-Agent header) that you want AWS WAF to inspect for cross-site scripting threats. Learn more

Geo match conditions

Name	Create condition
You don't have any geo match conditions. Choose **Create condition** to get started.	

A geo match condition lets you allow, block, or count web requests based on the geographic origin of the request. Learn more

Concepts overview

Web ACL example
if requests match

Rule 1, Bad User-Agents, then block

IP match condition
Suspicious IPs

and

String match condition
Bad bots

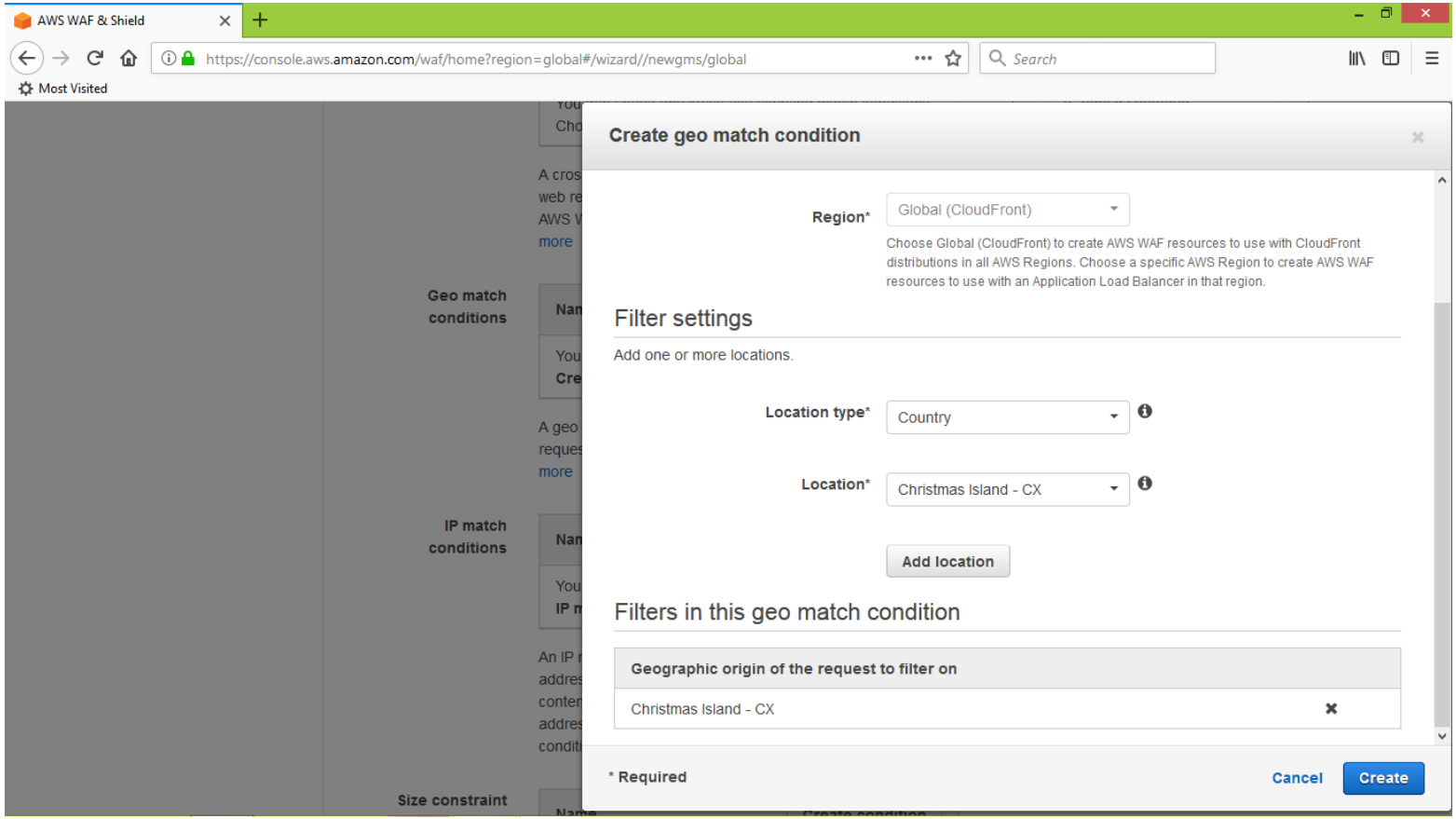
or if requests match

Rule 2, Detect SQLi, then block

SQL injection match condition
SQLi checks

otherwise, perform the default action

Geo Match Condition



AWF WAF Configuration

IP match conditions

Name	Create condition
You don't have any IP match conditions. Choose **Create IP match condition** to get started.	

An IP match condition specifies the IP addresses and/or IP address ranges that you want to use to control access to your content. Put IP addresses that you want to allow and IP addresses that you want to block into separate IP match conditions. Learn more

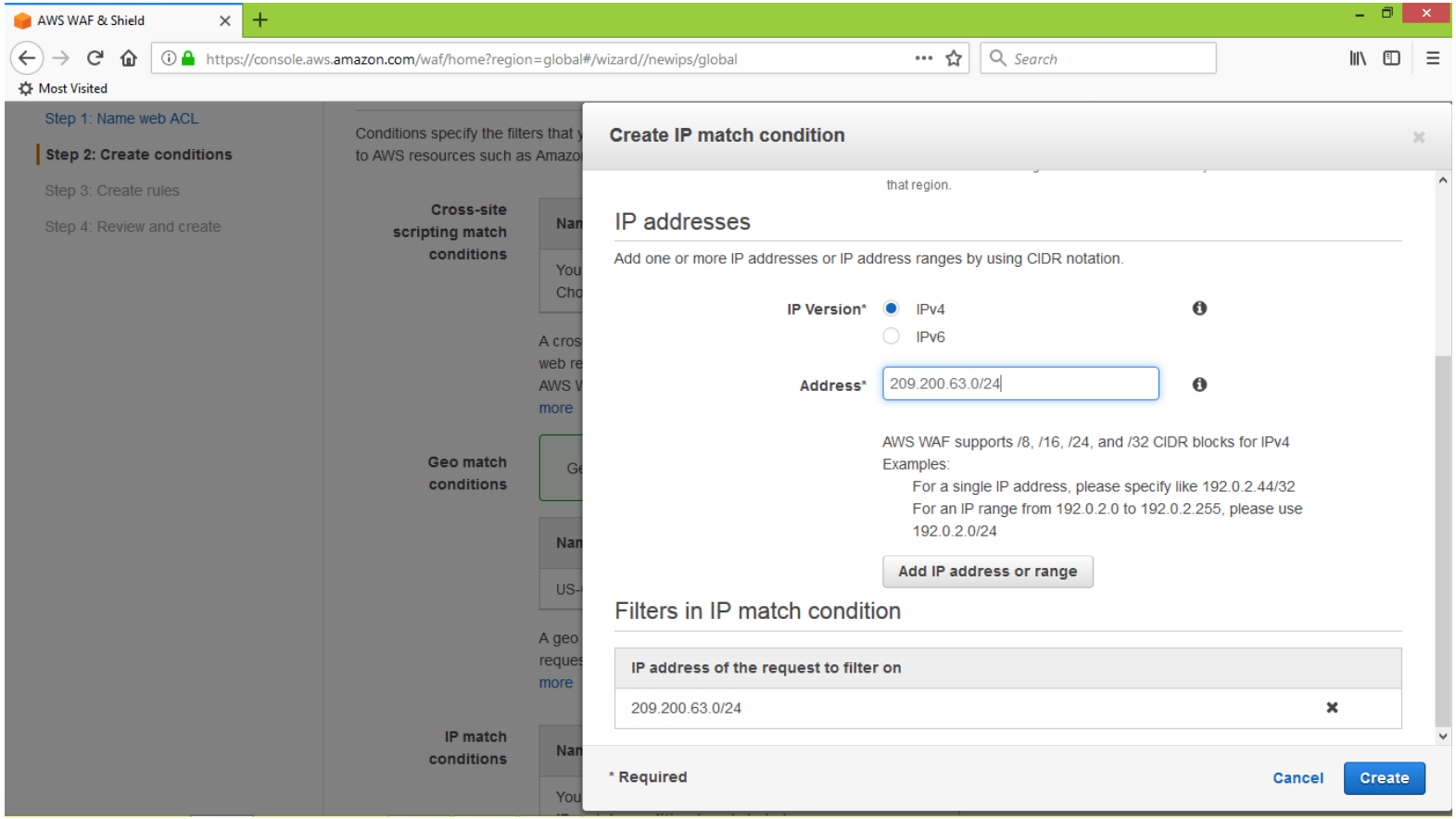
Size constraint conditions

Name	Create condition
You don't have any size constraint conditions. Choose **Create size constraint condition** to get started.	

A size constraint condition specifies the parts of a web request (such as a User-Agent header) that you want AWS WAF to compare to a set size. Learn more

Default action
Allow requests that don't match any rules

IP Match Condition



AWF WAF Configuration

SQL injection match conditions

Name	Create condition
You don't have any SQL injection match conditions. Choose **Create SQL injection match condition** to get started.	

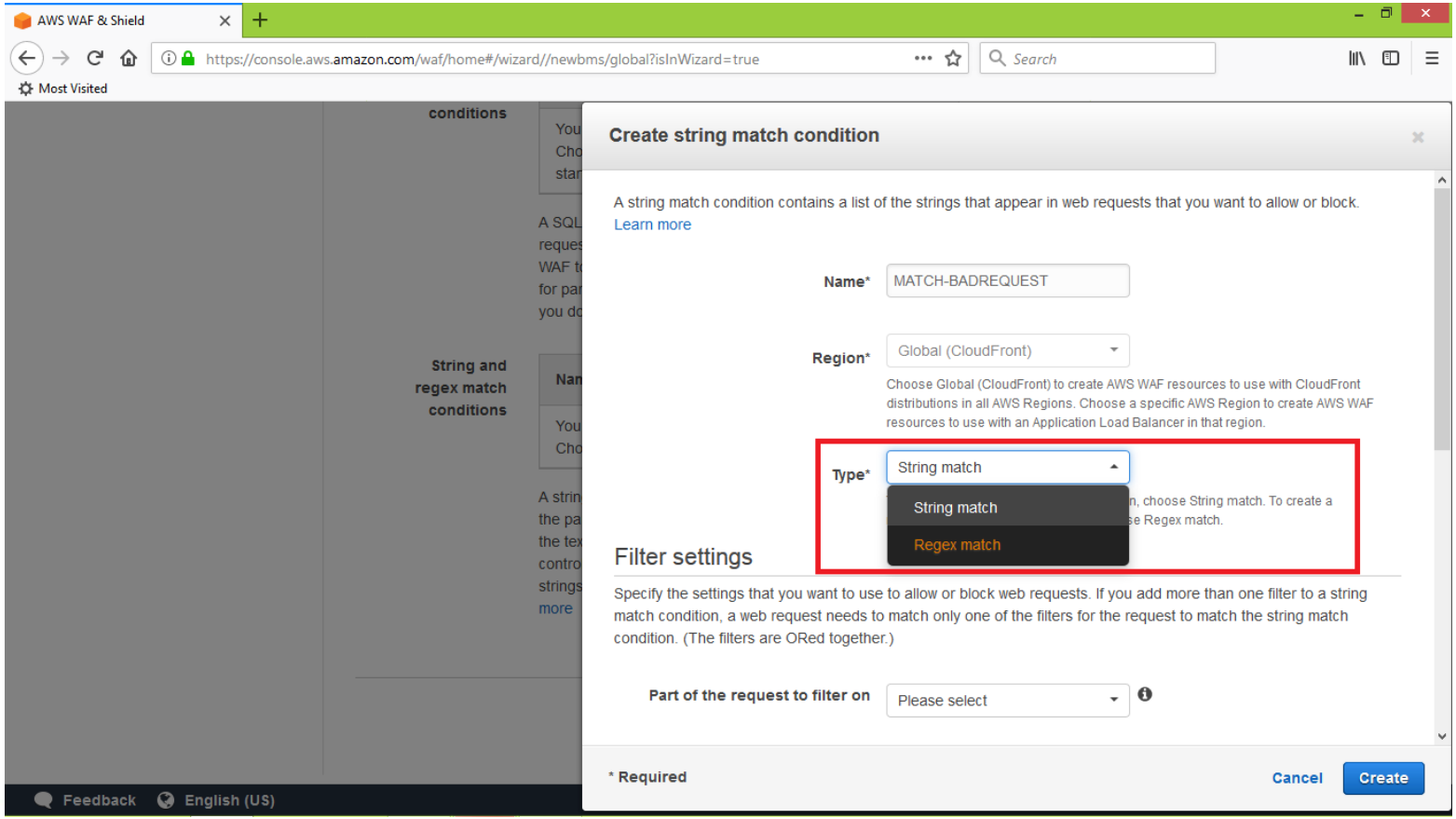
A SQL injection match condition specifies the parts of a web request (such as a User-Agent header) that you want AWS WAF to inspect for SQL queries. Create separate conditions for parts that you want to allow SQL queries in and parts that you don't. Learn more

String and regex match conditions

Name	Create condition
You don't have any string or regex match conditions. Choose **Create condition** to get started.	

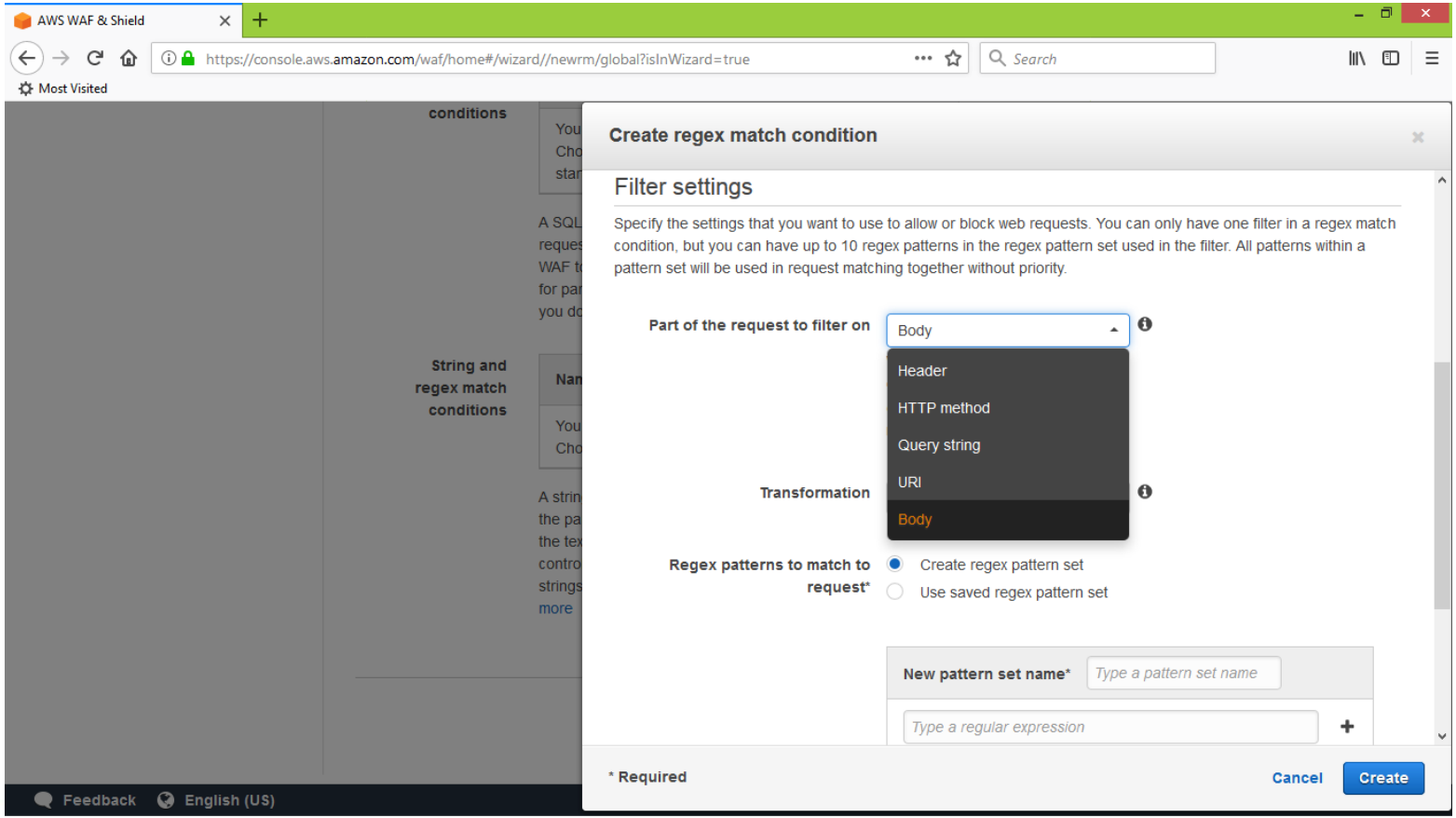
A string match condition, or a regex match condition, specifies the part of a web request (such as a User-Agent header) and the text (the value of the header) that you want to use to control access to your content. Create separate conditions for strings or regex patterns that you want to allow or block. Learn more

Regex Match Condition

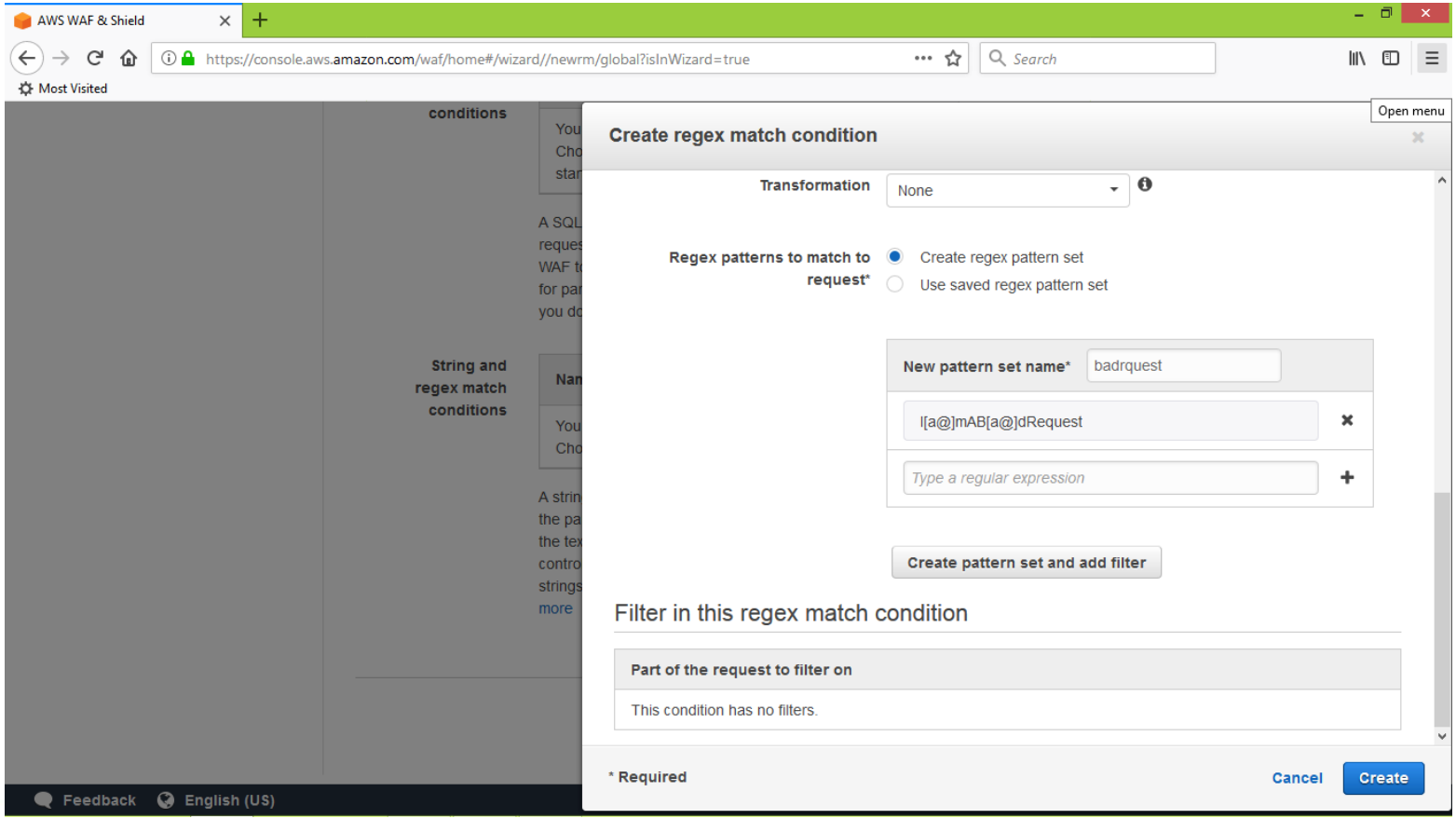


Pearson

Regex Match Condition

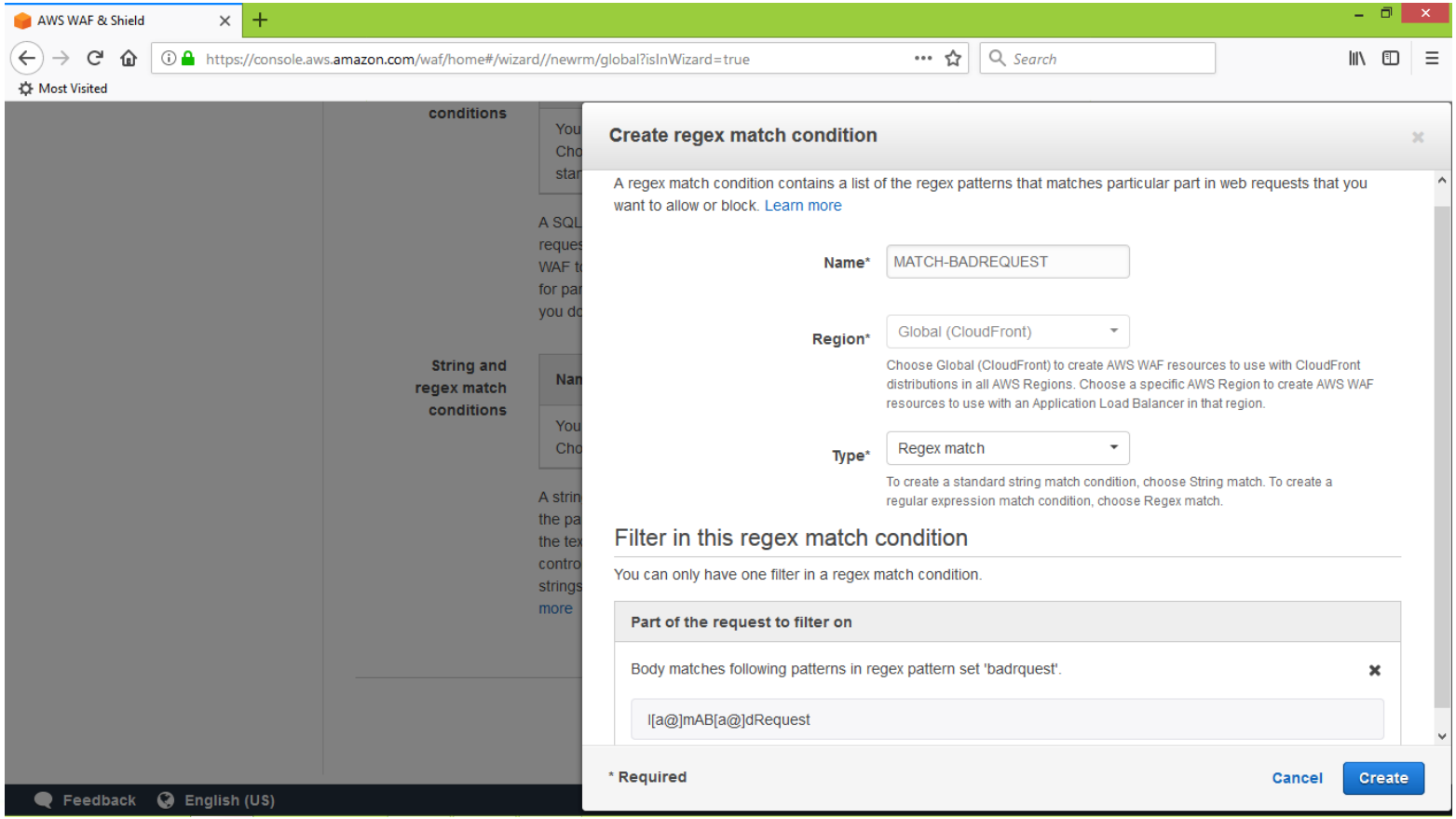


Regex Match Condition



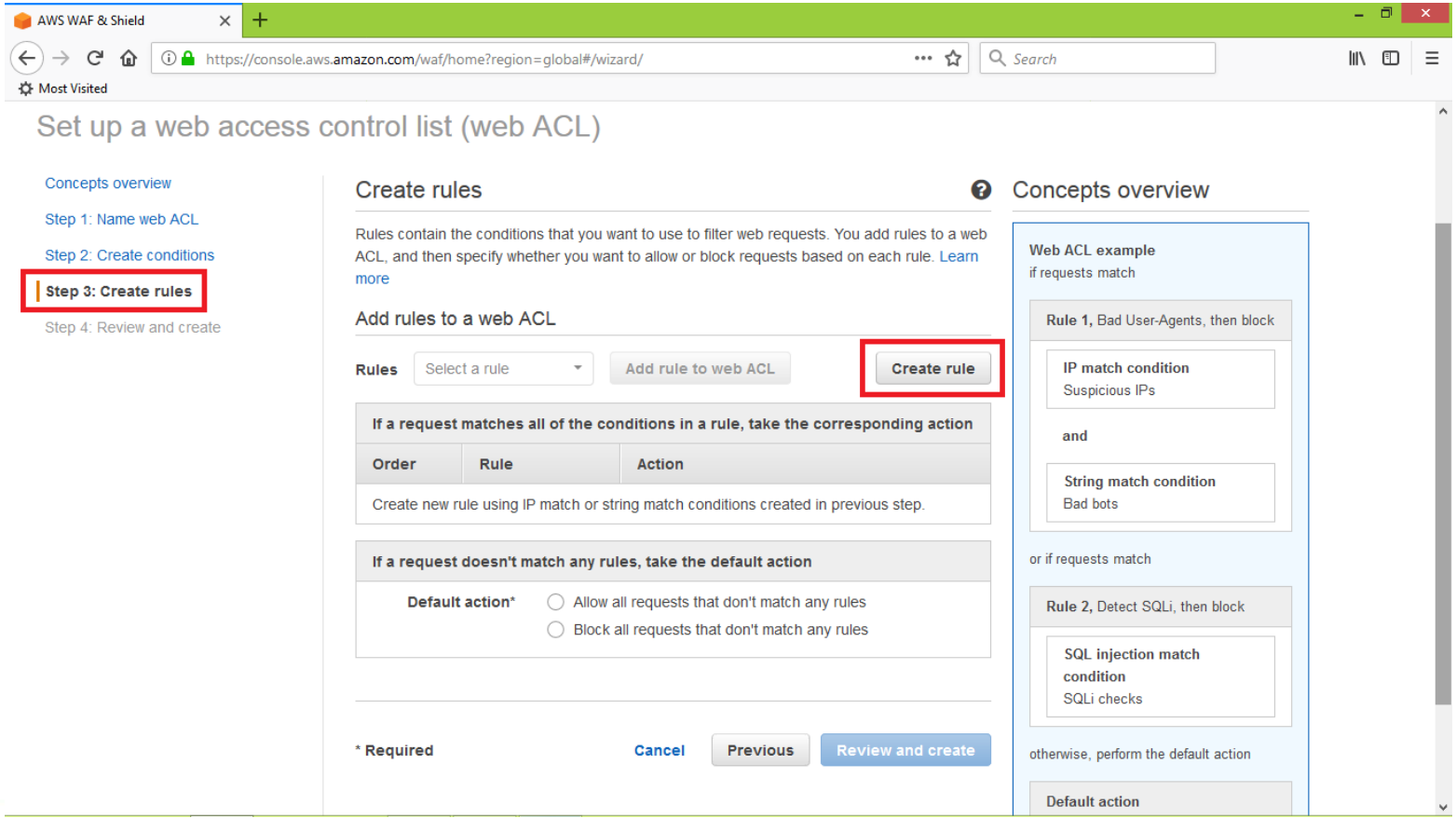
Pearson

Regex Match Condition

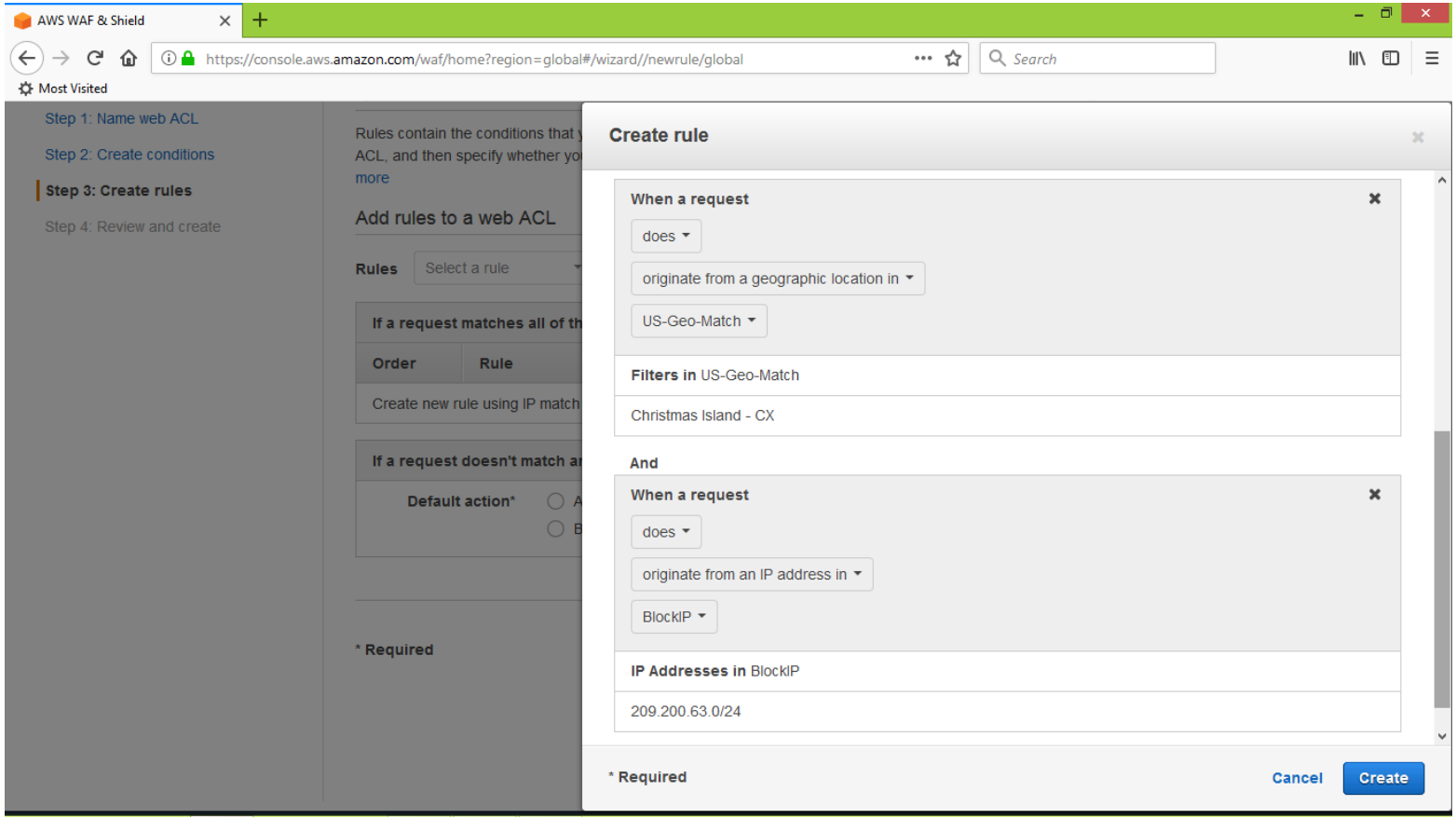


Pearson

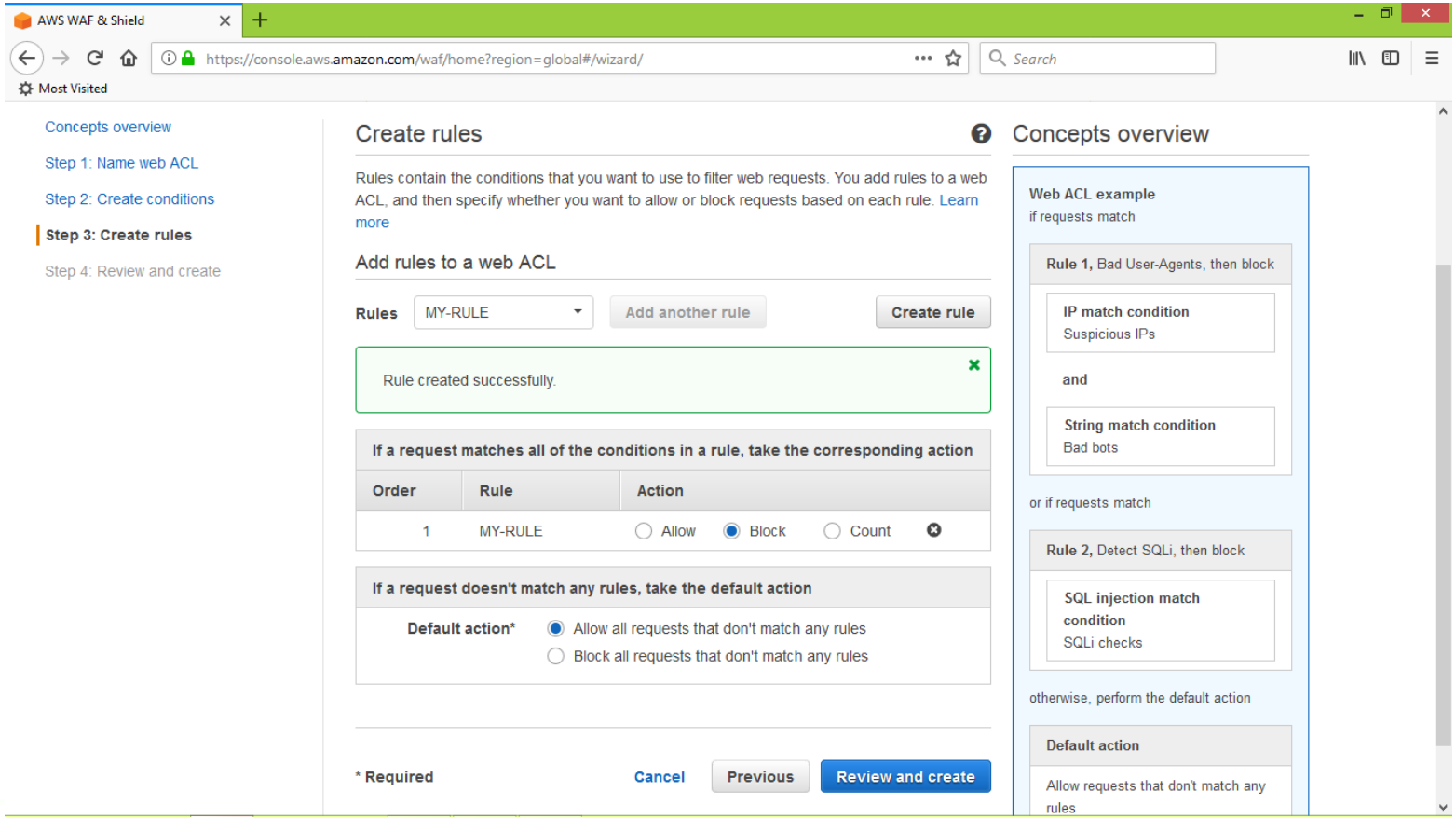
Create a Rule



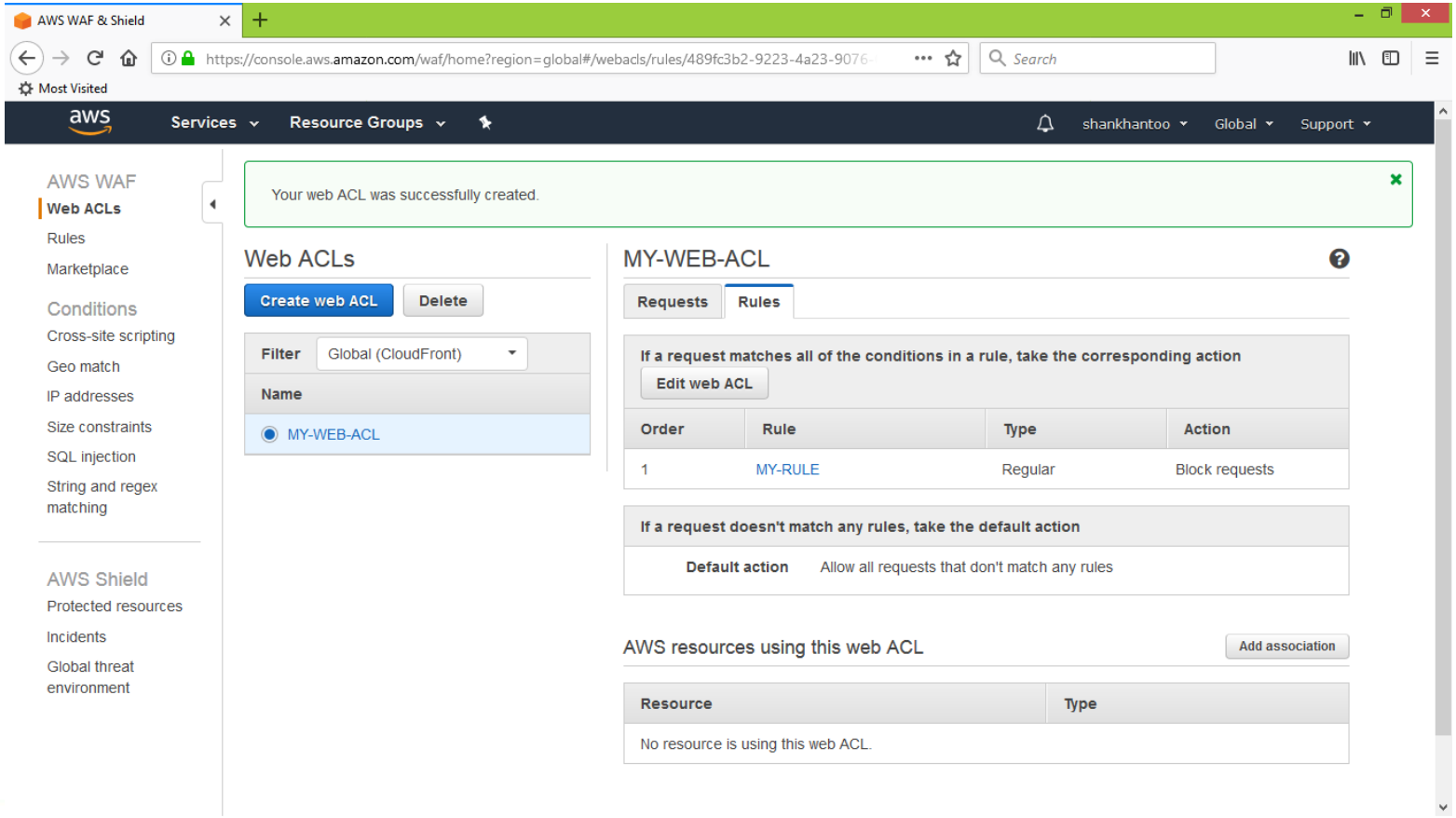
Create a Rule



Create a Rule

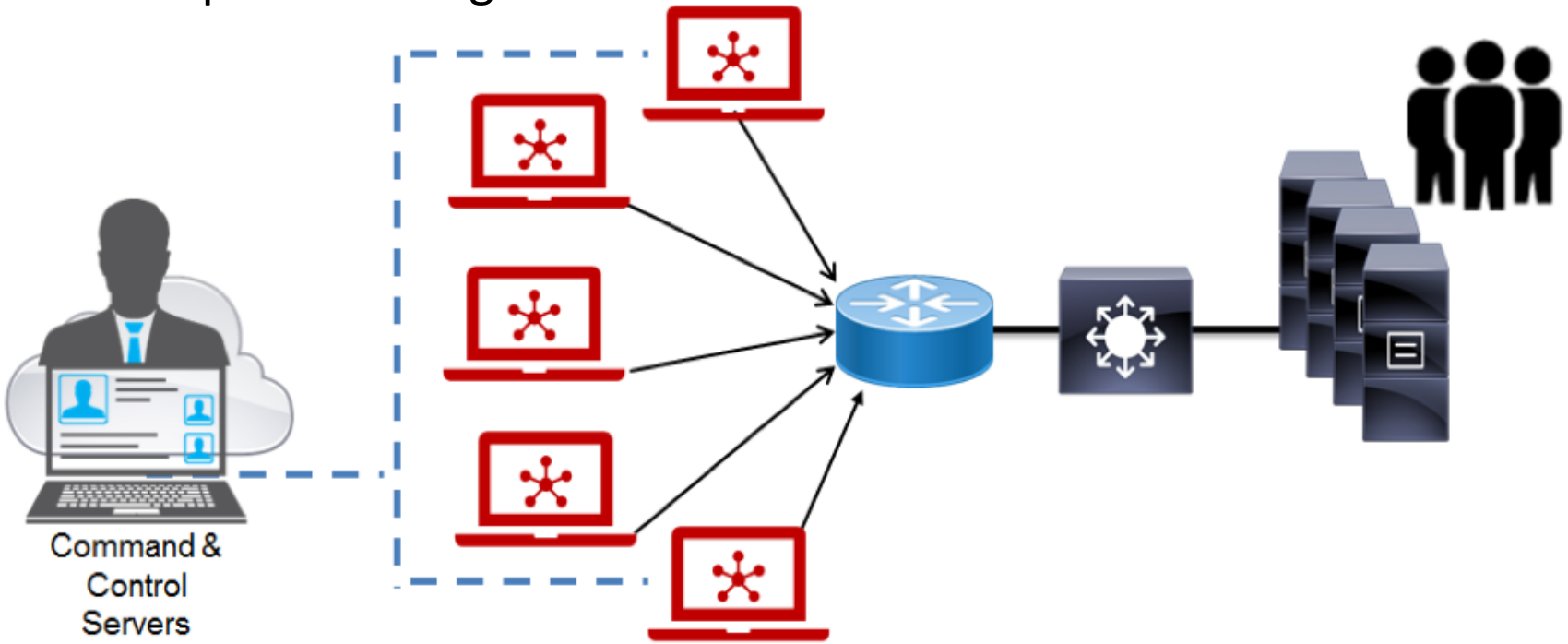


Associate Web ACL with Distribution



AWS Shield

- AWS provides AWS Shield Standard and AWS Shield Advanced for protection against DDoS attacks



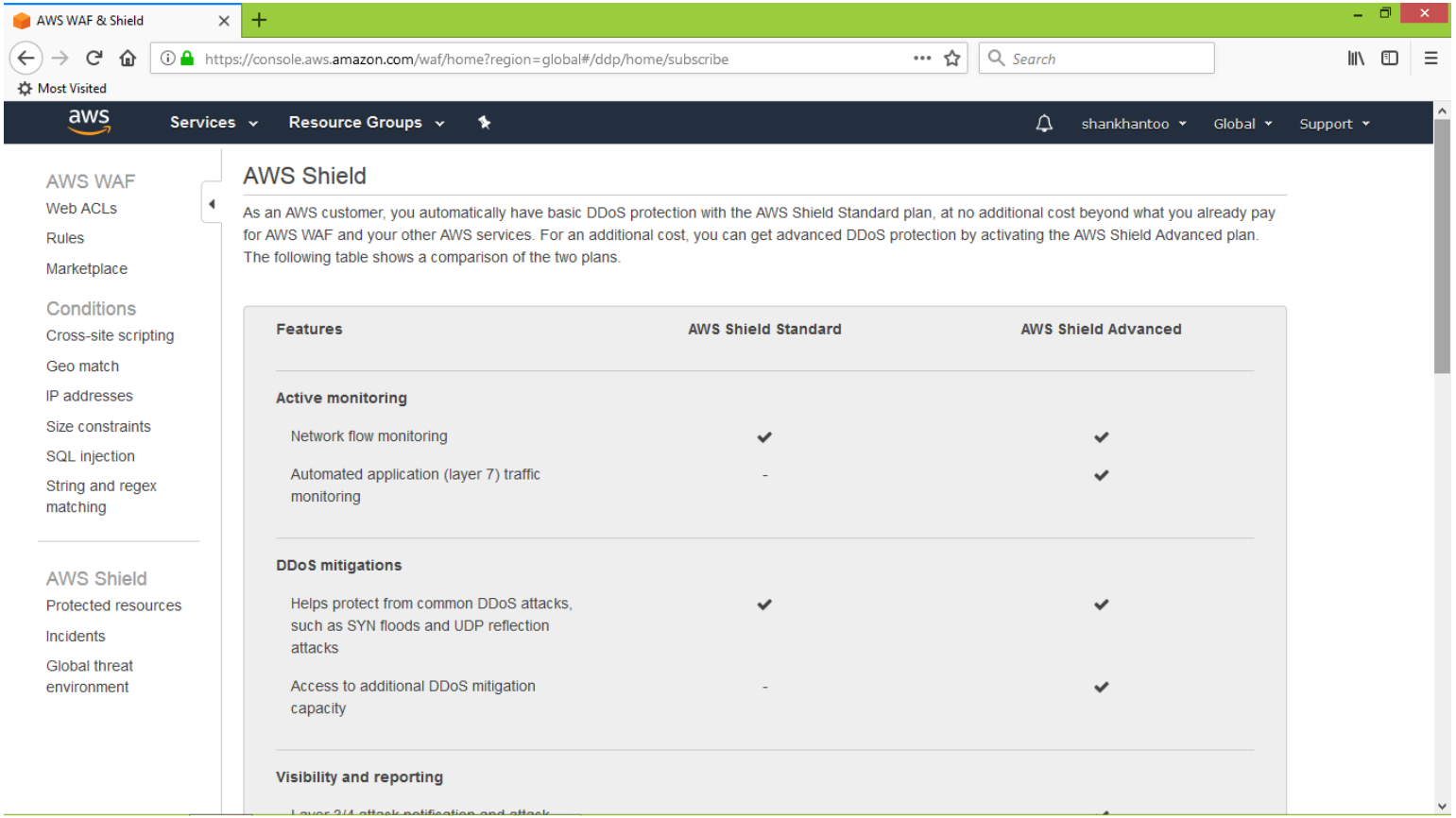
AWS Shield Standard

- Included with AWS WAF at no additional cost beyond what you are paying for AWS WAF and your other AWS services
- AWS technologies that are built from the ground up to provide resilience in the face of network and transport layer DDoS attacks
- For web application attacks, you also can use AWS WAF to configure web access control lists (web ACLs) that target network layer DDoS regex request patterns and help to minimize the effects of a DDoS attack

AWS Shield Advanced

- Provides expanded DDoS attack protection for your Elastic Load Balancing load balancers, CloudFront distributions, and Amazon Route 53 hosted zones
- Includes intelligent DDoS attack detection and mitigation for OSI layers 3 through 7
- You get 24x7 DDoS response team (DRT) assistance during a DDoS attack
- You have exclusive access to advanced, real-time metrics and reports for deep visibility into attacks on your AWS resources

AWS Shield


AWS WAF & Shield
https://console.aws.amazon.com/waf/home?region=global#/ddp/home/subscribe
Search
Most Visited
aws
Services
Resource Groups
shankhantoo
Global
Support
AWS WAF
Web ACLs
Rules
Marketplace
Conditions
Cross-site scripting
Geo match
IP addresses
Size constraints
SQL injection
String and regex matching
AWS Shield
Protected resources
Incidents
Global threat environment
AWS Shield
As an AWS customer, you automatically have basic DDoS protection with the AWS Shield Standard plan, at no additional cost beyond what you already pay for AWS WAF and your other AWS services. For an additional cost, you can get advanced DDoS protection by activating the AWS Shield Advanced plan. The following table shows a comparison of the two plans.
Features
AWS Shield Standard
AWS Shield Advanced
Active monitoring
Network flow monitoring
Automated application (layer 7) traffic monitoring
DDoS mitigations
Helps protect from common DDoS attacks, such as SYN floods and UDP reflection attacks
Access to additional DDoS mitigation capacity
Visibility and reporting

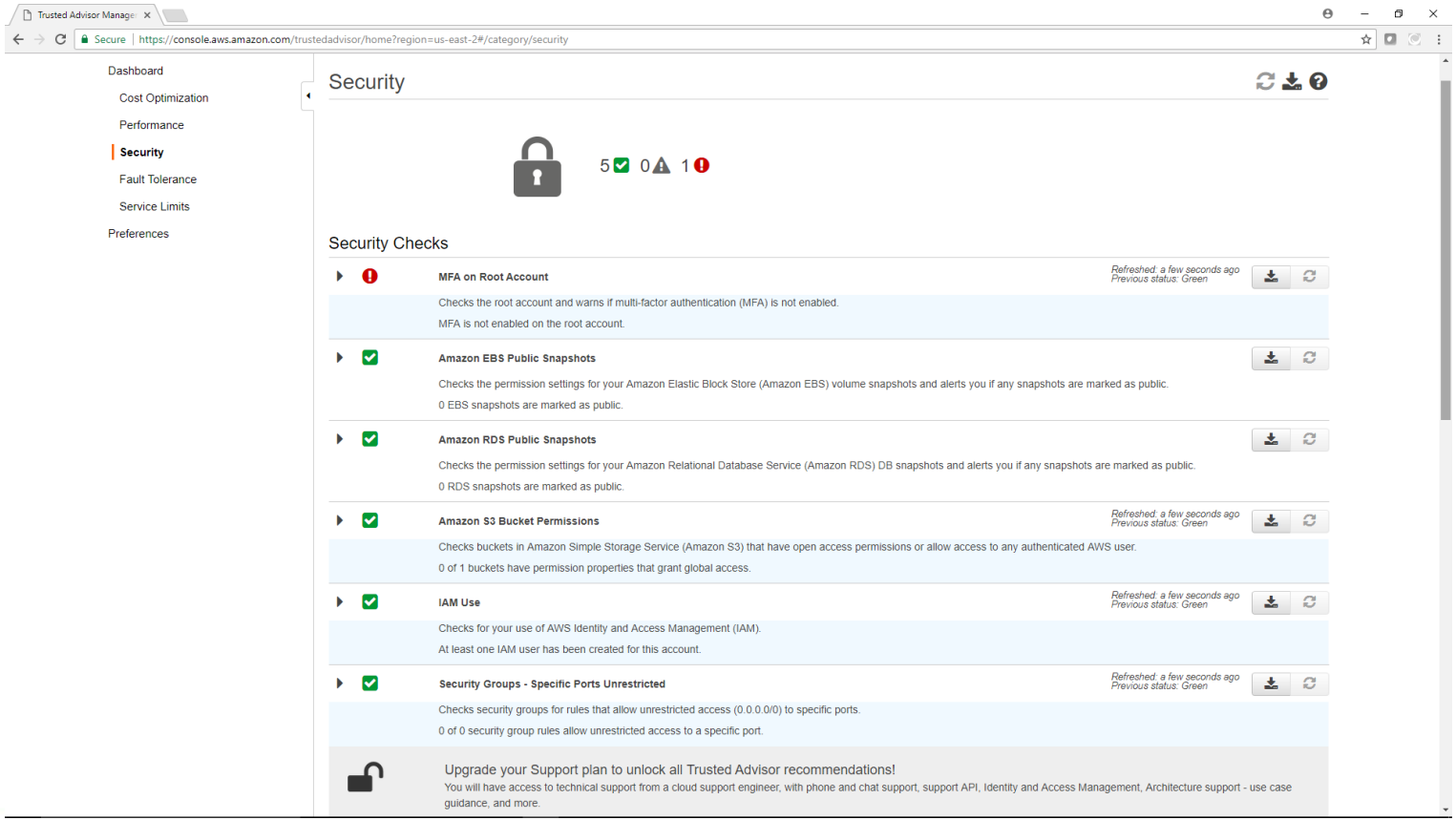
AWS Shield Threat Landscape Report

- The AWS Shield Threat Landscape Report (TLR) offers a summary of threats detected by AWS Shield
- The report is produced by the AWS Threat Research Team (TRT) that persistently monitors and evaluates the threat landscape to formulate security controls for AWS customers

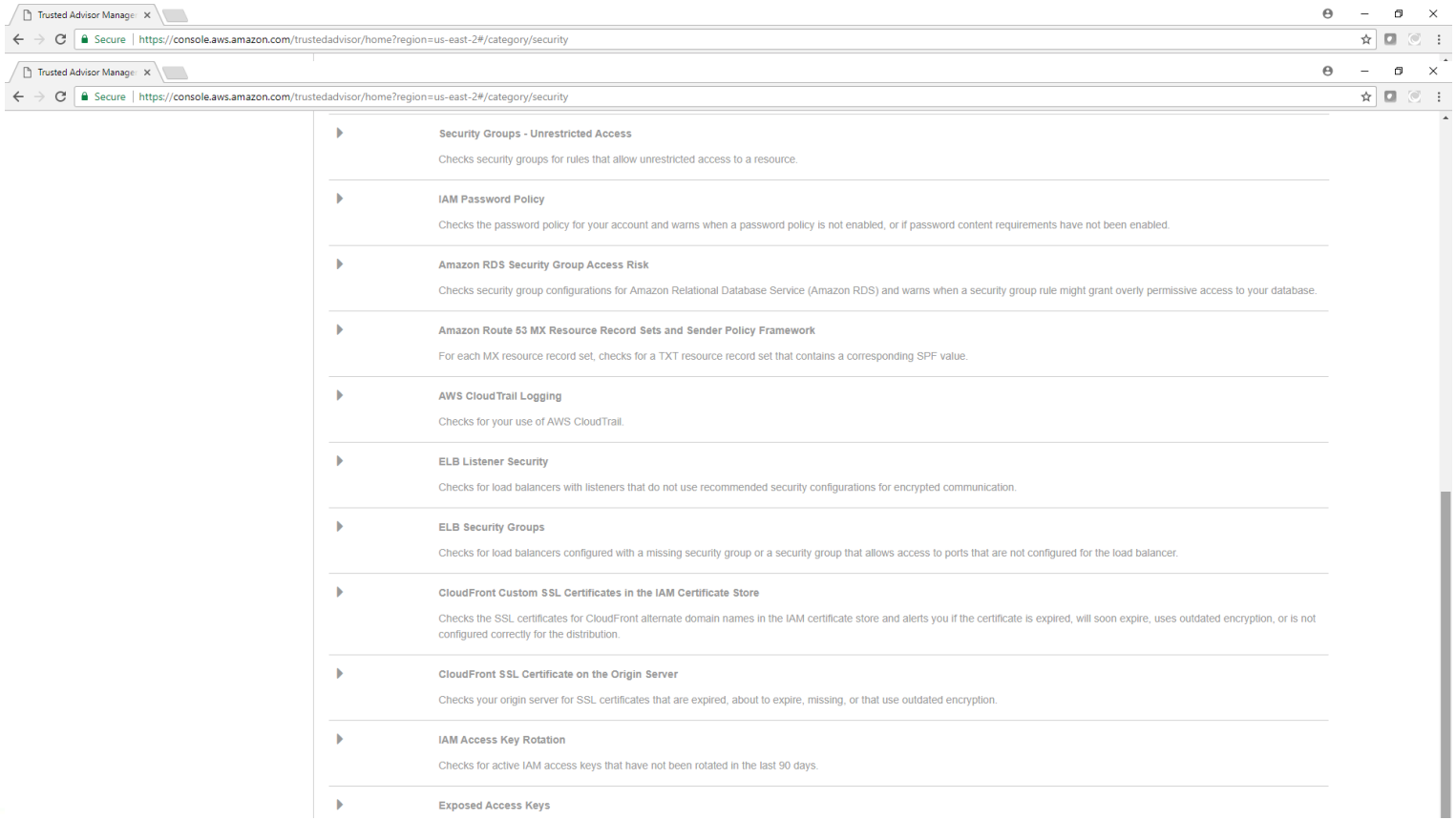
AWS Trusted Advisor

- Uses best practices derived from history of serving thousands of AWS customers
- Includes 27 individual chacks within 4 categories:

AWS Trusted Advisor



AWS Trusted Advisor



AWS Guard Duty

- Amazon GuardDuty is a managed threat detection service that continuously monitors for malicious or unauthorized behavior
- It monitors for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise (Zero Days)
- GuardDuty also detects potentially compromised instances or reconnaissance by attackers.
- Uses proprietary ML and AI along with strategic partners

AWS Guard Duty

- When GuardDuty detects suspicious or unexpected behavior it generates a finding - a notification that has the details about a impending security issue
- The finding details include information about what occurred, what AWS resources were involved in the suspicious activity, when this activity took place, and other data
- The finding type provides a description of the potential security issue: ***Recon:EC2/PortProbeUnprotectedPort***
- docs.aws.amazon.com: “Amazon GuardDuty Finding Types”

Enabling Security Hub

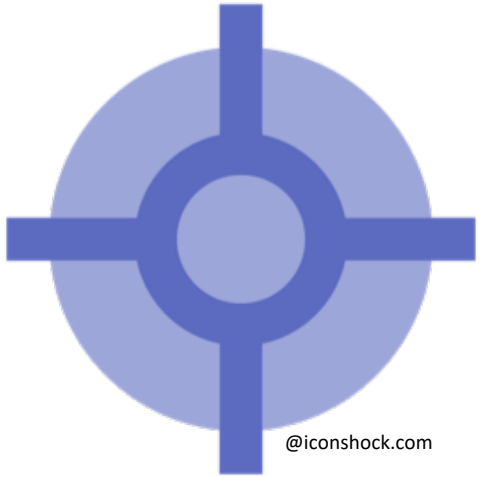
- Security Hub offers a consolidated view of your security status in AWS
- You can automate security checks, manage security findings, and classify the highest priority security issues across your AWS environment using:
  - Amazon GuardDuty
  - Amazon Inspector
  - S3 bucket policy findings from Amazon Macie
  - Plus integrated partner solutions

Security Hub Use Cases

- Continuously scan AWS accounts for configuration errors using:
  - **Center for Internet Security (CIS) AWS Foundations benchmarks**
  - **PCI DSS v3.2.1 benchmarks**
  - **AWS Foundational Bets Practices Standards**
- Report on security check results at the account and multi-account level to recognize your global security posture
- Use the Hub's summary dashboards and filtering rules to identify and prioritize which findings

Enabling Security Hub

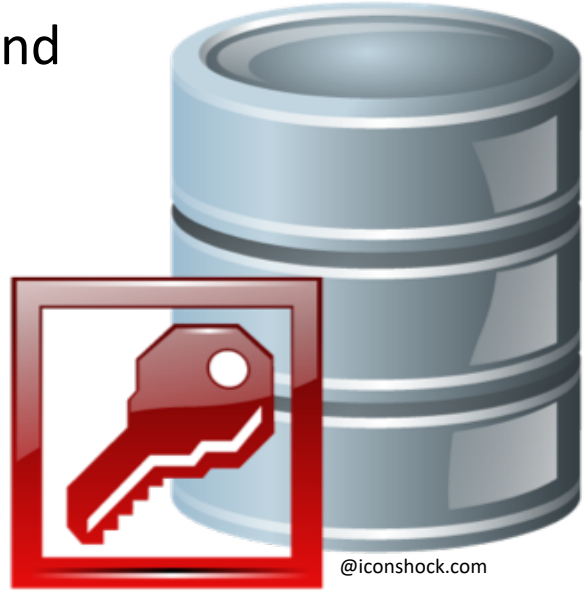
- Enabling Security Hub grants it permissions to import findings from:
  - Amazon GuardDuty
  - Amazon Inspector
  - Amazon Macie
  - AWS IAM Access Analyzer
  - AWS Firewall Manager
- **AWS offers a 30-day free trial**



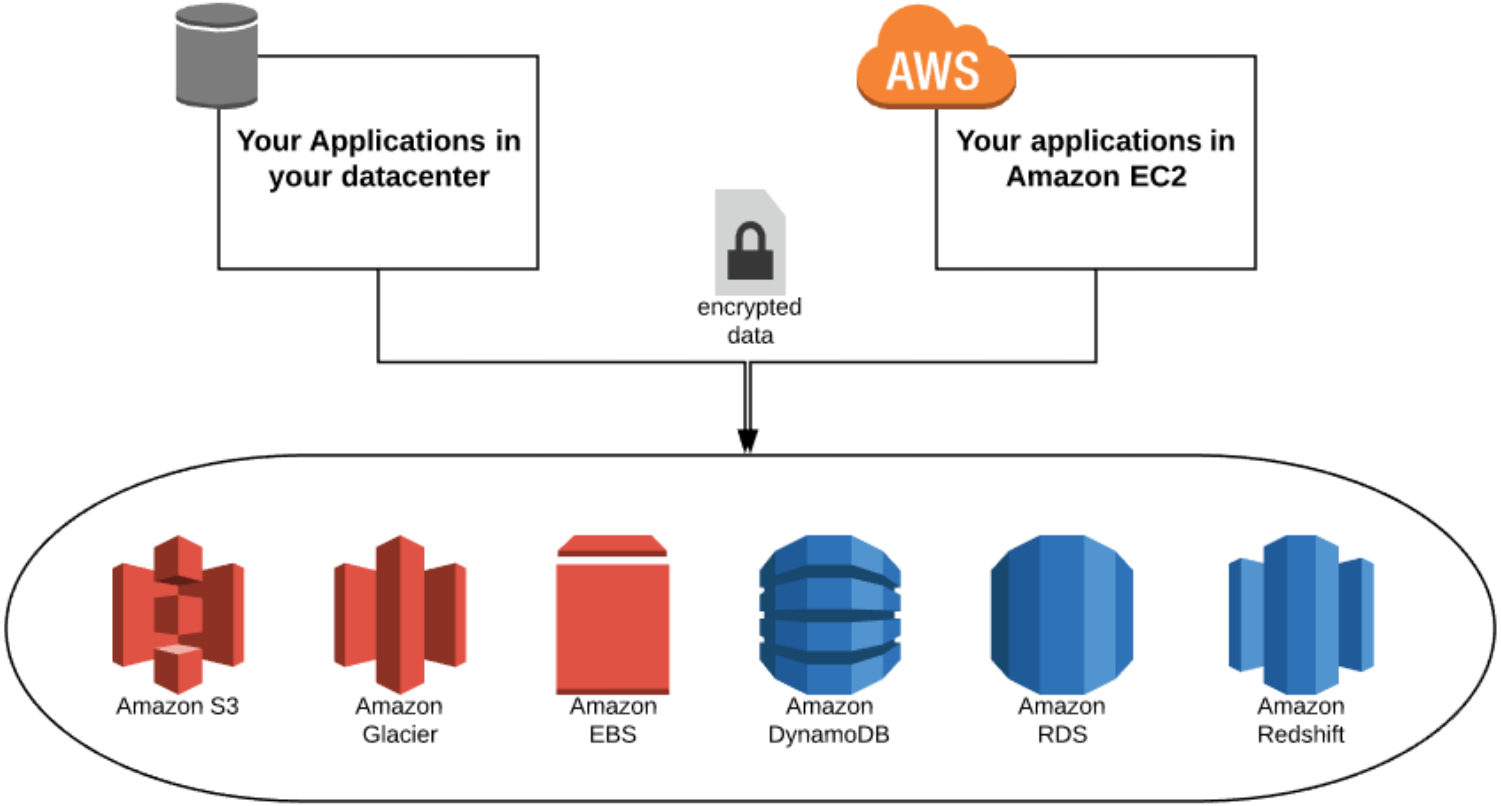
Segment 5: Key Management Service (KMS), Service-Specific Security (S3 and EBS), and Organizational Service Control Policies (SCP)

Encryption and Key Management in AWS

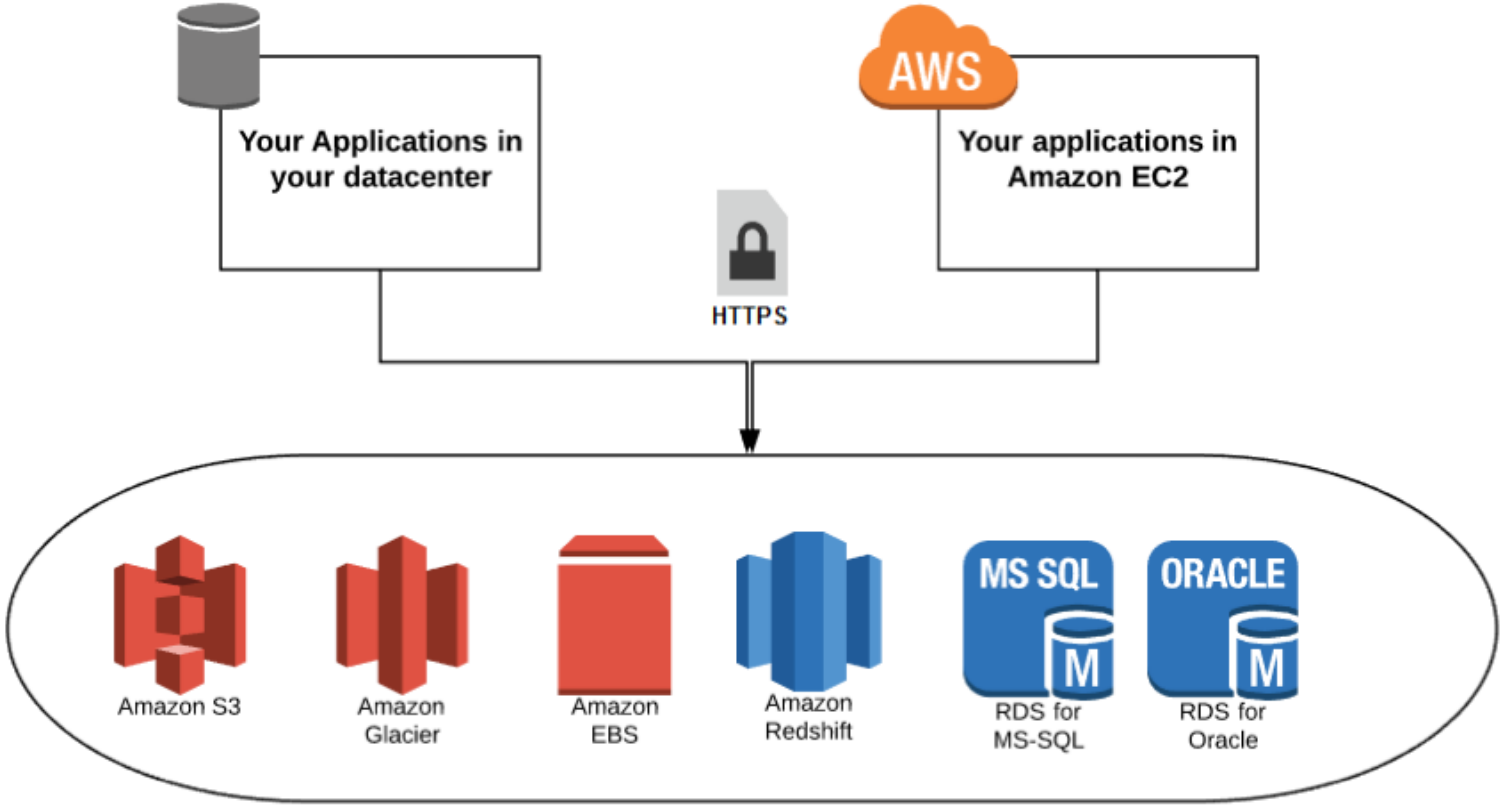
- Client-side encryption: You encrypt you data and manage your own keys
- Server-side encryption: AWS encrypts data and manages the keys for you
- Key Management
  - On your own
  - AWS Management Key Service (KMS)
  - AWS Partner Solutions (Sophos, Trend, etc.)
  - AWS Cloud HSM



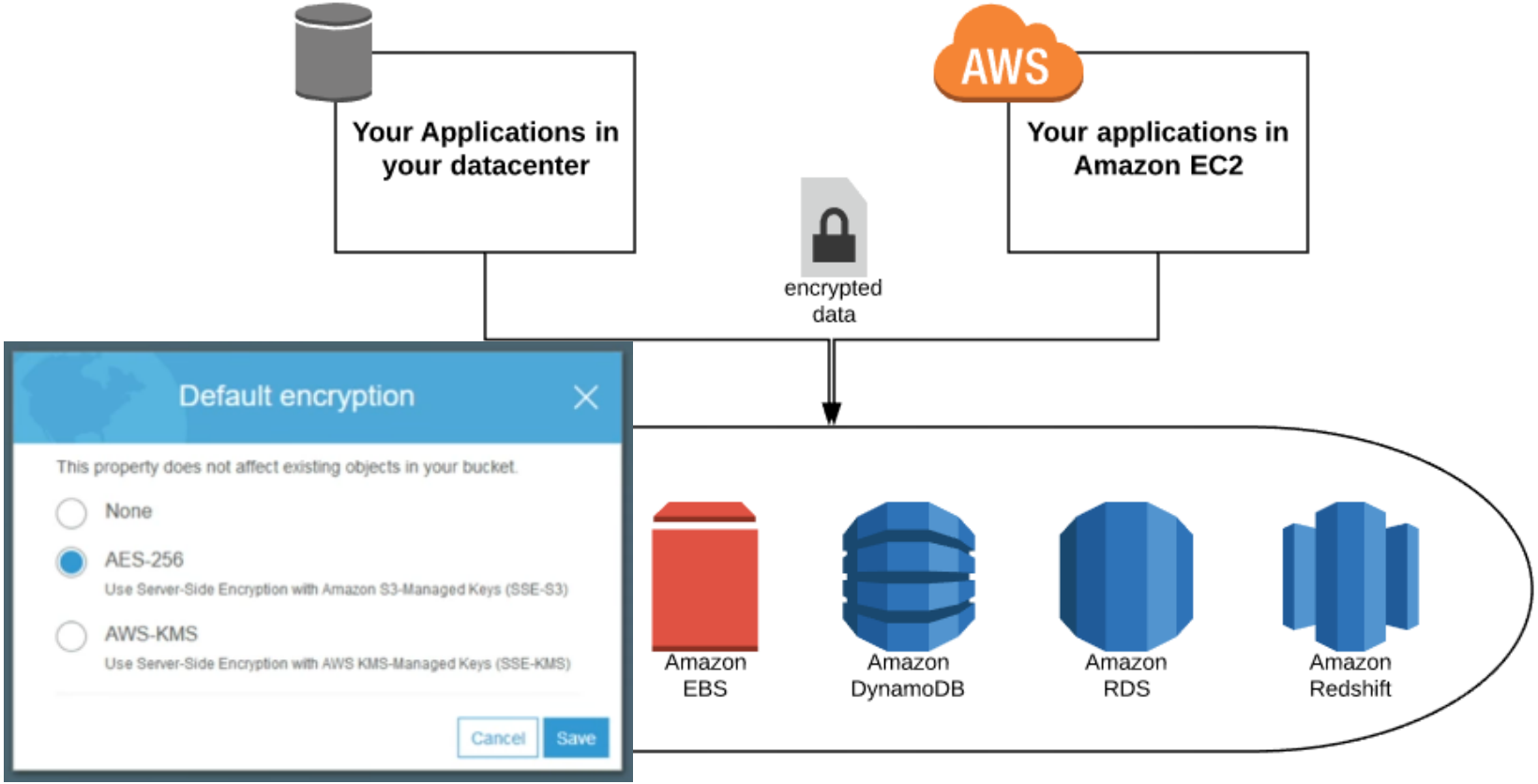
Client-side Encryption



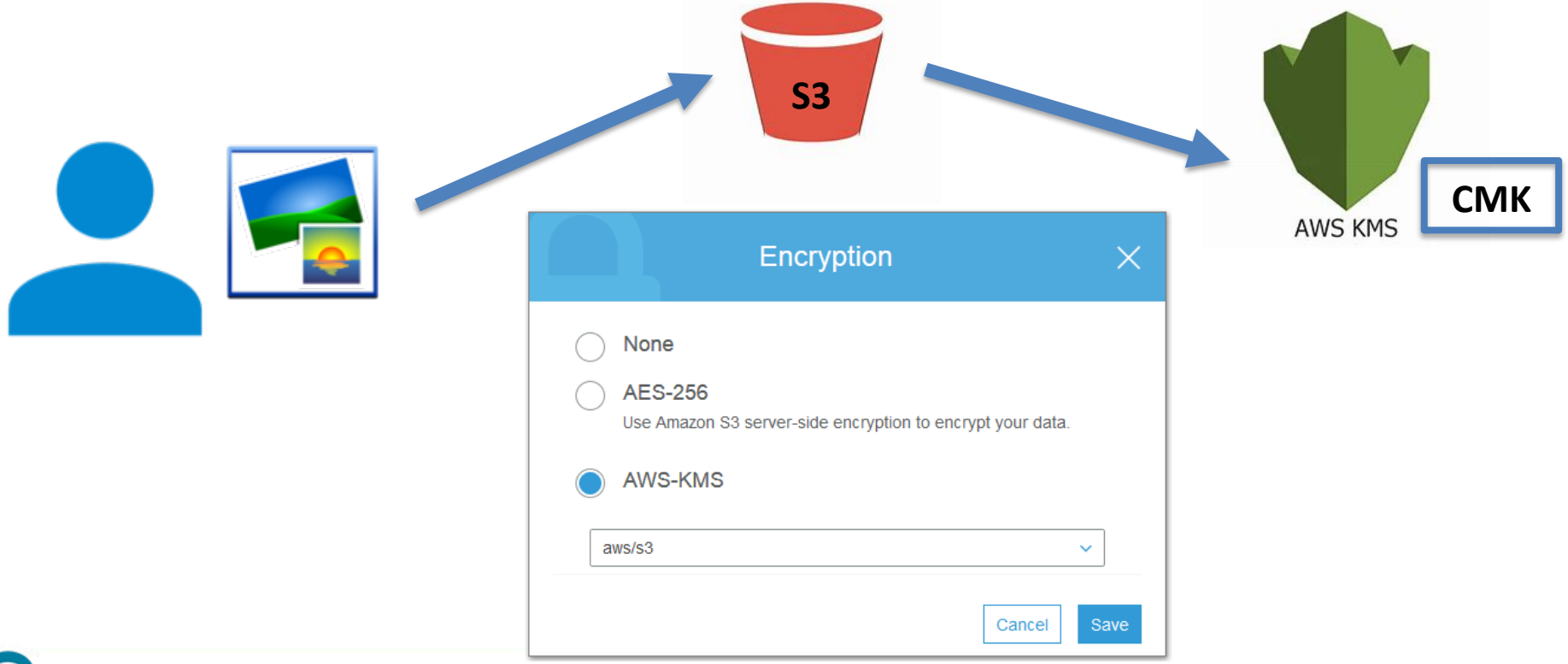
Server-side Encryption



AWS S3 Server-side Encryption



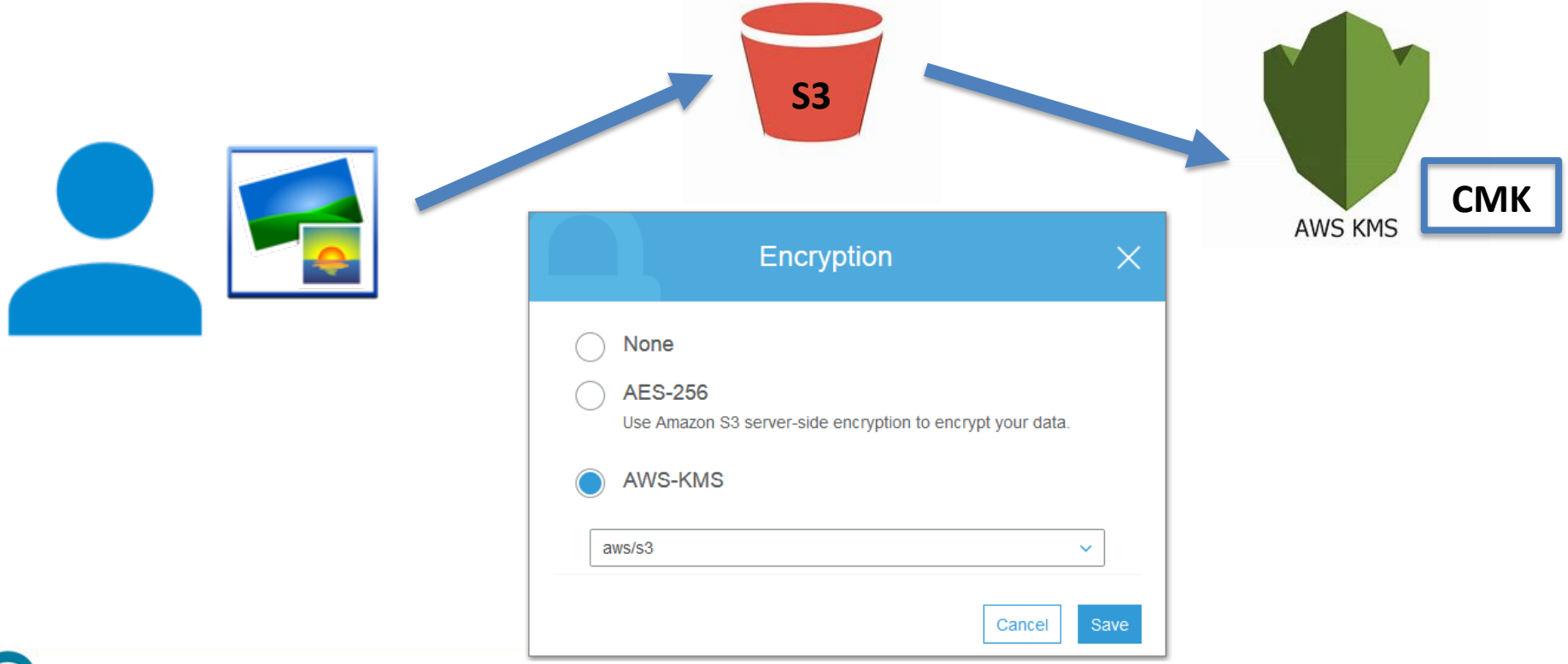
S3 SSE-KMS Encryption



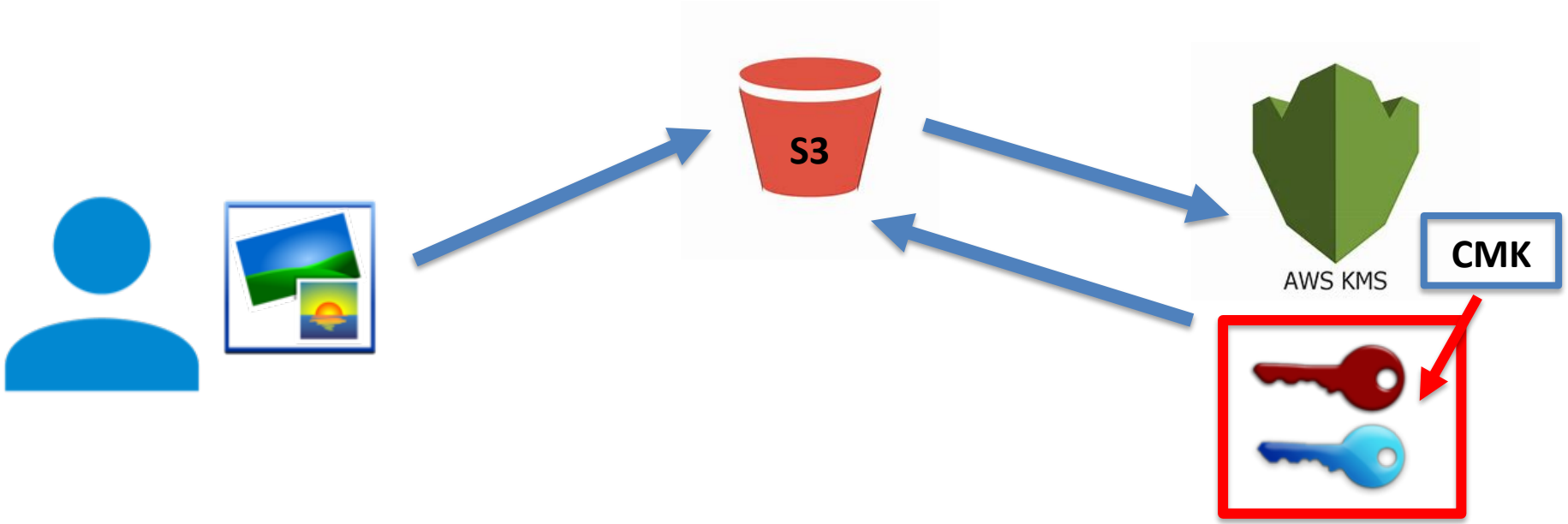
Types of CMKs

- There are three types of CMKs in AWS accounts: customer managed CMKs, AWS managed CMKs, and AWS owned CMKs
  - Customer managed CMKs are CMKs in your AWS account that you create, own, and manage
  - AWS managed CMKs are CMKs in your account that are created, managed, and used on your behalf by an AWS service that integrates with AWS KMS
  - AWS owned CMKs are not in your AWS account. They are part of a collection of CMKs that AWS owns and manages for use in multiple AWS accounts - AWS services can use AWS owned CMKs to protect your data

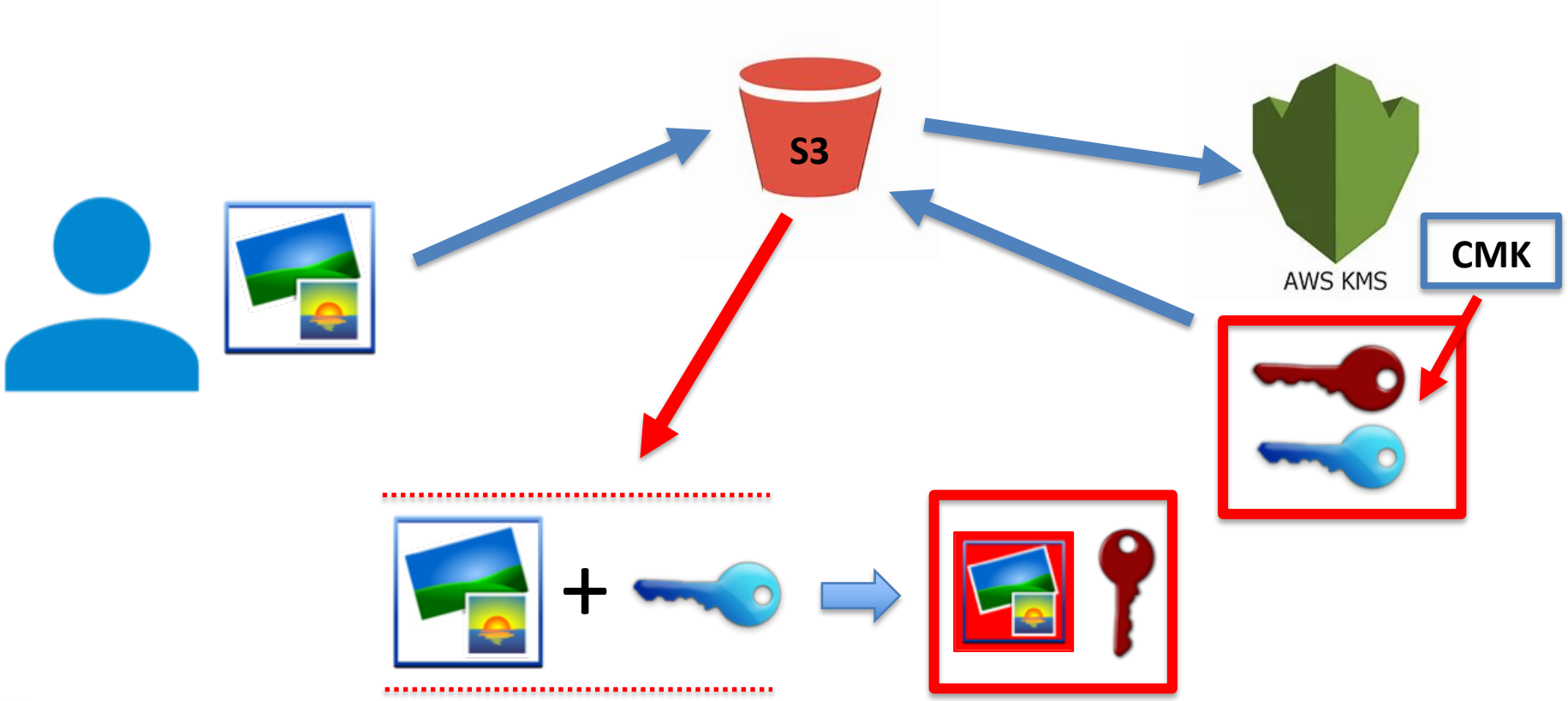
S3 SSE-KMS Encryption



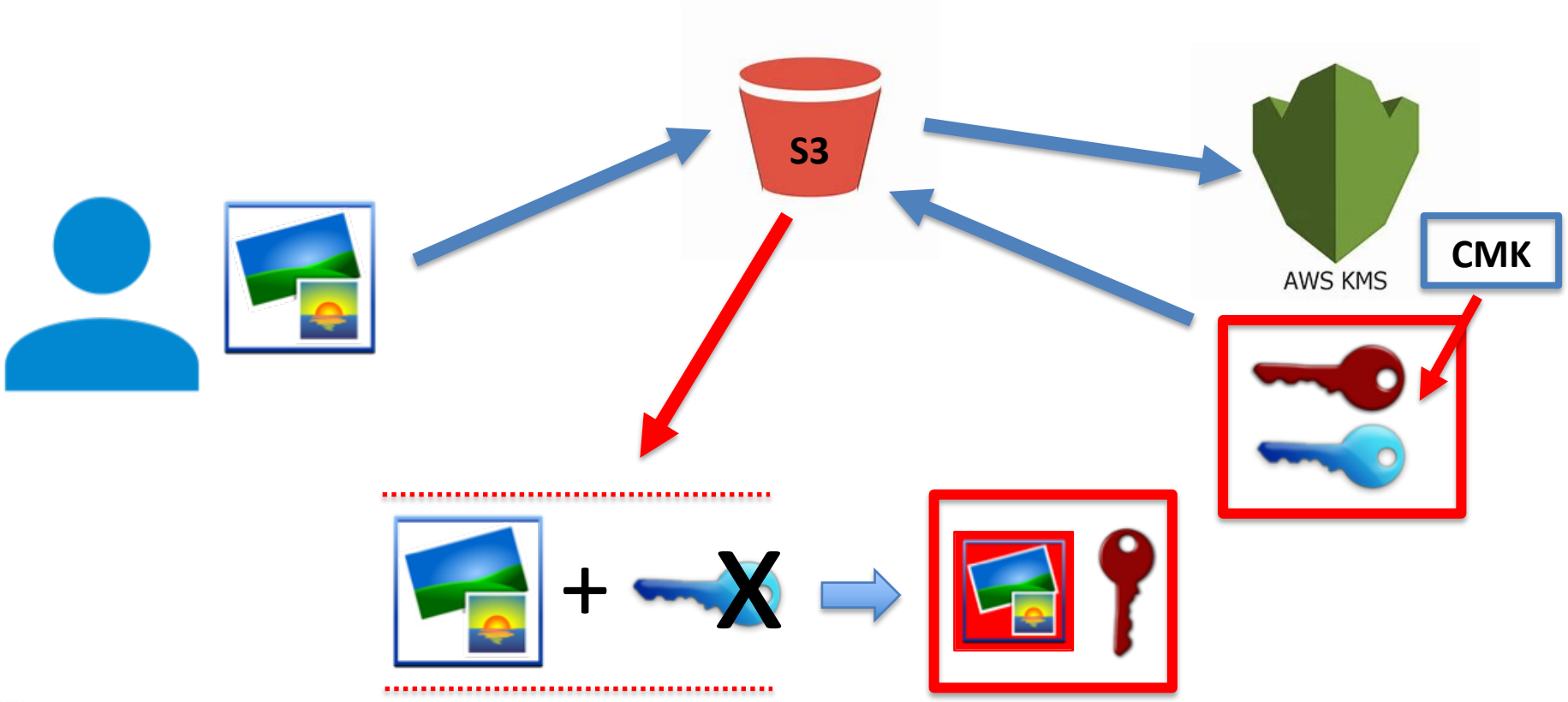
S3 SSE-KMS Encryption



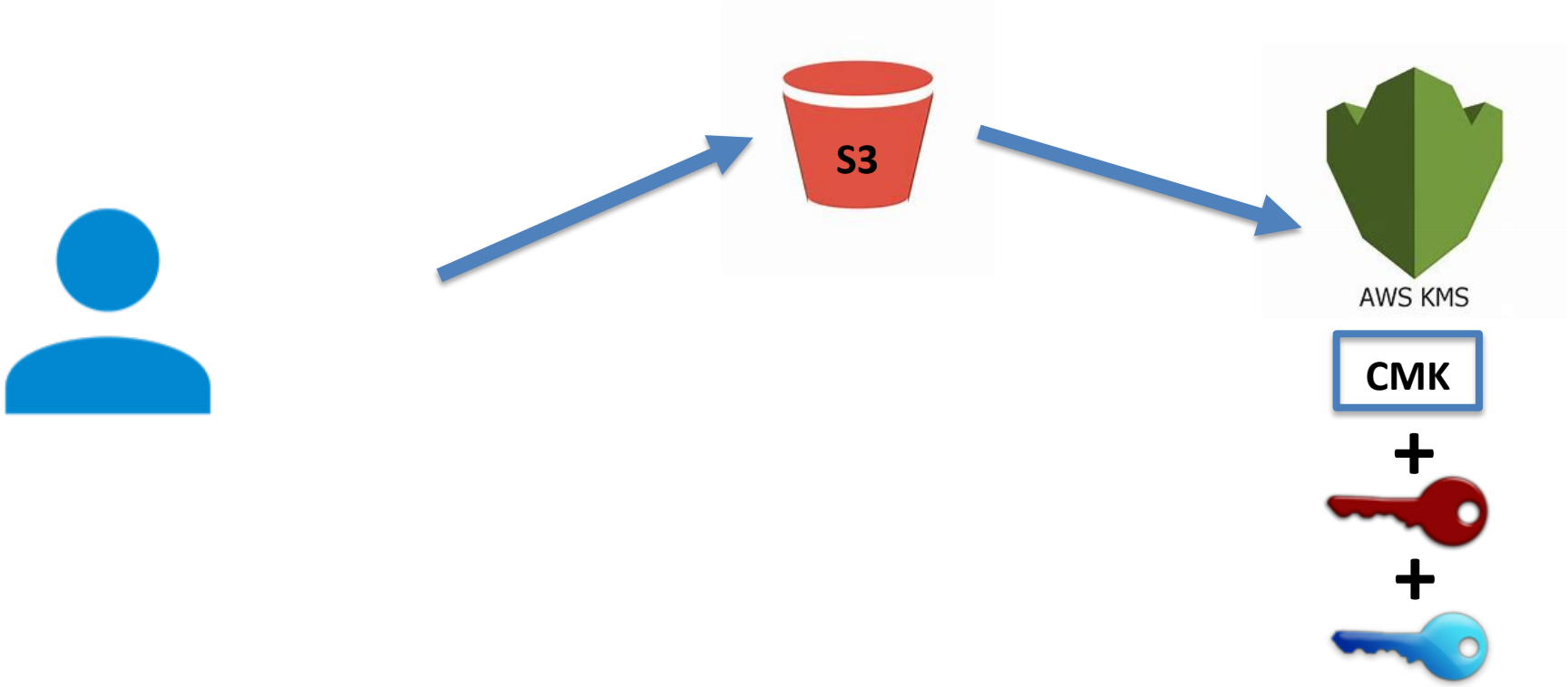
S3 SSE-KMS Encryption



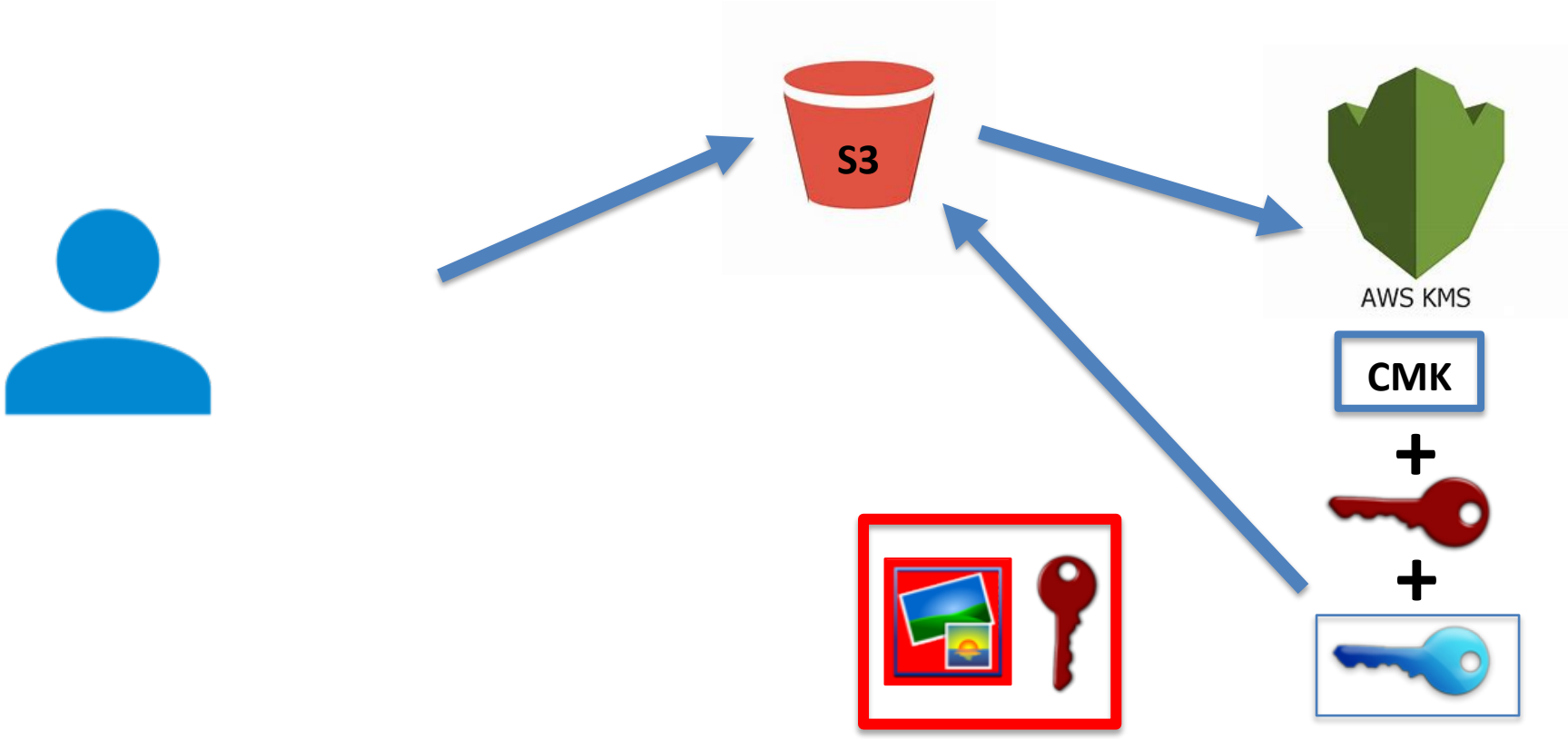
S3 SSE-KMS Encryption



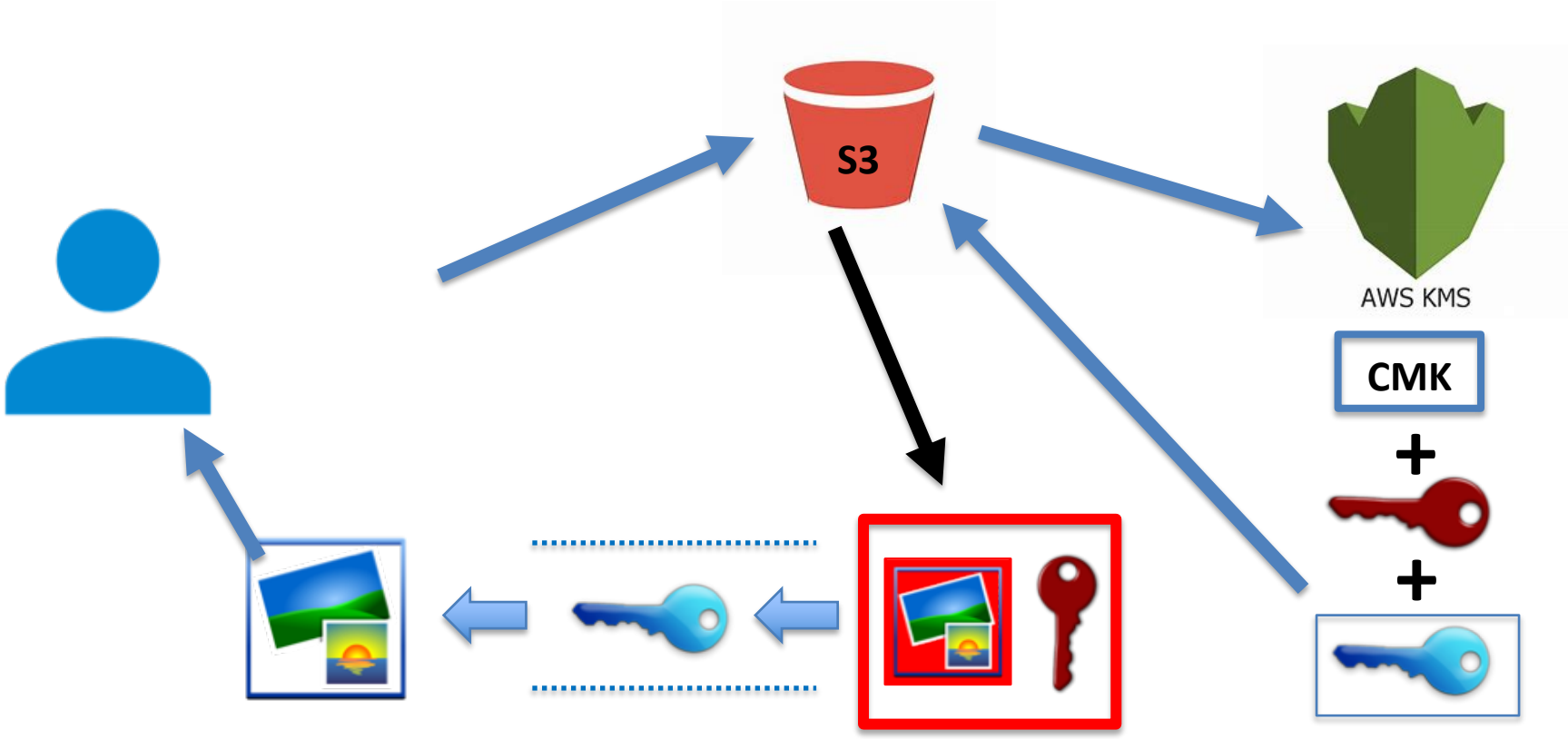
S3 SSE-KMS Decryption



S3 SSE-KMS Decryption



S3 SSE-KMS Decryption

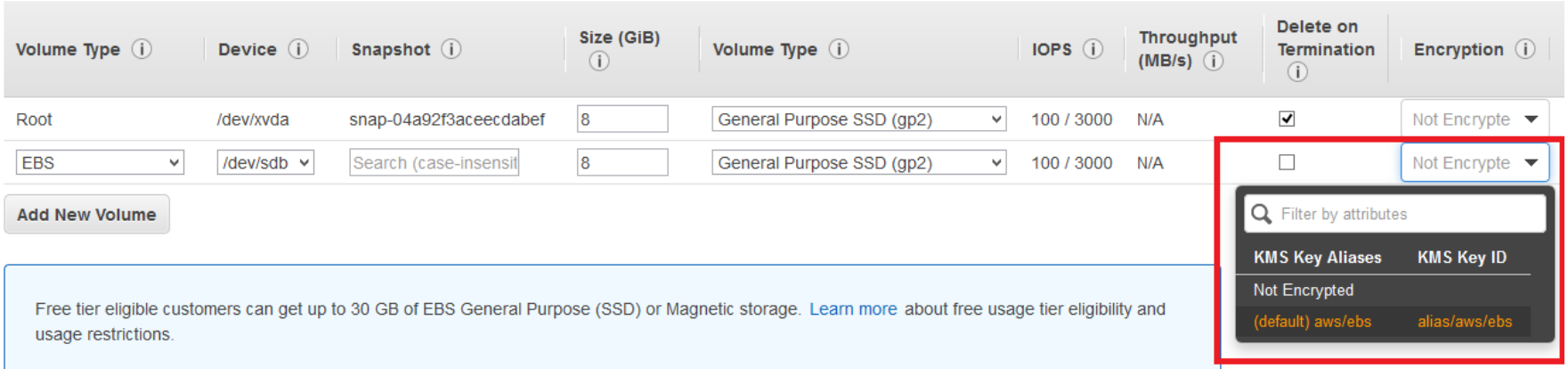


AWS EBS Encryption

- When you create an encrypted EBS volume and attach it to a supported instance type, the following types of data are encrypted:
  - Data at rest inside the volume
  - All data moving between the volume and the instance
  - All snapshots created from the volume
  - All volumes created from those snapshots
- You can encrypt both the boot and data volumes of an EC2 instance

@iconshock.com

AWS EBS Encryption



AWS EBS Encryption by Default

- You can enable the EBS Encryption by Default feature
  - AWS encrypts new EBS volumes on launch
  - AWS encrypts new copies of unencrypted snapshots
- Newly created EBS resources are encrypted to your account's default CMK unless you specify a custom CMK in the EC2 settings or at instance launch

```
aws ec2 enable-ebs-encryption-by-default
```

Simple Storage Service (Amazon S3)

- **Amazon Simple Storage Service (Amazon S3)** is an object storage service that offers industry-leading scalability, data availability, security, and performance
- Amazon S3 provides easy-to-use management features so you can organize your data and configure finely-tuned access controls to meet your specific business, organizational, and compliance requirements
- S3 is designed for 99.999999999% (11 9's) of durability, and stores data for millions of applications for companies all around the world

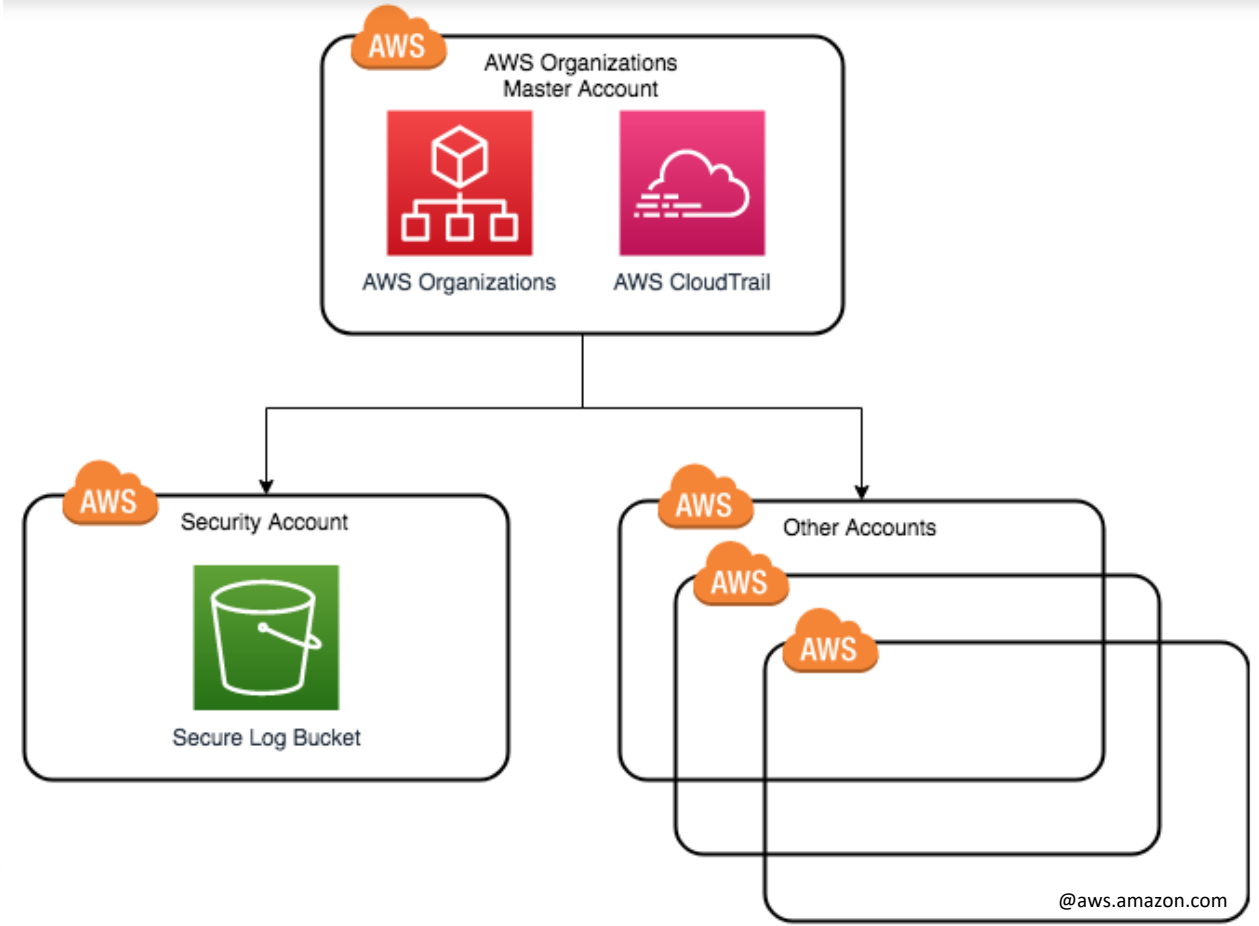
S3 Security Distinctives

- Amazon S3 standard storage offers the following features:
  - Backed with the Amazon S3 Service Level Agreement
  - Designed to provide 99.999999999% durability and 99.99% availability of objects over a given year
  - Designed to sustain the concurrent loss of data in two facilities
  - Amazon S3 further protects your data using versioning
  - Deploy VPC endpoints for accessing Amazon S3
  - Consider using Amazon Macie with Amazon S3

Create a Data Bunker

- A data bunker is a secure account which stores critical security data in a secure location
- Only select members of your security team should have access to this account
- Security teams should:
  - Create a new security account in a multi-account organization
  - Create a secure S3 bucket in that account
  - Turn on CloudTrail for the organization and send the logs to this bucket in the secure data account
- You may want to also consider what other data you need to store there (i.e. secure backups)

Create a Data Bunker

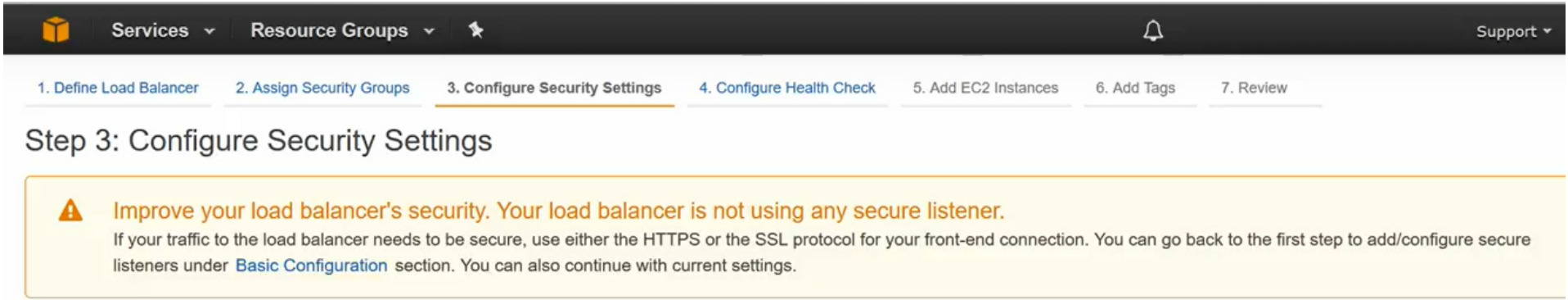


Amazon Elastic Load Balancing Security

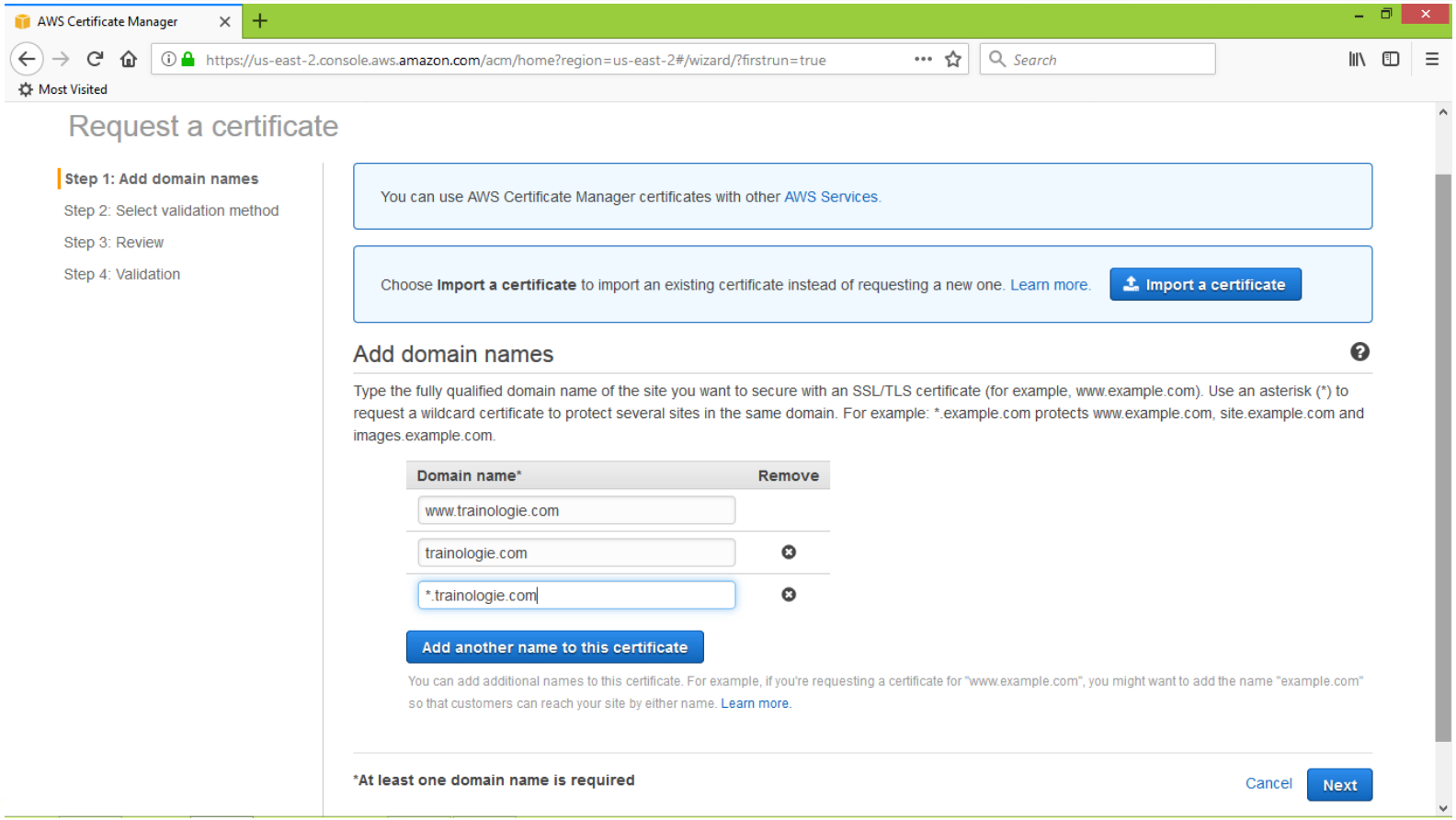
- ELB takes over the encryption and decryption work from the Amazon EC2 instances and manages it centrally on the load balancer
- Offers clients a single point of contact, and can also serve as the first line of defense against attacks on your network

@iconshock.com

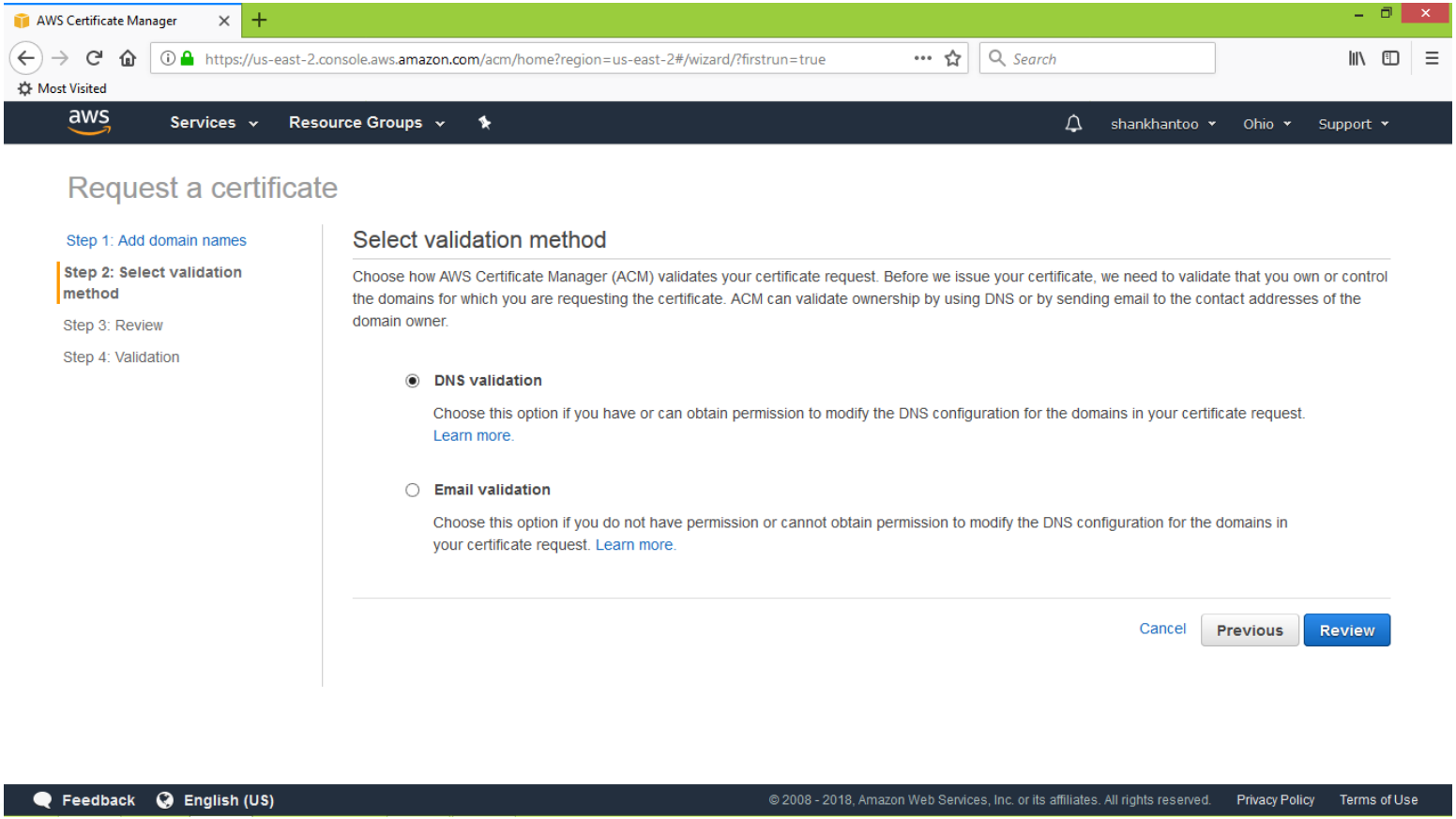
ELB Secure Listener



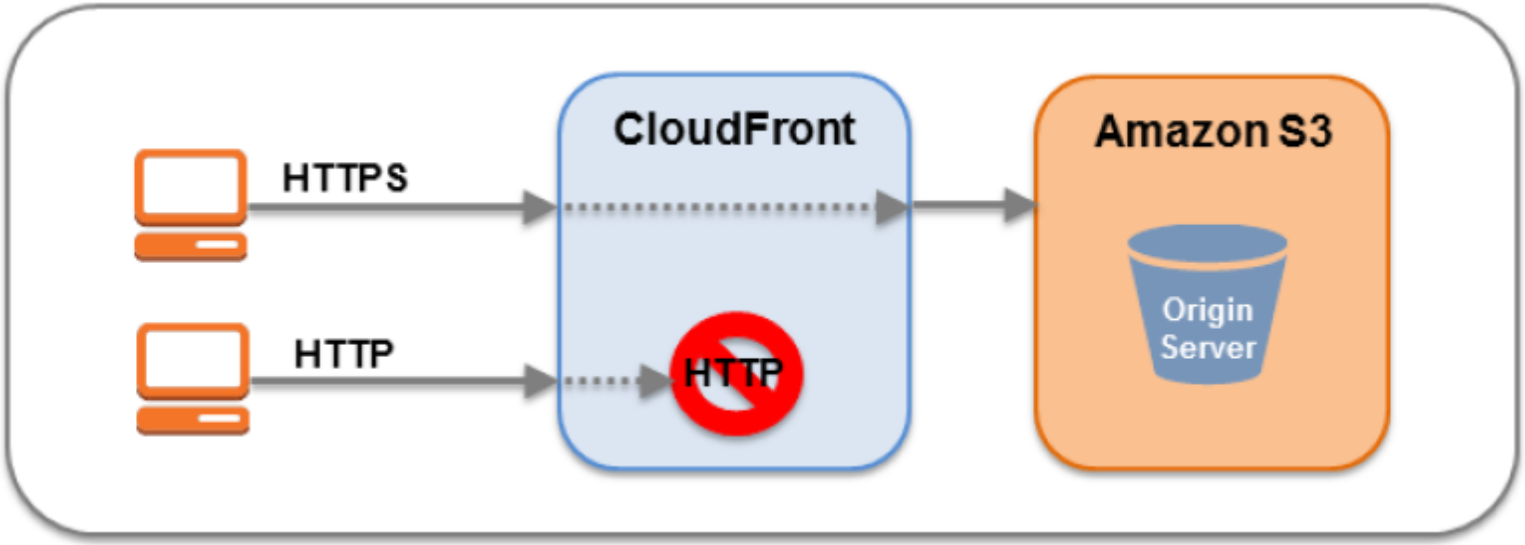
Use Certificate Manager with ELB



Use Certificate Manager with ELB



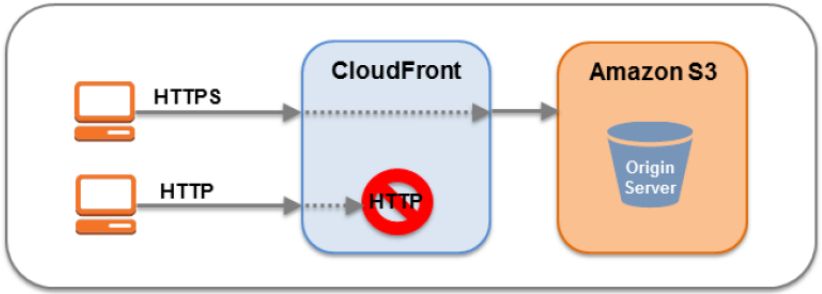
Amazon CloudFront Security



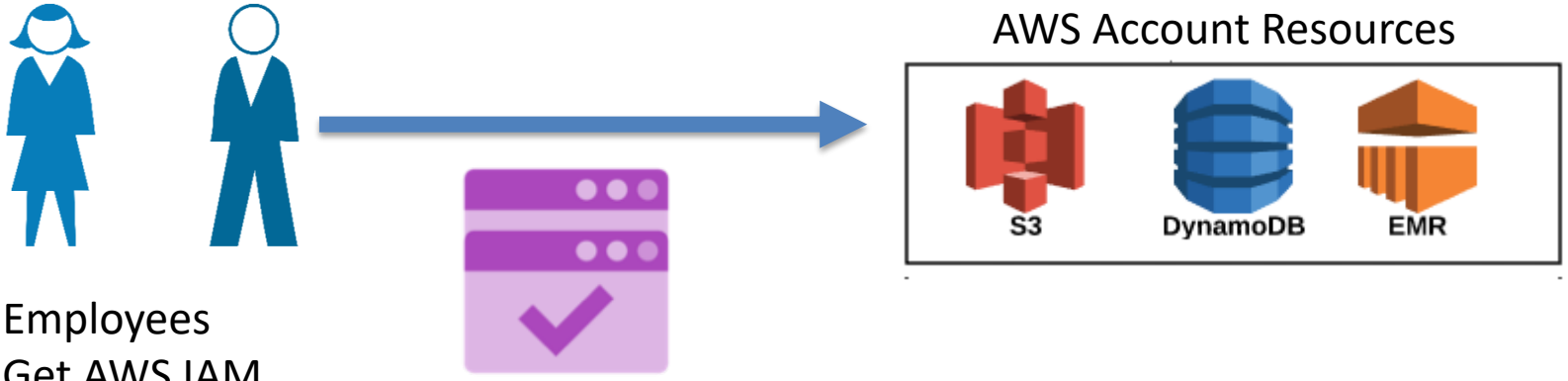
- Every request made to its control API be authenticated – signed with an HMAC-SHA1 signature only accessible through TLS-enabled endpoints
- Private Content Feature controls who can download content from CloudFront
- Origin Access Identities can control access to original copies of objects

Amazon CloudFront Security

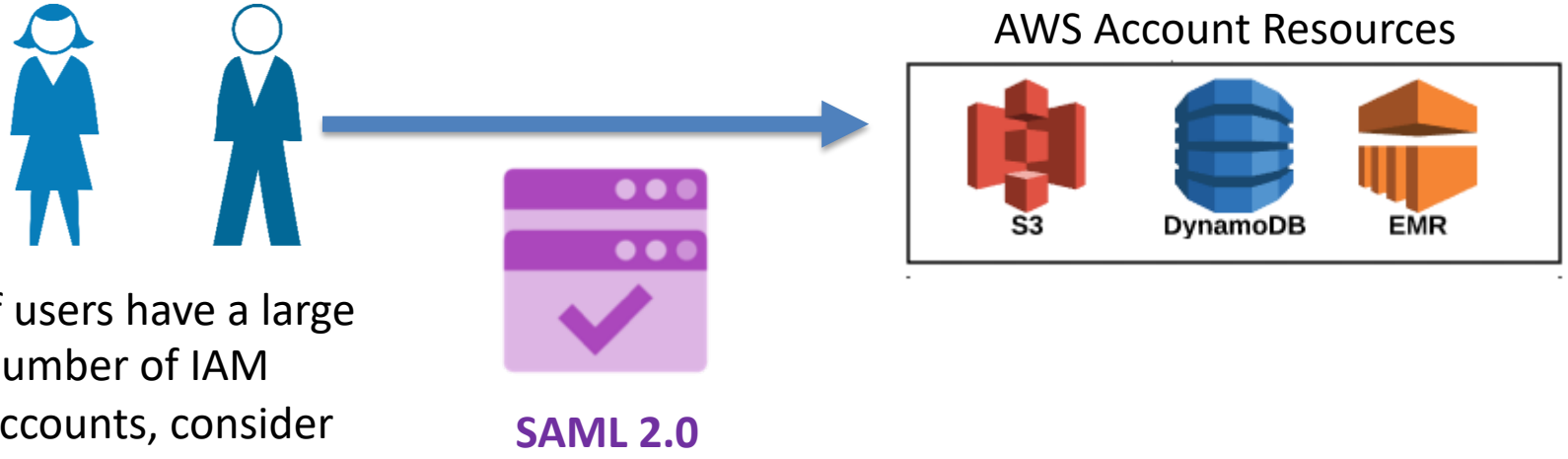
- Amazon CloudFront supports the TLSv1.1 and TLSv1.2 protocols for HTTPS connections between CloudFront and your custom origin webserver
- Selection of cipher suites includes ECDHE protocol on connections to both viewers and the origin



Default Access to AWS Resources



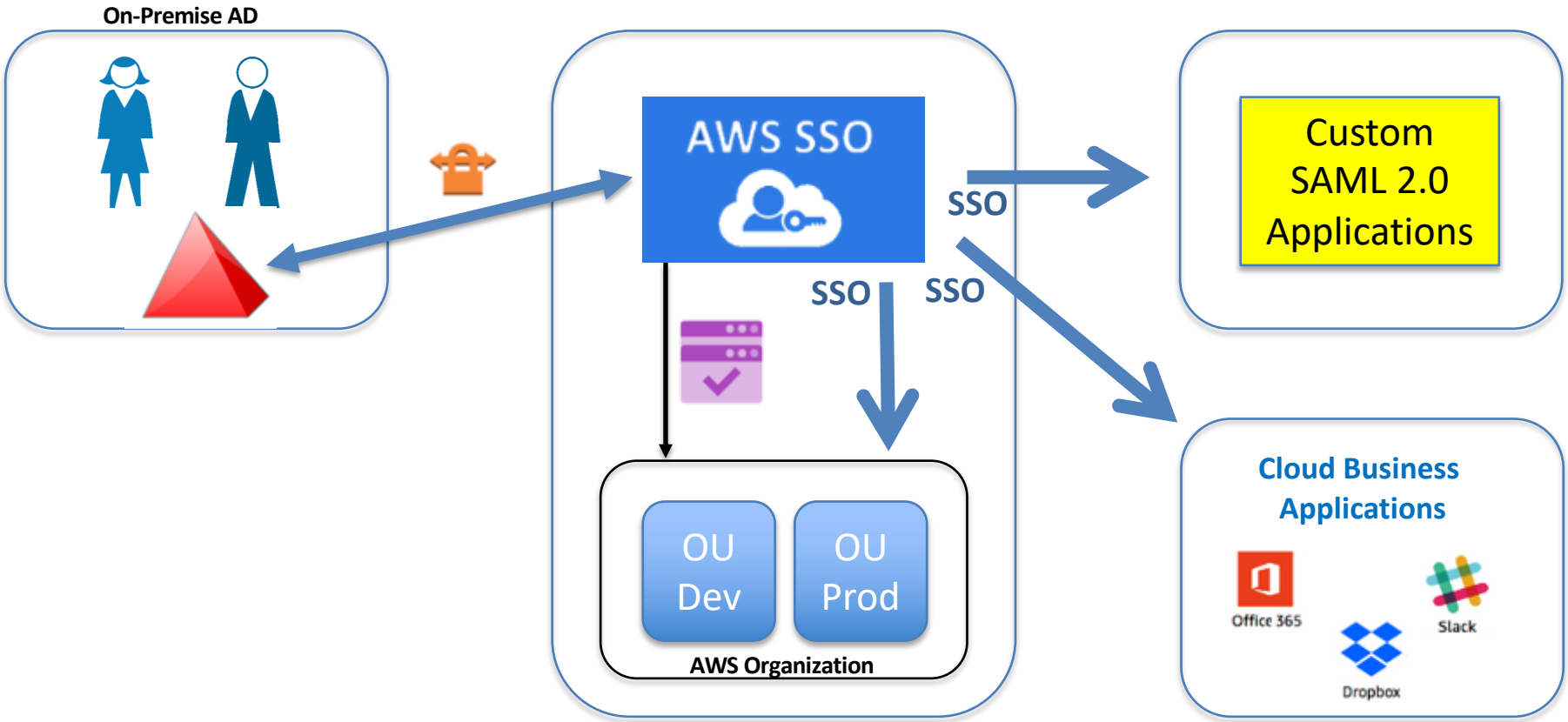
Single-Sign-On Access to AWS



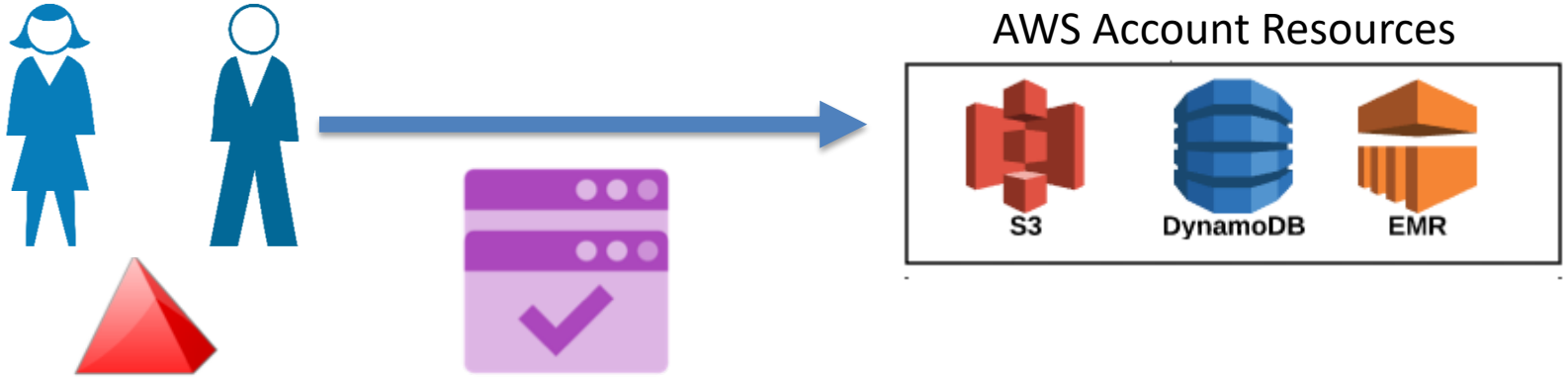
If users have a large number of IAM accounts, consider SAML 2.0 federation to enable single sign-on (SSO)

"Choose Your Own SAML Adventure: A Self-Directed Journey to AWS Identity Federation Mastery" at AWS

AWS Single Sign-On (SSO)



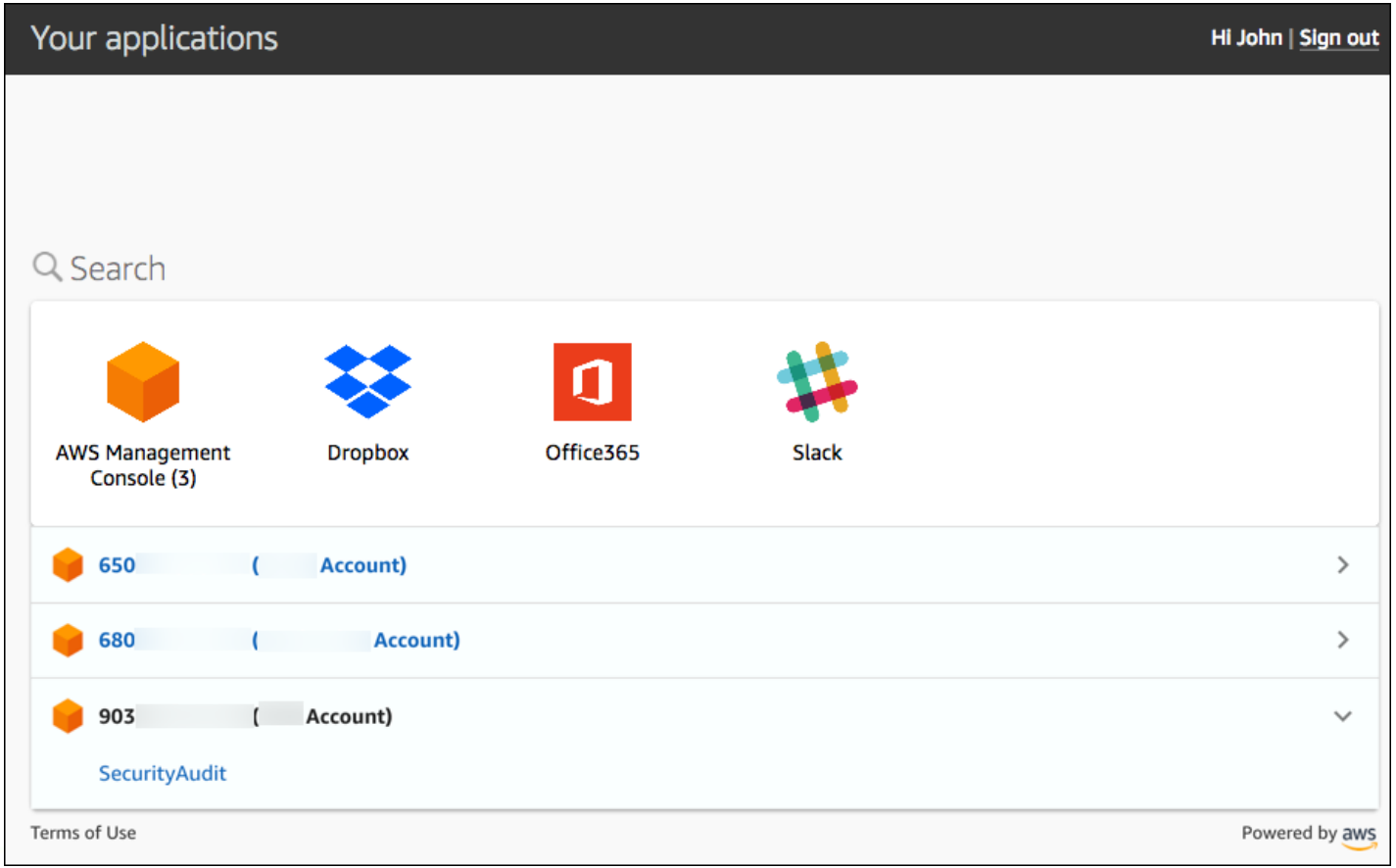
Single-Sign-On Access to AWS



Corporate Microsoft Active Directory

AWS SSO also integrates with Microsoft Active Directory (AD) through AWS Directory Service

AWS SSO Access to Resources



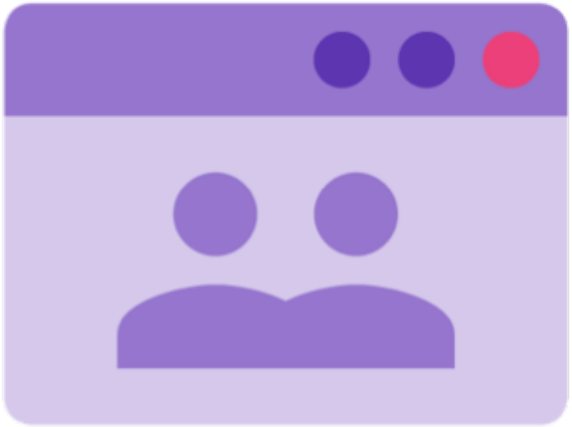
Pearson

Amazon Cognito

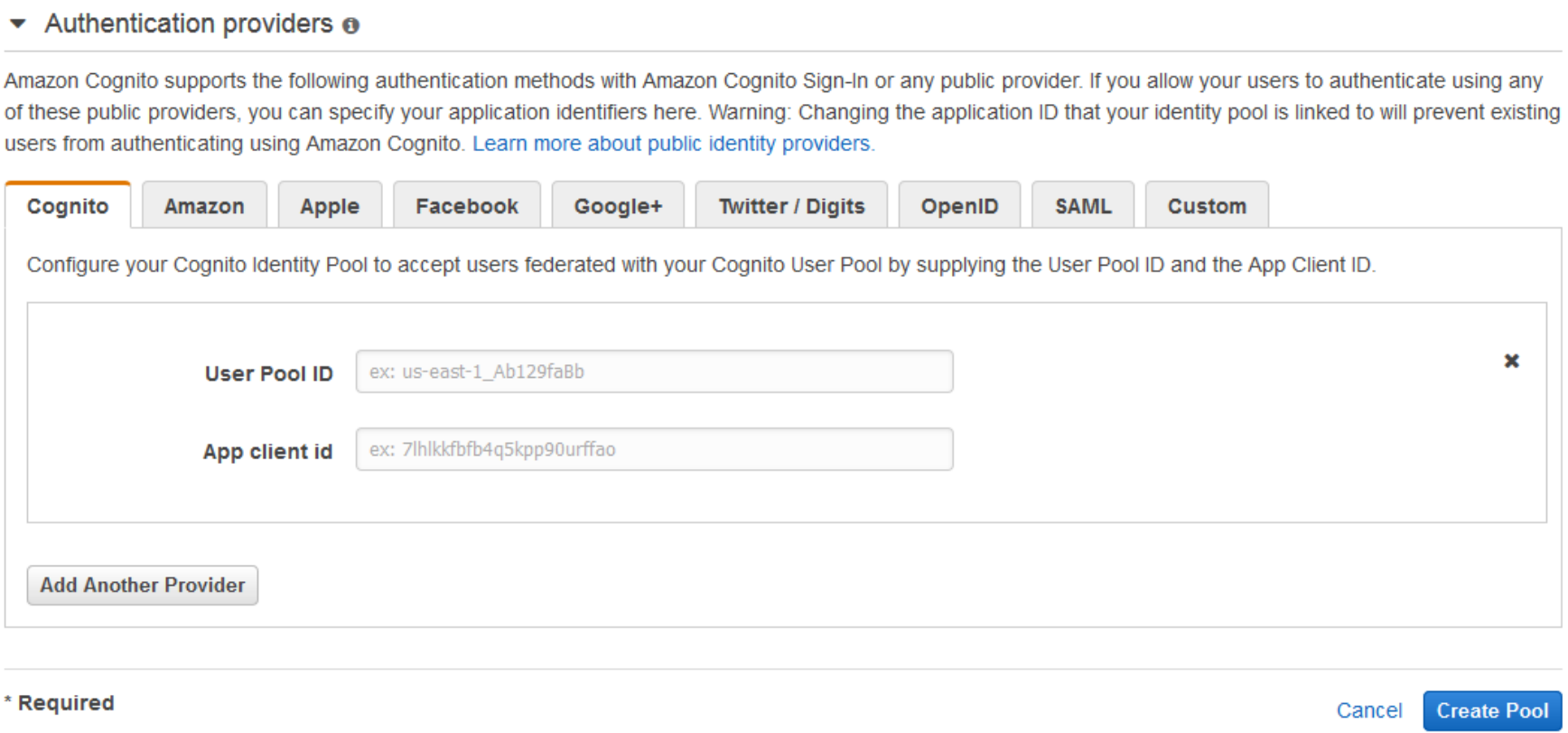
- Amazon Cognito provides user pools and identity pools
- User pools are custom directories that provide sign-up and sign-in options for your app users
- User Pools let you quickly, easily and securely augment sign-up and sign-in features to mobile and web apps
- It’s a fully-managed service that scales to support hundreds of millions of users

Amazon Cognito

- Identity pools offer AWS credentials to give your users access to other AWS services
- With Cognito Identity Pools, your app can get temporary credentials to access AWS services for anonymous guest users or for users who have signed in



Cognito Identity Pools Providers

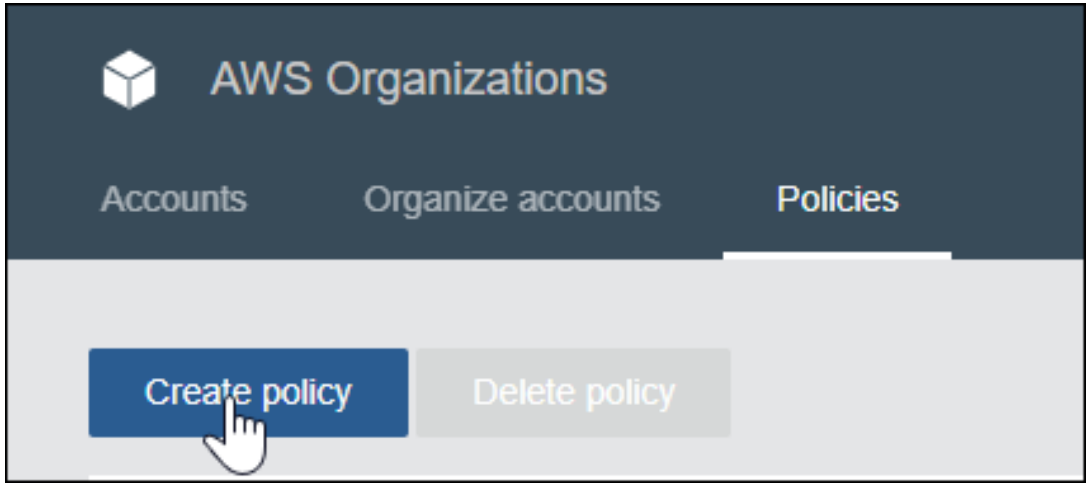


Pearson

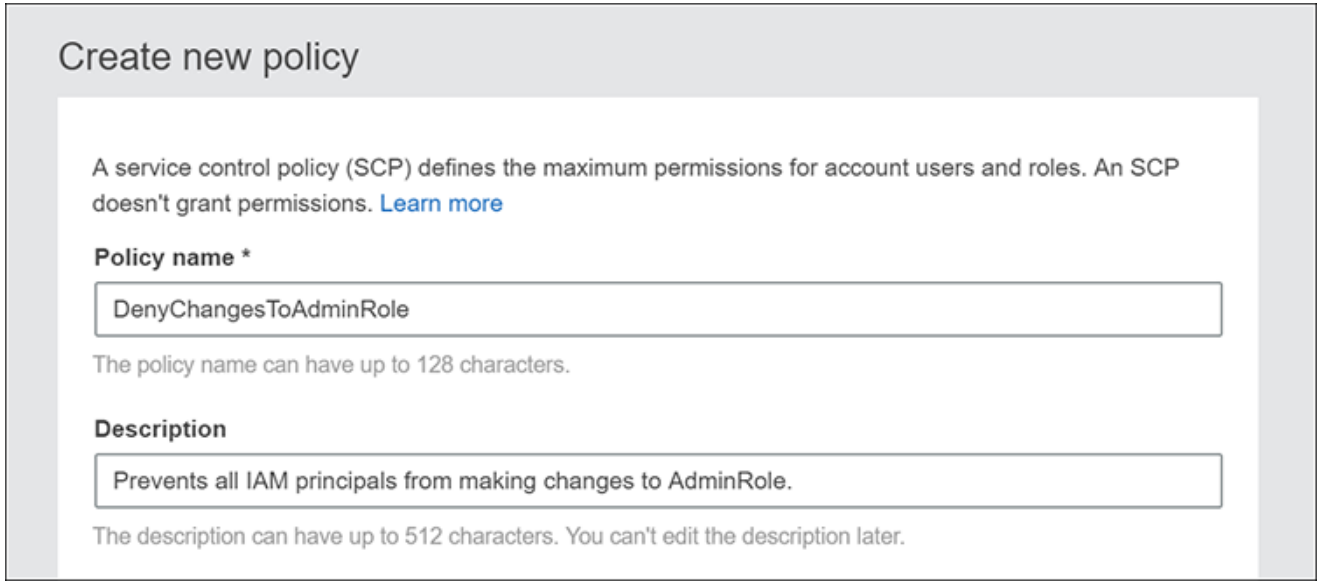
AWS Organizations

- AWS Organizations provide policy-based management for multiple AWS accounts
  - Create groups of accounts
  - Automate account creation
  - Apply and manage policies for account groups
- Can also use Organizations to automate the creation of new accounts through APIs
- Organizations centrally manage Service Control Policies (SCPs) across multiple accounts without using custom scripts or manual processes

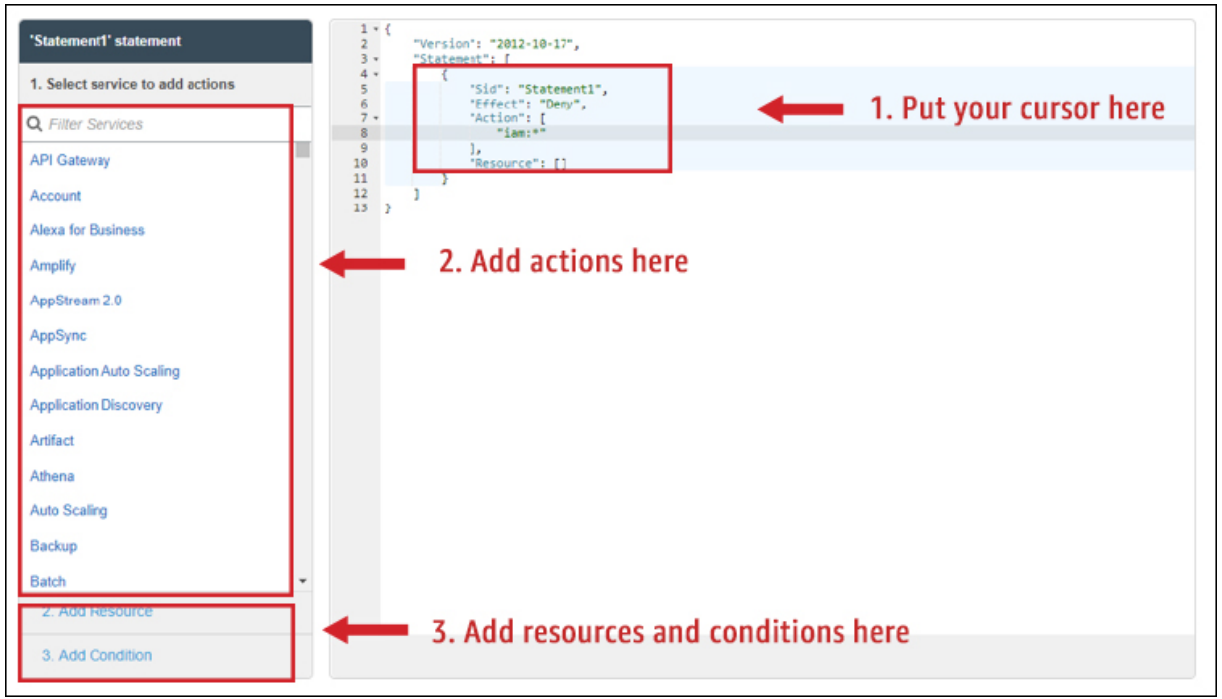
SCP Guardrails



SCP Guardrails



SCP Guardrails



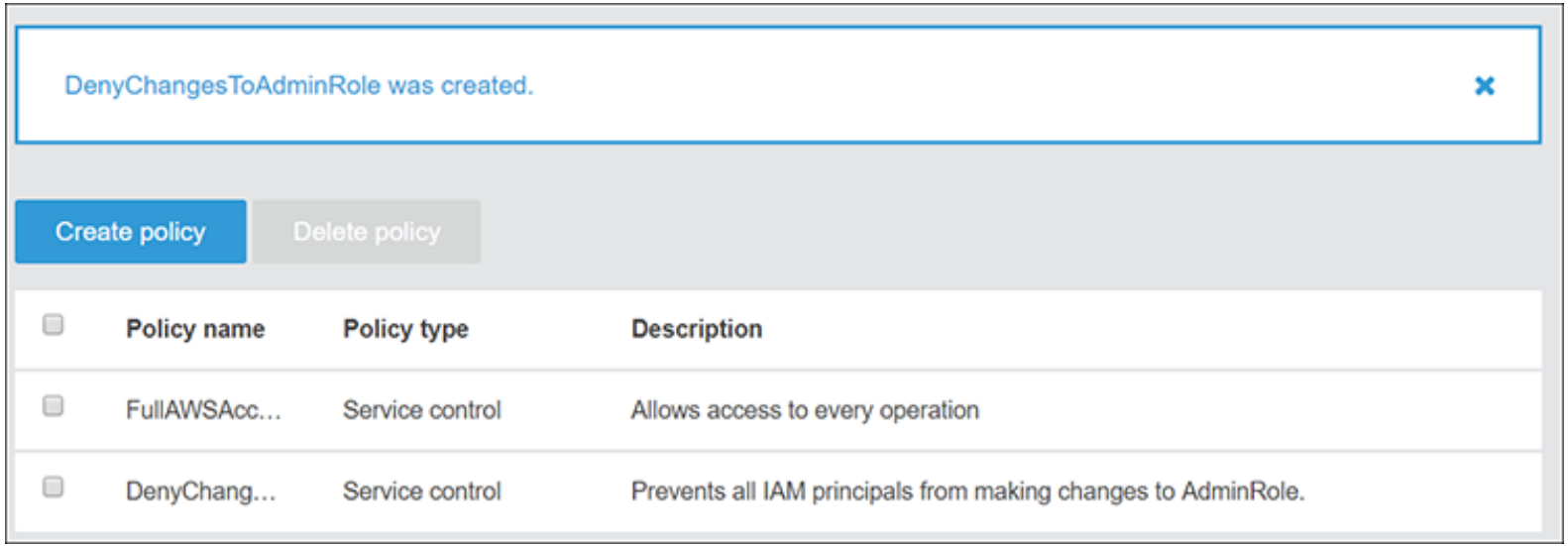
SCP Guardrails

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyChangesToAdminRole",
            "Effect": "Deny",
            "Action": [],
            "Resource": []
        }
    ]
}
```

SCP Guardrails

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Deny",
            "NotAction": [
                "iam:GetContextKeysForPrincipalPolicy",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:ListAttachedRolePolicies",
                "iam:ListInstanceProfilesForRole",
                "iam:ListRolePolicies",
                "iam:ListRoleTags"
            ],
            "Resource": []
        }
    ]
}
```

SCP Guardrails



AWS Security Crash Course

Michael J. Shannon

THANK YOU FOR ATTENDING!