Track 5 | Session 3

迎戰DDoS攻擊的資安最佳實踐

Retro Kuo
Sr. Cloud Support Engineer
Amazon Web Services

aws SUMMIT ONLINE

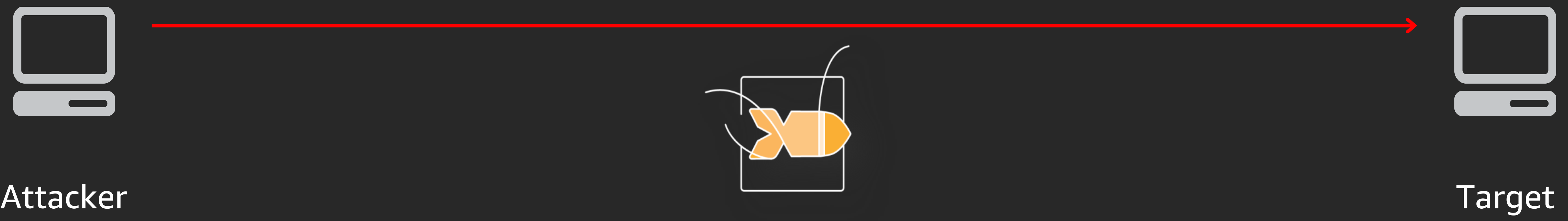
Agenda

- DDoS threats and trends
- Introduction to AWS Support and AWS Shield
- True stories and lesson learned
- Frequently asked questions

DDoS threats and trends

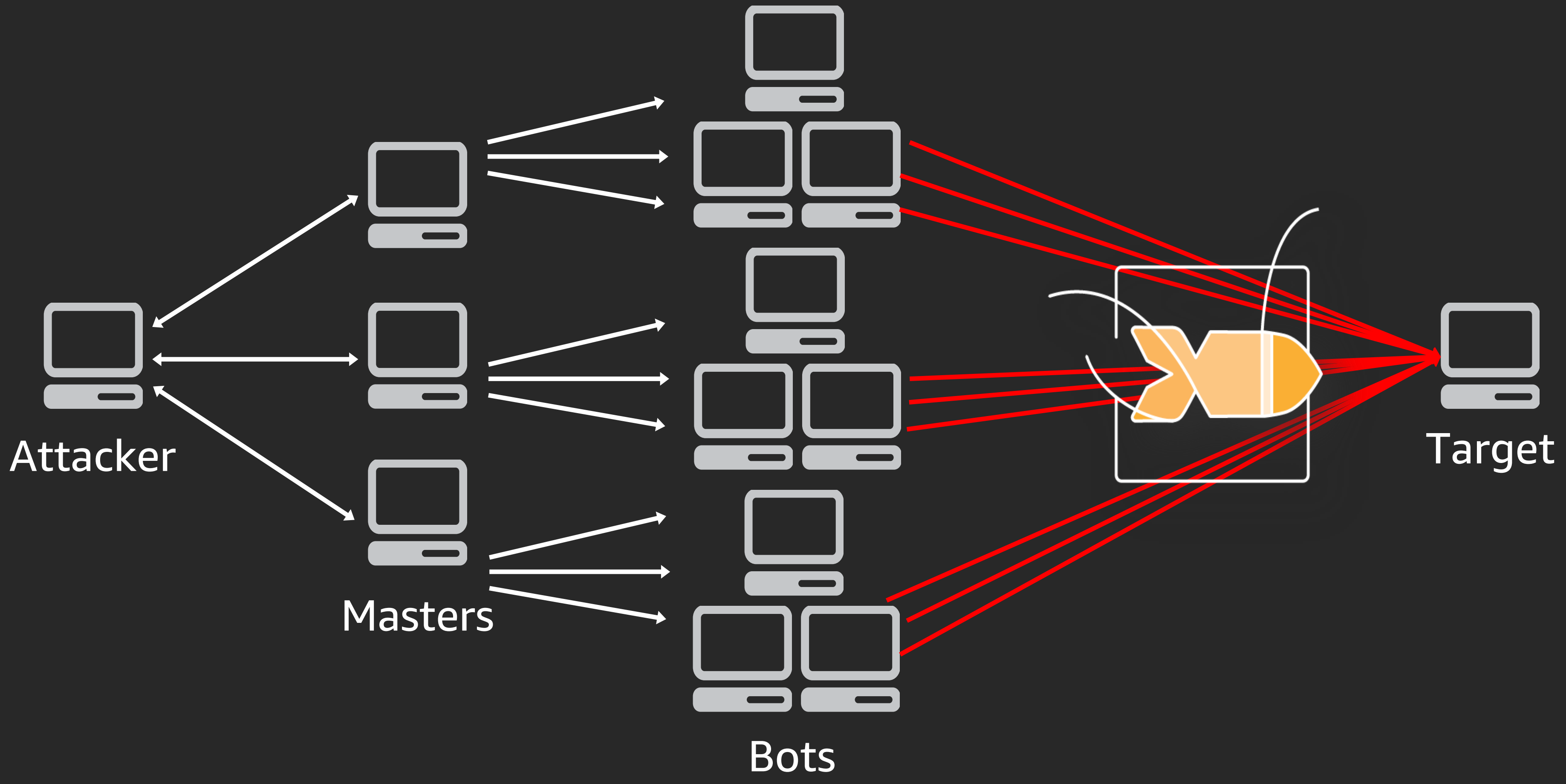
DoS (Denial of Service)

Disrupt access for legitimate users using a variety of techniques that consume large amounts of network bandwidth or tie up other system resources from a single source

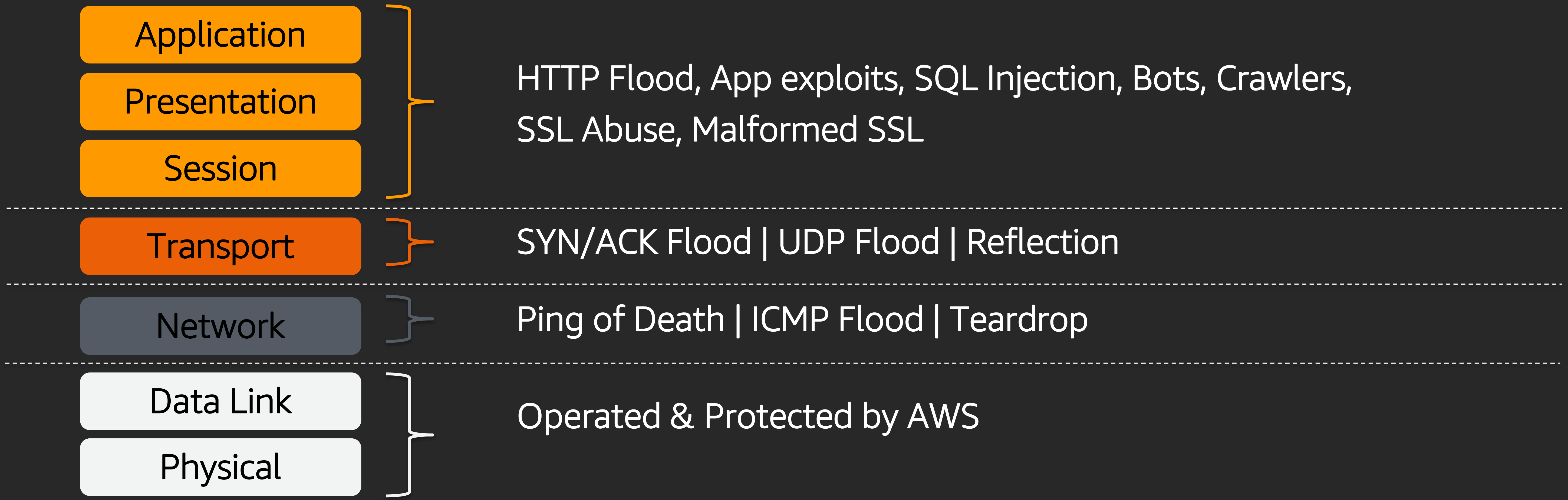


DDoS (Distributed Denial of Service)

Generate a flood of packets or requests to overwhelm a target using multiple sources – which may be distributed groups of malware infected computers, routers, IoT devices, and other endpoints



Types of threats



Application

Presentation

Session

HTTP Flood, App exploits, SQL Injection, Bots, Crawlers, SSL Abuse, Malformed SSL

Transport

SYN/ACK Flood | UDP Flood | Reflection

Network

Ping of Death | ICMP Flood | Teardrop

Data Link

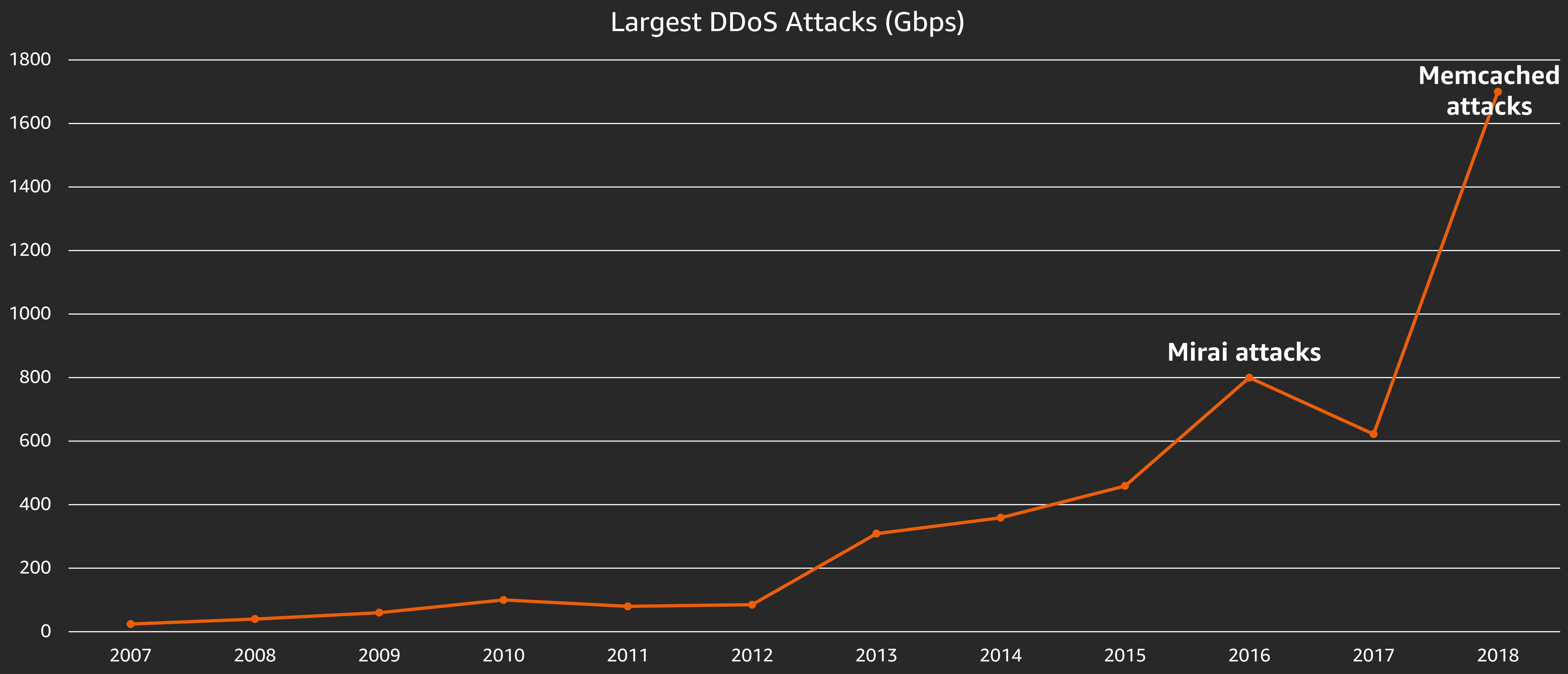
Physical

Operated & Protected by AWS

Types of threats (cont.)

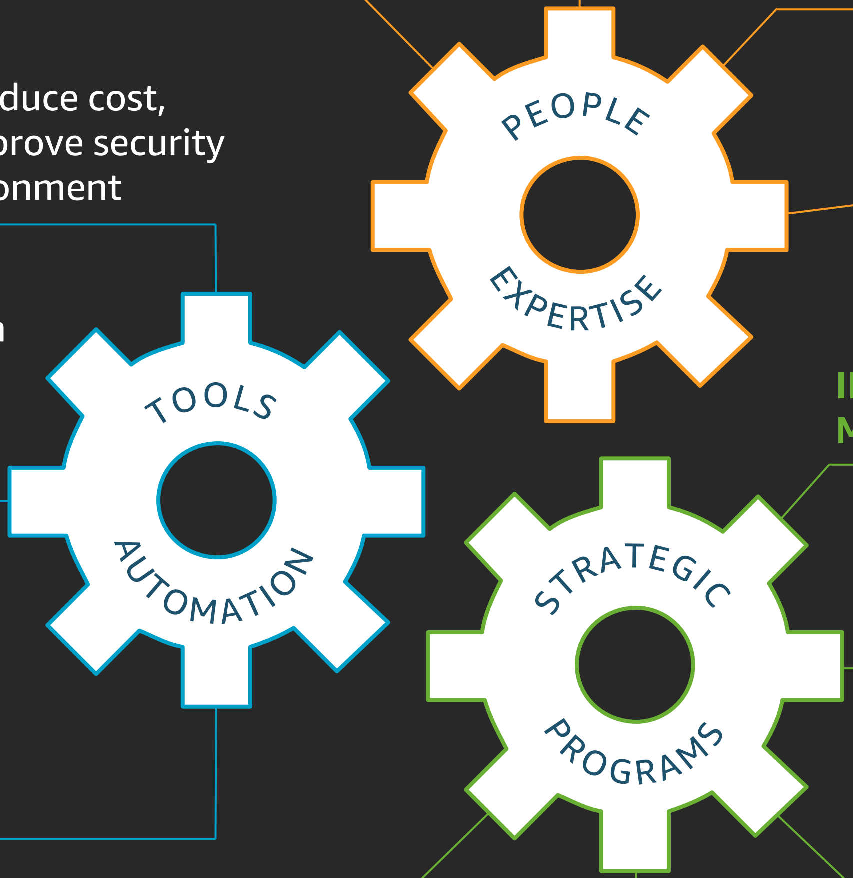
	DDoS	Application Attacks	Bad Bots
Application Layer	HTTP floods Slowloris	SQL injection Application exploits	Crawlers Content scrapers Scanners & probes
Network/ Transport Layer	UDP floods SSL abuse SYN floods UDP reflection		

DDoS size trends



Introduction to AWS Support and AWS Shield

What is AWS Support



TECHNICAL ACCOUNT MANAGER (TAM) Designated technical point of contact to all necessary AWS expertise

SMEs Cloud Support Engineers, Solutions Architects, and product teams are available for guidance

SUPPORT CONCIERGE Dedicated team of enterprise account specialists to help with billing and account subjects

ABUSE TEAM Assists you when AWS resources are impacted by things such as Spam, Port scanning, Denial of Service attacks (DDoS), or malware

TRUSTED ADVISOR (TA) Online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment

PERSONAL HEALTH DASHBOARD (PHD) Delivers alerts and remediation guidance when AWS is experience events that may impact your environment

SUPPORT API Programmatic access to AWS Support Center features to create, manage, and close your support cases, and operationally manage your TA check requests and status

INFRASTRUCTURE EVENT MANAGEMENT (IEM) Focused planning and support business-critical events (e.g. launches or migrations)

WELL-ARCHITECTED REVIEW Detailed review of your architecture guidance on how to best design your systems

ARCHITECTURE SUPPORT Consultative reviews of your application architecture and how to align it with AWS

OPERATIONS SUPPORT Consultative reviews of your cloud operations and advice for optimization

TRAINING Credits for online self-paced labs provided through an AWS training provider

AWS Support plans

	Developer	Business	Enterprise
Email/Live Phone/Chat/Screen Share	Email	✓	✓
3rd Party Software Support**		✓	✓
AWS Trusted Advisor	7 Checks	✓	✓
Response Times	< 12 Hours*	< 1 Hour	< 15 Mins
Technical Account Manager			✓
Infrastructure Event Management		Addt'l Fee	✓

*Business hours are generally defined as 8:00 AM to 6:00 PM in the customer country as set in My Account console, excluding holidays and weekends. These times may vary in countries with multiple time zones.

**For the list of supported third-party software, please visit: http://amzn.to/2wMrK0n

AWS Shield – Standard and Advanced

Built-in DDoS Protection for Everyone	**Point and Protect Wizard**	
Automatic Protection across customers	**Enhanced Protection baselined to you**	**24x7 access to DDoS Response Team (DRT)**
CloudWatch Metrics	**Attack Diagnostics**	**Global Threat Environment Dashboard**
AWS WAF at no additional cost *For protected resources*	**AWS Firewall Manager at no additional cost**	**Cost Protection for scaling**

True stories and lesson learned

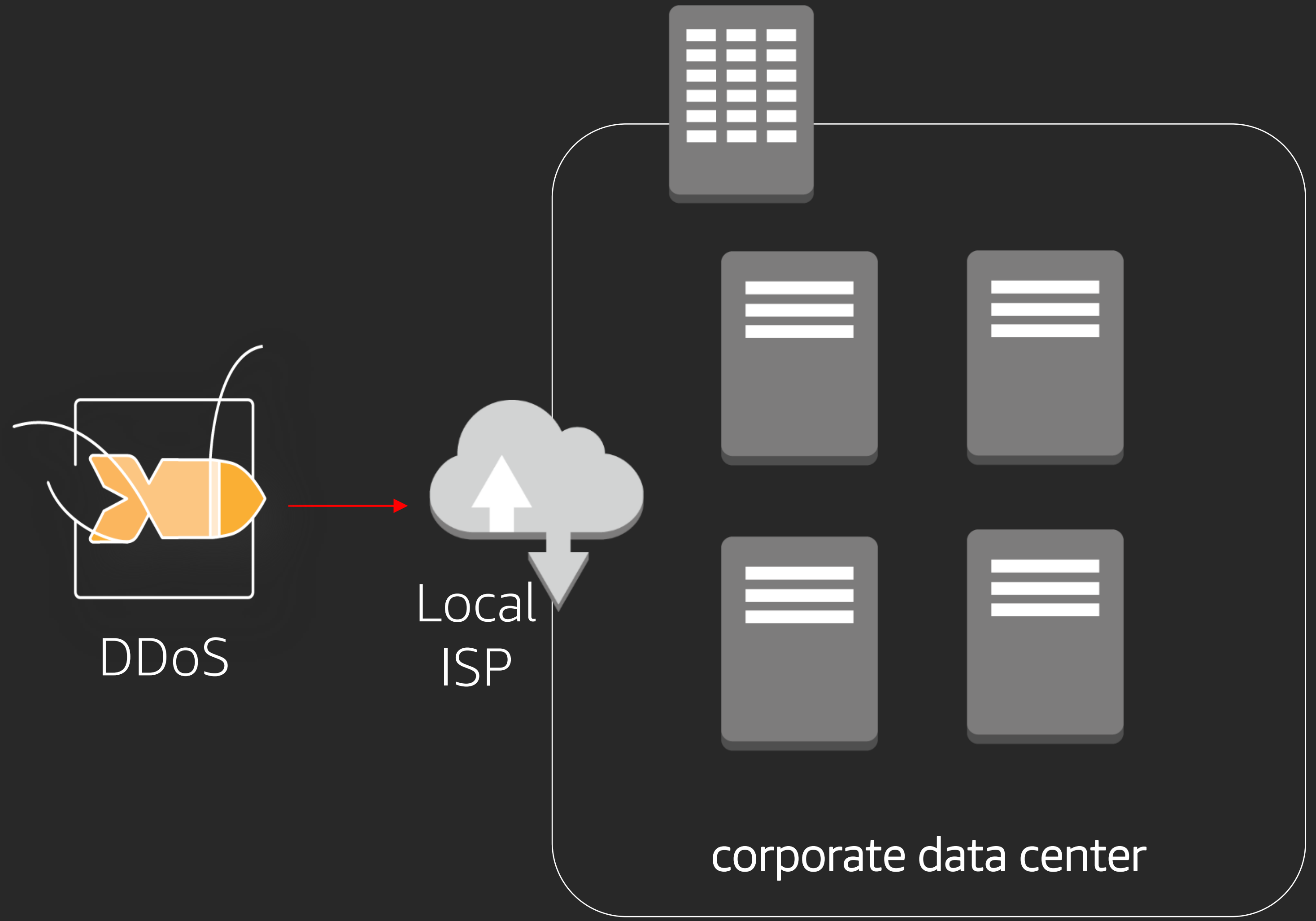
True story #1 (1/3)

Situation

- An Enterprise Support customer's website was under attack

- Not a Shield Advanced customer

- The website was hosted on-premises

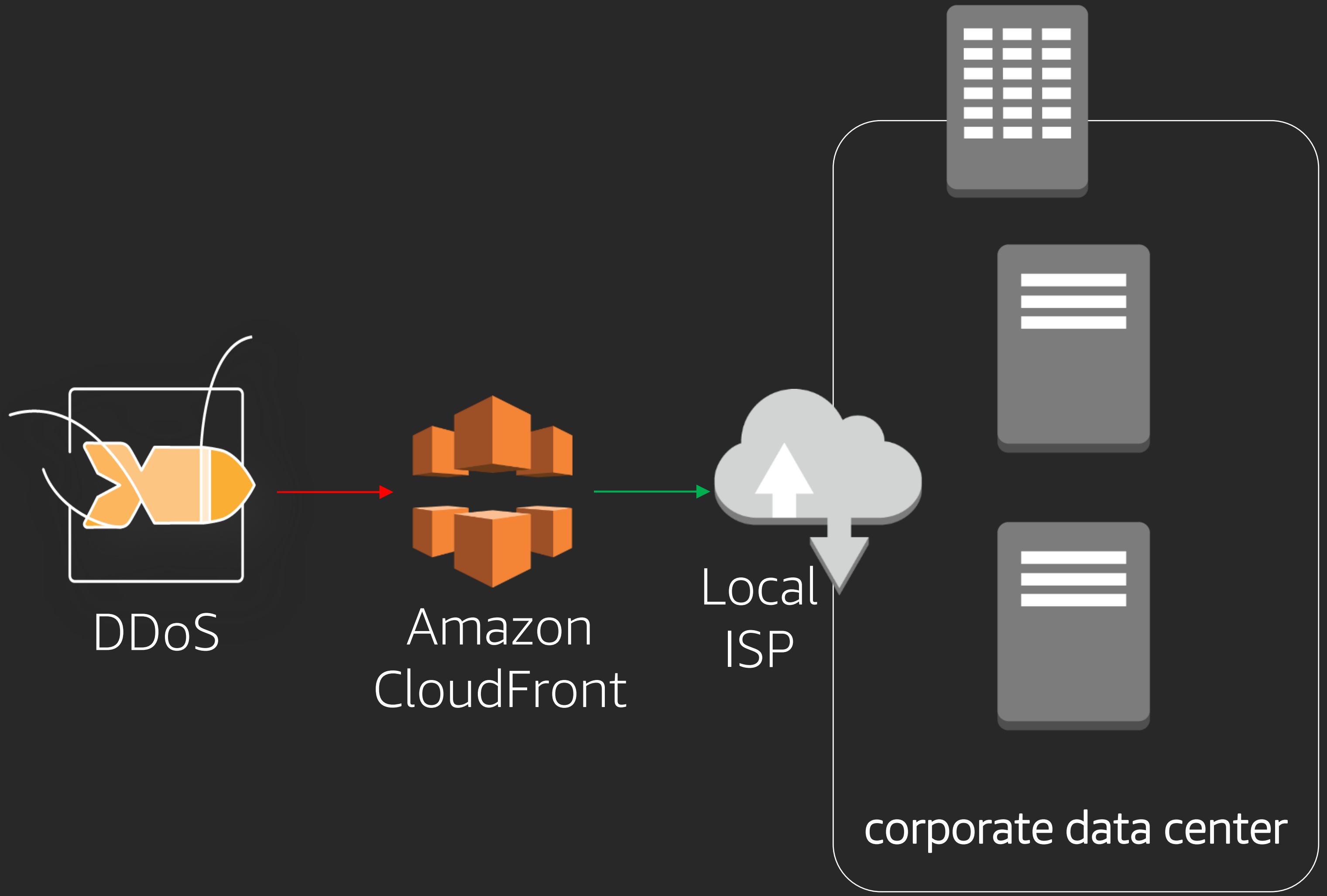


True story #1 (2/3)

Action and Result

- A Cloud Support Engineer (CSE) participated in the call to provide solutions and guide the customer's engineering team to configure AWS resources

- The DDoS attack was mitigated by securing the on-premises servers with Amazon CloudFront



True story #1 (3/3)

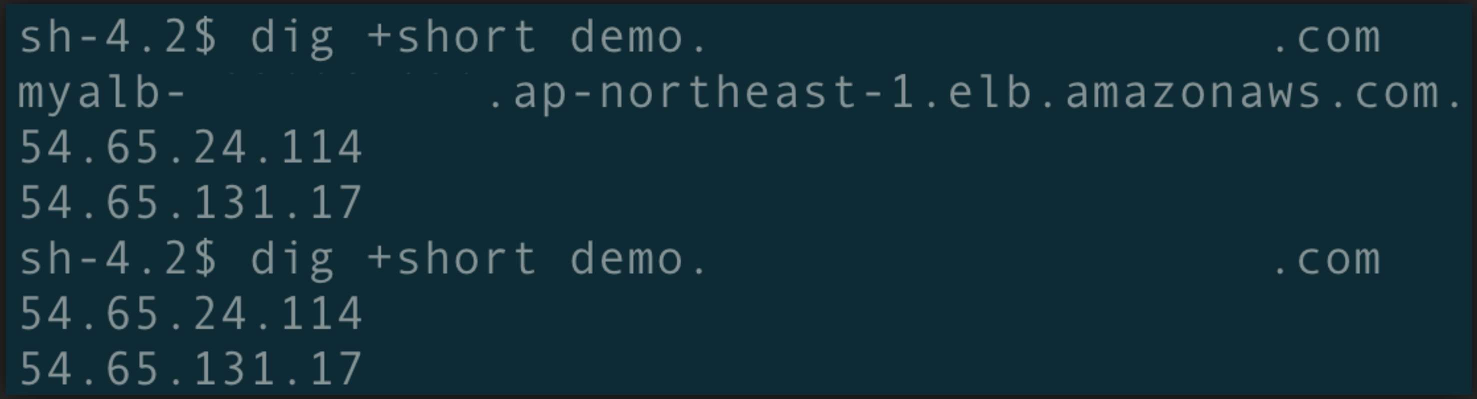
Recommendation and Tips

- Avoid exposure of your origin's domain names and IP addresses

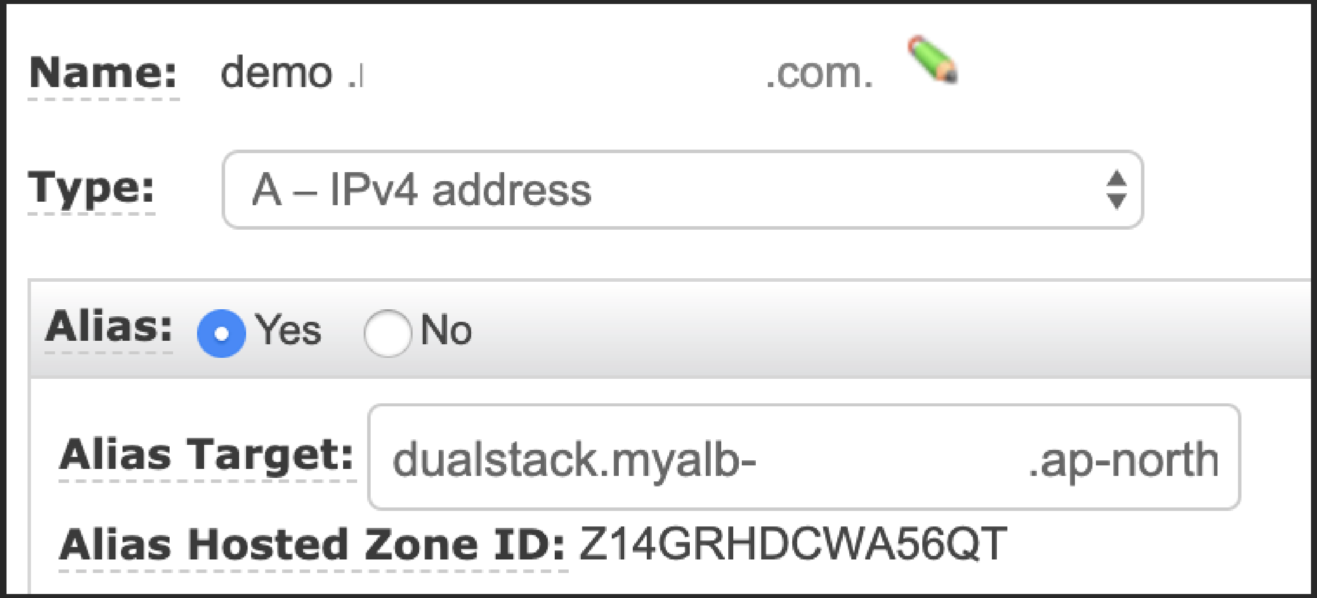
- Whitelist CloudFront IP ranges to enhance security of your origin

- Associate AWS WAF rate limiting rules with CloudFront to mitigate HTTP request flood

- Subscribe to the Business Support plan to create a production system down support case (SLA < 1 hour)



```
sh-4.2$ dig +short demo.                   .com
myalb-          .ap-northeast-1.elb.amazonaws.com.
54.65.24.114
54.65.131.17
sh-4.2$ dig +short demo.                   .com
54.65.24.114
54.65.131.17
```



Name: demo .   .com.

Type: A – IPv4 address

Alias: ● Yes ○ No

Alias Target: dualstack.myalb-   .ap-north

Alias Hosted Zone ID: Z14GRHDCWA56QT

True story #1 (3/3)

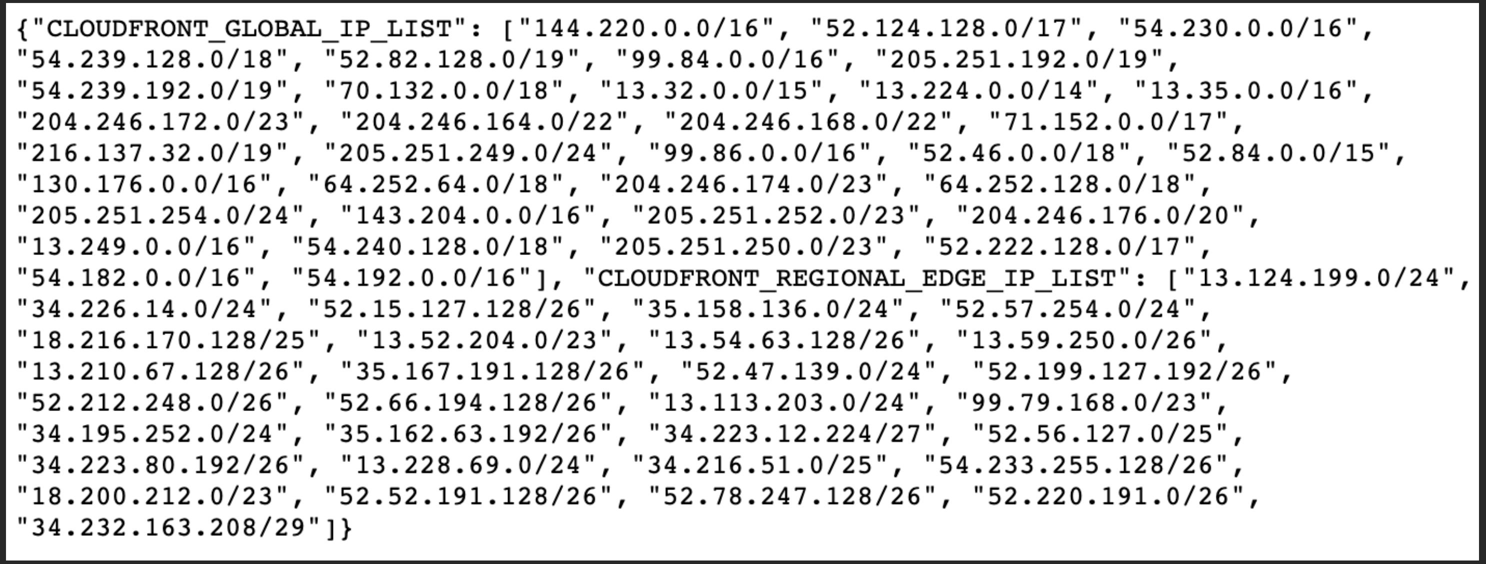
Recommendation and Tips

- Avoid exposure of your origin's domain names and IP addresses

- Whitelist CloudFront IP ranges to enhance security of your origin

- Associate AWS WAF rate limiting rules with CloudFront to mitigate HTTP request flood

- Subscribe to the Business Support plan to create a production system down support case (SLA < 1 hour)



```
{"CLOUDFRONT_GLOBAL_IP_LIST": ["144.220.0.0/16", "52.124.128.0/17", "54.230.0.0/16",
"54.239.128.0/18", "52.82.128.0/19", "99.84.0.0/16", "205.251.192.0/19",
"54.239.192.0/19", "70.132.0.0/18", "13.32.0.0/15", "13.224.0.0/14", "13.35.0.0/16",
"204.246.172.0/23", "204.246.164.0/22", "204.246.168.0/22", "71.152.0.0/17",
"216.137.32.0/19", "205.251.249.0/24", "99.86.0.0/16", "52.46.0.0/18", "52.84.0.0/15",
"130.176.0.0/16", "64.252.64.0/18", "204.246.174.0/23", "64.252.128.0/18",
"205.251.254.0/24", "143.204.0.0/16", "205.251.252.0/23", "204.246.176.0/20",
"13.249.0.0/16", "54.240.128.0/18", "205.251.250.0/23", "52.222.128.0/17",
"54.182.0.0/16", "54.192.0.0/16"], "CLOUDFRONT_REGIONAL_EDGE_IP_LIST": ["13.124.199.0/24",
"34.226.14.0/24", "52.15.127.128/26", "35.158.136.0/24", "52.57.254.0/24",
"18.216.170.128/25", "13.52.204.0/23", "13.54.63.128/26", "13.59.250.0/26",
"13.210.67.128/26", "35.167.191.128/26", "52.47.139.0/24", "52.199.127.192/26",
"52.212.248.0/26", "52.66.194.128/26", "13.113.203.0/24", "99.79.168.0/23",
"34.195.252.0/24", "35.162.63.192/26", "34.223.12.224/27", "52.56.127.0/25",
"34.223.80.192/26", "13.228.69.0/24", "34.216.51.0/25", "54.233.255.128/26",
"18.200.212.0/23", "52.52.191.128/26", "52.78.247.128/26", "52.220.191.0/26",
"34.232.163.208/29"]}
```

Tips: CloudFront IP ranges - https://amzn.to/2m4g48M

How-to: Update security groups automatically using AWS Lambda - https://amzn.to/2ma44Cq

True story #1 (3/3)

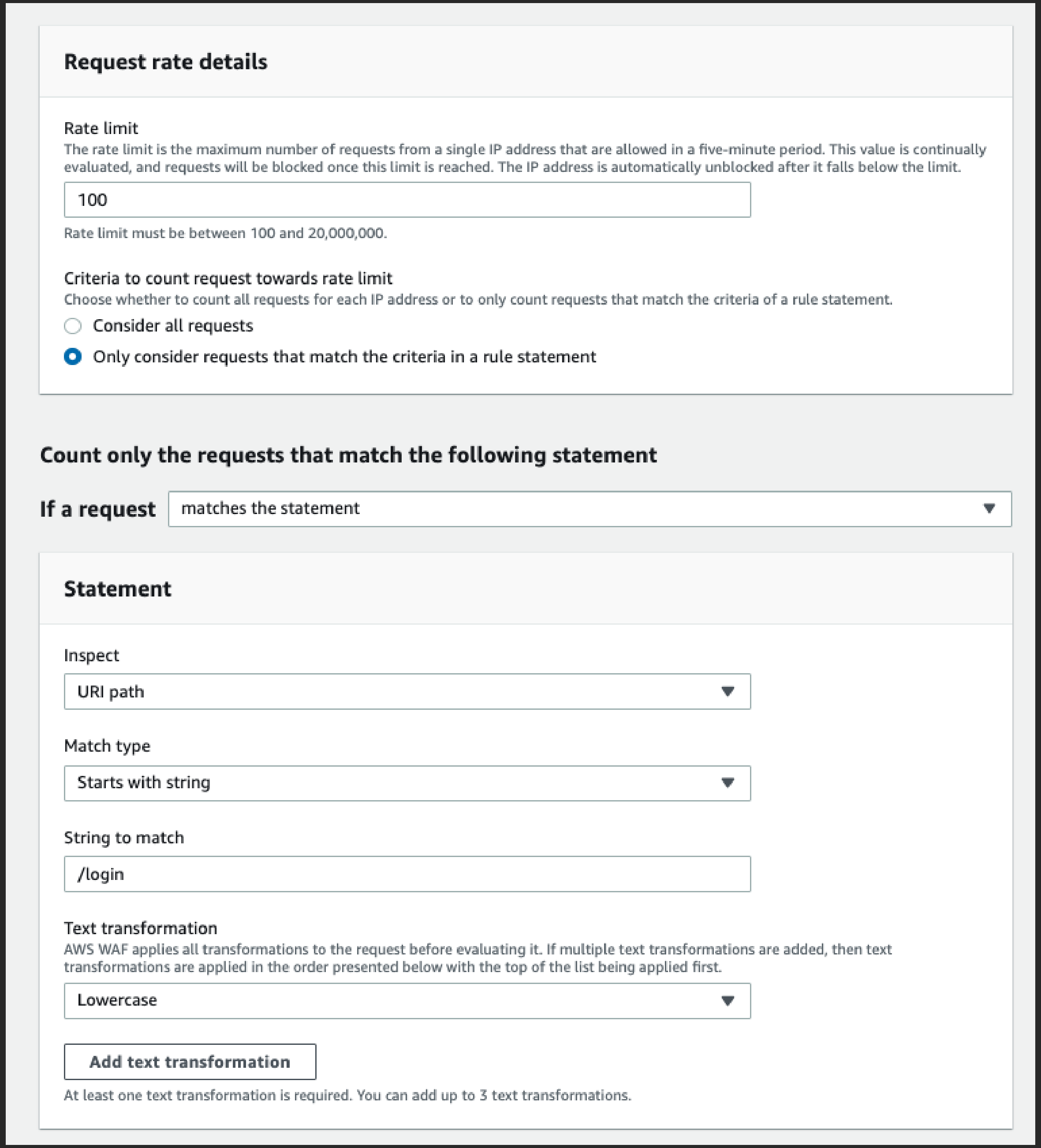
Recommendation and Tips

- Avoid exposure of your origin's domain names and IP addresses

- Whitelist CloudFront IP ranges to enhance security of your origin

- Associate AWS WAF rate limiting rules with CloudFront to mitigate HTTP request flood

- Subscribe to the Business Support plan to create a production system down support case (SLA < 1 hour)



Request rate details

Rate limit

The rate limit is the maximum number of requests from a single IP address that are allowed in a five-minute period. This value is continually evaluated, and requests will be blocked once this limit is reached. The IP address is automatically unblocked after it falls below the limit.

100

Rate limit must be between 100 and 20,000,000.

Criteria to count request towards rate limit

Choose whether to count all requests for each IP address or to only count requests that match the criteria of a rule statement.

○ Consider all requests

● Only consider requests that match the criteria in a rule statement

Count only the requests that match the following statement

If a request matches the statement ▼

Statement

Inspect

URI path ▼

Match type

Starts with string ▼

String to match

/login

Text transformation

AWS WAF applies all transformations to the request before evaluating it. If multiple text transformations are added, then text transformations are applied in the order presented below with the top of the list being applied first.

Lowercase ▼

At least one text transformation is required. You can add up to 3 text transformations.

How-to: Configure AWS WAF rate-based rules - https://amzn.to/3hCmEvt

True story #1 (3/3)

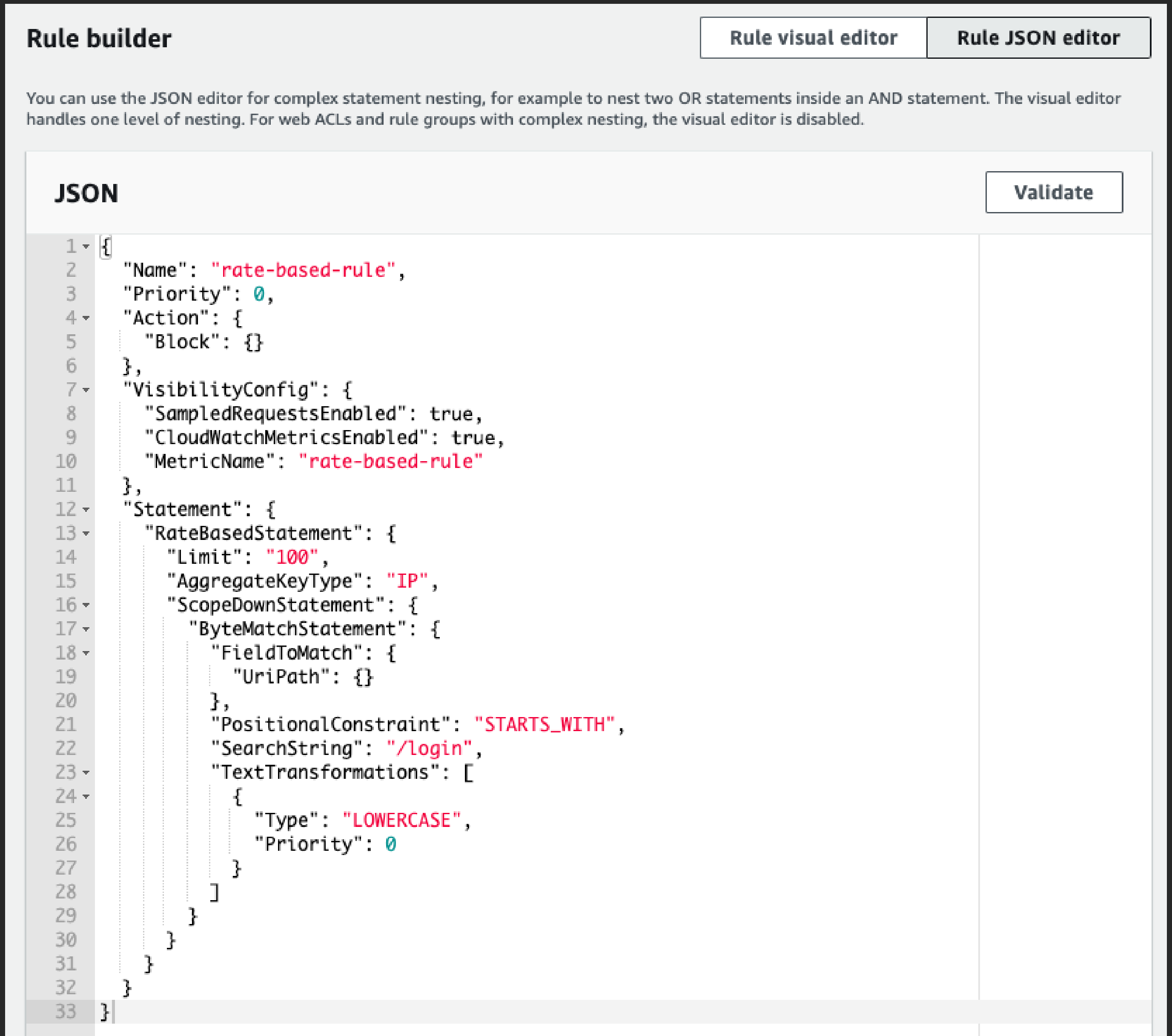
Recommendation and Tips

- Avoid exposure of your origin's domain names and IP addresses

- Whitelist CloudFront IP ranges to enhance security of your origin

- Associate AWS WAF rate limiting rules with CloudFront to mitigate HTTP request flood

- Subscribe to the Business Support plan to create a production system down support case (SLA < 1 hour)



Rule builder

You can use the JSON editor for complex statement nesting, for example to nest two OR statements inside an AND statement. The visual editor handles one level of nesting. For web ACLs and rule groups with complex nesting, the visual editor is disabled.

JSON

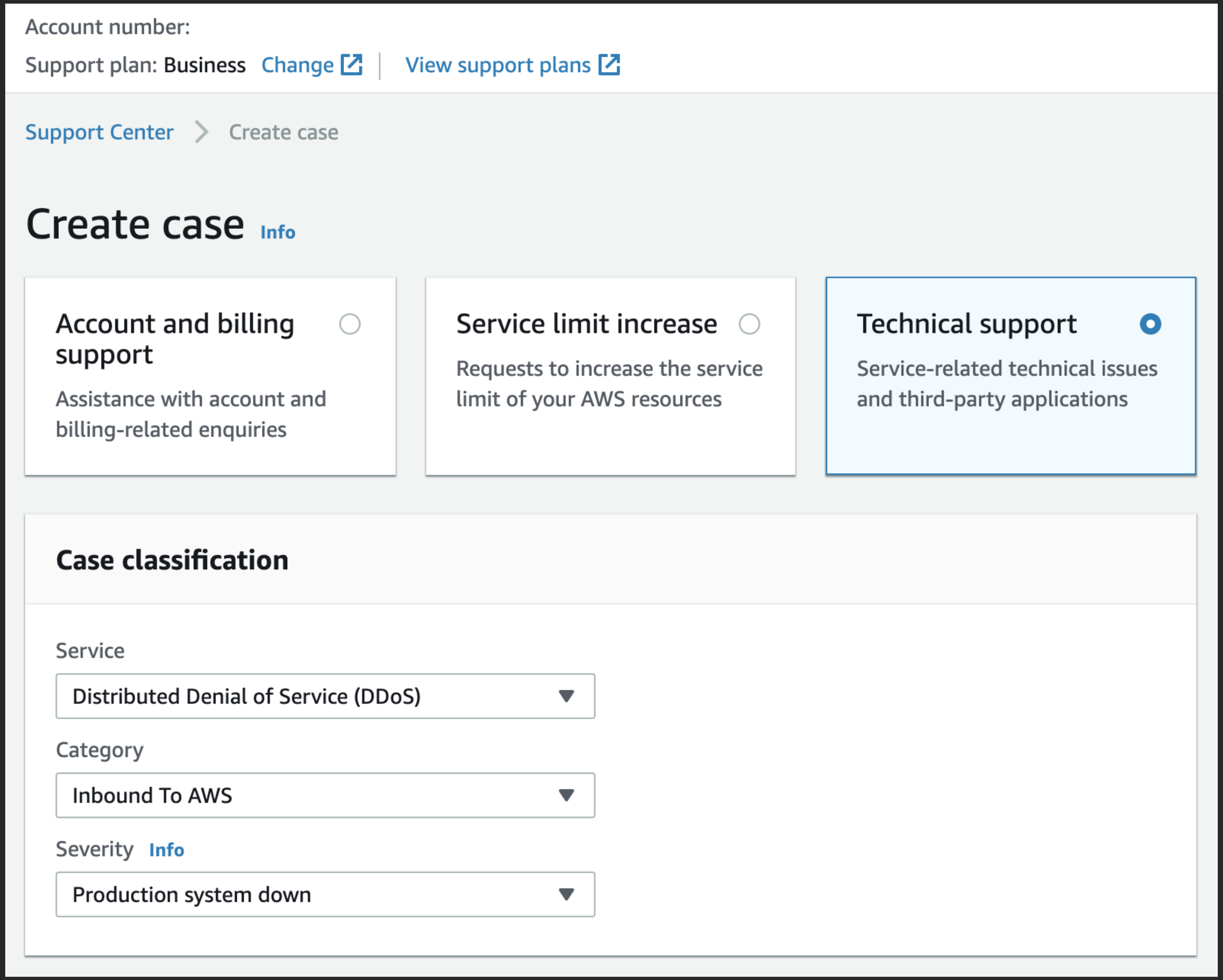
```
{
  "Name": "rate-based-rule",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "rate-based-rule"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": "100",
      "AggregateKeyType": "IP",
      "ScopeDownStatement": {
        "ByteMatchStatement": {
          "FieldToMatch": {
            "UriPath": {}
          },
          "PositionalConstraint": "STARTS_WITH",
          "SearchString": "/login",
          "TextTransformations": [
            {
              "Type": "LOWERCASE",
              "Priority": 0
            }
          ]
        }
      }
    }
  }
}
```

How-to: Configure AWS WAF rate-based rules - https://amzn.to/3hCmEvt

True story #1 (3/3)

Recommendation and Tips

- Avoid exposure of your origin's domain names and IP addresses
- Whitelist CloudFront IP ranges to enhance security of your origin
- Associate AWS WAF rate limiting rules with CloudFront to mitigate HTTP request flood
- Subscribe to the Business Support plan to create a production system down support case (SLA < 1 hour)



Account number:

Support plan: Business Change | View support plans

Support Center > Create case

Create case Info

Account and billing support ○
Assistance with account and billing-related enquiries

Service limit increase ○
Requests to increase the service limit of your AWS resources

Technical support ●
Service-related technical issues and third-party applications

Case classification

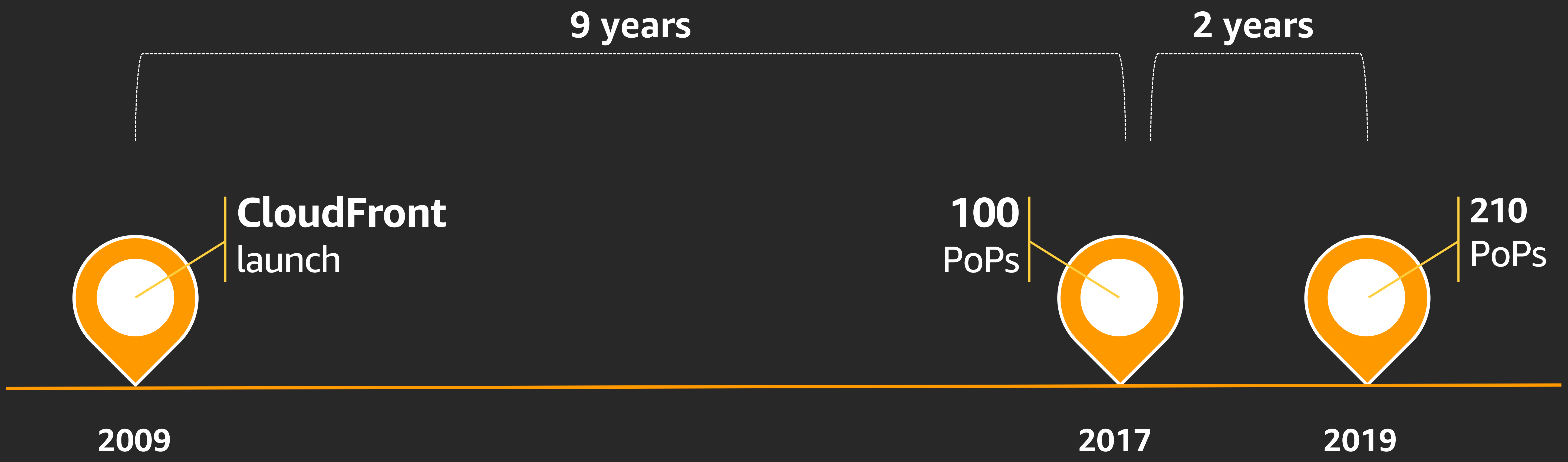
Service: Distributed Denial of Service (DDoS)

Category: Inbound To AWS

Severity Info: Production system down

Amazon CloudFront

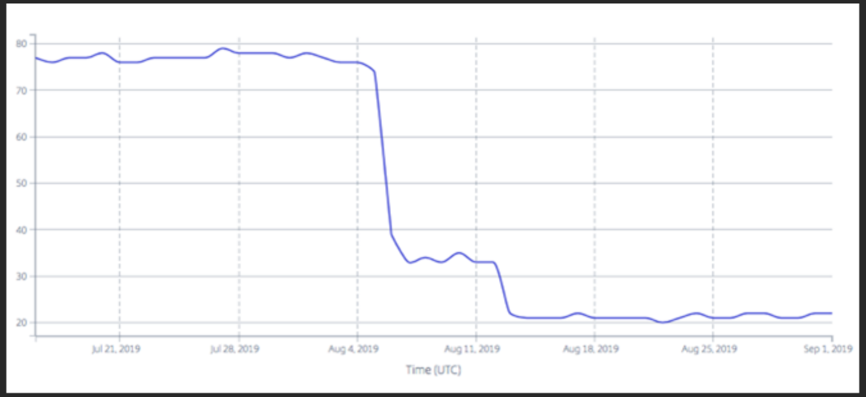
110 new PoPs in the last two years



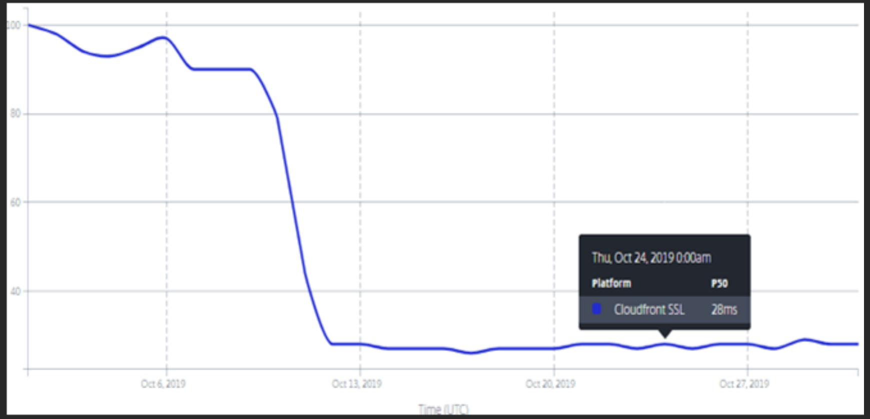
Latency benefits with PoP launches

PoP launches ensure connectivity with majority views and redundant AWS backbone

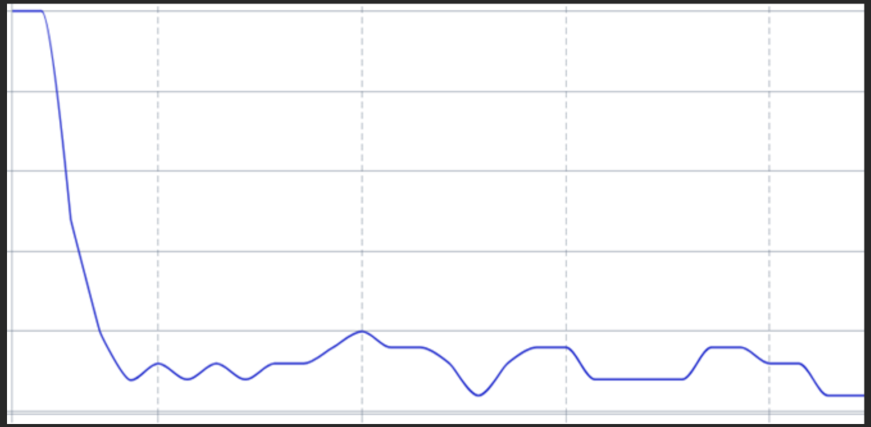
Israel
75% Latency reduction
78 ms → 20 ms



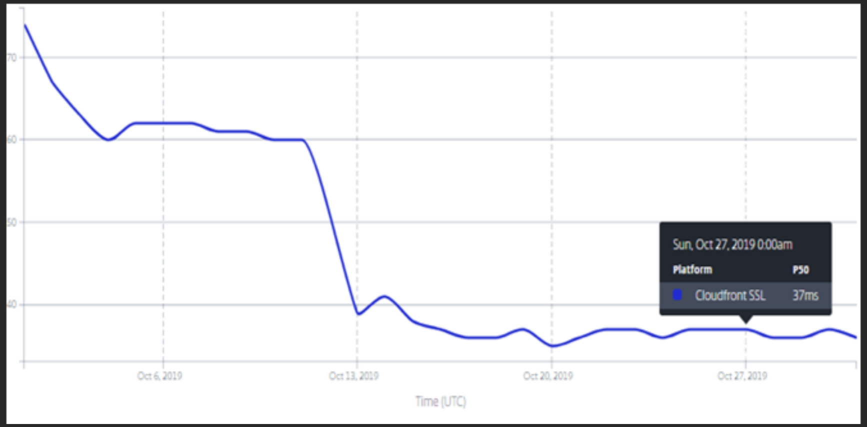
Chile
73% Latency reduction
104 ms → 28 ms



Bahrain:
40% Latency reduction
38 ms → 27 ms



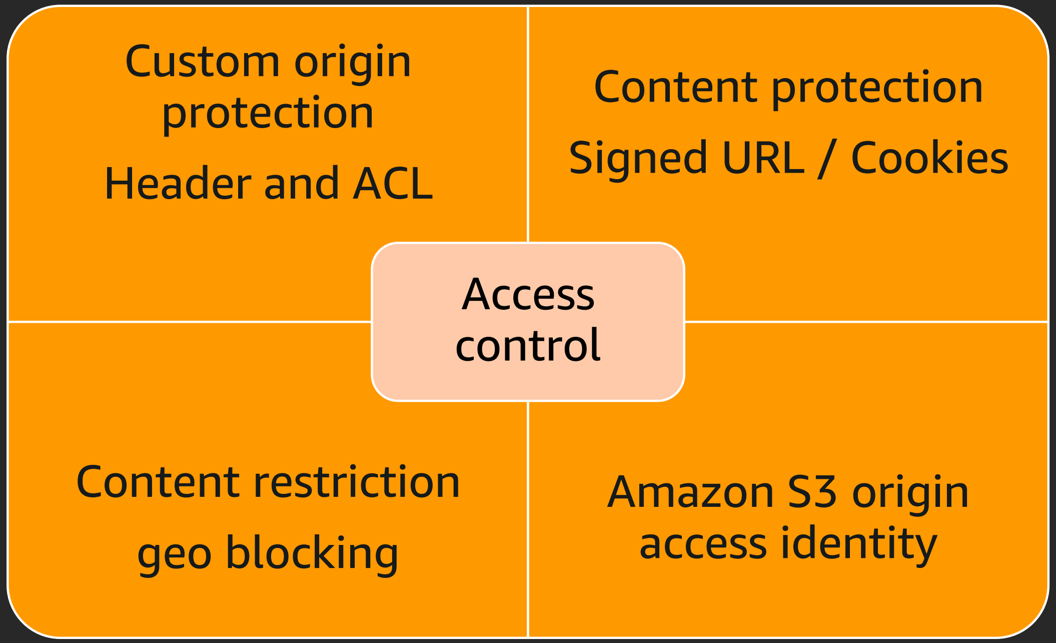
Argentina
55% Latency reduction
79 ms → 35 ms



P50 FBL according to Cedexis

Advanced security capabilities

Robust content protection controls & encryption



Custom origin protection

Header and ACL

Content protection

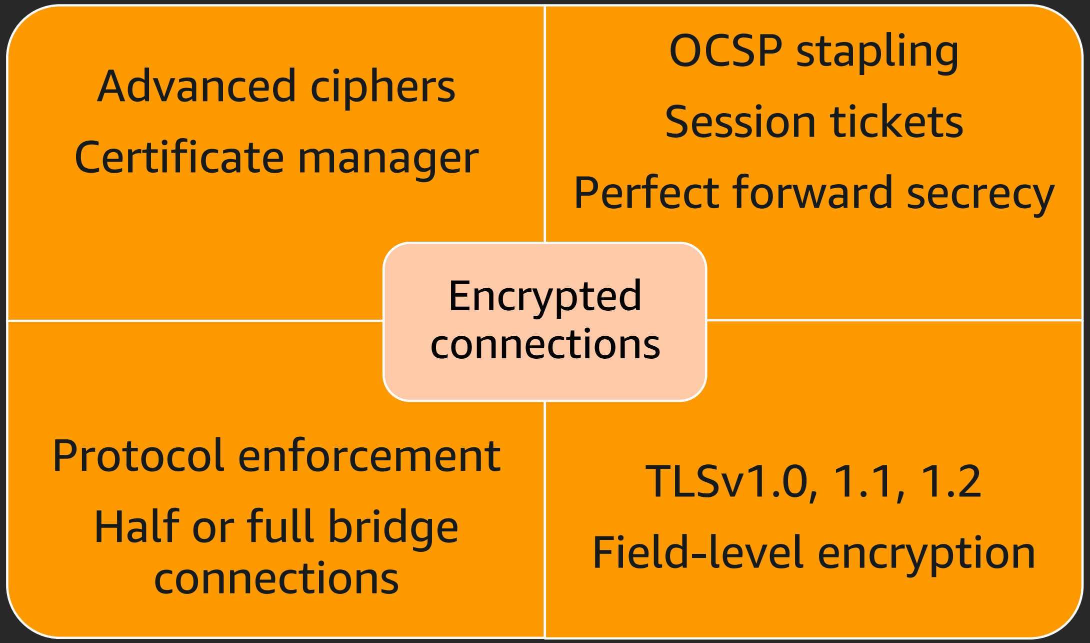
Signed URL / Cookies

Access control

Content restriction

geo blocking

Amazon S3 origin access identity



Advanced ciphers

Certificate manager

OCSP stapling

Session tickets

Perfect forward secrecy

Encrypted connections

Protocol enforcement

Half or full bridge connections

TLSv1.0, 1.1, 1.2

Field-level encryption

Integrations with AWS security services

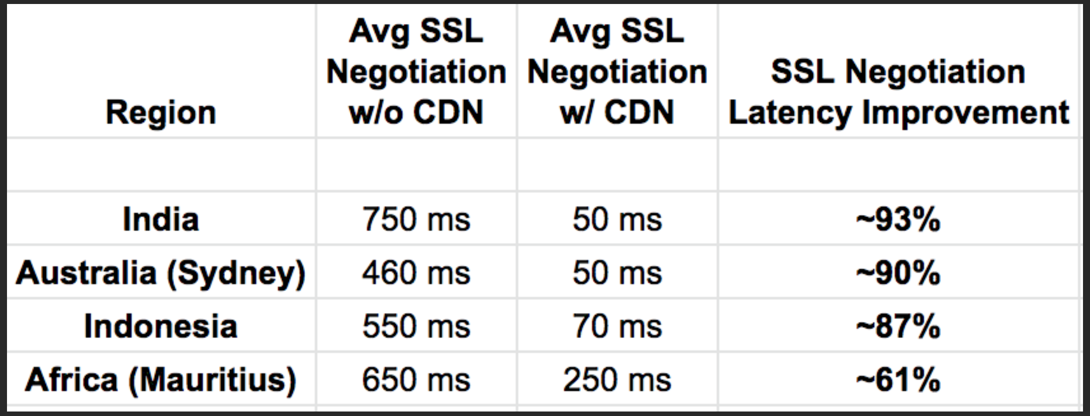
- AWS WAF
- AWS Shield
- AWS Certificate Manager (ACM)
- AWS Identity and Access Management (IAM)
- AWS Config
- AWS CloudTrail

API acceleration with CloudFront

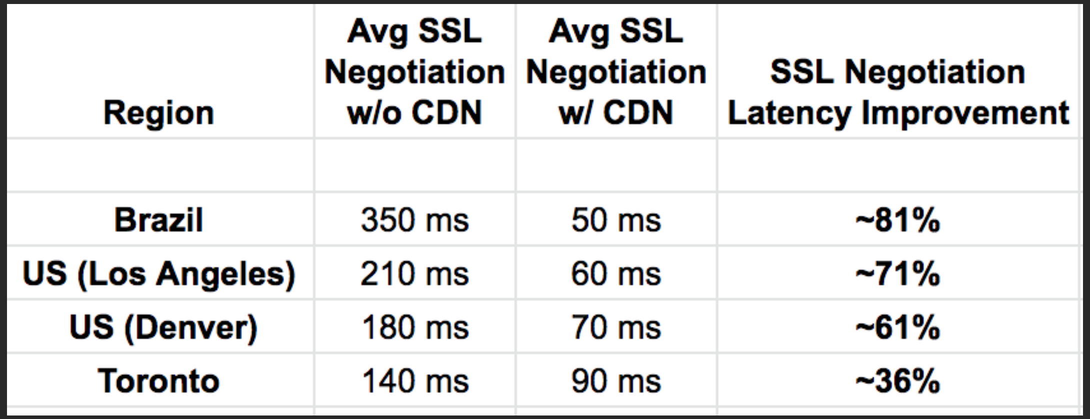
- TLS termination at edge
- Network optimizations: persistent connections, connection pooling, keep-alive
- AWS private backbone
- Edge DDoS protection

“The performance gains are amazing, positively impacting our app’s usage across the globe, especially in Regions further from US EAST 1.”

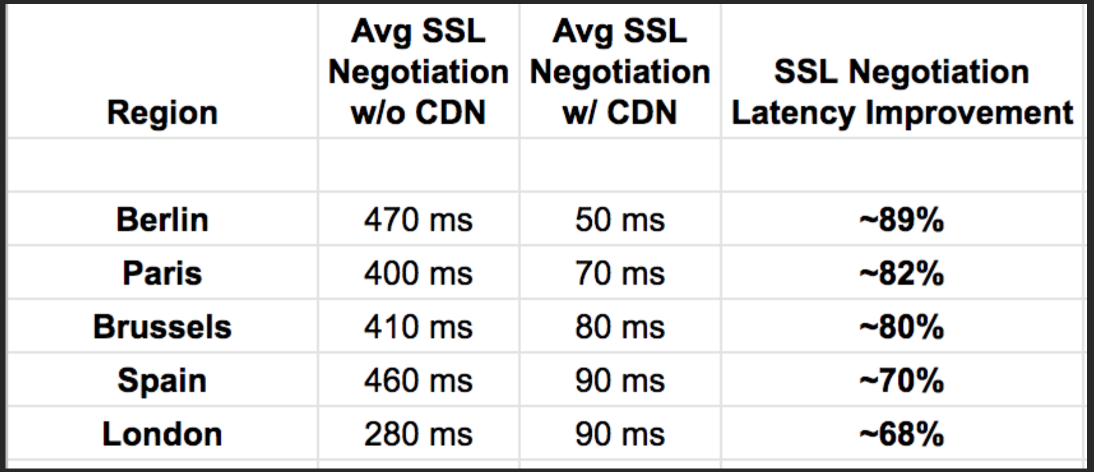
Sample data from a customer test



Region	Avg SSL Negotiation w/o CDN	Avg SSL Negotiation w/ CDN	SSL Negotiation Latency Improvement
India	750 ms	50 ms	~93%
Australia (Sydney)	460 ms	50 ms	~90%
Indonesia	550 ms	70 ms	~87%
Africa (Mauritius)	650 ms	250 ms	~61%



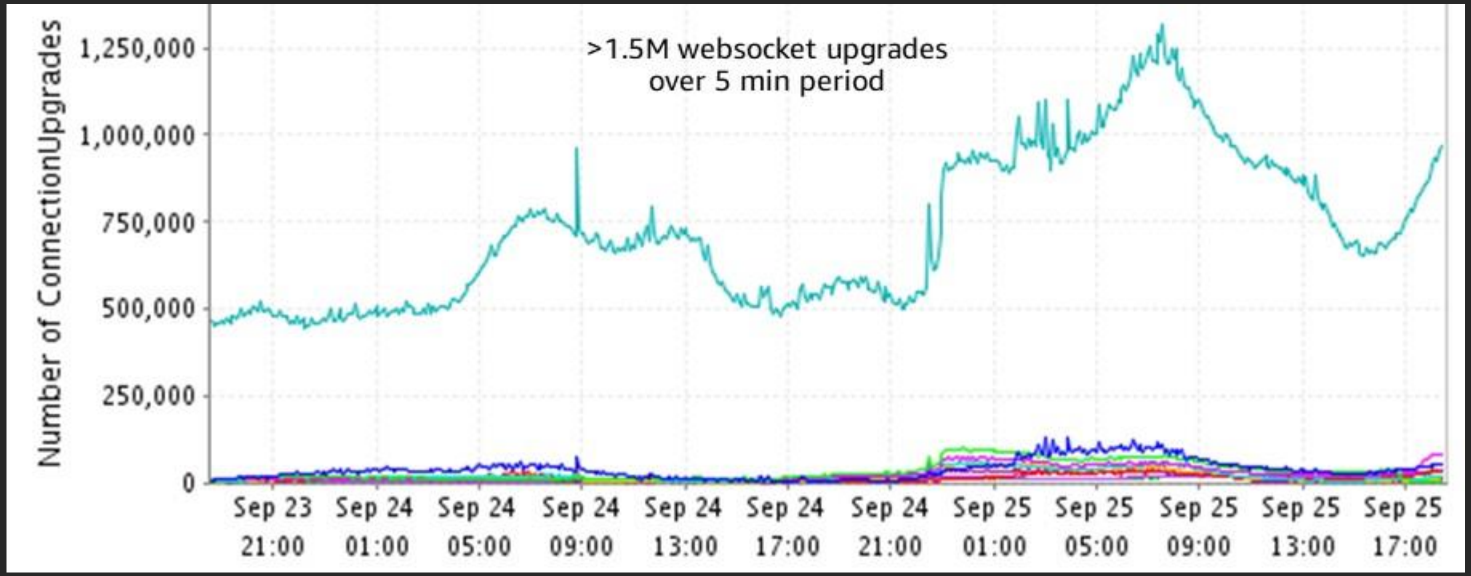
Region	Avg SSL Negotiation w/o CDN	Avg SSL Negotiation w/ CDN	SSL Negotiation Latency Improvement
Brazil	350 ms	50 ms	~81%
US (Los Angeles)	210 ms	60 ms	~71%
US (Denver)	180 ms	70 ms	~61%
Toronto	140 ms	90 ms	~36%



Region	Avg SSL Negotiation w/o CDN	Avg SSL Negotiation w/ CDN	SSL Negotiation Latency Improvement
Berlin	470 ms	50 ms	~89%
Paris	400 ms	70 ms	~82%
Brussels	410 ms	80 ms	~80%
Spain	460 ms	90 ms	~70%
London	280 ms	90 ms	~68%

Dynamic content: WebSocket support

- Use cases: Bi-directional and real-time communication between client and server
- Commonly used for chat applications, online collaboration platforms, and financial trading platforms



"CloudFront WebSocket support means that we can simplify our infrastructure and further improve customer satisfaction. CloudFront edge locations will now contribute to better user performance in WebSocket apps"

coins.ph

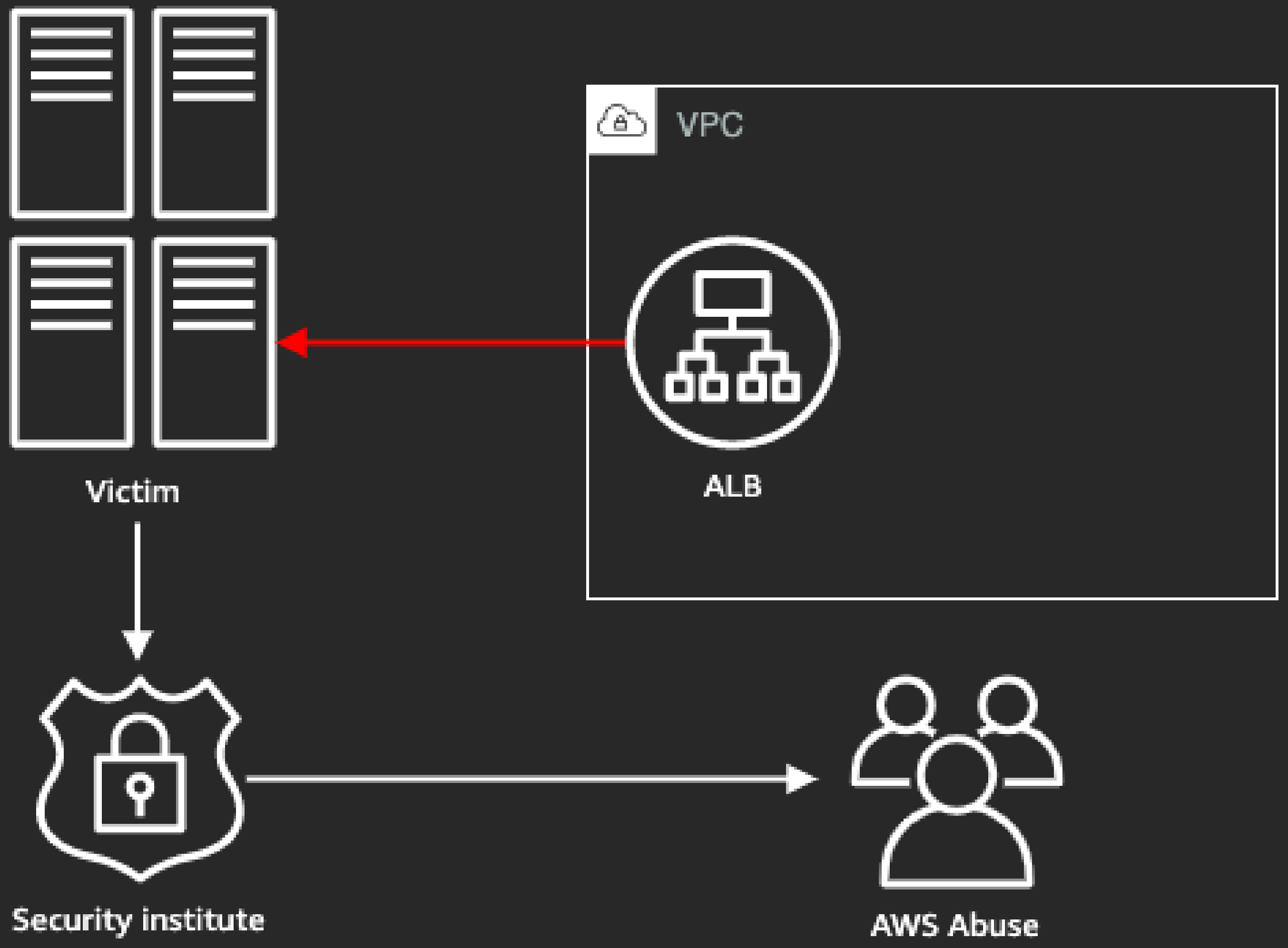
"CloudFront now supporting WebSockets enables us to consolidate both our dynamic and static content delivery under a single distribution, improving global reach, enhancing app security, and simplifying our delivery architecture all at the same time. "

Evolution Gaming

True story #2 (1/3)

Situation

- An Enterprise Support customer's Elastic Load Balancer was reported as the source of attacks (sending SYN-ACK to port 22) by a third-party security institute

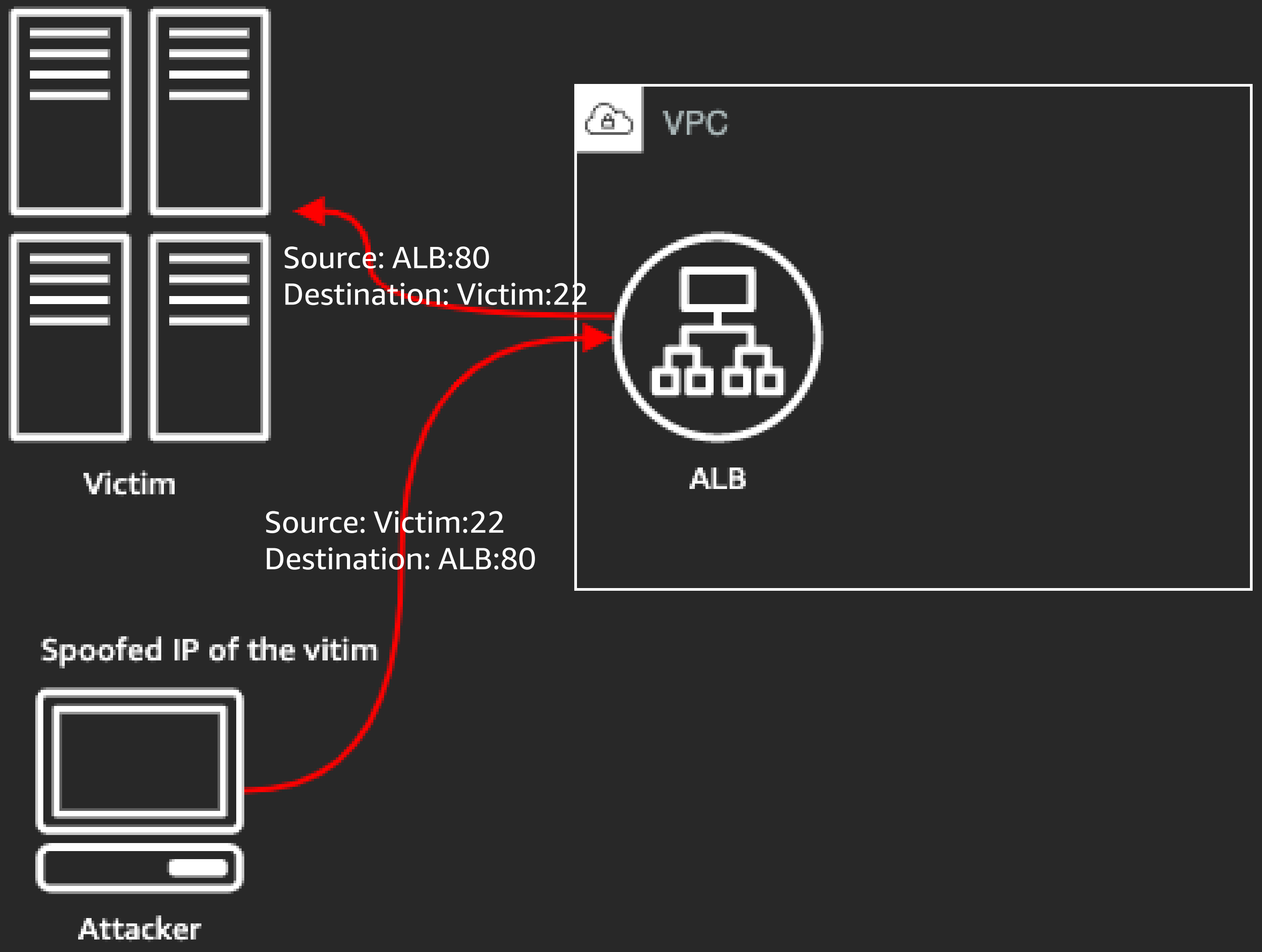


True story #2 (2/3)

Action and Result

- The monitoring tool and metrics show that the load balancer didn't initiate attack traffic; instead the load balancer was responding to valid traffic with spoofed source IP addresses

- The investigation performed by the AWS Support and engineering team indicates that this was a reflection attack



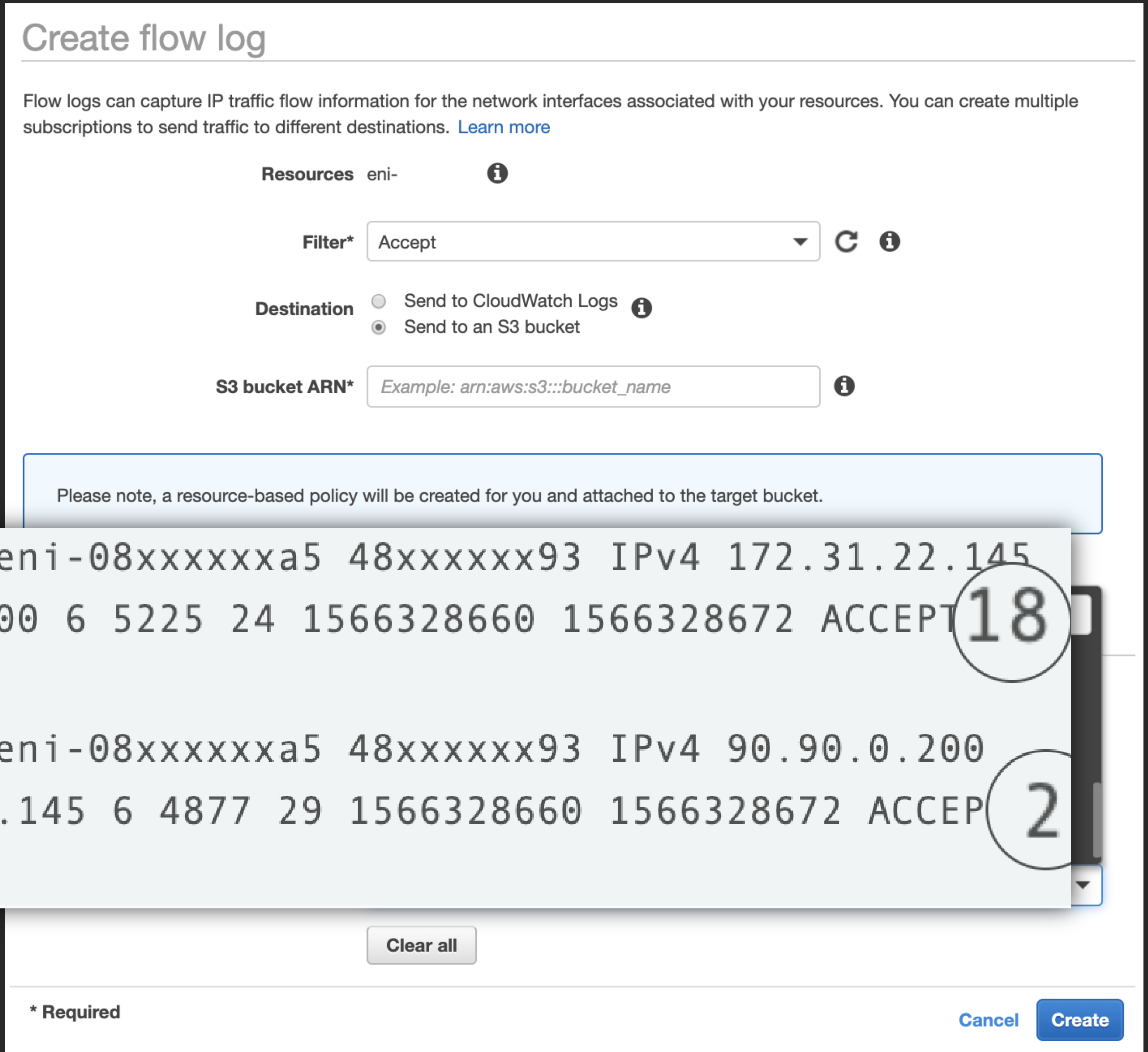
True story #2 (3/3)

Recommendation and Tips

- Enable VPC flow logs with additional metadata to inspect your network traffic

- Configure security groups and network ACLs to a
in th

- Co
vuln
AWS services



Create flow log

Flow logs can capture IP traffic flow information for the network interfaces associated with your resources. You can create multiple subscriptions to send traffic to different destinations. Learn more

Resources eni-

Filter* Accept

Destination ○ Send to CloudWatch Logs ● Send to an S3 bucket

S3 bucket ARN* Example: arn:aws:s3:::bucket_name

Please note, a resource-based policy will be created for you and attached to the target bucket.

* Required

```
3 vpc-exxxxxx2 subnet-8xxxxf3 i-0bfxxxxxxaf eni-08xxxxxxa5 48xxxxxx93 IPv4 172.31.22.145
90.90.0.200 22 62897 172.31.22.145 90.90.0.200 6 5225 24 1566328660 1566328672 ACCEPT 18
OK
3 vpc-exxxxxx2 subnet-8xxxxf3 i-0bfxxxxxxaf eni-08xxxxxxa5 48xxxxxx93 IPv4 90.90.0.200
172.31.22.145 62897 22 90.90.0.200 172.31.22.145 6 4877 29 1566328660 1566328672 ACCEP 2
OK
```

Amazon VPC traffic mirroring

Amazon VPC traffic mirroring duplicates the traffic going into an EC2 instance and shares it with security and monitoring tools

- Duplicate traffic to inspect for threats, network troubleshooting, and performance
- Extract only the traffic of interest
- Extend your capabilities with third-party solutions in the AWS Marketplace and partner solutions

big switch networks

CISCO Stealthwatch Cloud

ExtraHop

Gigamon®

IronNet

NUBEVA

paloalto NETWORKS®

kentik

JASK

riverbed

BLUEHEXAGON

RSA

Fidelis Cybersecurity

FIREEYE®

Flowmon Driving Network Visibility

VECTRA™

corelight

Symantec

DARKTRACE

NETSCOUT.

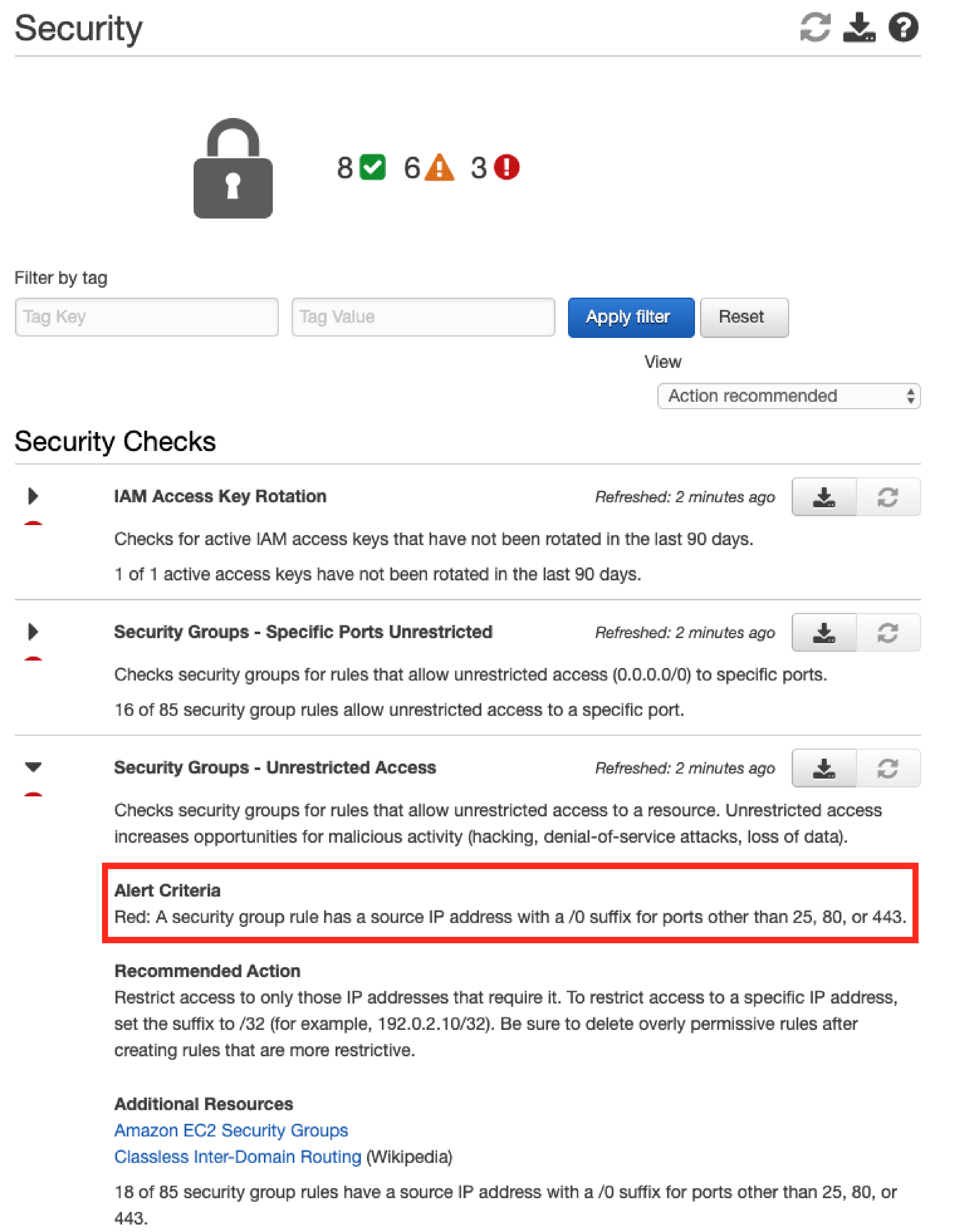
True story #2 (3/3)

Recommendation and Tips

- Enable VPC flow logs with additional metadata to inspect your network traffic

- Configure security groups and network ACLs to allow access to service ports only (included in the Trusted Advisor best practice checks)

- Contact AWS immediately if you discover any vulnerabilities or have security concerns about AWS services



Security Checks

IAM Access Key Rotation *Refreshed: 2 minutes ago*

Checks for active IAM access keys that have not been rotated in the last 90 days.

1 of 1 active access keys have not been rotated in the last 90 days.

Security Groups - Specific Ports Unrestricted *Refreshed: 2 minutes ago*

Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports.

16 of 85 security group rules allow unrestricted access to a specific port.

Security Groups - Unrestricted Access *Refreshed: 2 minutes ago*

Checks security groups for rules that allow unrestricted access to a resource. Unrestricted access increases opportunities for malicious activity (hacking, denial-of-service attacks, loss of data).

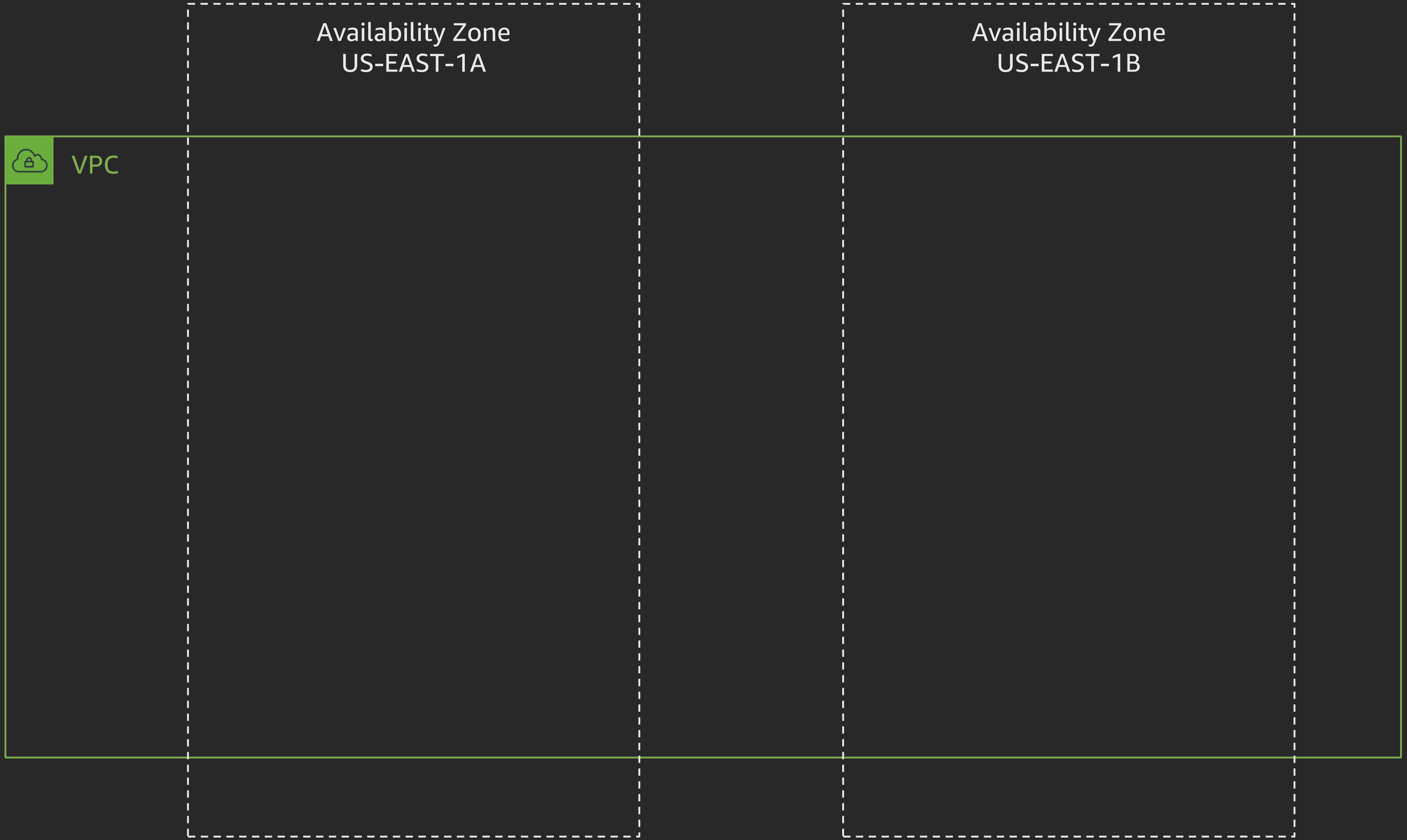
Alert Criteria
Red: A security group rule has a source IP address with a /0 suffix for ports other than 25, 80, or 443.

Recommended Action
Restrict access to only those IP addresses that require it. To restrict access to a specific IP address, set the suffix to /32 (for example, 192.0.2.10/32). Be sure to delete overly permissive rules after creating rules that are more restrictive.

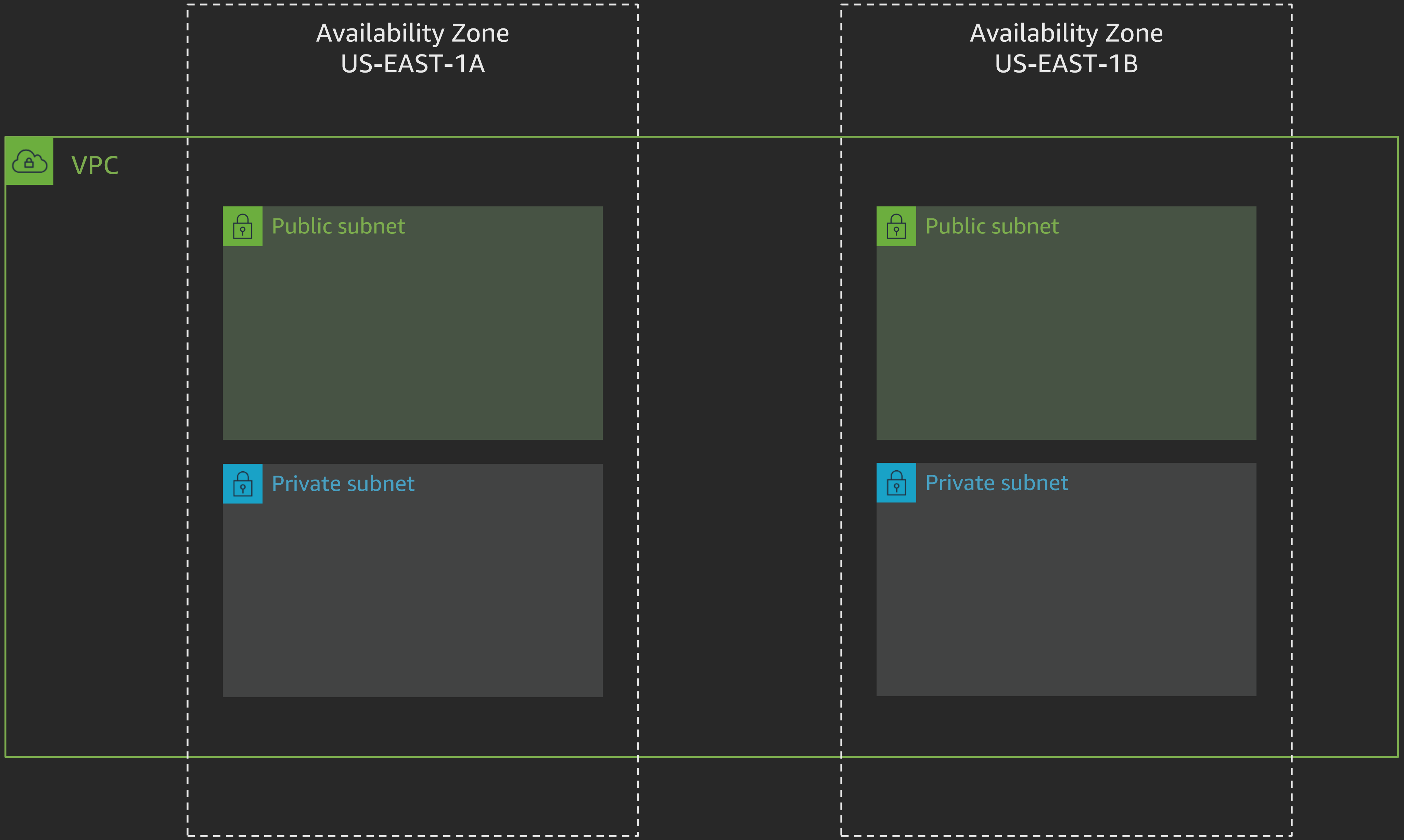
Additional Resources
Amazon EC2 Security Groups
Classless Inter-Domain Routing (Wikipedia)

18 of 85 security group rules have a source IP address with a /0 suffix for ports other than 25, 80, or 443.

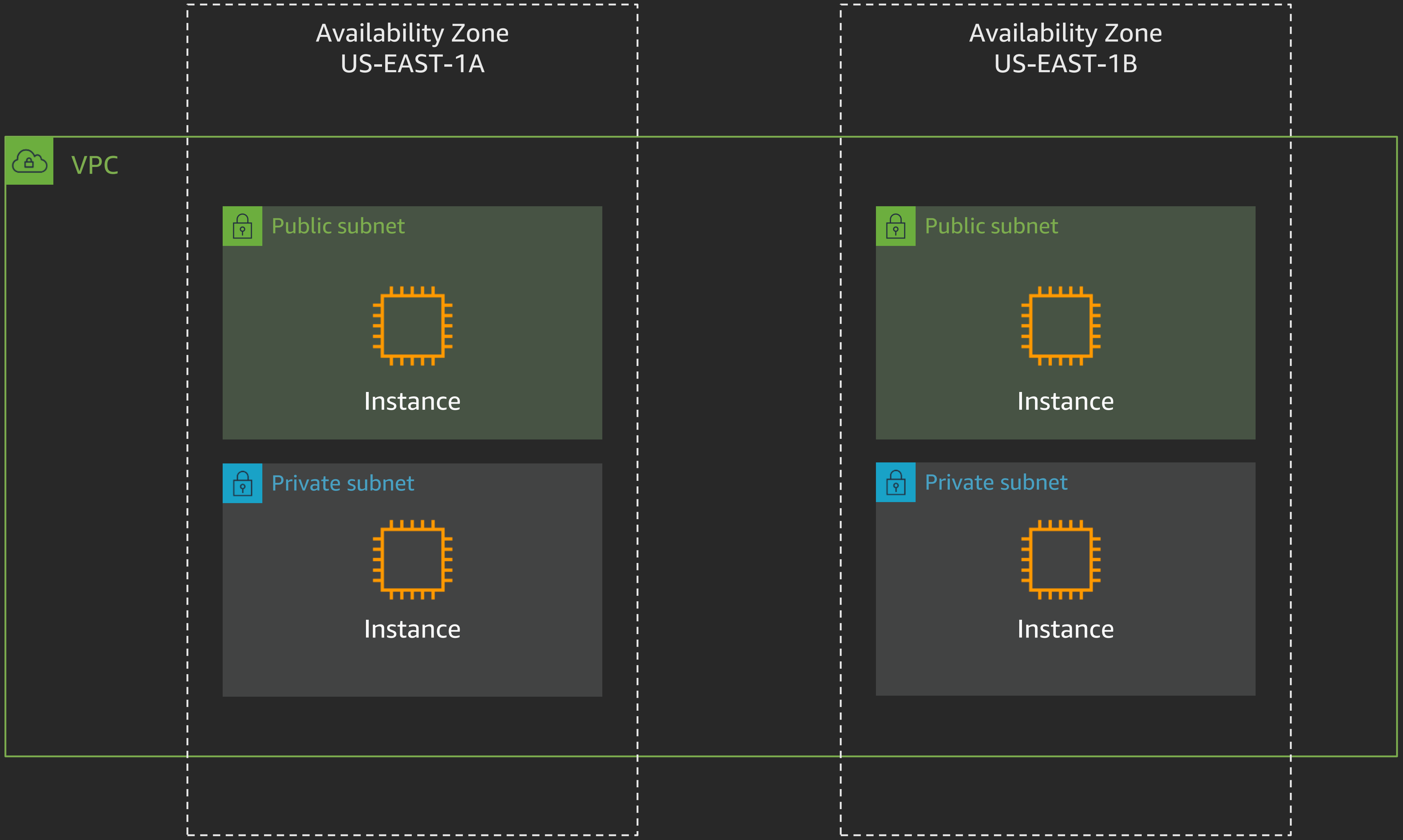
Amazon Virtual Private Cloud



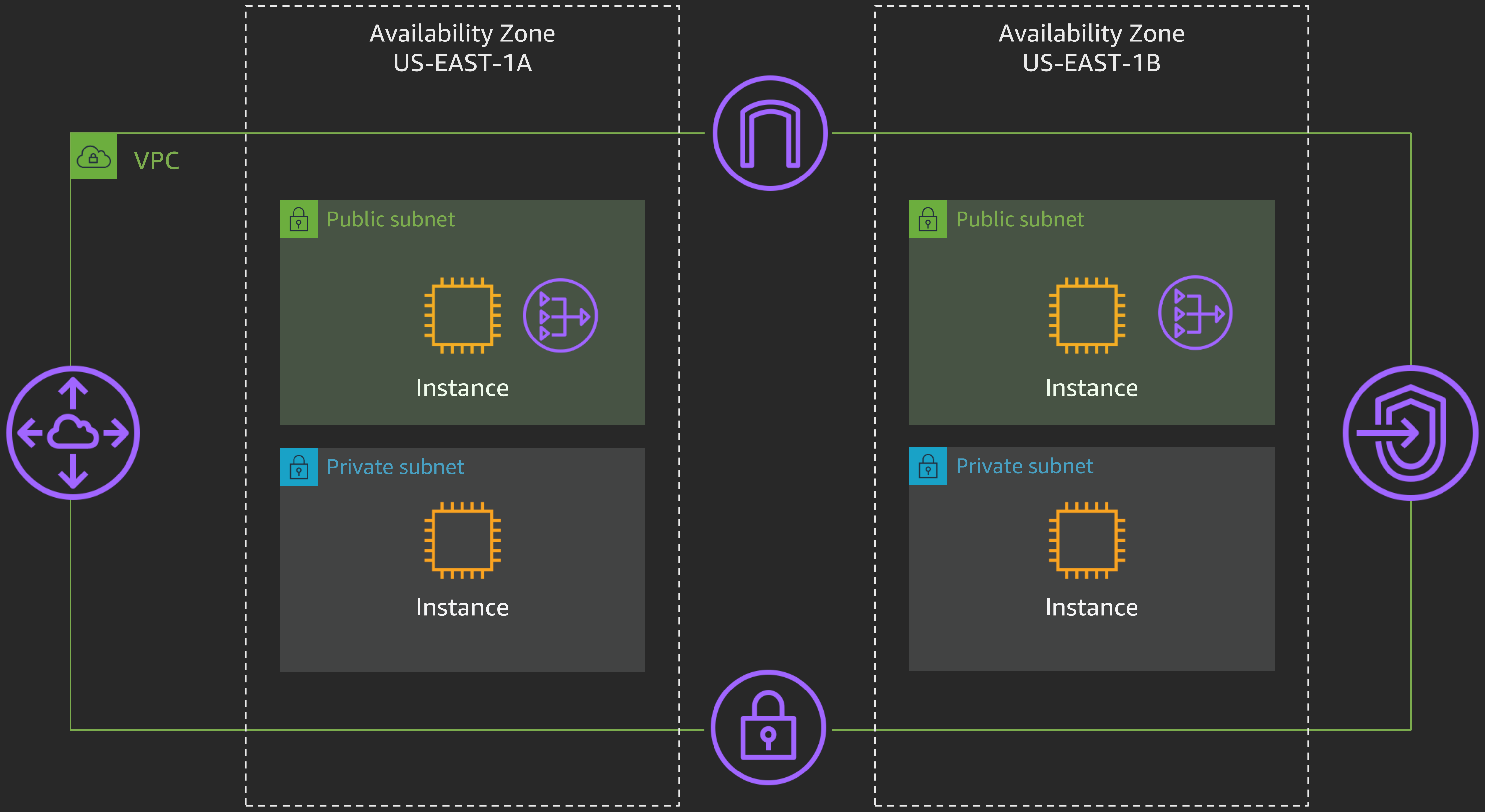
Subnets


Availability Zone
US-EAST-1A
Availability Zone
US-EAST-1B
VPC
Public subnet
Public subnet
Private subnet
Private subnet

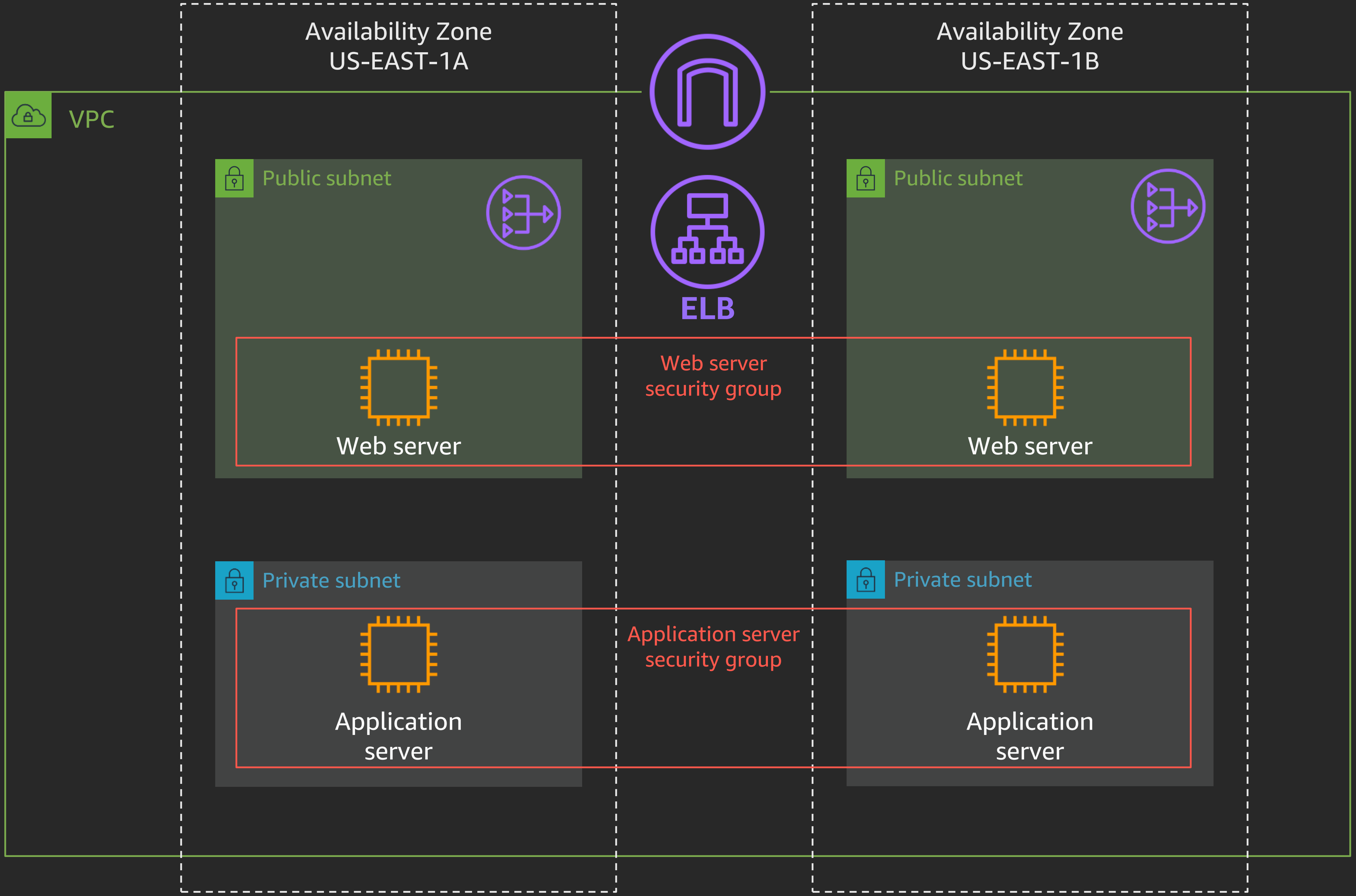
EC2 instances



Gateways, endpoints & peering



Example web application



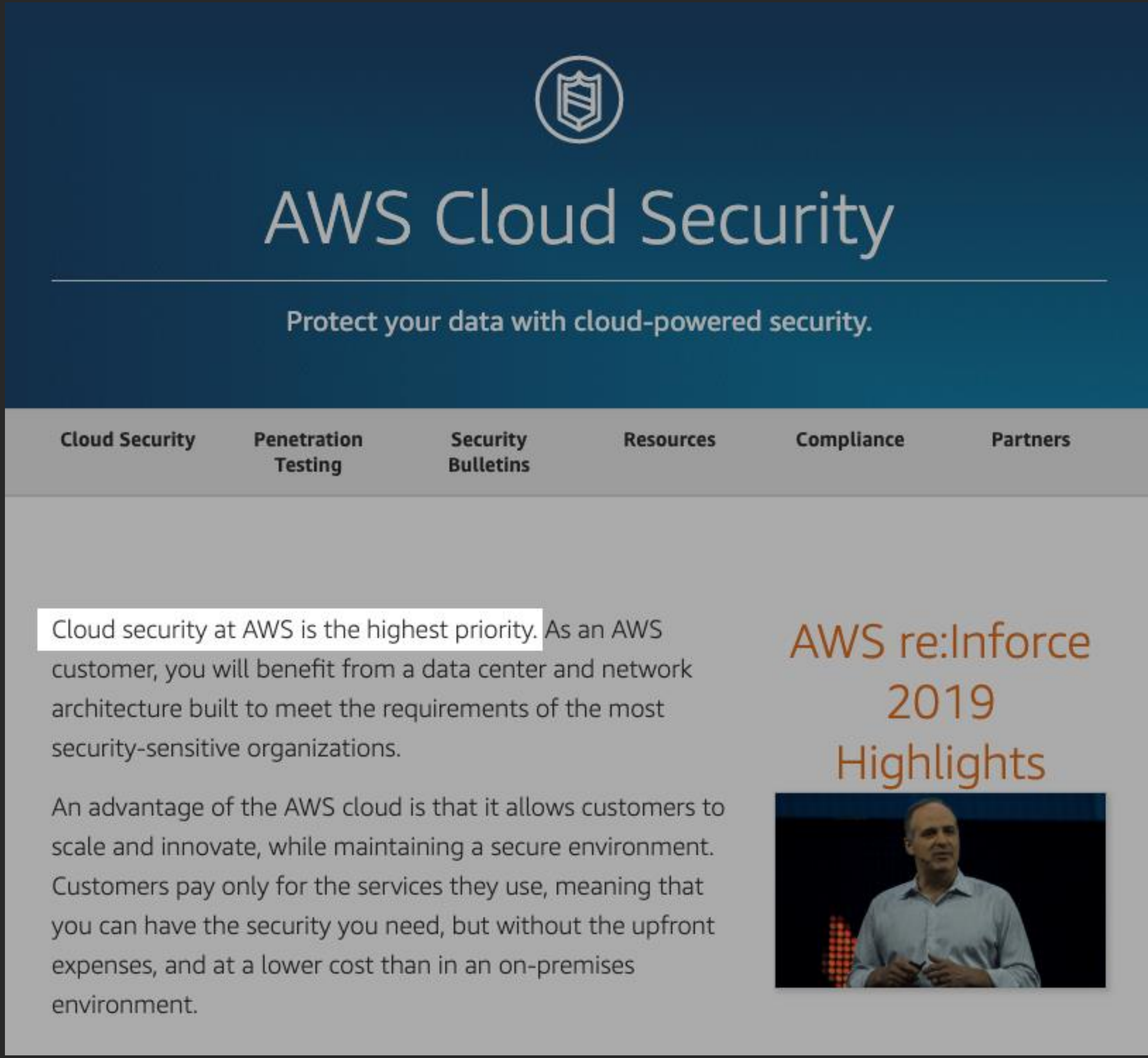
True story #2 (3/3)

Recommendation and Tips

- Enable VPC flow logs with additional metadata to inspect your network traffic

- Configure security groups and network ACLs to allow access to service ports only (included in the Trusted Advisor best practice checks)

- Contact AWS immediately if you discover any vulnerabilities or have security concerns about AWS services



AWS Cloud Security

Protect your data with cloud-powered security.

Cloud security at AWS is the highest priority. As an AWS customer, you will benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations.

An advantage of the AWS cloud is that it allows customers to scale and innovate, while maintaining a secure environment. Customers pay only for the services they use, meaning that you can have the security you need, but without the upfront expenses, and at a lower cost than in an on-premises environment.

Email: aws-security@amazon.com
Web: https://go.aws/30RQC8I

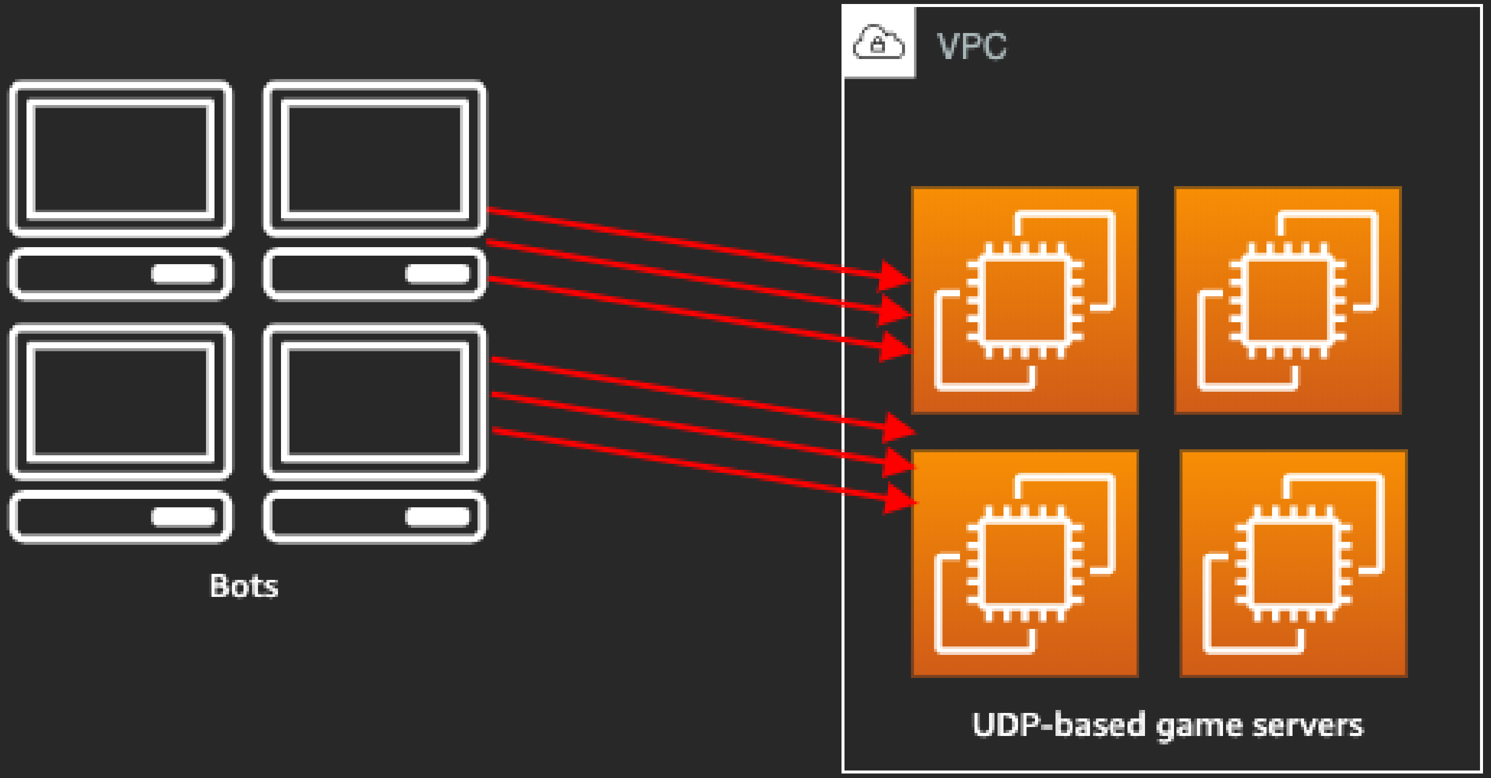
True story #3 (1/4)

Situation

- A Basic Support customer's UDP-based game servers hosted on EC2 instances were under attack

- Unsatisfied with Shield Advanced as users were impacted after the subscription of Shield Advanced

- Attack volume wasn't massive but targeted the service ports

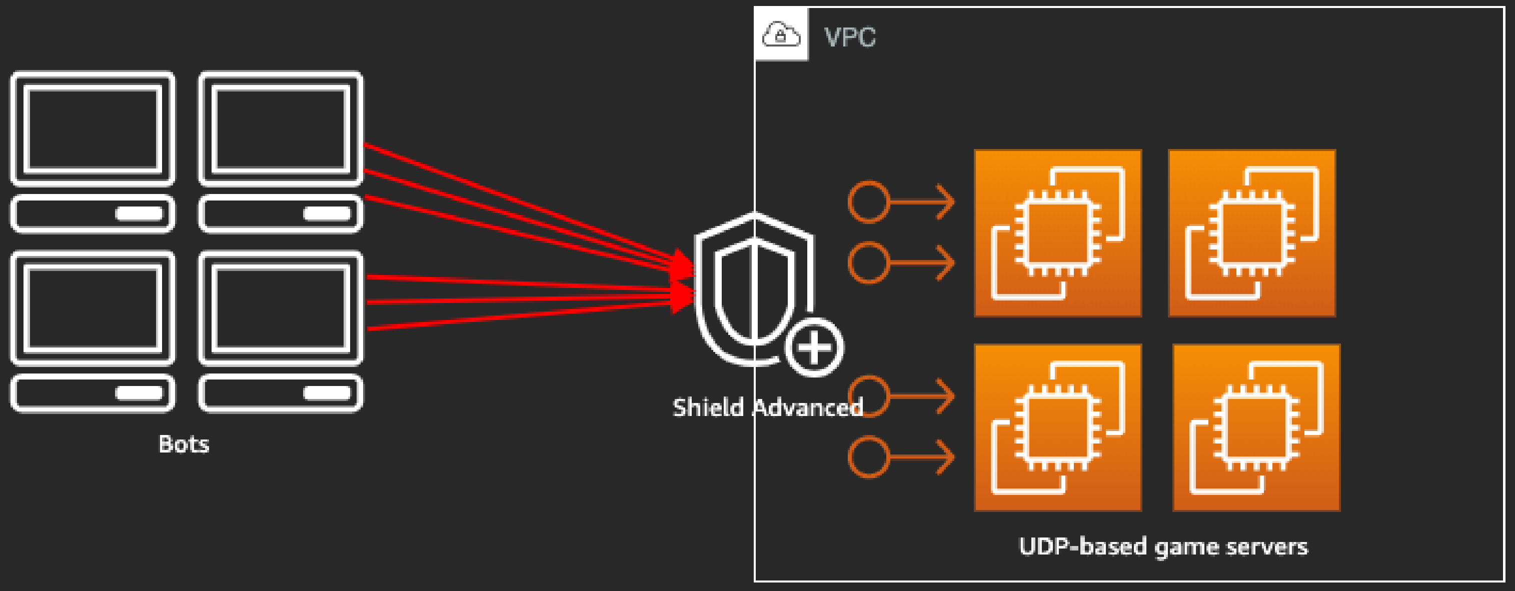


True story #3 (2/4)

Action and Result

- A CSE served as a bridge between the customer and DDoS Response Team (DRT) to facilitate communication

- The attack was mitigated by whitelisting certain countries to access game servers (custom mitigation rules configured by the DRT)



True story #3 (3/4)

Recommendation and Tips

- Baseline your traffic and be familiar with your packet format

- Drop/Shape network traffic using security groups, network ACLs, and iptables

- Scale your servers by choosing the right instance type and size, enabling Enhanced Networking, and using AWS Auto Scaling with AWS Global Accelerator and AWS Elastic Load Balancing

```
// The length module matches packet size
$ iptables -m length --length 256:65535

// The u32 module matches arbitrary byte patterns
$ iptables -m u32 --u32 "16=0xE0000001"
```

How-to: Write iptables rules to drop packets that do not match your application format - http://bit.ly/2mG3XPn

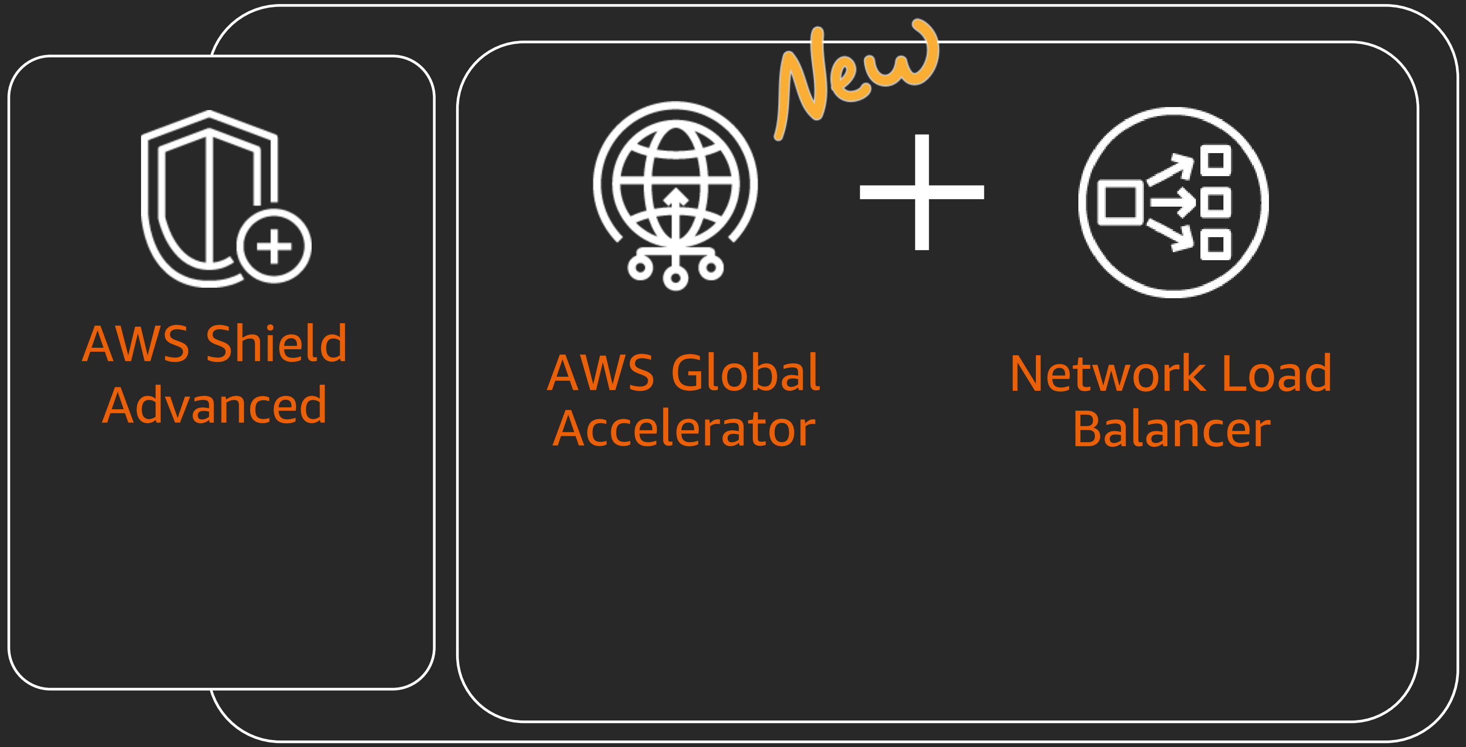
True story #3 (3/4)

Recommendation and Tips

- Baseline your traffic and be familiar with your packet format

- Drop/Shape network traffic using security groups, network ACLs, and iptables

- Scale your servers by choosing the right instance type and size, enabling Enhanced Networking, and using AWS Auto Scaling with AWS Global Accelerator and AWS Elastic Load Balancing



Whitepaper: AWS Best Practices for DDoS Resiliency - http://bit.ly/2ldui6W

AWS Global Accelerator

New Relic

Improve global application availability and performance using the AWS global network

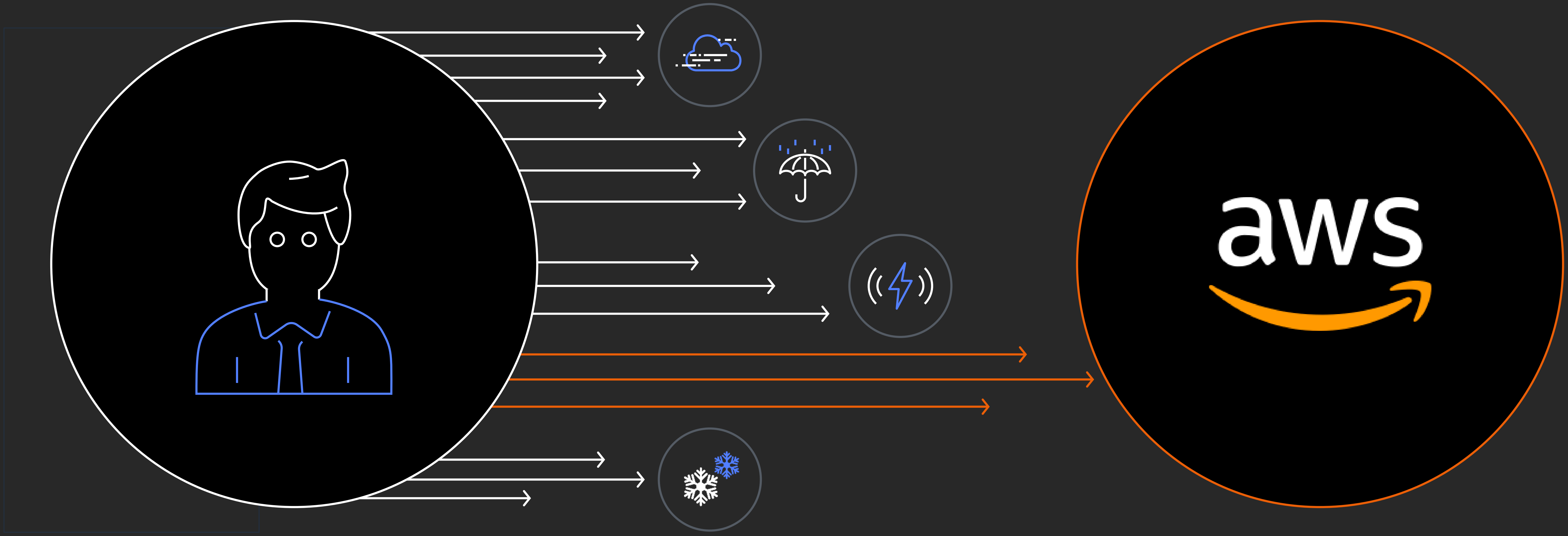
New in 2019:

- Launched in 10 new Regions in 2019
- Client IP preservation for ALB and Amazon EC2 instances

> “We use AWS Global Accelerator to ingest telemetry data onto AWS, taking advantage of the static IP addresses it provides, along with traffic-shifting capabilities and many points of presence around the globe.”

Ken Gavranovic
SVP, Product Management
New Relic

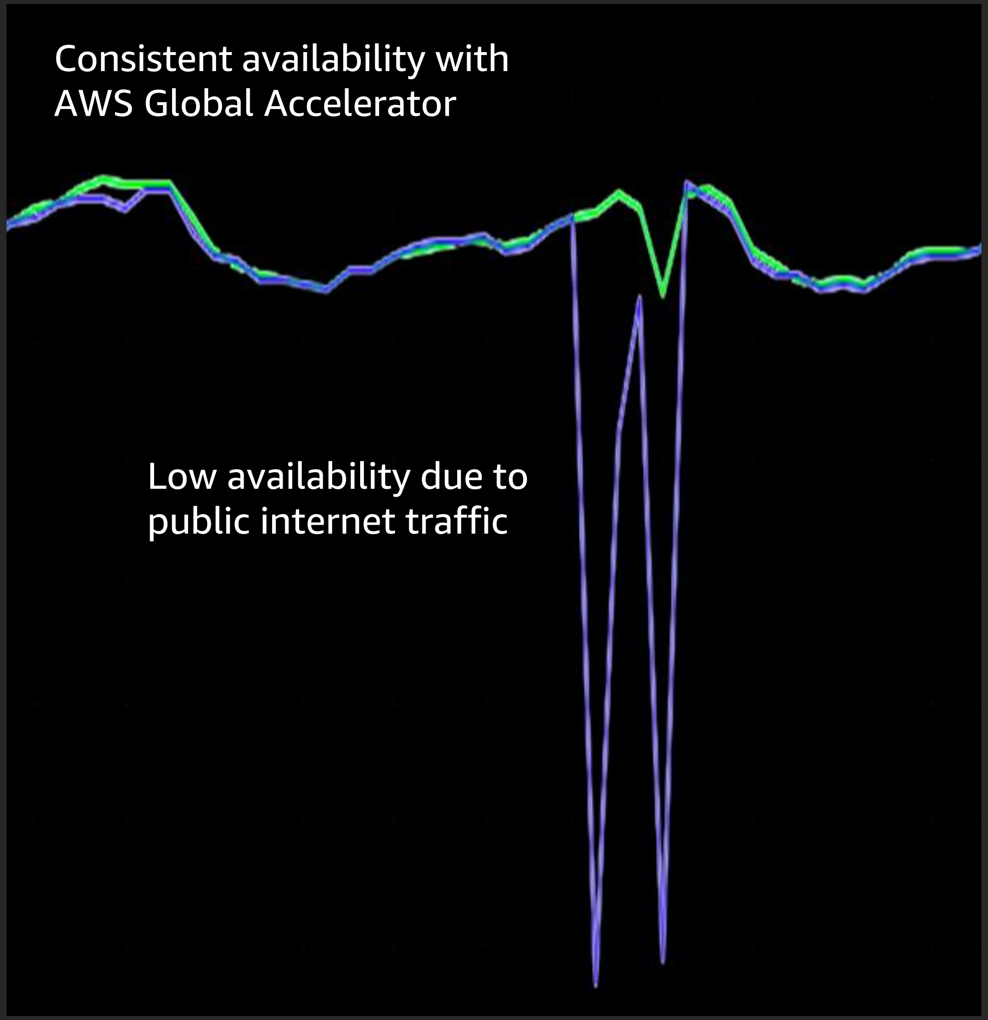
Internet weather



Let’s say you have an internet-facing application…

Starts in the USA…

Availability

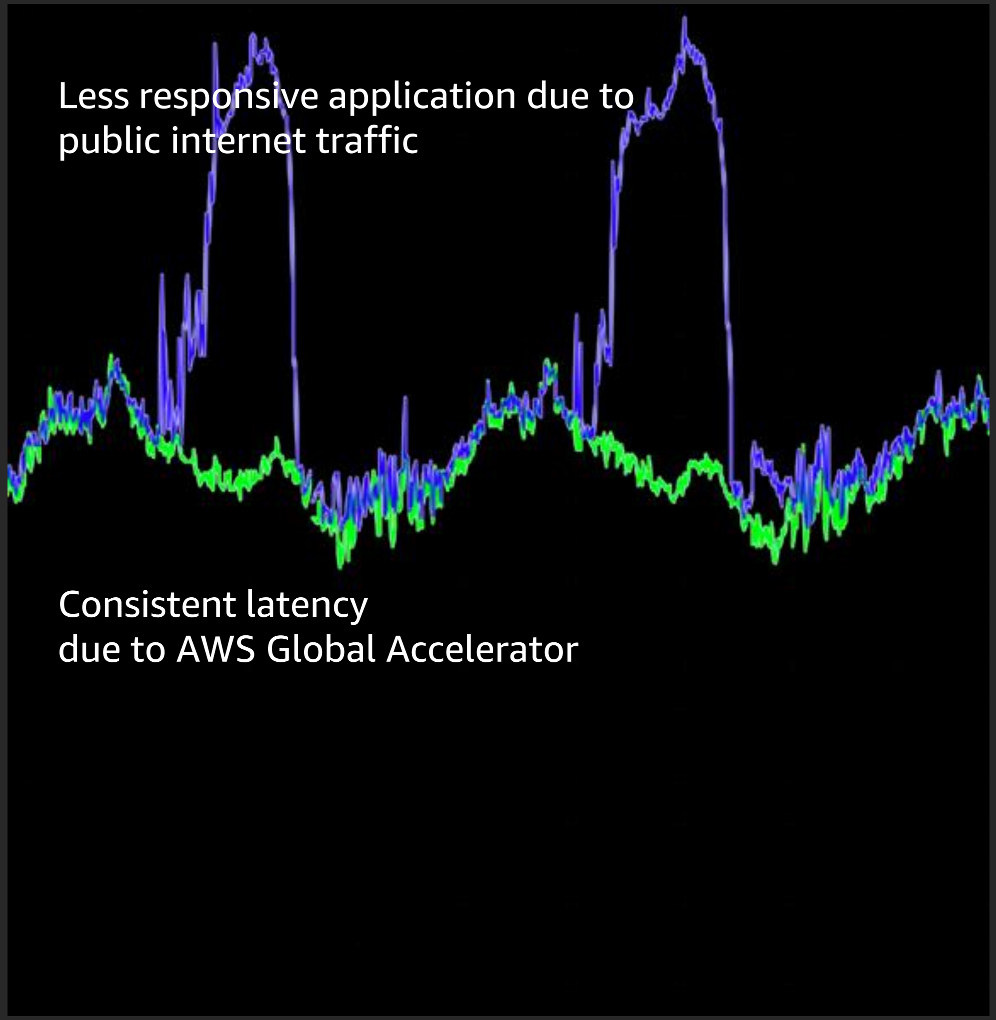


Consistent availability with AWS Global Accelerator

Low availability due to public internet traffic

…expands to Europe…

First byte latency

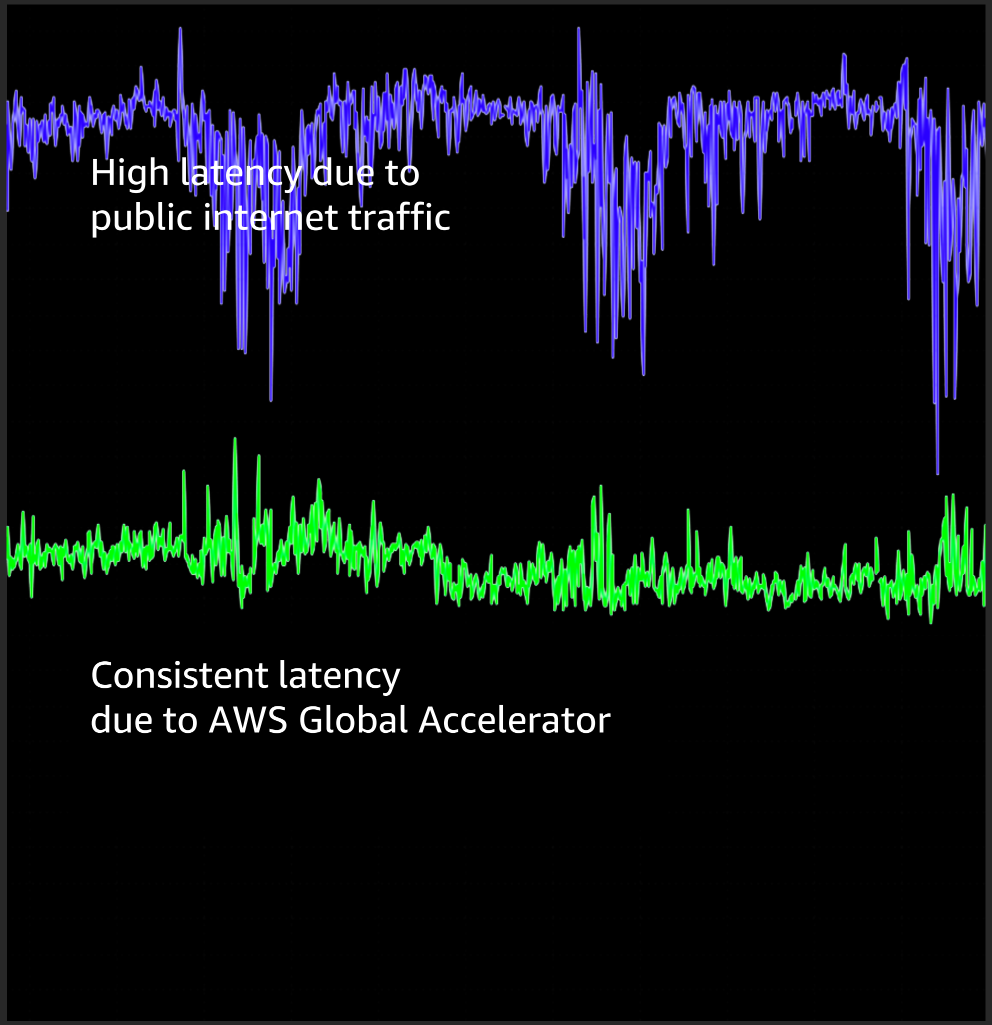


Less responsive application due to public internet traffic

Consistent latency due to AWS Global Accelerator

…and then adds Asia

First byte latency



High latency due to public internet traffic

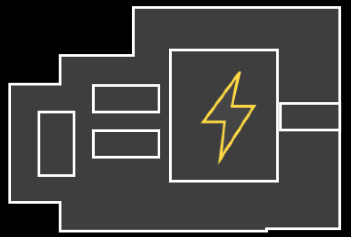
Consistent latency due to AWS Global Accelerator

● AWS Global Accelerator ● Direct to AWS Region via public internet

Availability measured by clients on the internet using third-party measurement systems

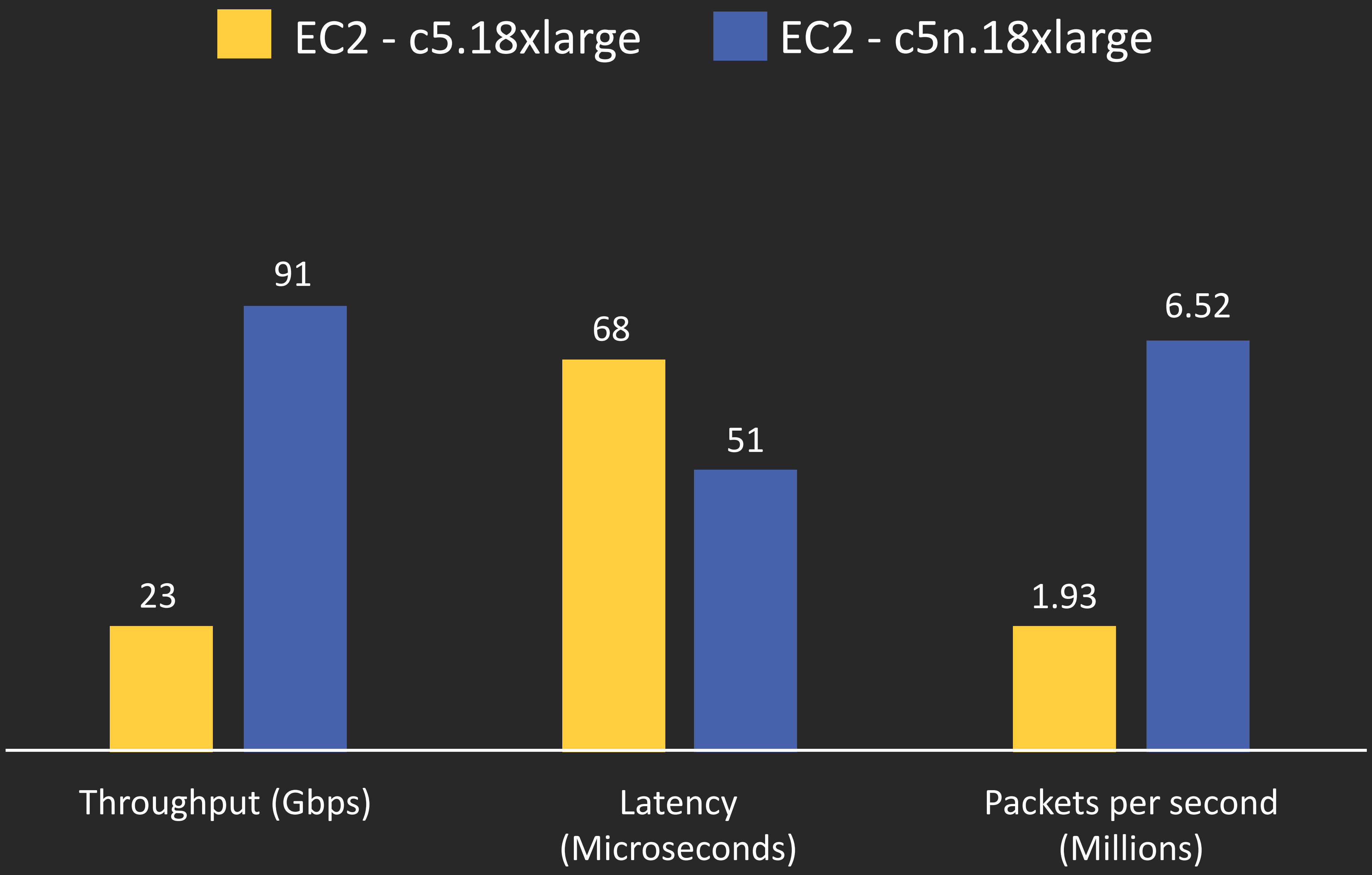
Networking innovation, enabled by AWS Nitro System

Nitro Card



Networking, monitoring, and security

AWS network benchmarking data, March 2019

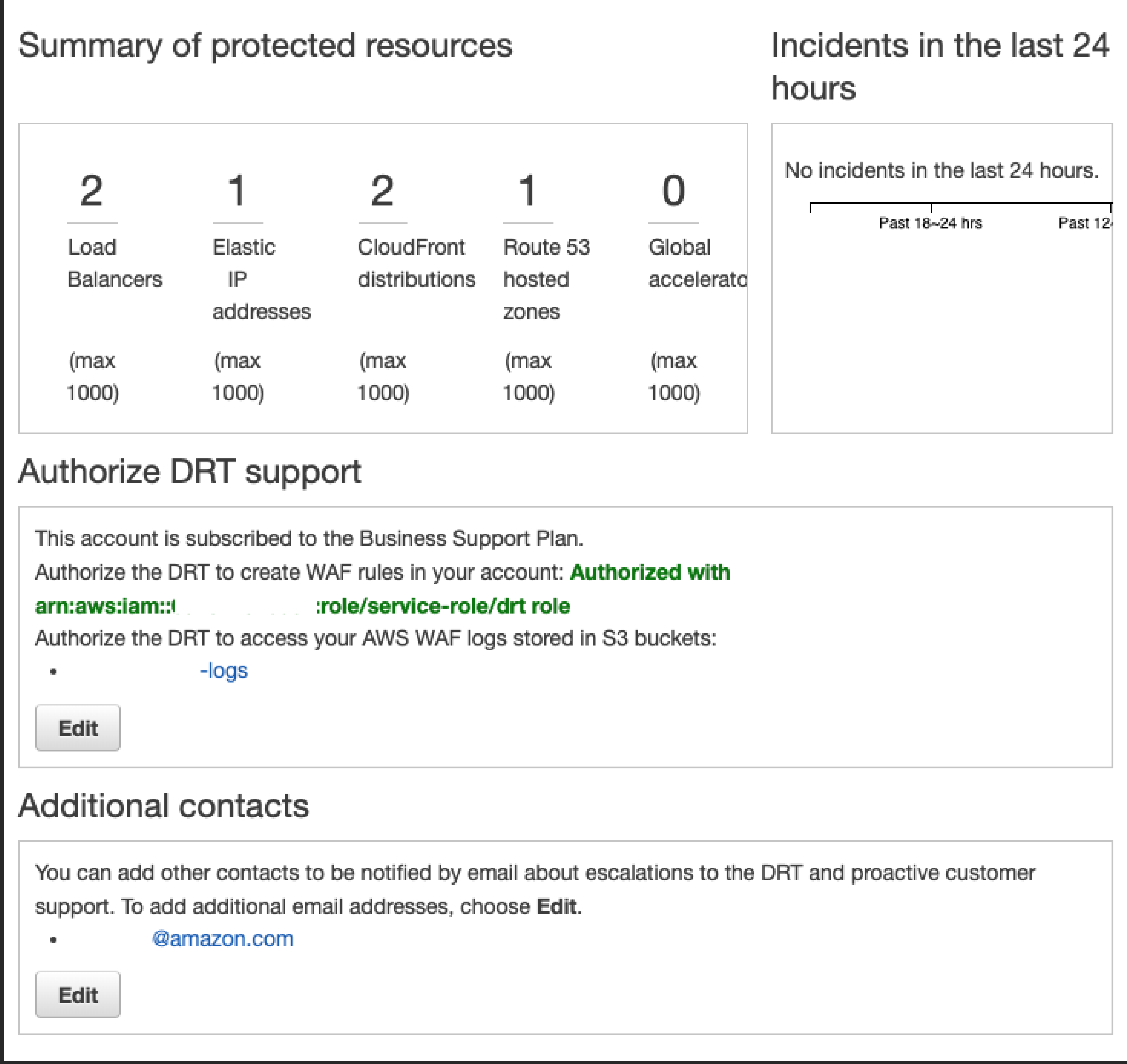


True story #3 (4/4)

Recommendation and Tips

- Be prepared – work with the DRT to build your custom mitigation rules, authorize the DRT to access your logs, review operational practices periodically

- Automate the process – deploy the AWS Shield Engagement Lambda function to shorten the time to engage AWS Support and the DRT, monitor AWS Shield Advanced metrics to be informed of DDoS attacks via Slack or PagerDuty



Summary of protected resources

2	1	2	1	0
Load Balancers	Elastic IP addresses	CloudFront distributions	Route 53 hosted zones	Global accelerato
(max 1000)	(max 1000)	(max 1000)	(max 1000)	(max 1000)

Incidents in the last 24 hours

No incidents in the last 24 hours.

Authorize DRT support

This account is subscribed to the Business Support Plan.

Authorize the DRT to create WAF rules in your account: **Authorized with arn:aws:iam::[redacted]:role/service-role/drt role**

Authorize the DRT to access your AWS WAF logs stored in S3 buckets:

- [redacted]-logs

Edit

Additional contacts

You can add other contacts to be notified by email about escalations to the DRT and proactive customer support. To add additional email addresses, choose **Edit**.

- [redacted]@amazon.com

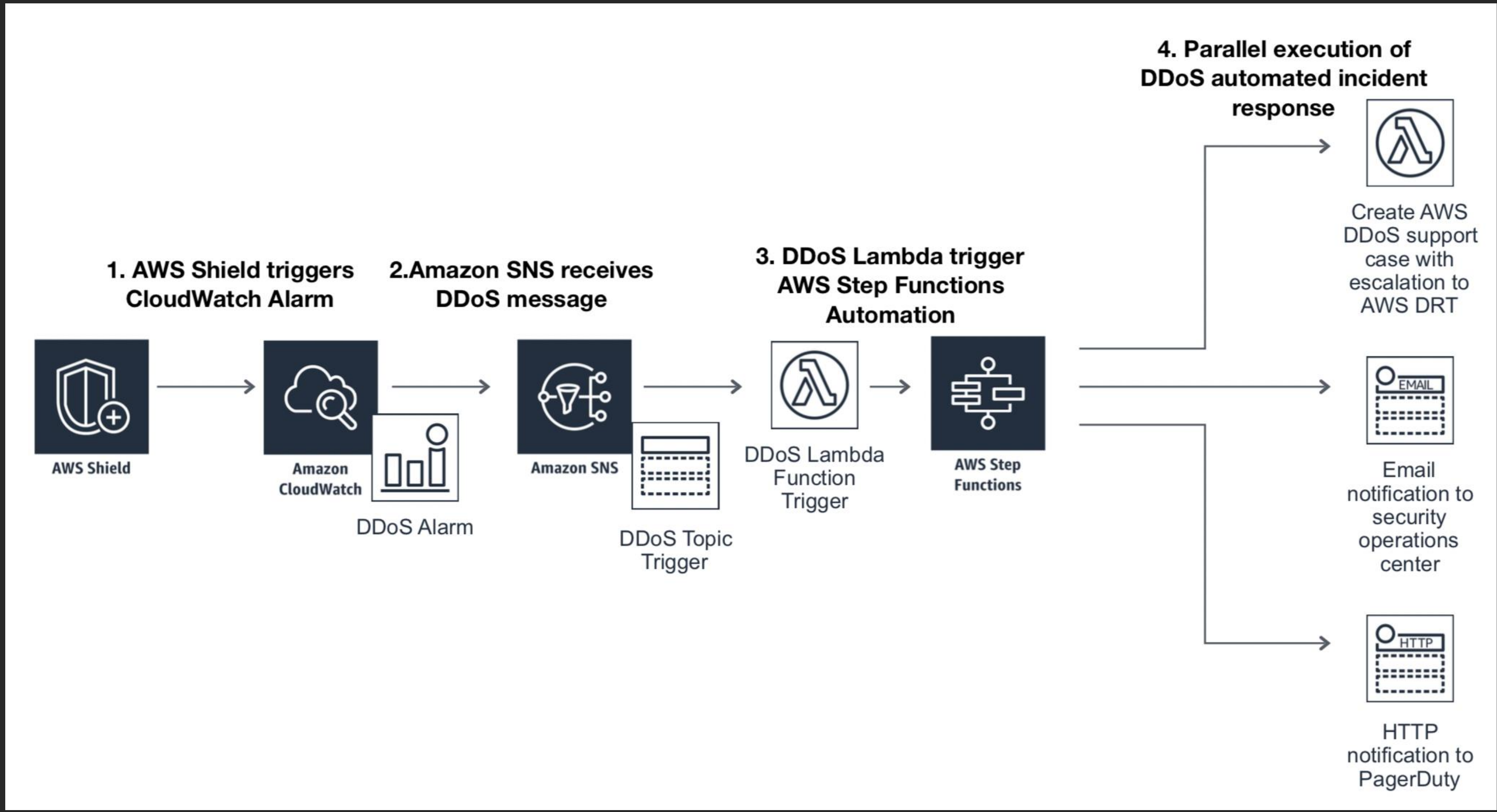
Edit

True story #3 (4/4)

Recommendation and Tips

- Be prepared – work with the DRT to build your custom mitigation rules, authorize the DRT to access your logs, review operational practices periodically

- Automate the process – deploy the AWS Shield Engagement Lambda function to shorten the time to engage AWS Support and the DRT, monitor AWS Shield Advanced metrics to be informed of DDoS attacks via Slack or PagerDuty


1. AWS Shield triggers CloudWatch Alarm
2.Amazon SNS receives DDoS message
3. DDoS Lambda trigger AWS Step Functions Automation
4. Parallel execution of DDoS automated incident response
AWS Shield
Amazon CloudWatch
DDoS Alarm
Amazon SNS
DDoS Topic Trigger
DDoS Lambda Function Trigger
AWS Step Functions
Create AWS DDoS support case with escalation to AWS DRT
EMAIL
Email notification to security operations center
HTTP
HTTP notification to PagerDuty

How-to: Set up AWS Shield Engagement Lambda - http://bit.ly/2ldui6W

Which one do you need – AWS Support and AWS Shield Advanced

AWS Support

- Provides people, technology, and programs to assist you with DDoS attacks

- For instance, SMEs to help you build a DDoS-resilient architecture; Trusted Advisor to make sure your environment is secure and well utilized and performed

- Recommended for customers running production workloads on AWS

AWS Shield Advanced

- Provides access to the DRT, additional cost/resource protection, and metrics to help you deal with more complex and sophisticated DDoS attacks

- For instance, DRT to build mitigation rules tailored for your application; using AWS WAF with no additional cost; credits for charges incurred due to attacks

- Recommended for customers running business critical workloads on AWS

Frequently asked questions

aws SUMMIT ONLINE

Frequently asked question #1

Q: How quickly will attacks be mitigated?

99% of infrastructure layer attacks detected by AWS Shield are mitigated in less than

- 1 second for attacks on CloudFront/Route 53
- 5 minutes for attacks on ELB

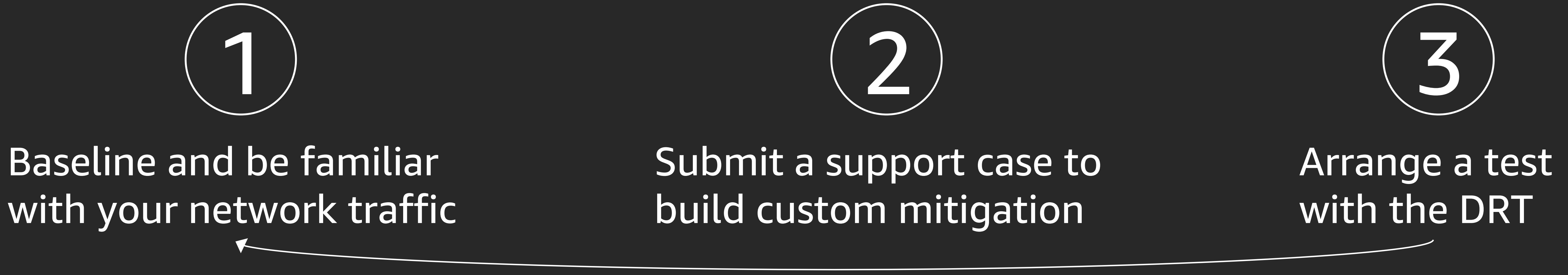
1% of infrastructure layer attacks are typically mitigated in under 20 minutes

Application layer attacks are mitigated by writing rules on AWS WAF, which are inspected and mitigated inline with incoming traffic

Frequently asked question #2

Q: AWS Shield Advanced didn't mitigate the attack against my application

Building the mitigation rules tailored for your application takes time and effort. We recommend you reach out to us as early as possible to get prepared for DDoS attacks.



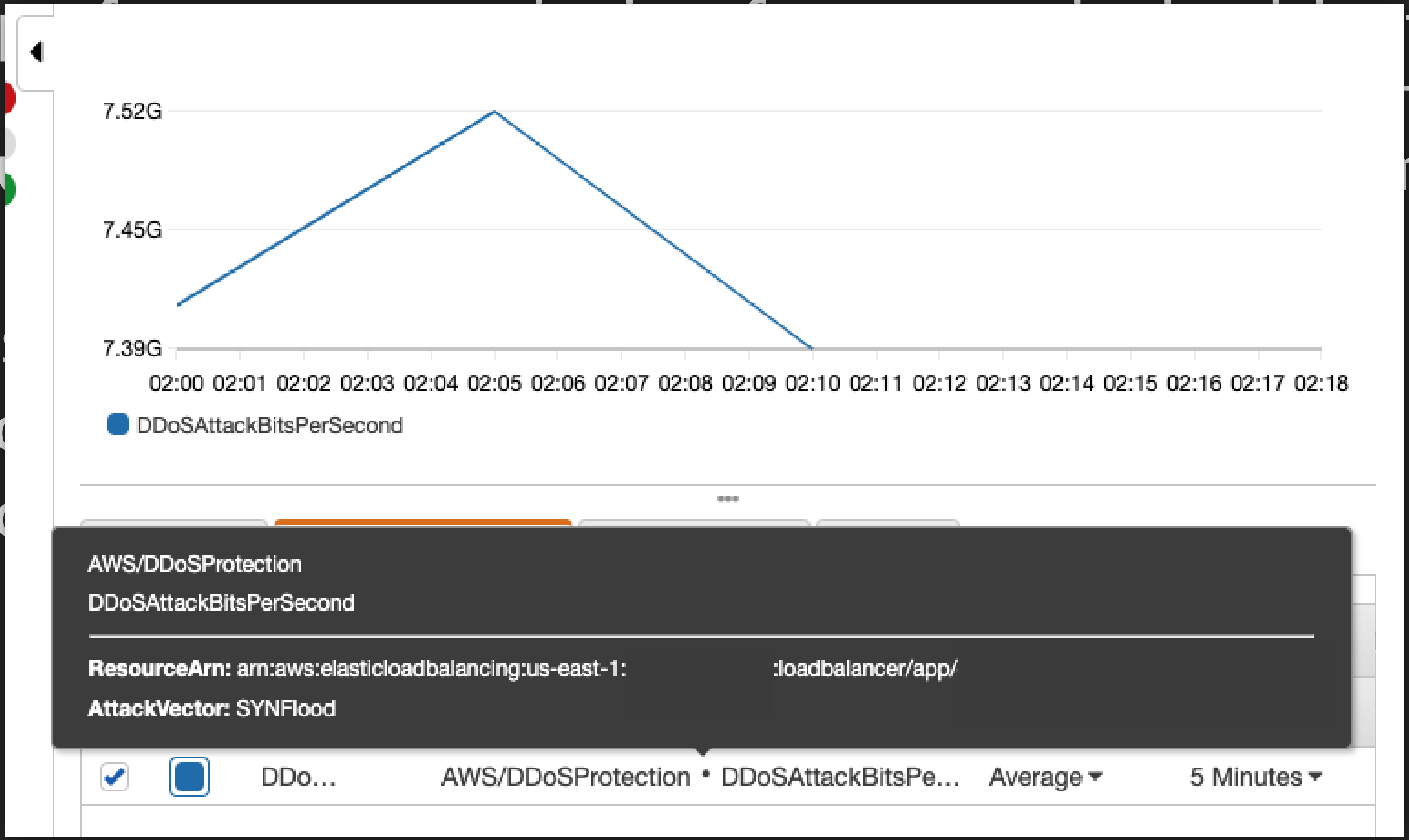
1. Baseline and be familiar with your network traffic
2. Submit a support case to build custom mitigation
3. Arrange a test with the DRT

Frequently asked question #3

Q: How much traffic did AWS Shield drop?

Availability and f your application.
We recommend tiveness. If you
would like to ga netrics:

- DDoSAttackBit
- DDoSAttackPa
- DDoSAttackRe



AWS/DDoSProtection
DDoSAttackBitsPerSecond

ResourceArn: arn:aws:elasticloadbalancing:us-east-1: :loadbalancer/app/
AttackVector: SYNFlood

☑ 🟦 DDo... AWS/DDoSProtection • DDoSAttackBitsPe... Average ▾ 5 Minutes ▾

Learn networking with AWS Training and Certification

Resources created by the experts at AWS to help you build and validate cloud networking skills

Free digital courses cover topics related to networking and content delivery, including Introduction to Amazon CloudFront and AWS Transit Gateway Networking and Scaling

Validate expertise with the AWS Certified Advanced Networking – Specialty exam

Visit the advanced networking learning path at aws.amazon.com/training/path-advanced-networking