
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

NET314

Building DDoS-resilient applications using AWS Shield

Oliver Sturrock (he/him)

General Manager, AWS Shield
AWS

Paul Bodmer (he/him)

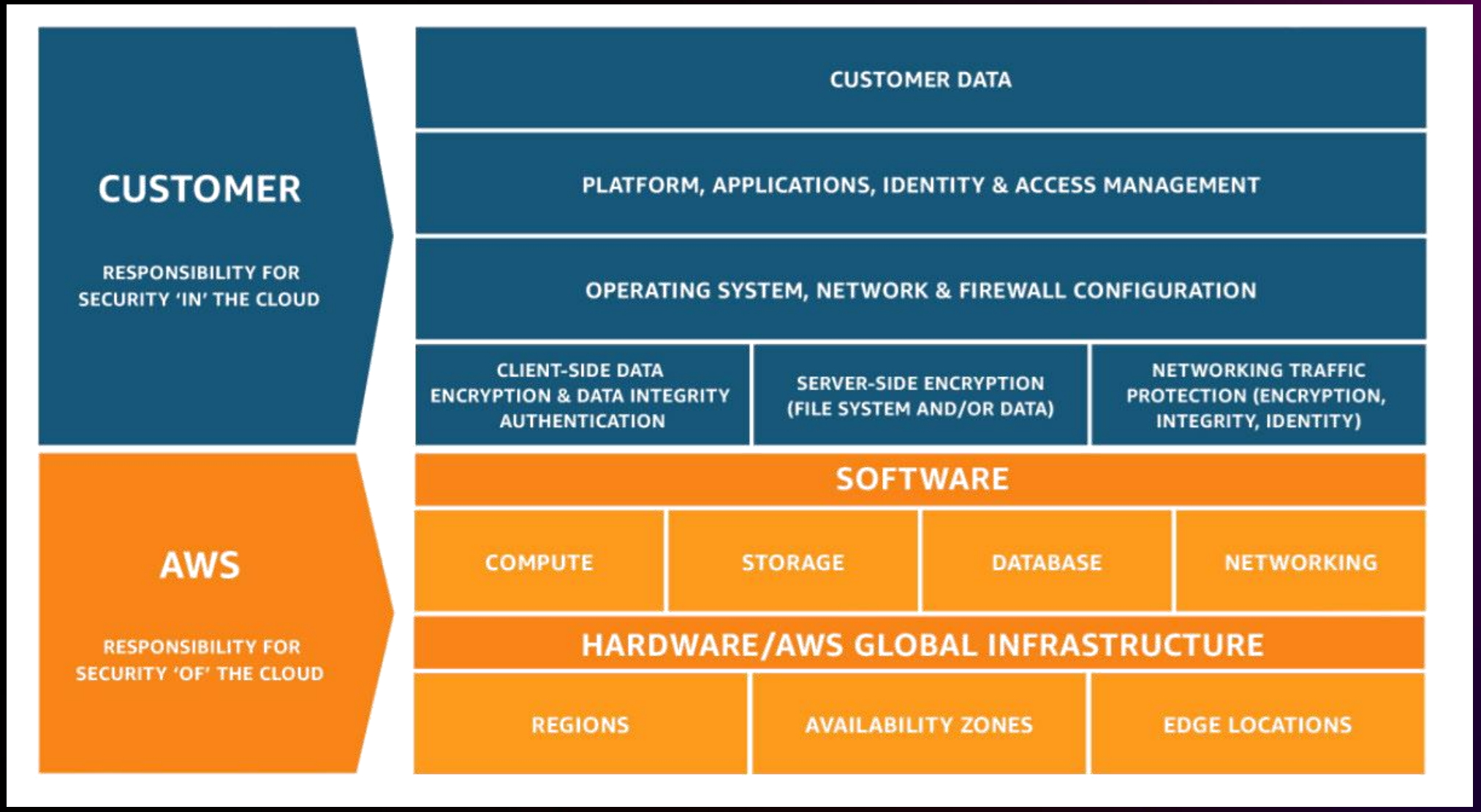
Security Manager, AWS Shield
AWS

Agenda

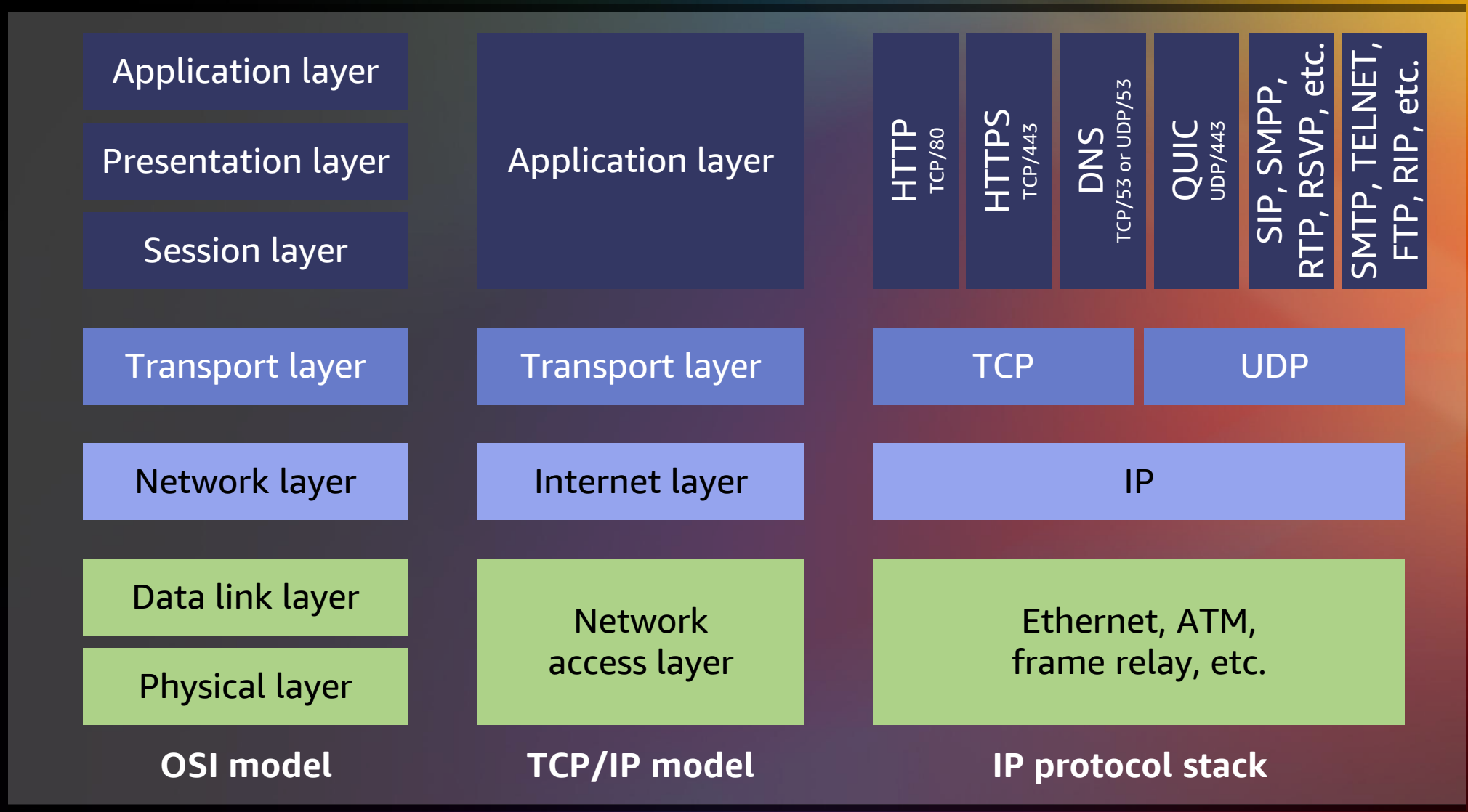
1. **Protecting the availability of the AWS network**
   - Web traffic
   - DNS
   - Traffic from impacted AWS customers
2. **How we stop DDoS before the first attack packet**
   - Threat intelligence
   - Monitoring botnets
3. **Framework for thinking about DDoS resilience**

Protecting the availability of the AWS network

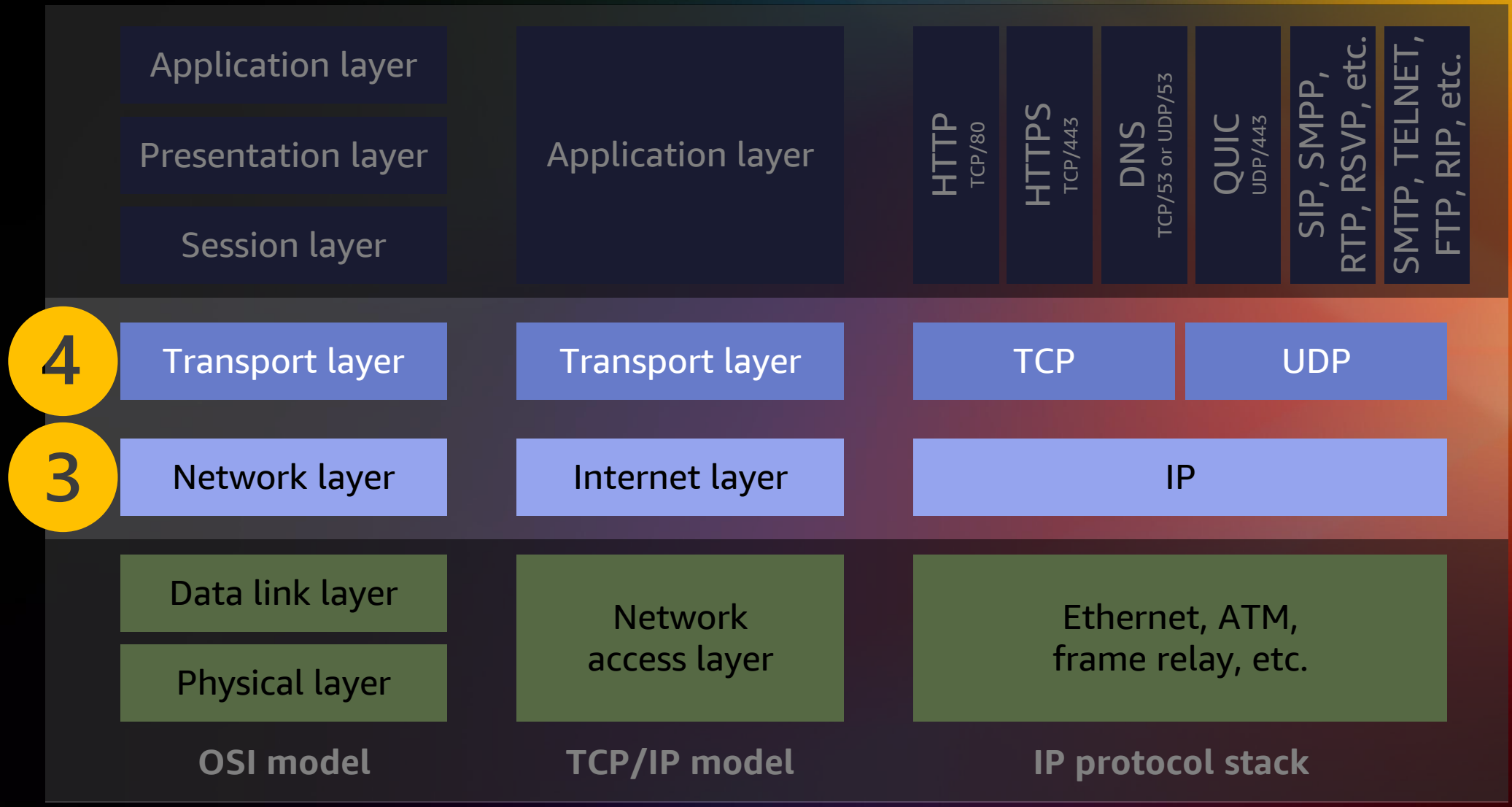
AWS shared responsibility model



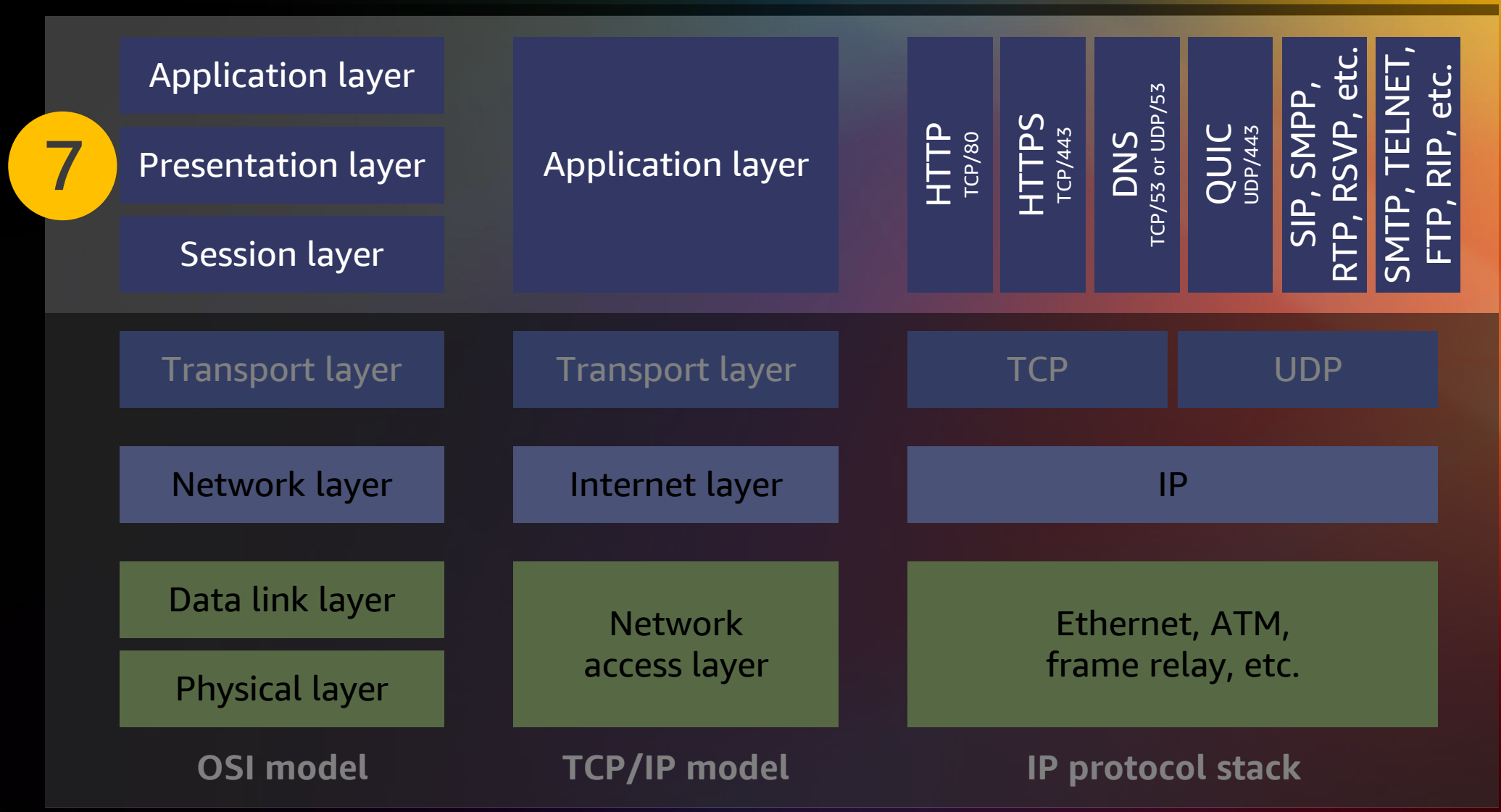
Network layer attacks



Network layer attacks



Application layer attacks



Challenges of scale

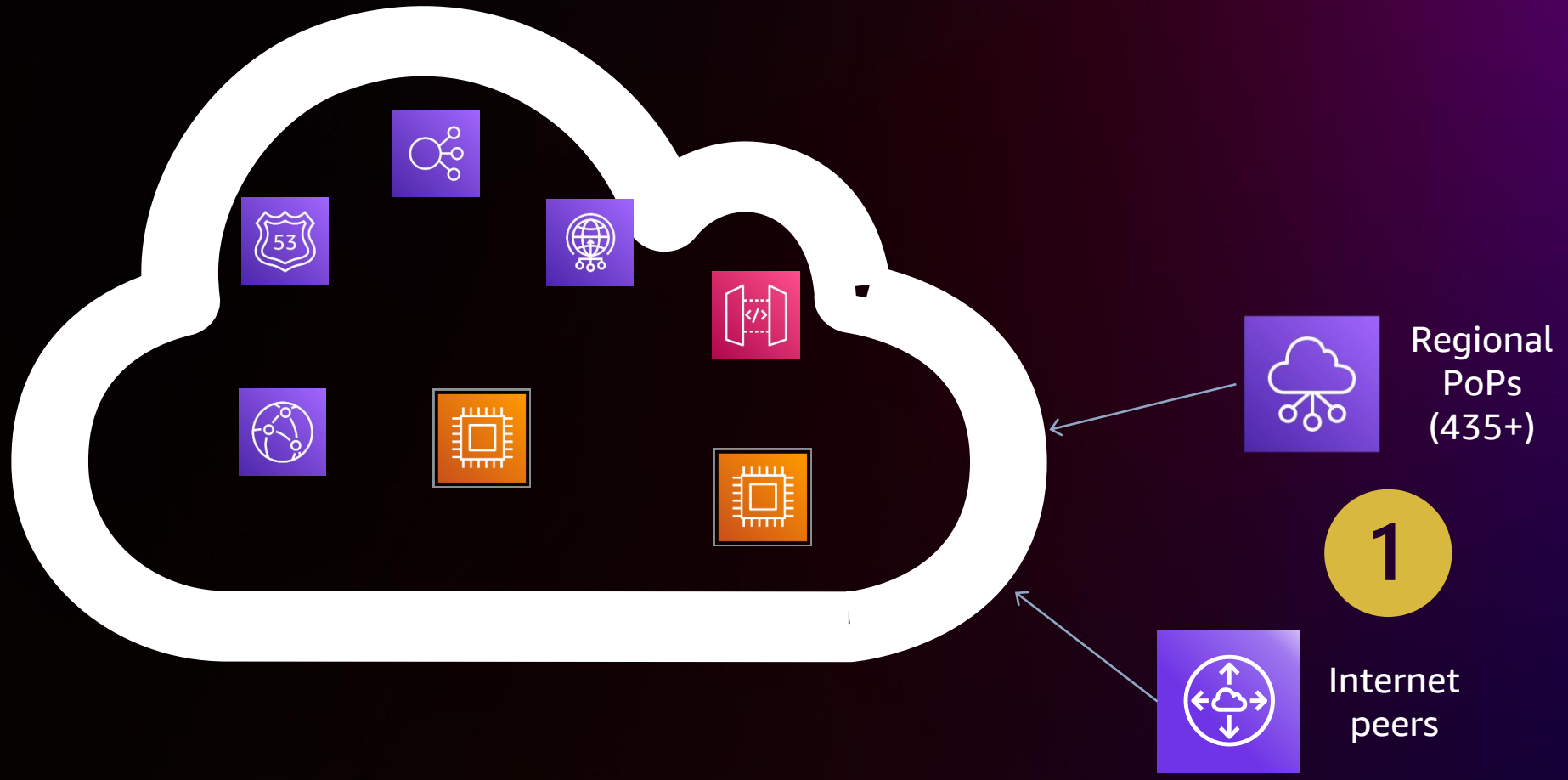
- Many possible points of ingress for internet traffic
- Monitoring on a very large network
- Destination endpoint capacity varies (a lot)
- Distinguishing legitimate traffic from the malicious
- Picking the best mitigation strategy

How big is big?

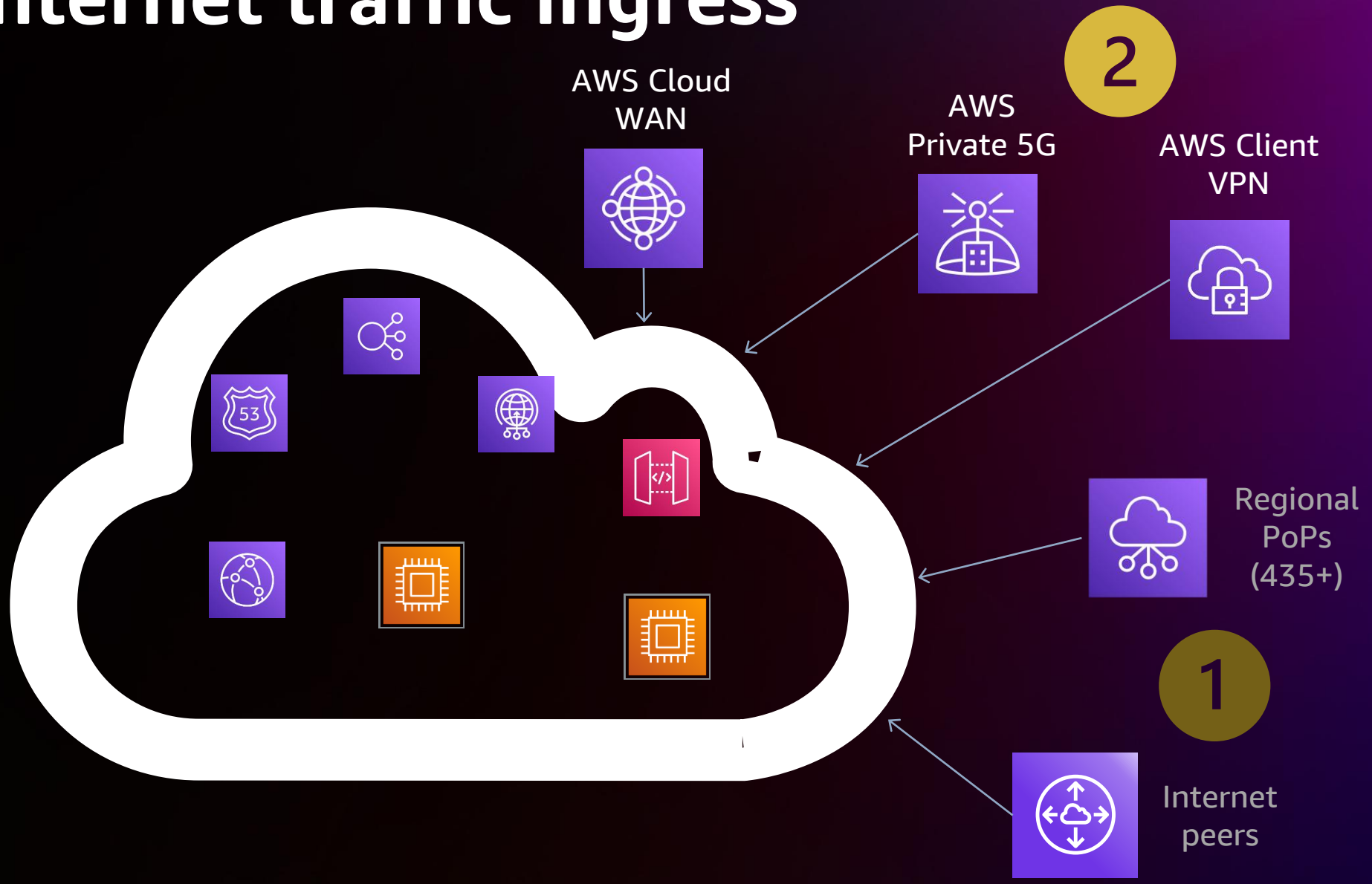
- ~1 million DDoS attacks per year
- Exabytes of data analyzed every minute
- 1,000s of DDoS attacks mitigated every day
- 100+ billion AMR requests processed per day
- 300 GB of flow logs ingested every second

Traffic routes (utopia)

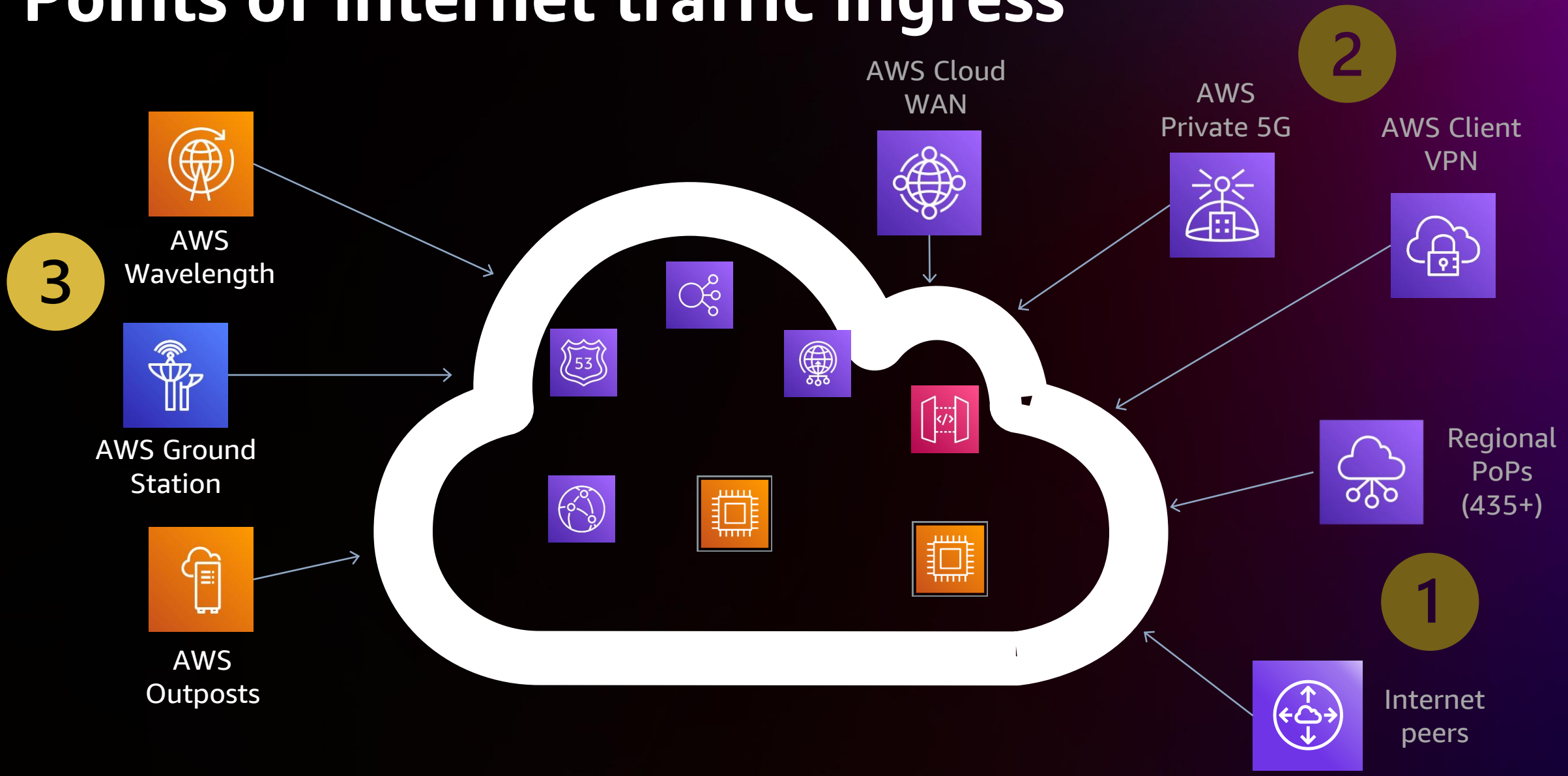
Points of internet traffic ingress



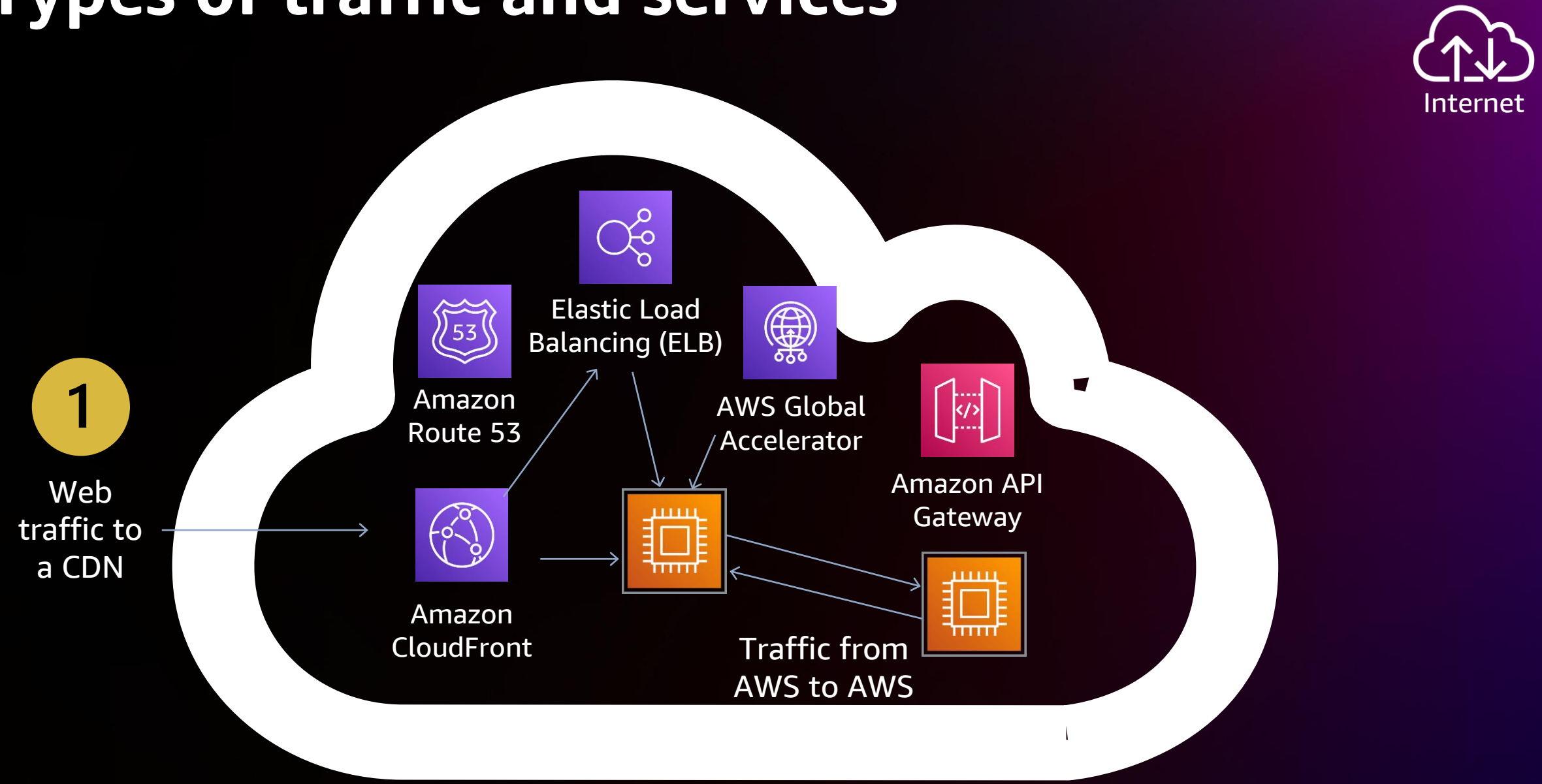
Points of internet traffic ingress



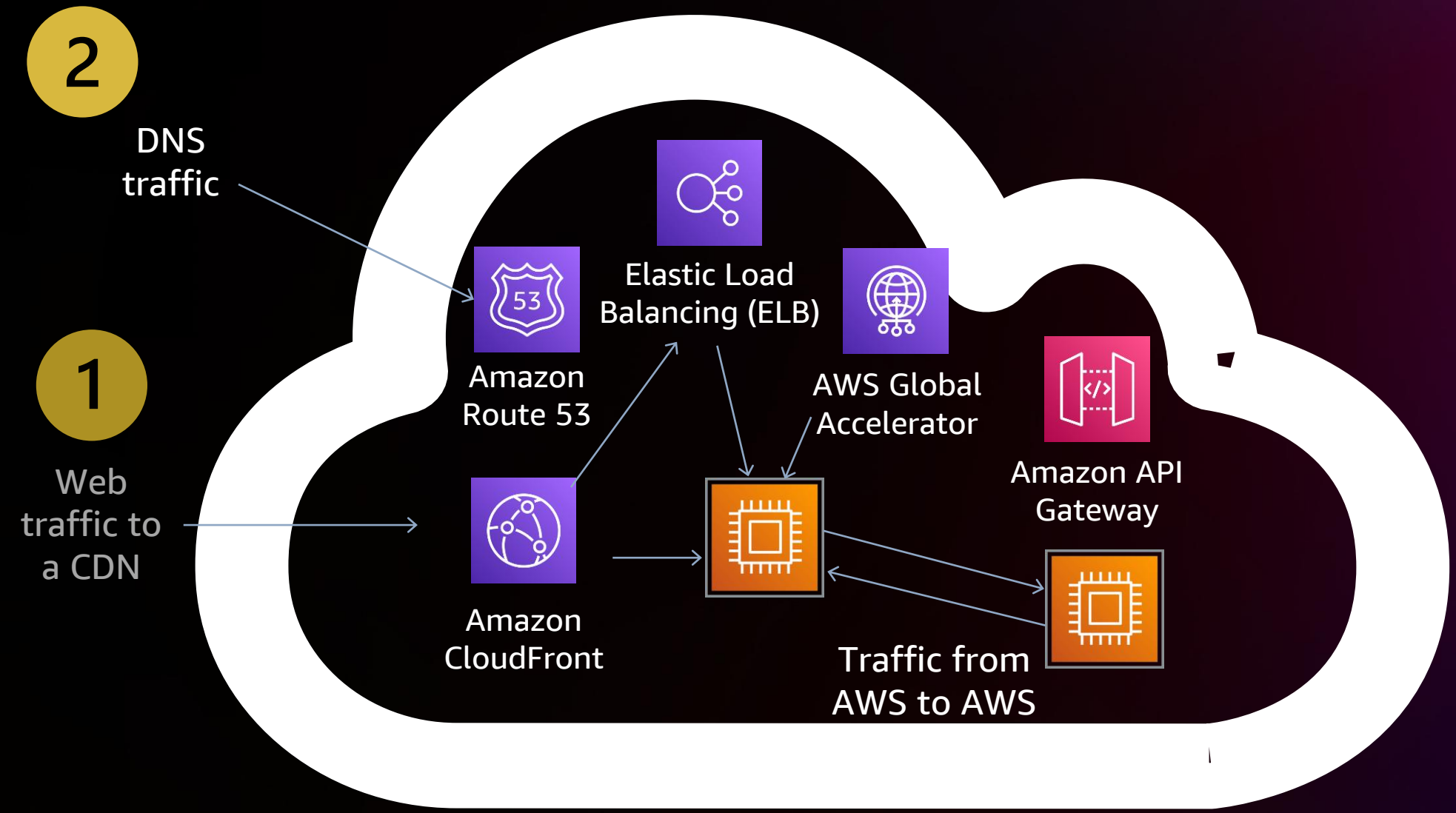
Points of internet traffic ingress



Types of traffic and services



Types of traffic and services



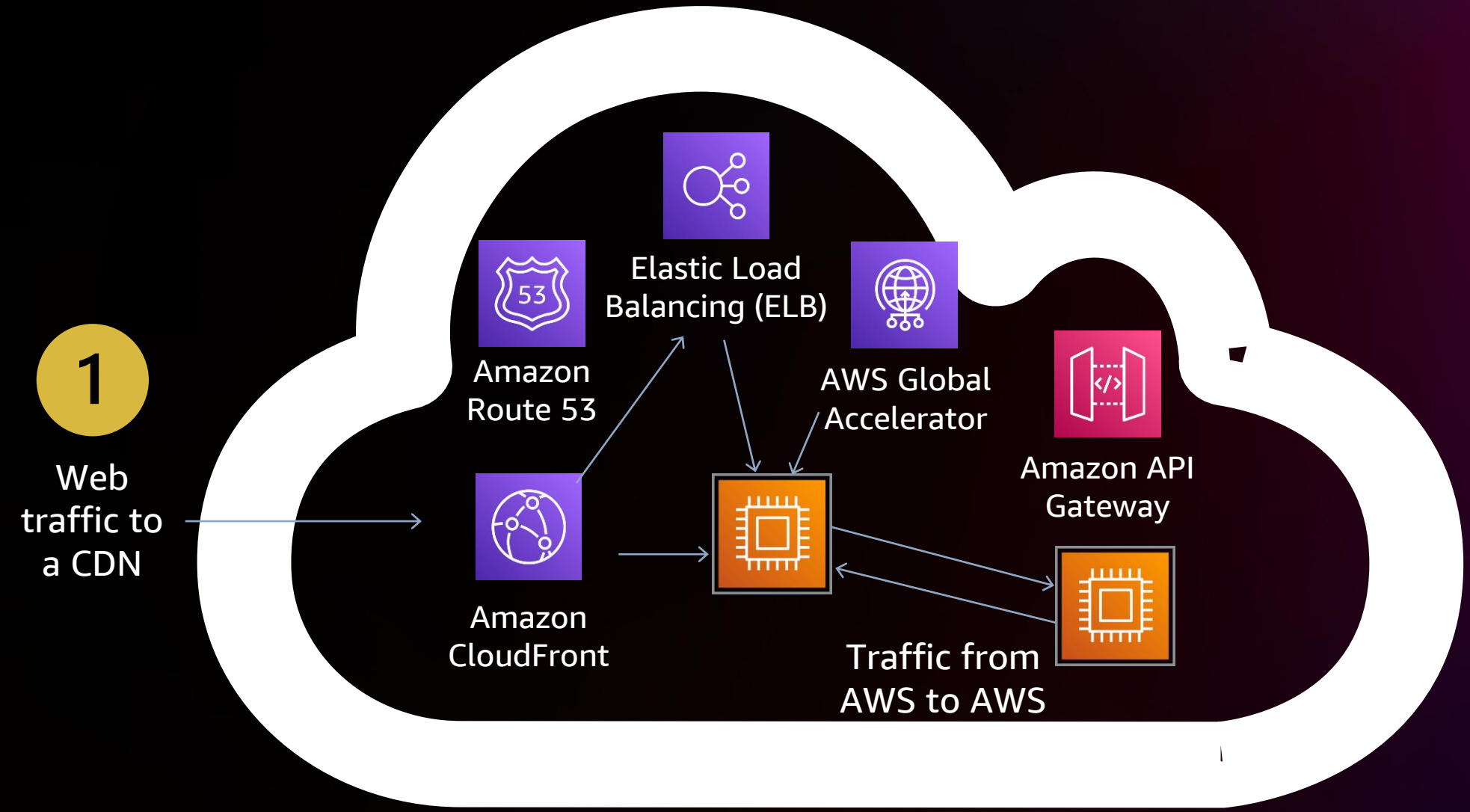
Types of traffic and services

Types of traffic and services

Possible traffic routes (more like the reality)

Every route into AWS is a potential DDoS entry point

Types of traffic and services



DDoS protection: Web traffic to CloudFront

Expected traffic well defined
(TCP/HTTP/QUIC/:80/:443)

Amazon CloudFront

PoP

PoP

PoP

Request flood

Detect

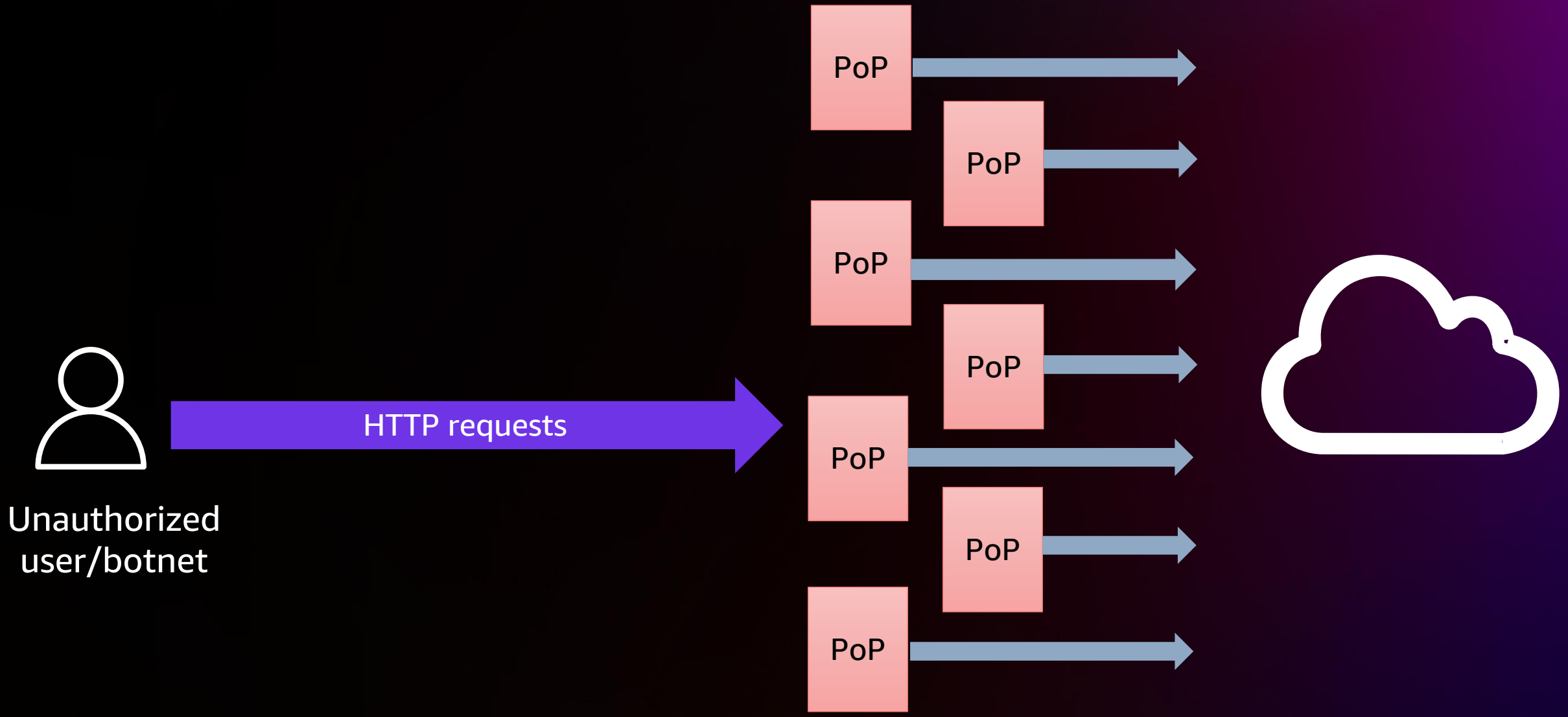
Mitigate

Learn

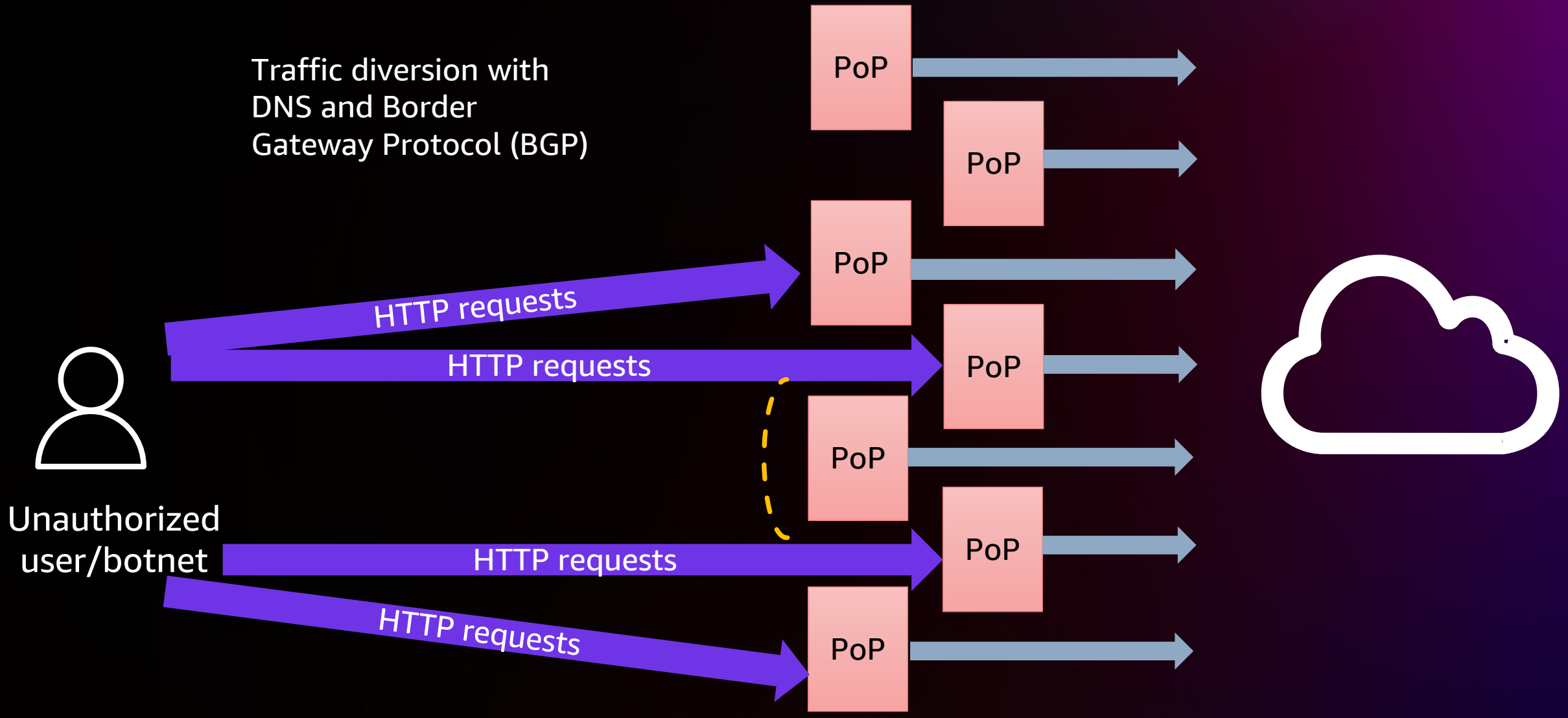
Observe

AWS Shield

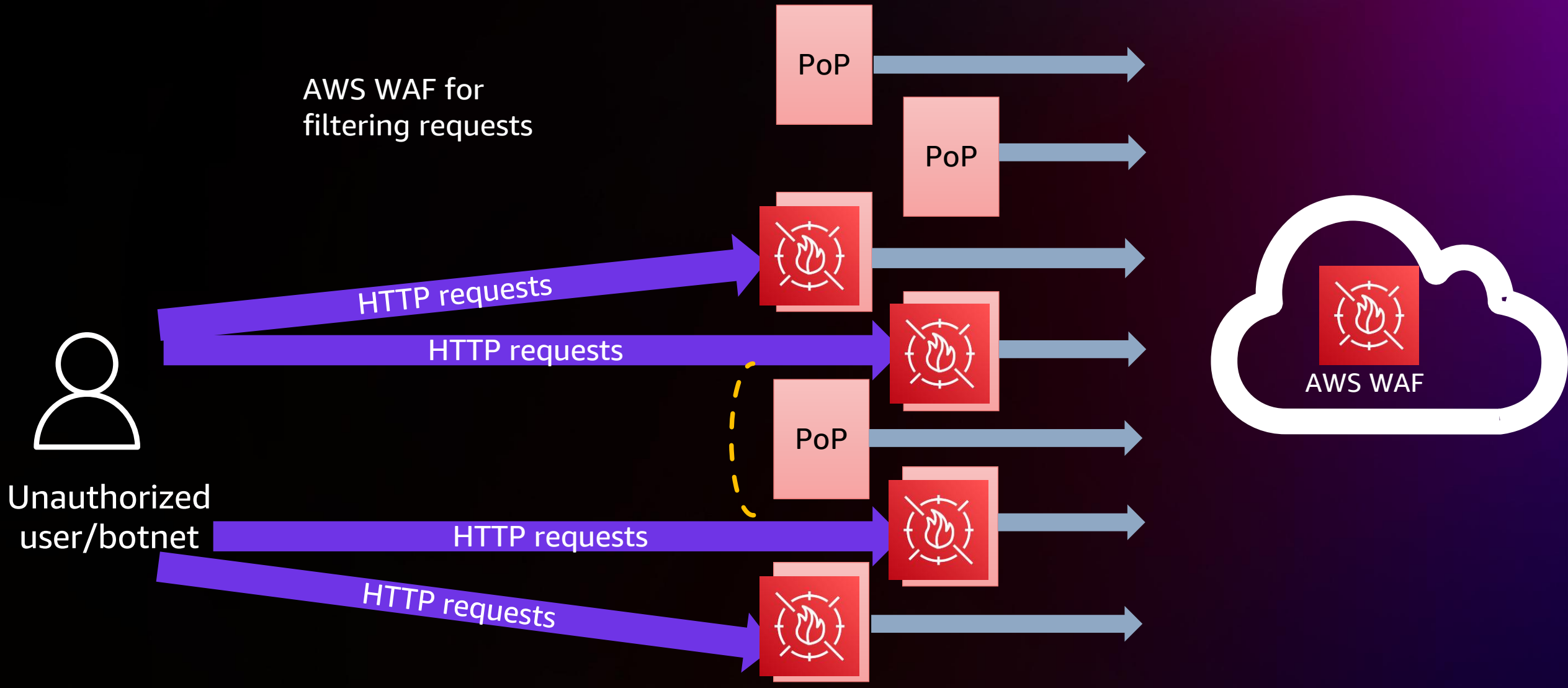
The request flood attack



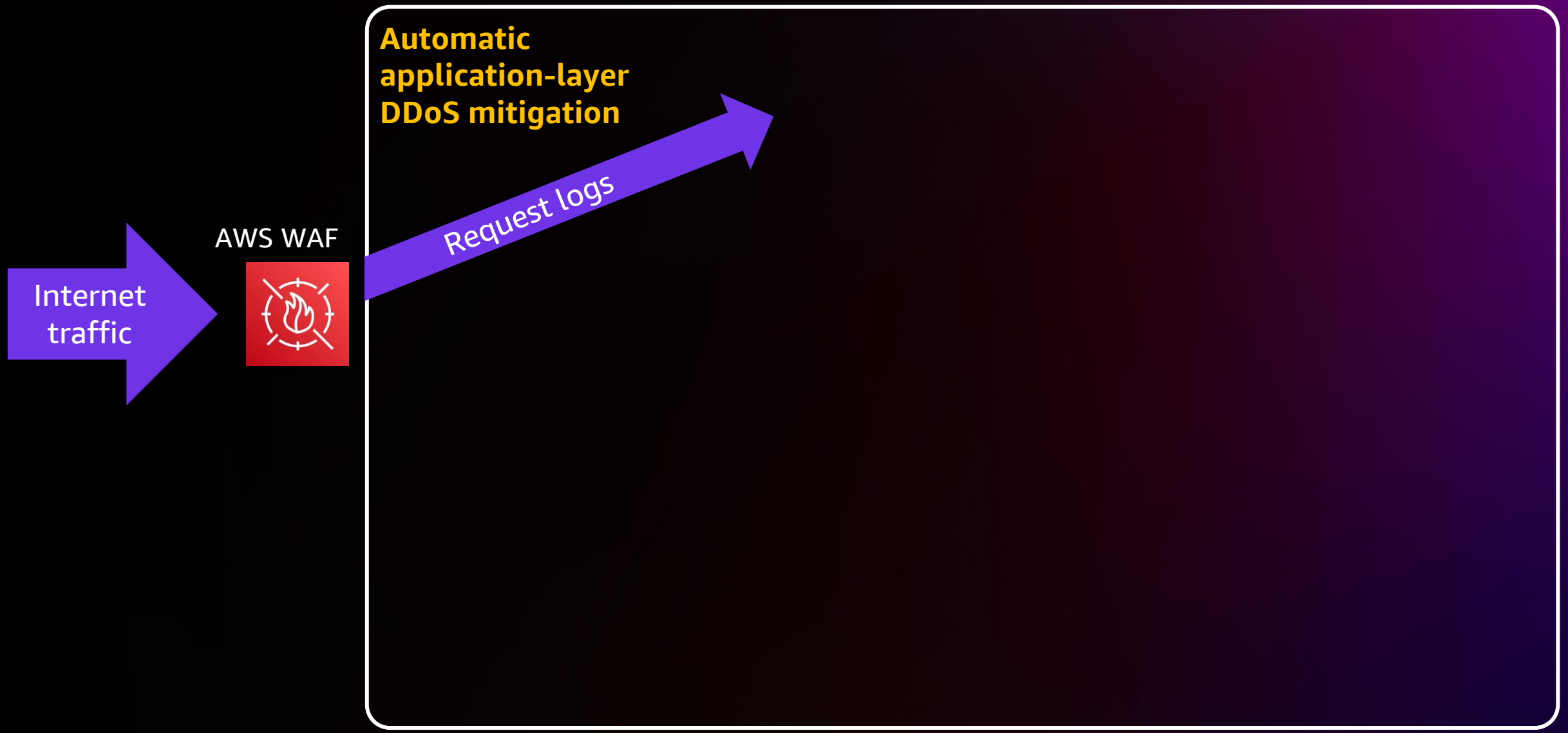
The request flood attack



The request flood attack



L7 auto mitigation with AWS Shield Advanced



L7 auto mitigation with AWS Shield Advanced

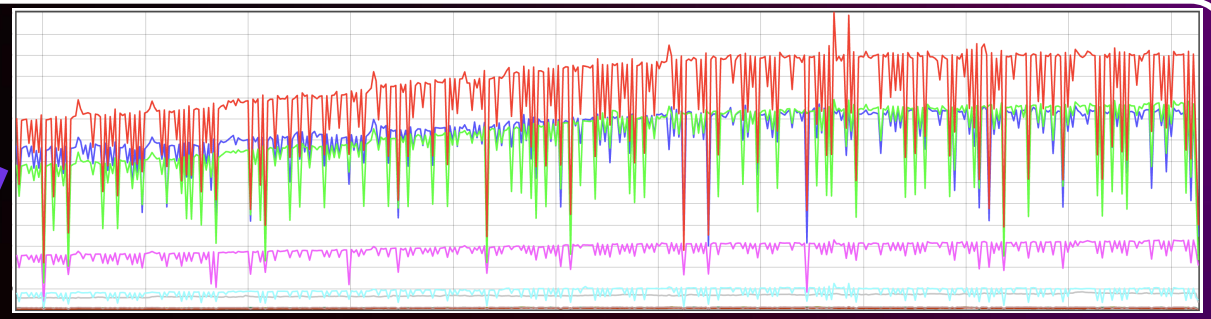
L7 auto mitigation with AWS Shield Advanced

Automatic application-layer DDoS mitigation

Internet traffic

AWS WAF

Request logs



Per-resource baseline

L7 auto mitigation with AWS Shield Advanced

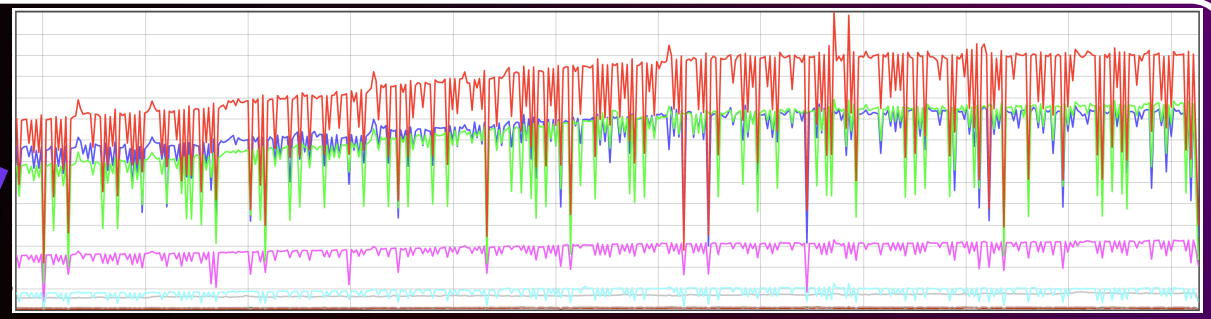
Automatic application-layer DDoS mitigation

Internet traffic

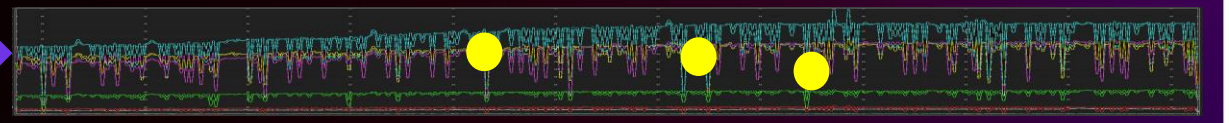
AWS WAF

Request logs

Request logs



Per-resource baseline



Continuous anomaly detection

L7 auto mitigation with AWS Shield Advanced

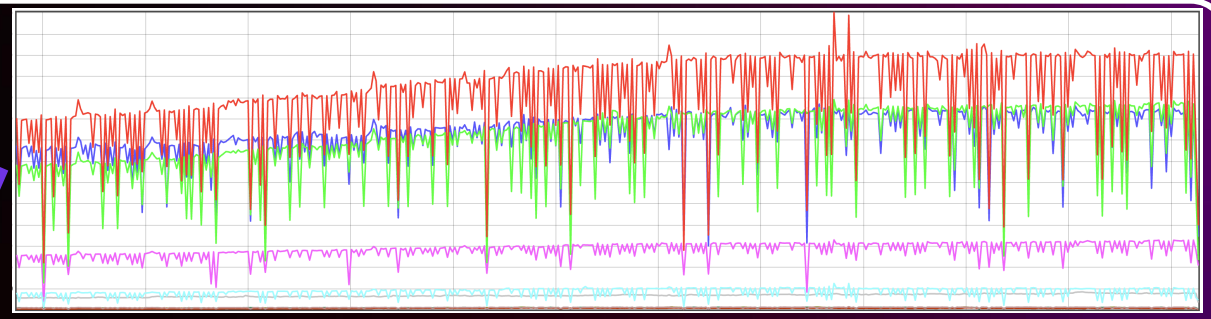
Automatic application-layer DDoS mitigation

Internet traffic

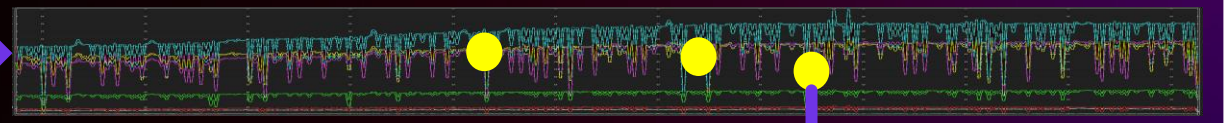
AWS WAF

Request logs

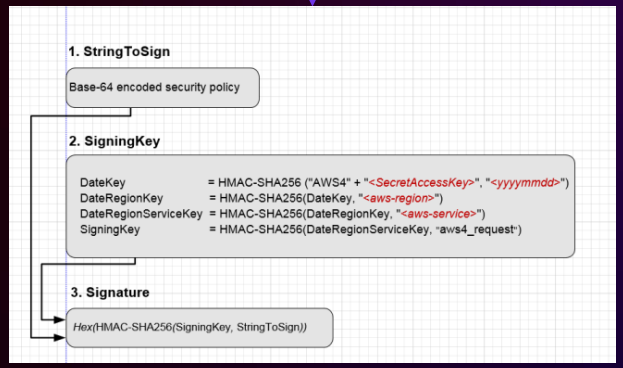
Request logs



Per-resource baseline



Continuous anomaly detection



Attack signatures

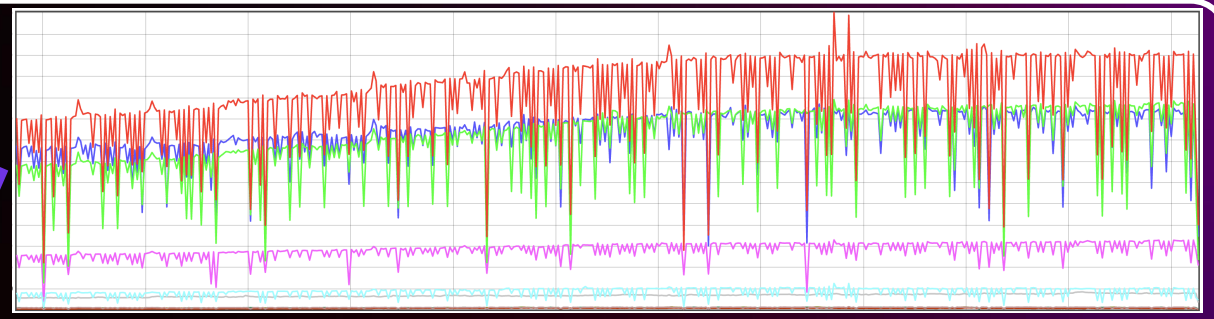
L7 auto mitigation with AWS Shield Advanced

Automatic application-layer DDoS mitigation

Internet traffic

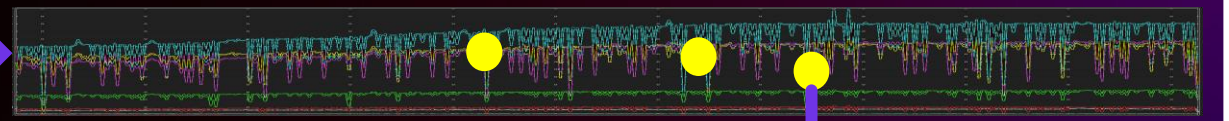
AWS WAF

Request logs



Per-resource baseline

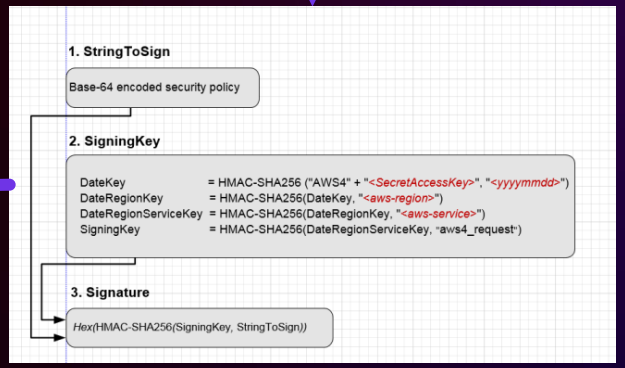
Request logs



Continuous anomaly detection

```
{
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
},
  "Statement": {
    "SizeConstraintStatement": {
      "FieldToMatch": { "QueryString": {} },
      "ComparisonOperator": "GT",
    }
  }
}
```

Builds AWS WAF rules



Attack signatures

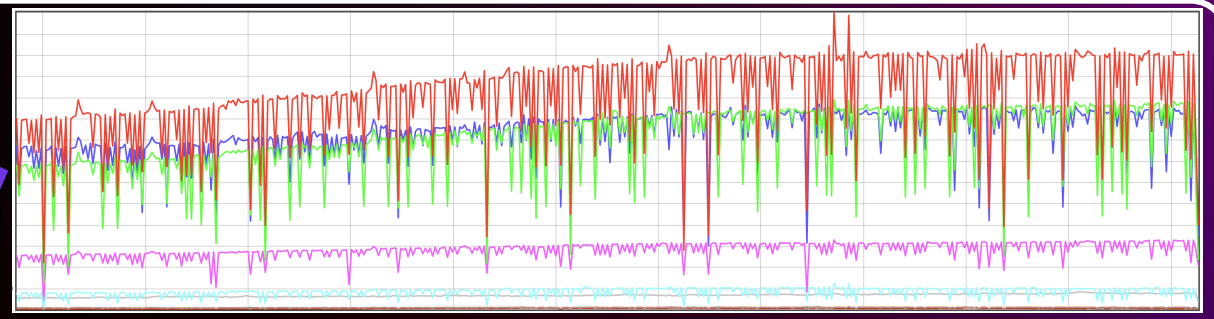
L7 auto mitigation with AWS Shield Advanced

Automatic application-layer DDoS mitigation

Internet traffic

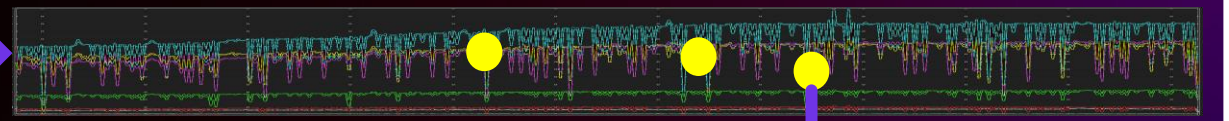
AWS WAF

Request logs



Per-resource baseline

Request logs

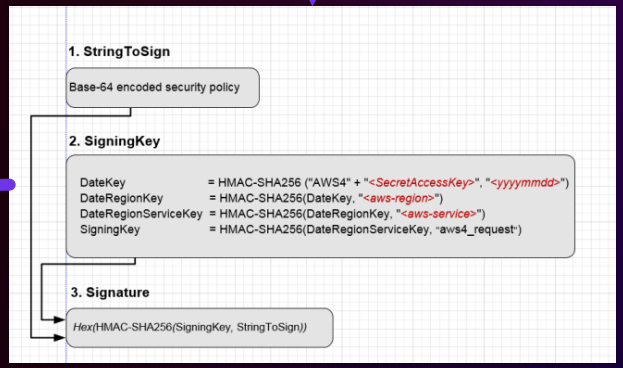


Continuous anomaly detection

Auto-placed

```
{
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
},
  "Statement": {
    "SizeConstraintStatement": {
      "FieldToMatch": { "QueryString": {} },
      "ComparisonOperator": "GT",
    }
  }
}
```

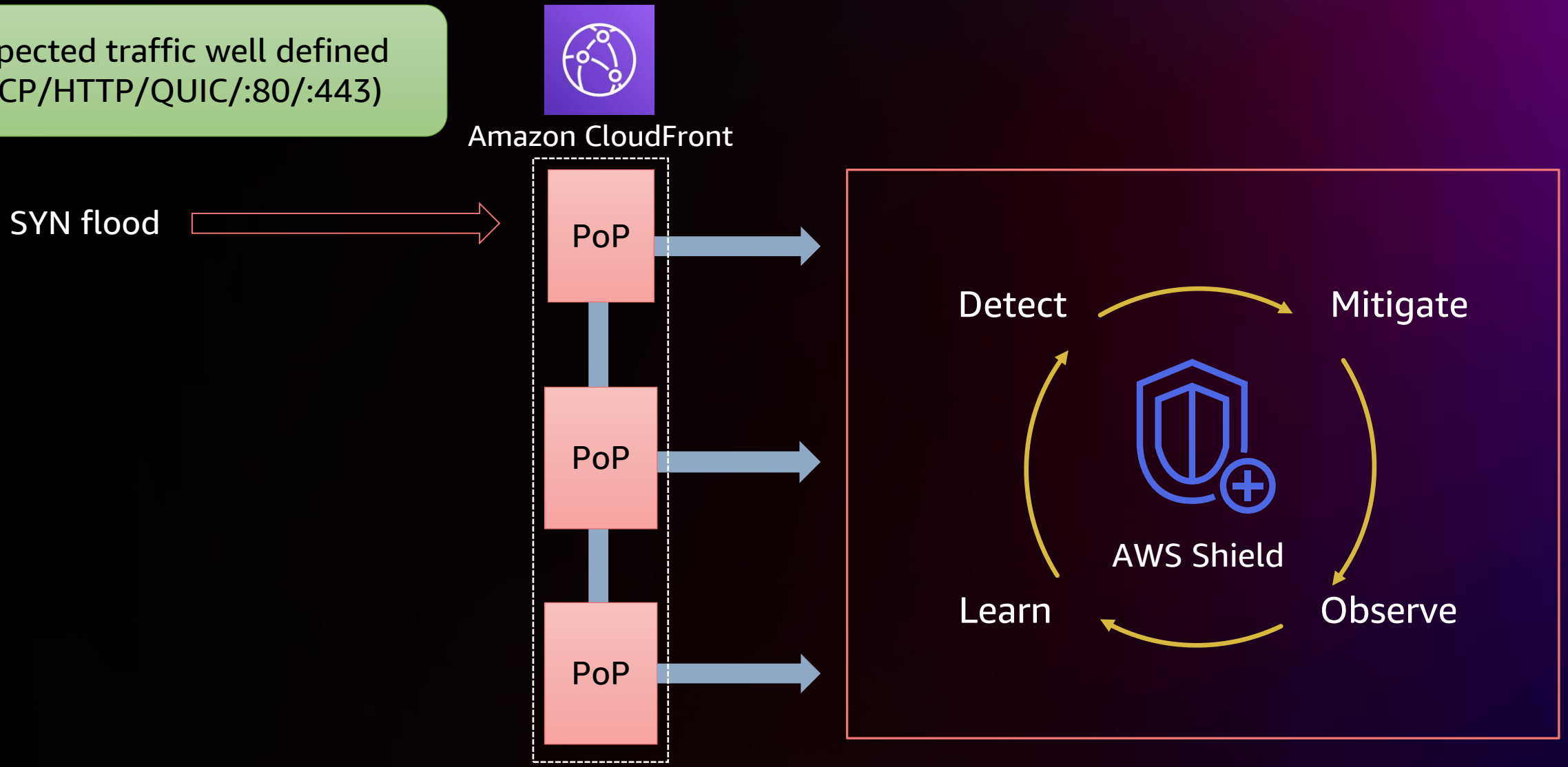
Builds AWS WAF rules



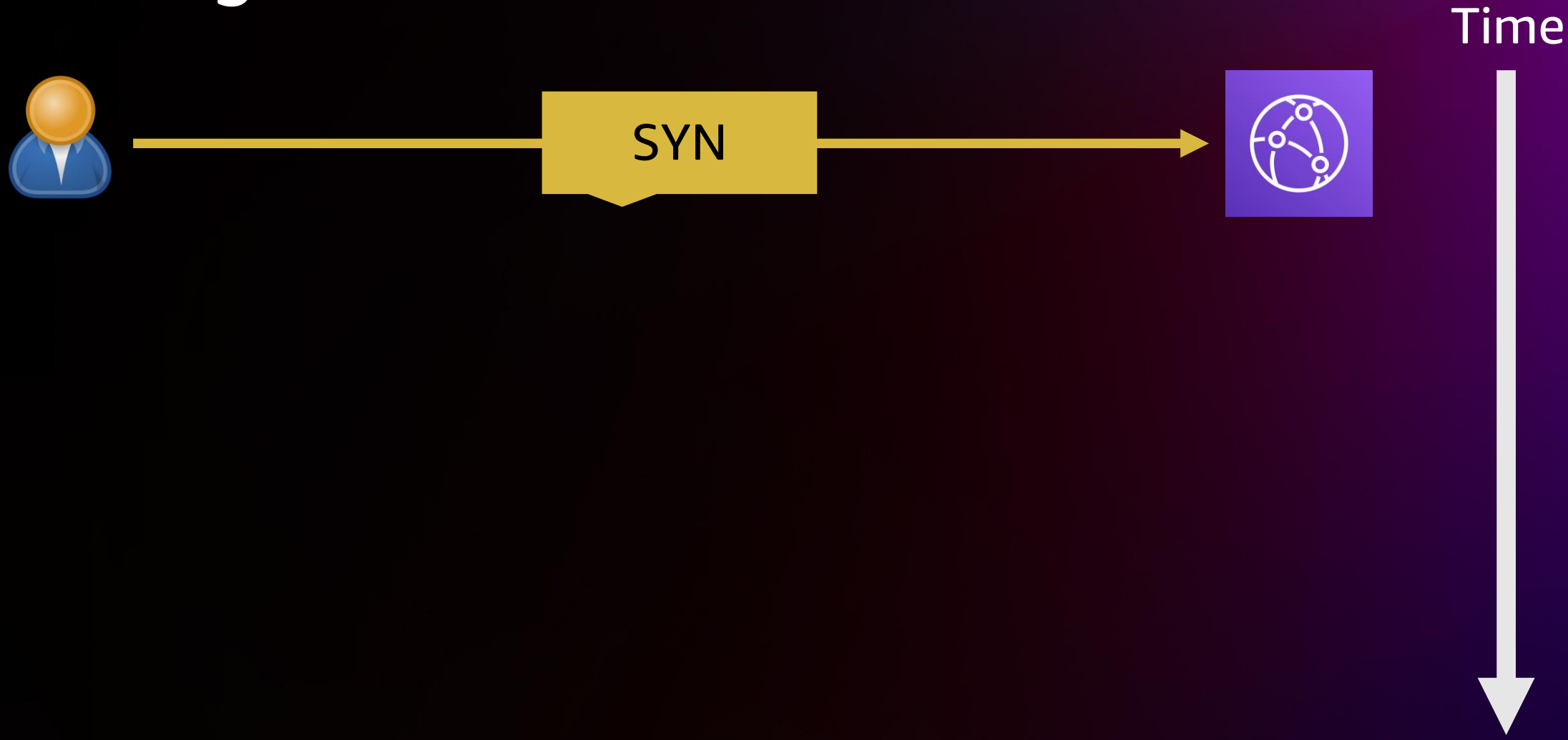
Attack signatures

DDoS protection: Web traffic to a CDN

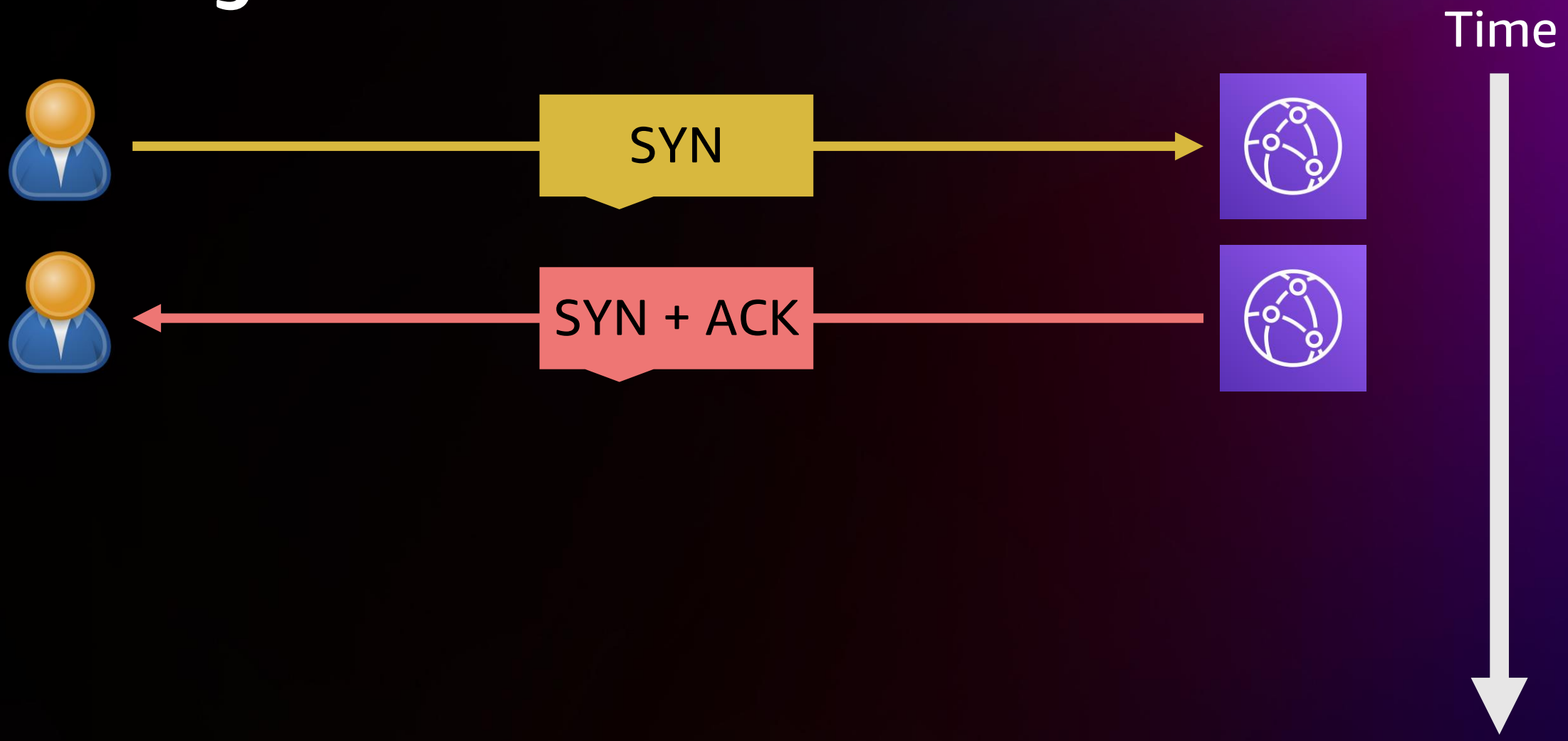
Expected traffic well defined
(TCP/HTTP/QUIC/:80/:443)



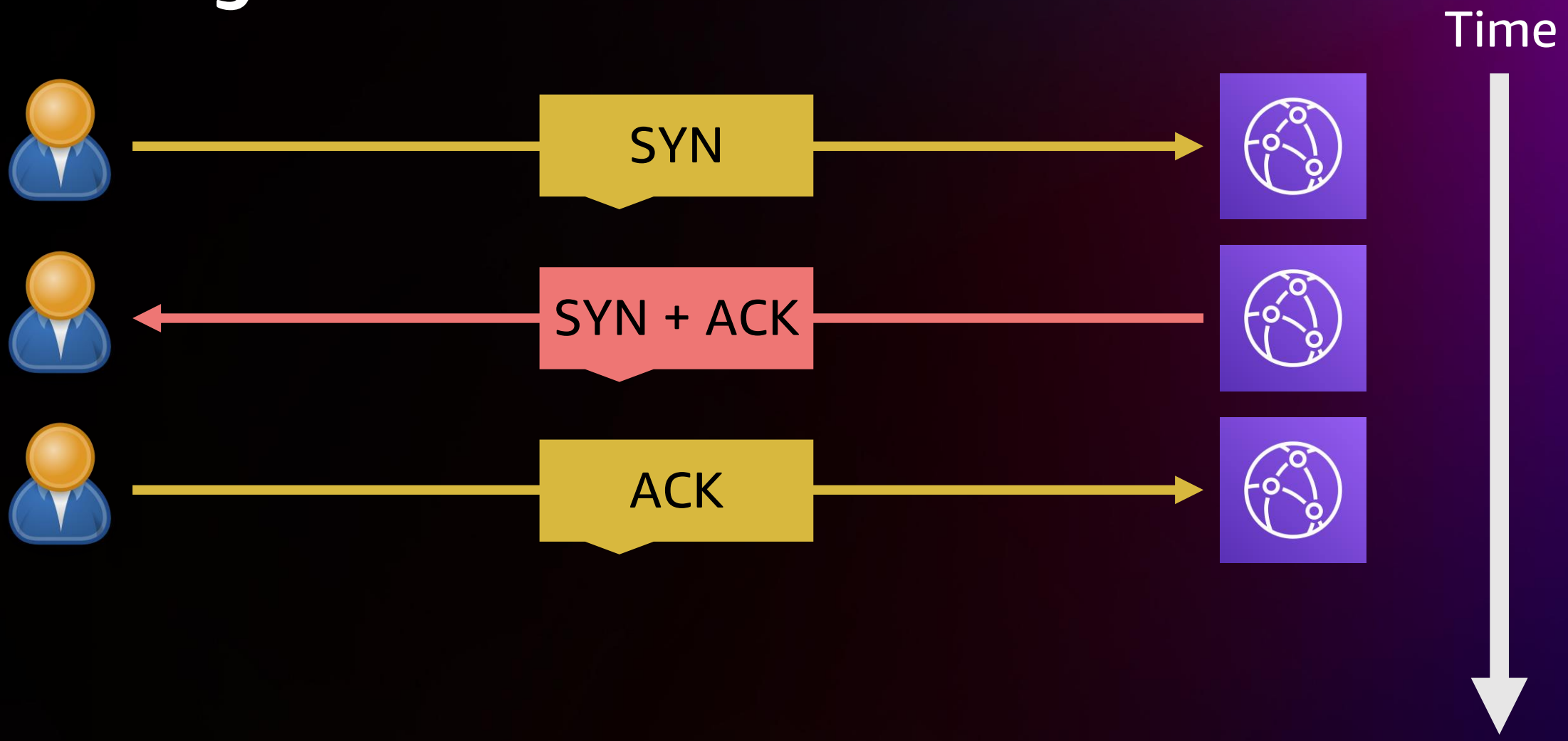
Connecting to Amazon CloudFront



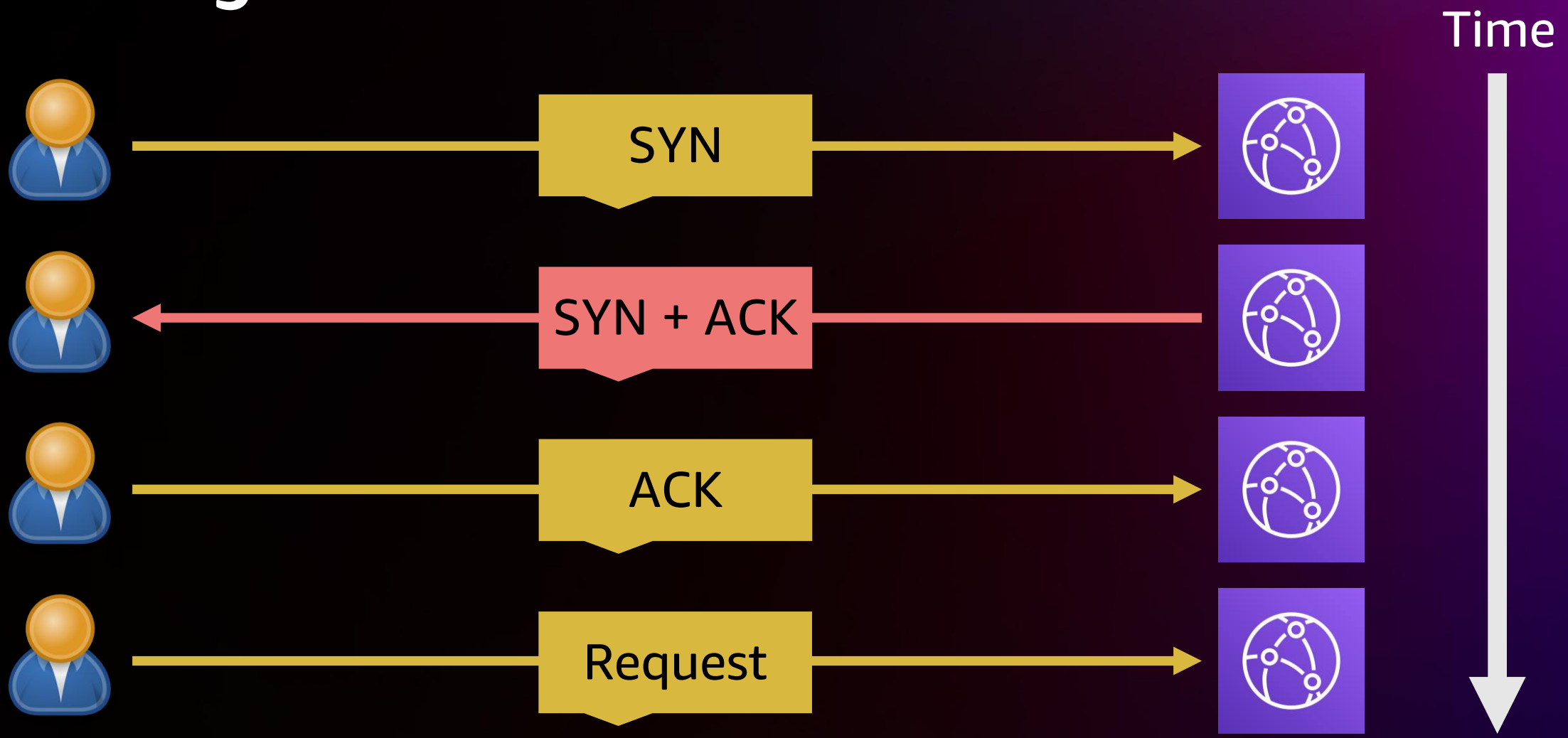
Connecting to Amazon CloudFront



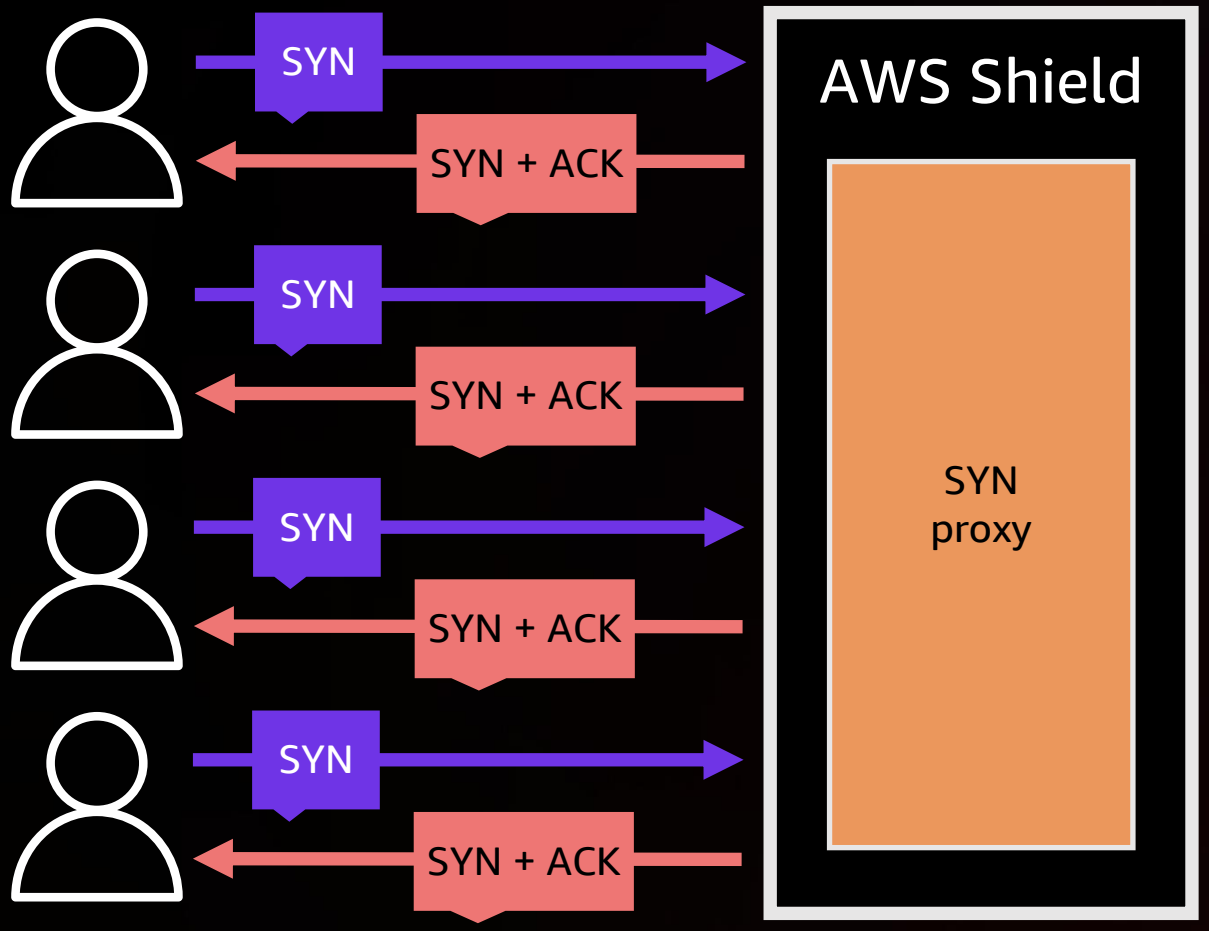
Connecting to Amazon CloudFront



Connecting to Amazon CloudFront



SYN proxy mitigation: During the event



DDoS protection: Web traffic to a CDN

Expected traffic well defined
(TCP/HTTP/QUIC/:80/:443)

Amazon CloudFront

UDP amplification

PoP

PoP

PoP

Detect

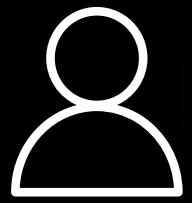
Mitigate

AWS Shield

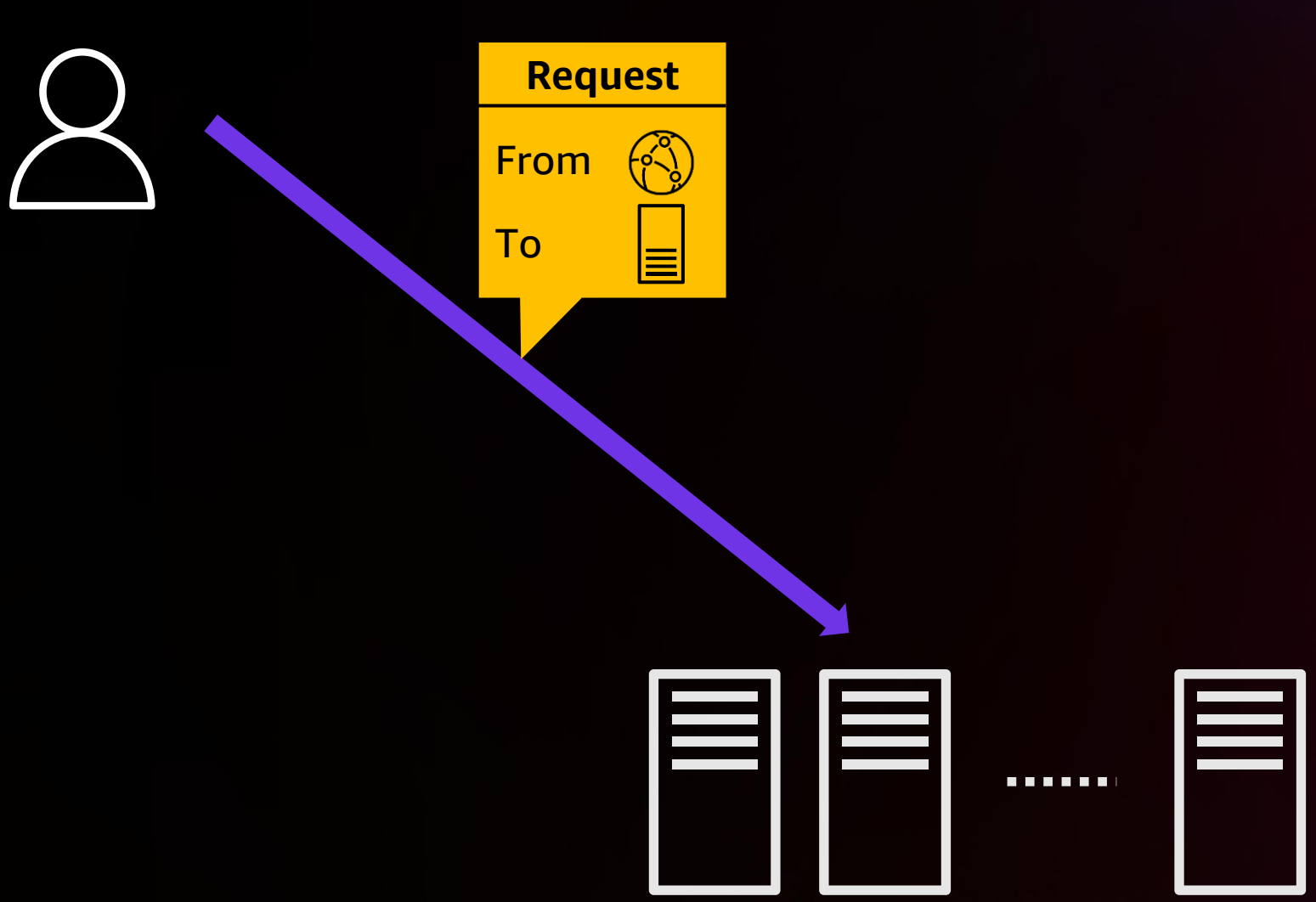
Learn

Observe

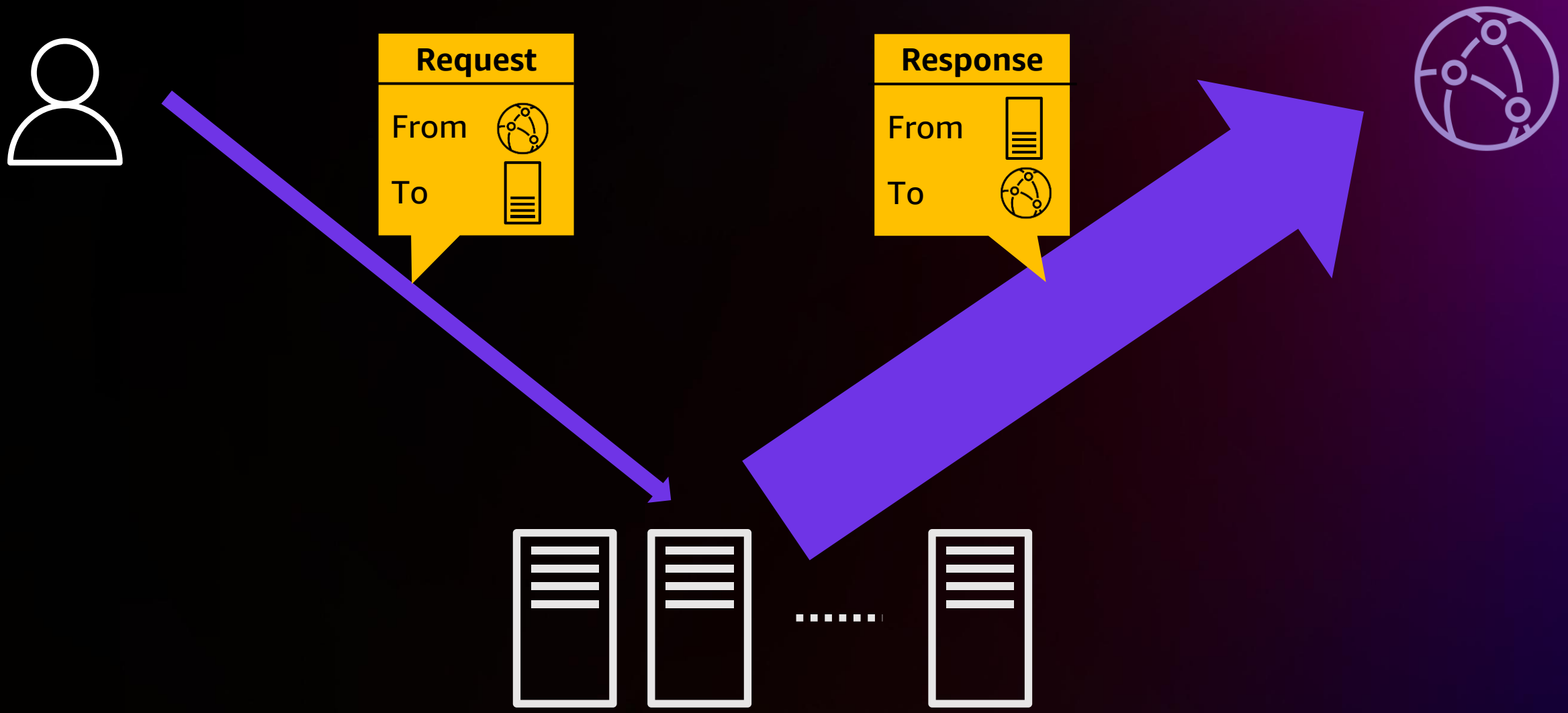
The amplification attack



The amplification attack



The amplification attack

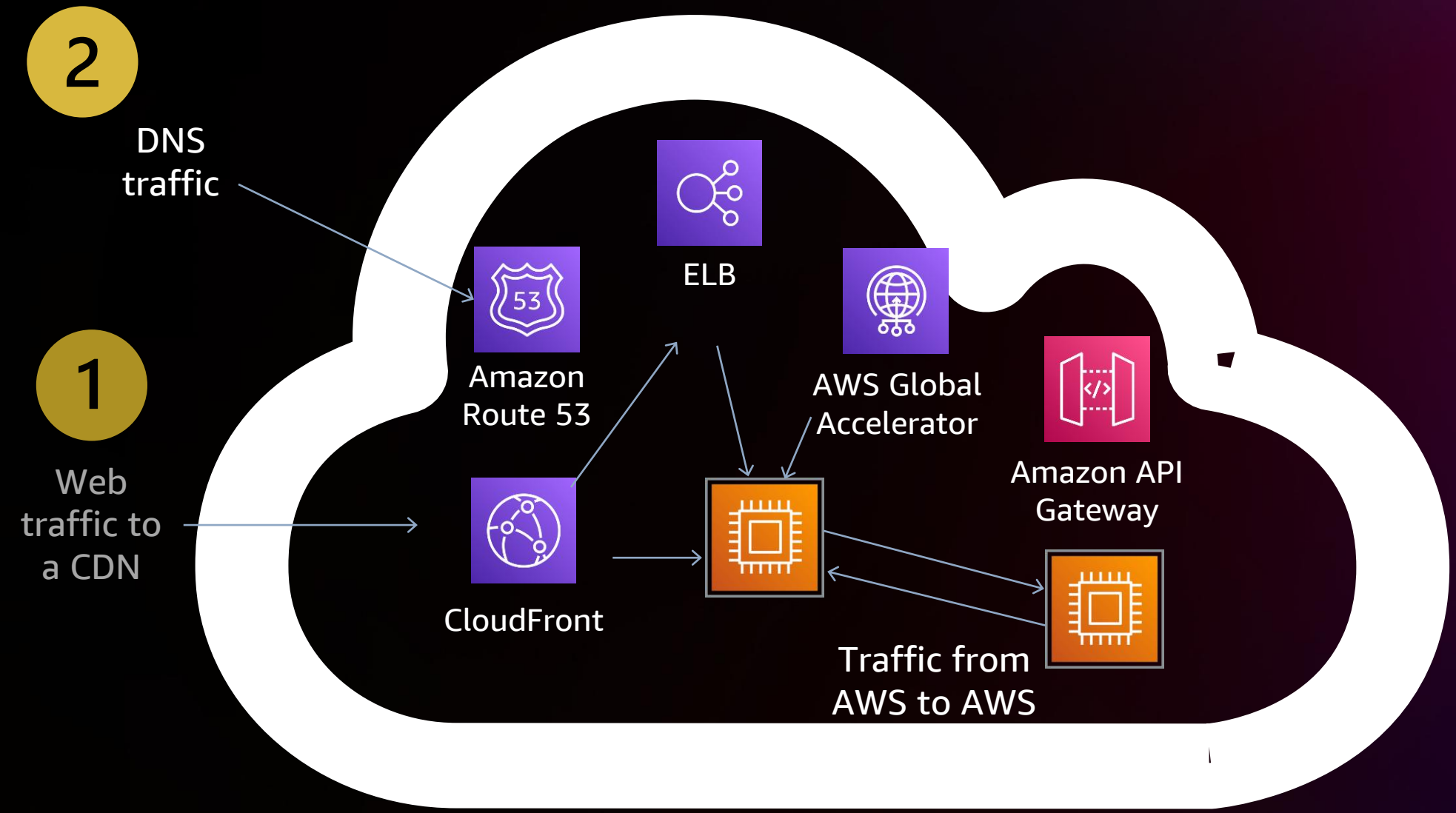


Protocols and bandwidth amplification factor

Protocol	Bandwidth amplification factor
DNS	28 to 54
NTP	556.9
SSDP	30.8
CharGEN	358.8
RIPv1	131.24
CLDAP	56 to 70
Memcached	10,000 to 51,000

Source: https://www.us-cert.gov/ncas/alerts/TA14-017A

Types of traffic and services

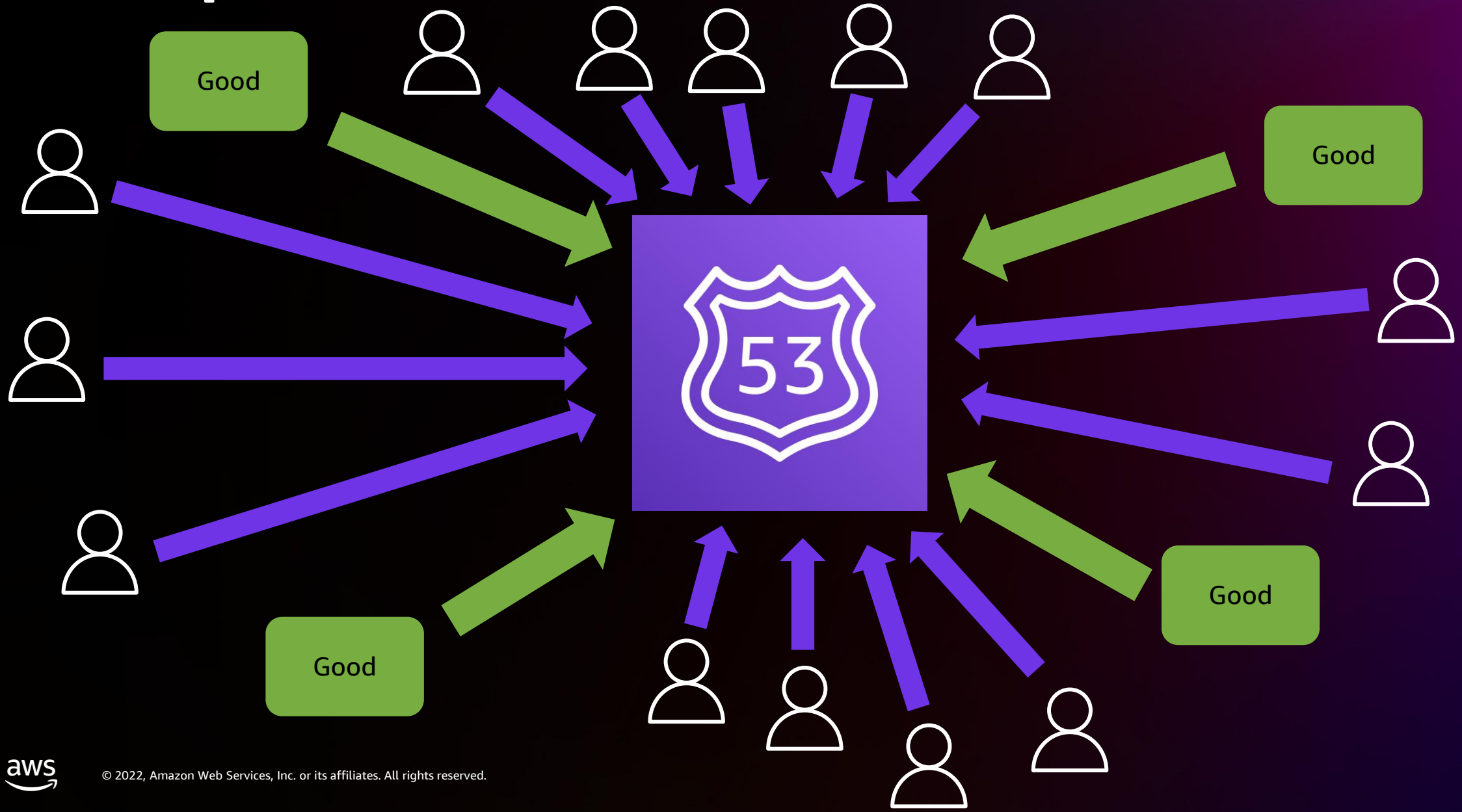


DDoS protection: DNS traffic to Route 53

Amazon Route 53

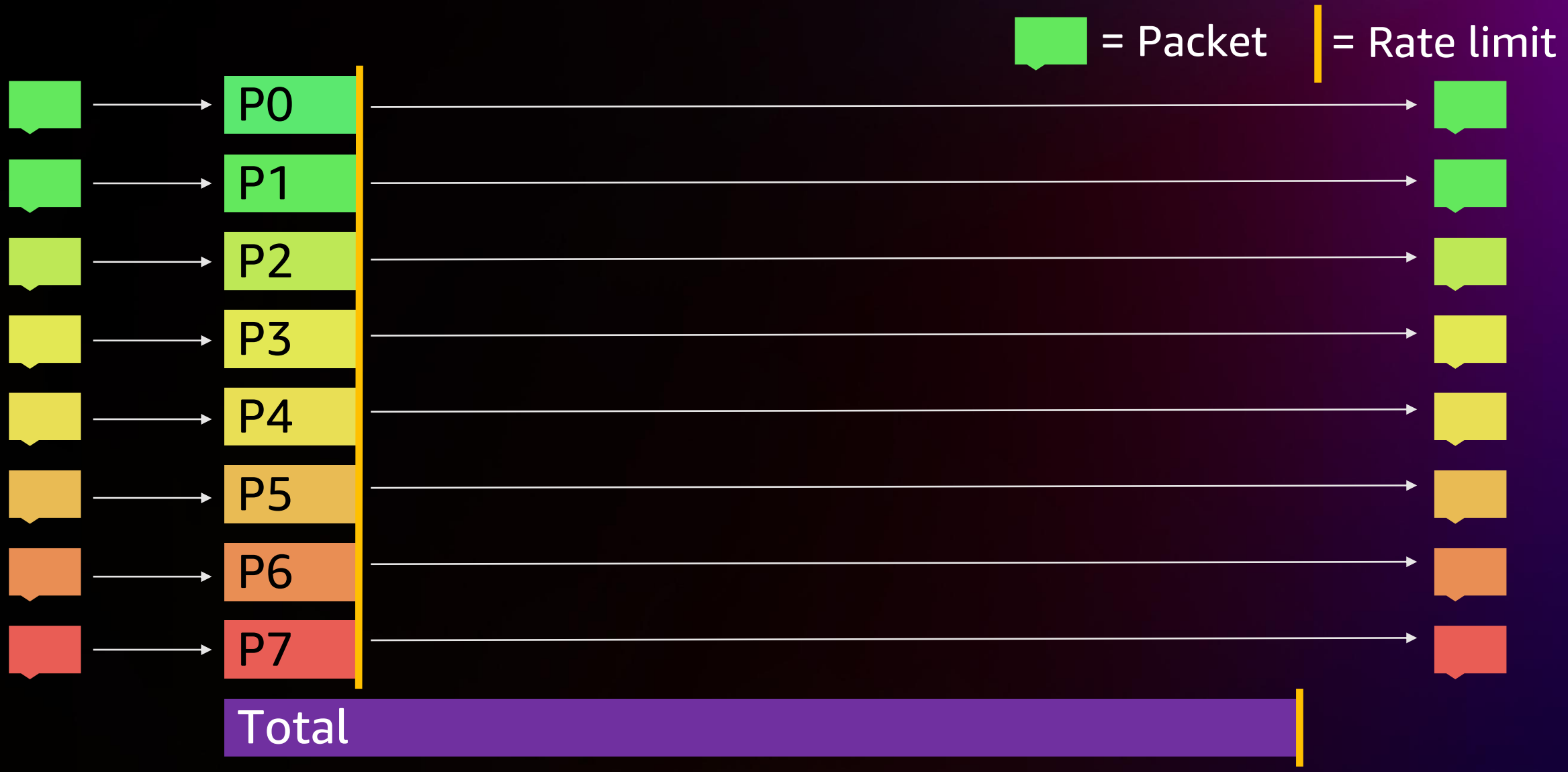
AWS Shield

DDoS protection: DNS traffic to Route 53

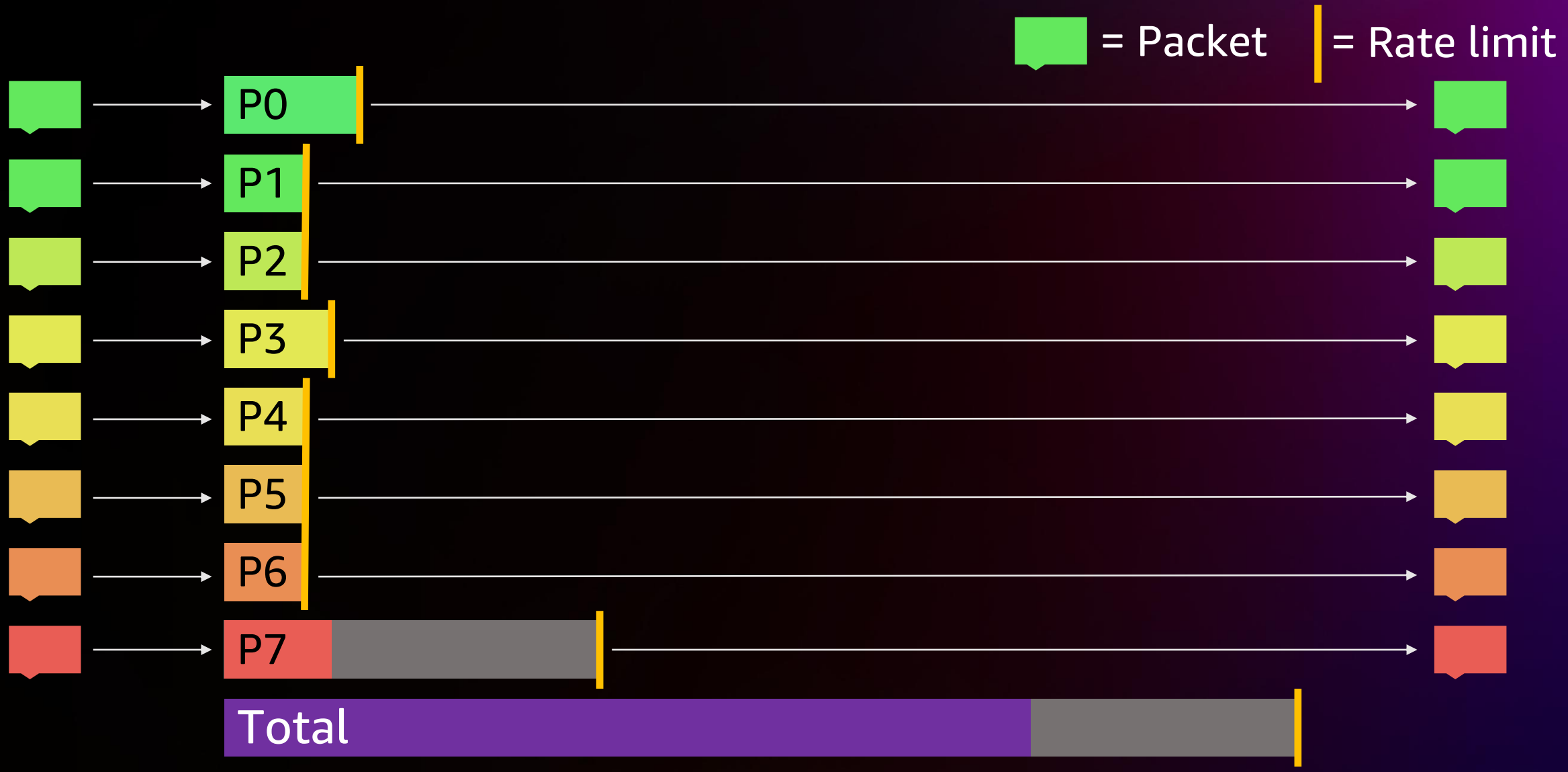


DNS known good resolvers (DKGR) mitigation

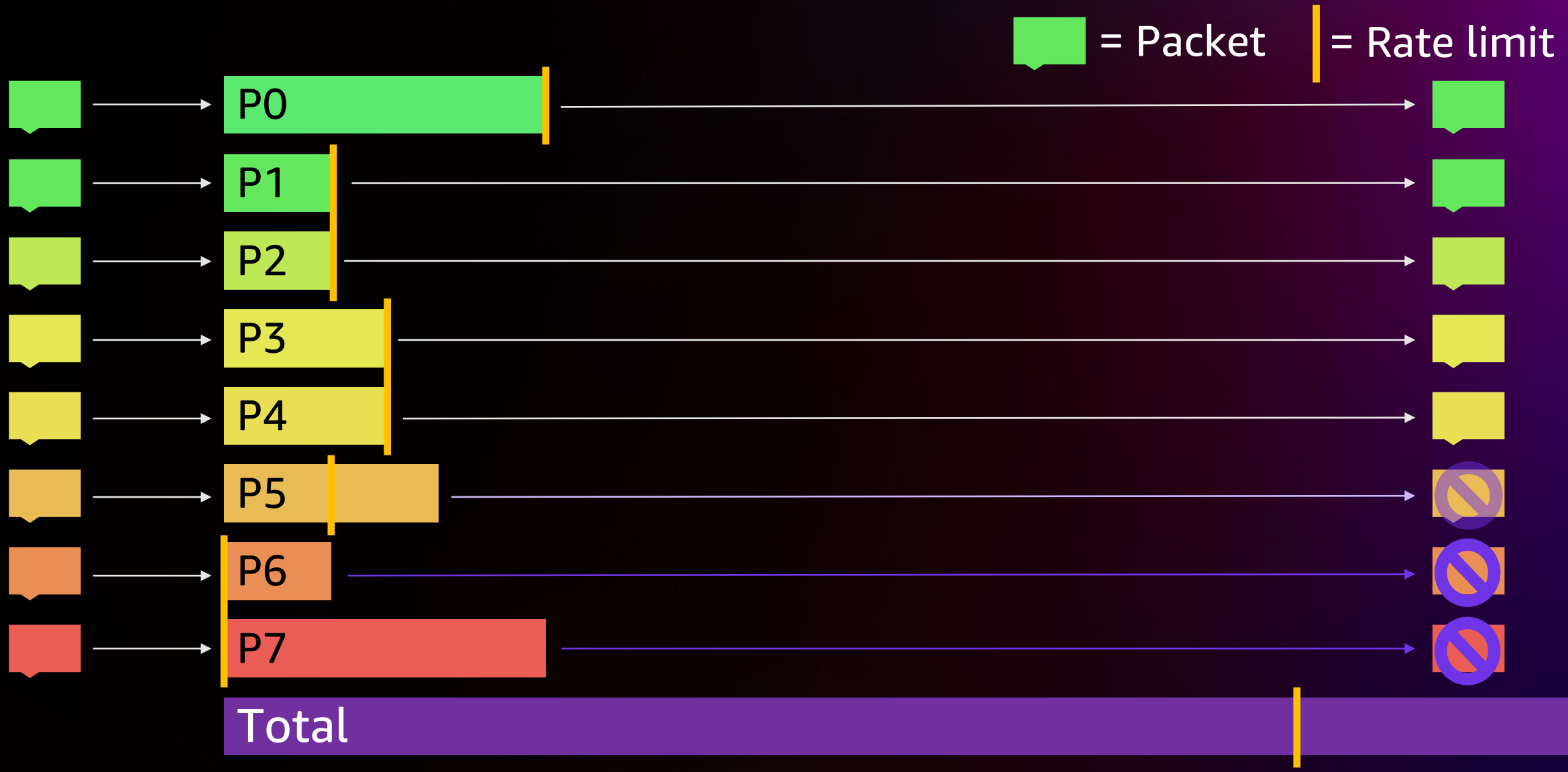
Traffic shaping mitigation



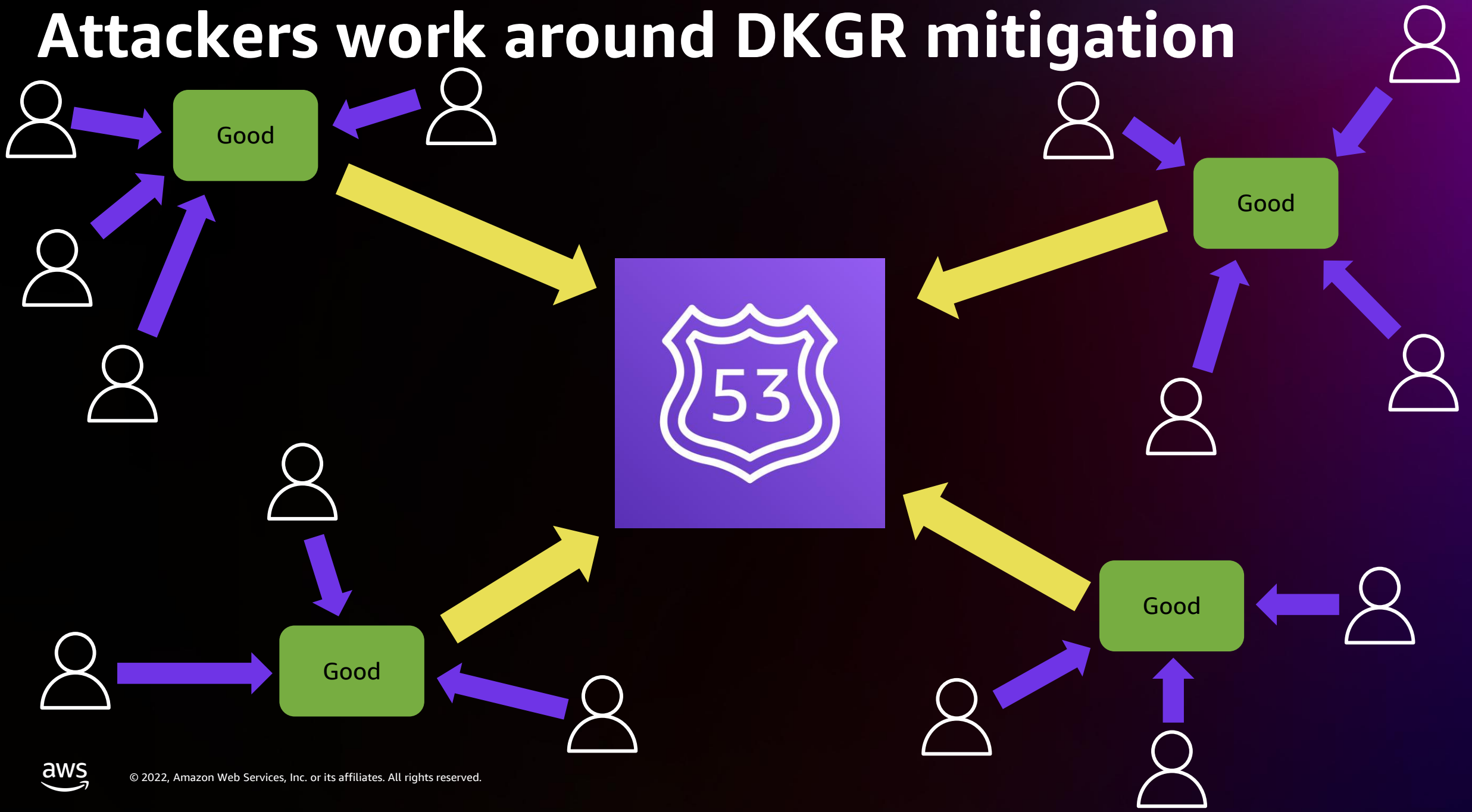
Traffic shaping: Below rate limit



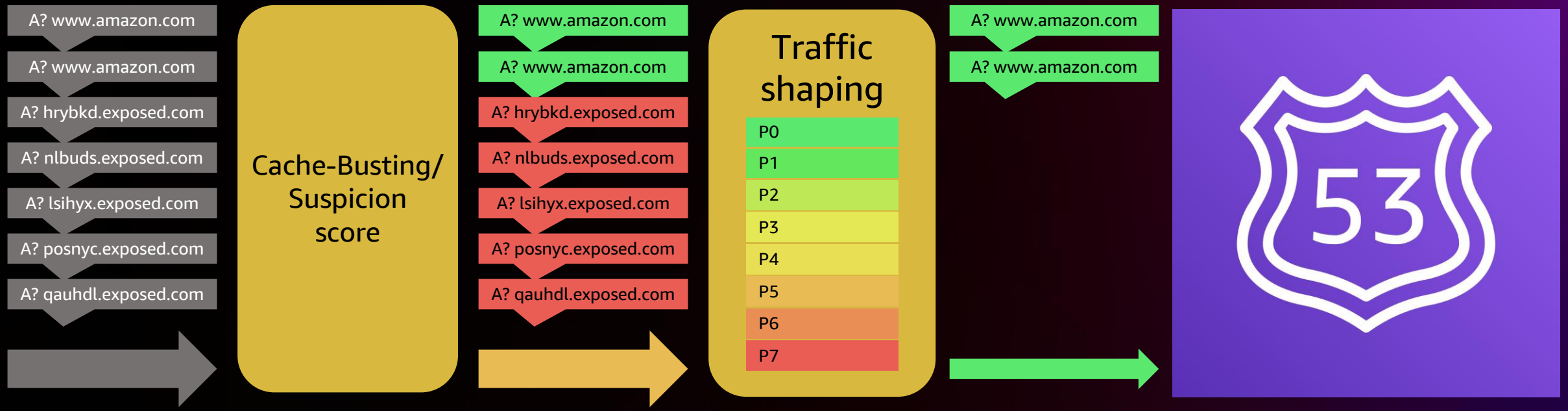
Traffic shaping: Above rate limit



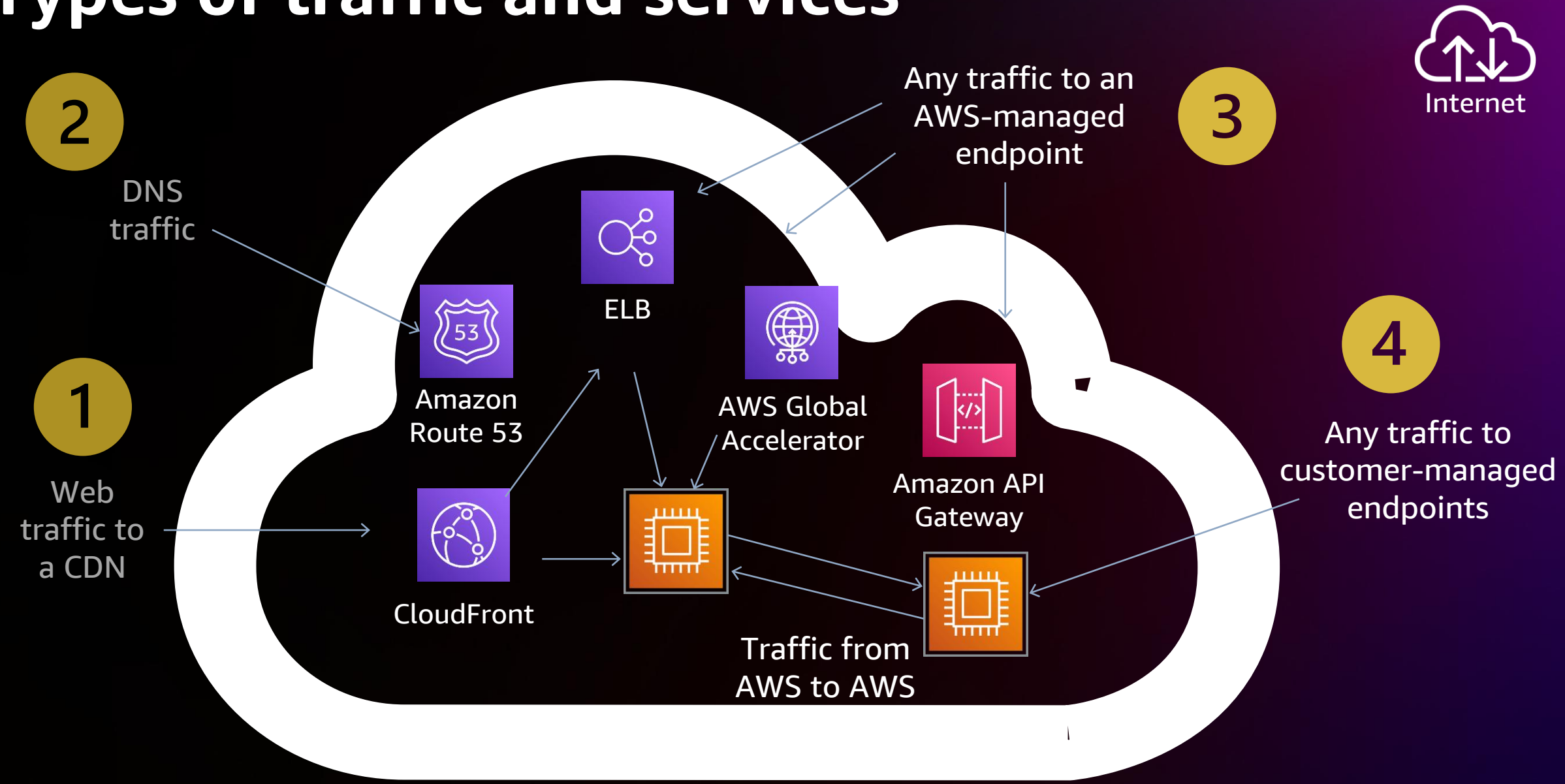
Attackers work around DKGR mitigation



Mitigating cache-busting attacks



Types of traffic and services



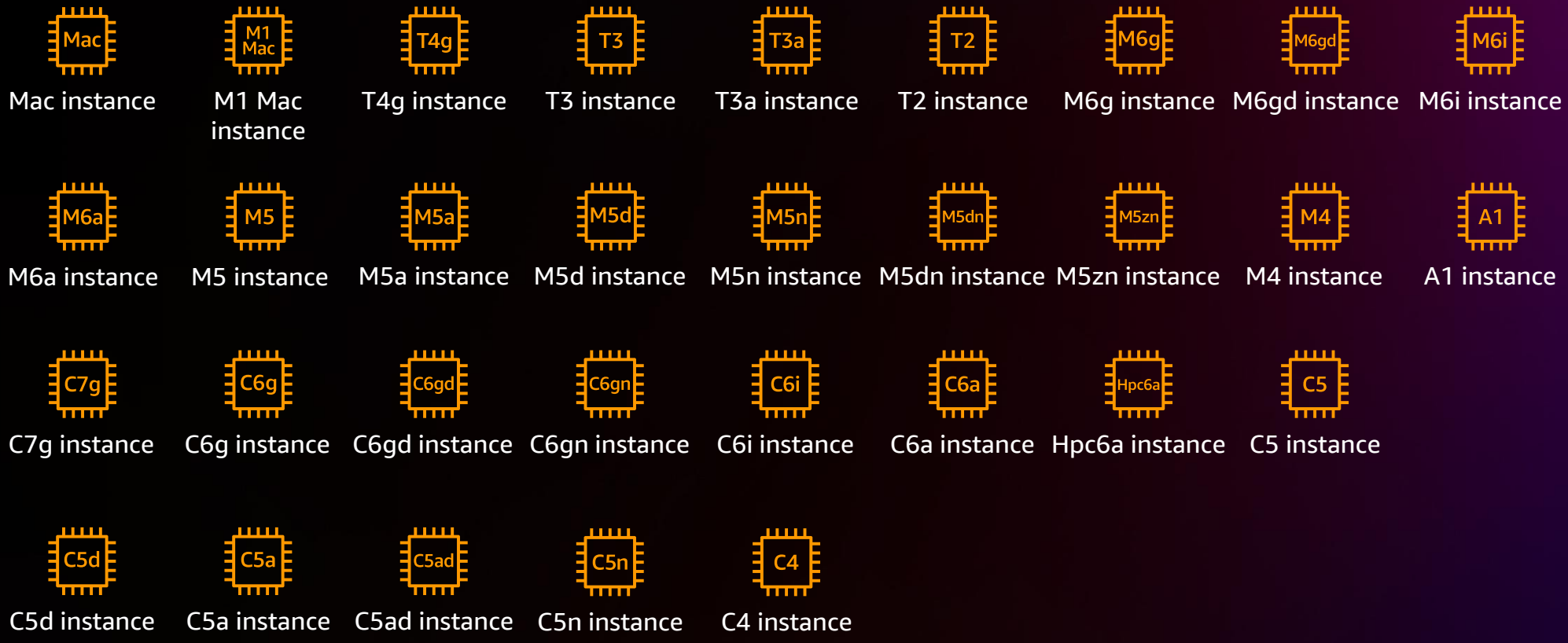
DDoS protection: Any traffic to any endpoint

Any Protocol
Port

Web applications
VoIP
Non-HTTP apps
Content streaming
DNS
IoT
…

DDoS protection: Any traffic to any endpoint

"Just monitor endpoint capacity"



DDoS protection: Any traffic to any endpoint

Challenges

1. Legitimate layer 7 traffic is determined by your application
2. Understanding NetFlow traffic at scale: 50 TB collected per day
3. Delays in detection and mitigation latency

DDoS protection: NACL

VPC

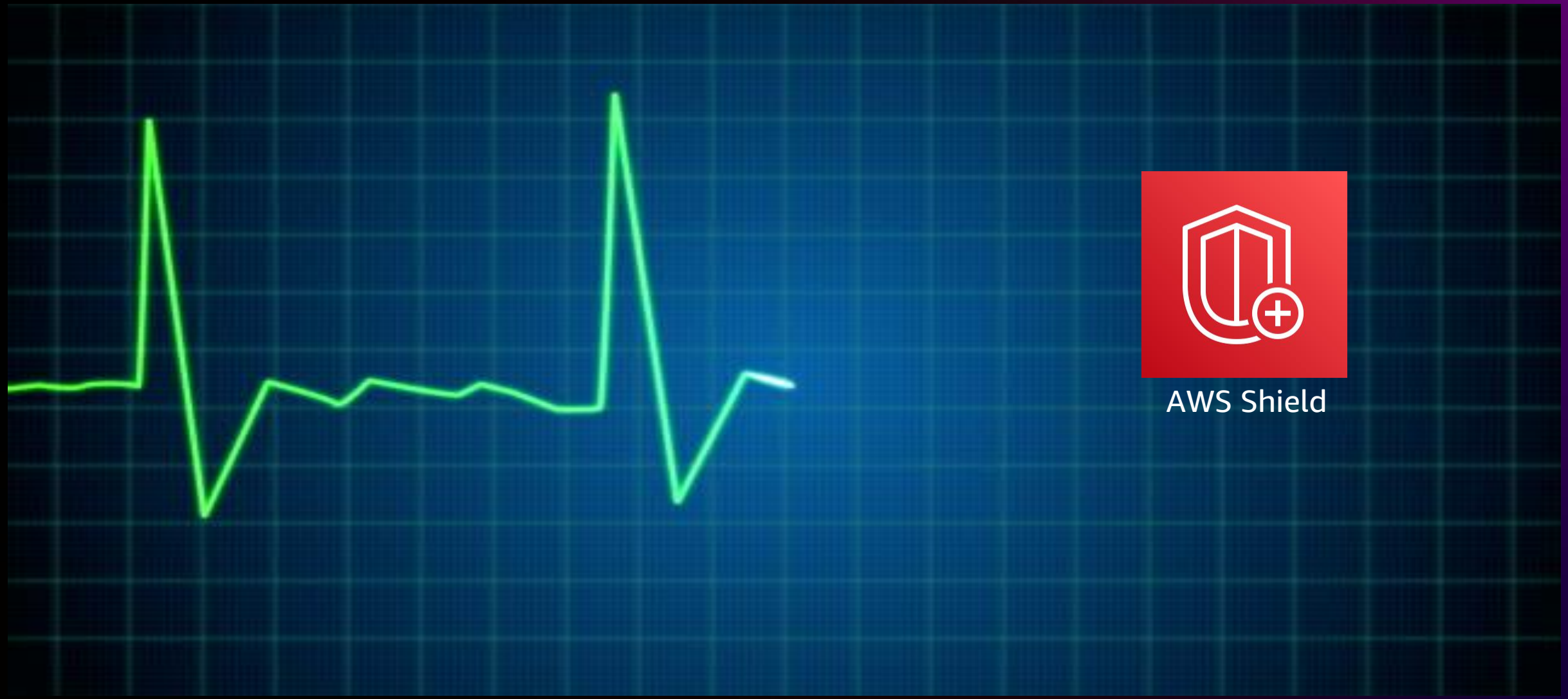
ALLOW | TCP | 80
ALLOW | TCP | 443
DENY | UDP | ALL

DDoS protection: Byte match

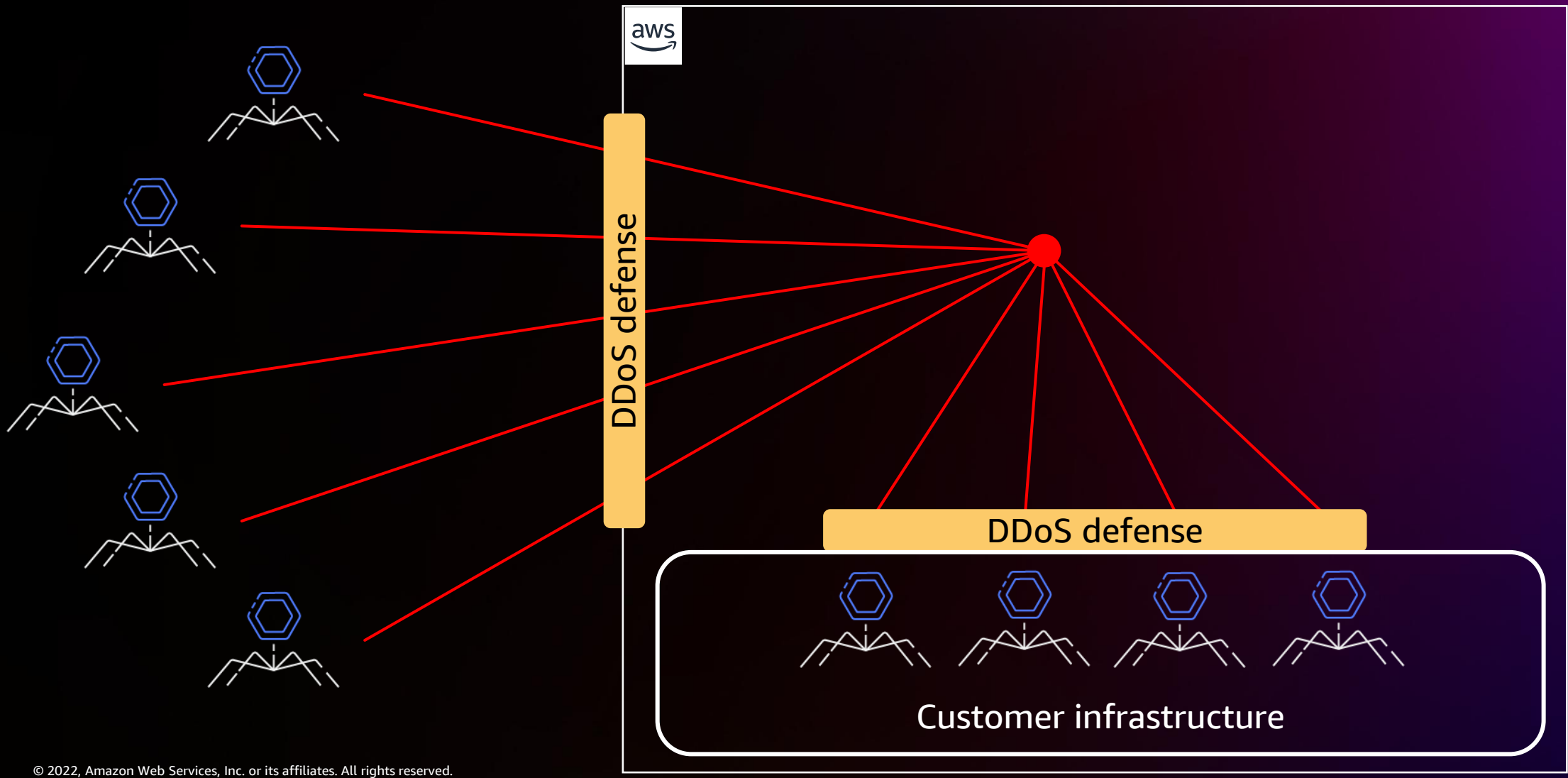
```
0000  5d a2 c8 22 02 00 00 00 ad d3 00 00 23 56 73 25   ].."........#Vs%
0010  fa 61 32 4c 00 00 00 00 f0 d9 49 4e 00 00 00 00   .a2L......IN....
0020  79 61 25 0b 03 00 00 00 7b 61 25 0b 9e 27 00 00   ya%.....{a%..'..
0030  a6 02 00 00 fe ff ff ff 6d 6e 00 00 03 00 70 02   ........mn....p.
0040  a5 02 2f 00 ff ff f9 ff ff c1 3f                  ../.......?
```

AWS Shield

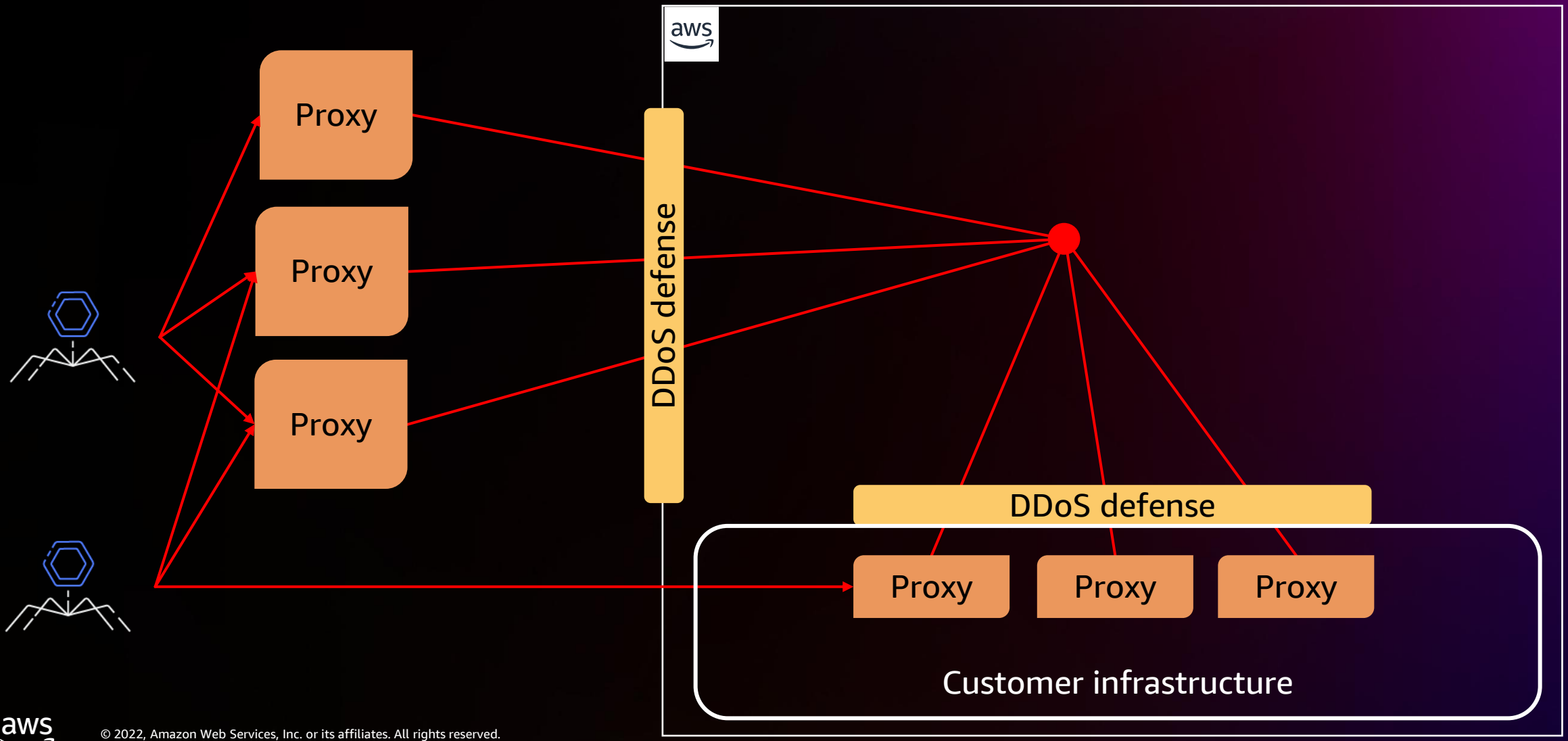
DDoS protection: Health-based detection



DDoS protection: When AWS is the source



DDoS protection: When AWS is the source



Stopping DDoS before the first attack packet

We have a time machine

Intel collected, now protect our customers

1. A suspicious source IP address sending us the exploit attempt
2. The signature of their exploit attempt
3. A suspicious endpoint IP address hosting malware
4. The malware binary itself
5. A treasure map to the command and control (C2) server

Update managed firewall rules

AWS Network Firewall

AWS WAF

Update malware detection signatures

Amazon GuardDuty

Cut out the “brain”

Takedown time

C2 attack commands

C2 endpoint

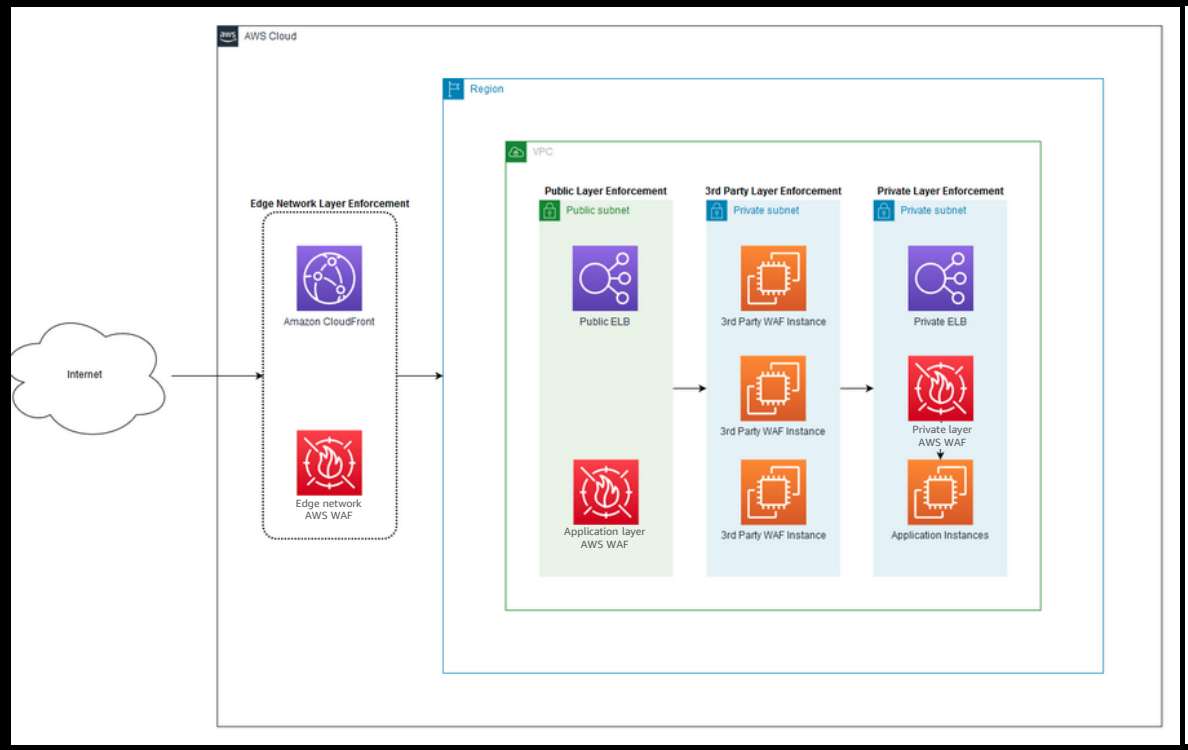
Vector	Target IP and port	Attack parameters
! STOMP	54.38.125.000 30120	100 32 ALL 10 1024
! UDP	70.70.70.000 80 40000	32 0 10
! TCP	45.142.122.000 80	60 32 ACK 0 10
! STD	45.142.122.000 80	60
! HTTP	178.237.56.000 80	10

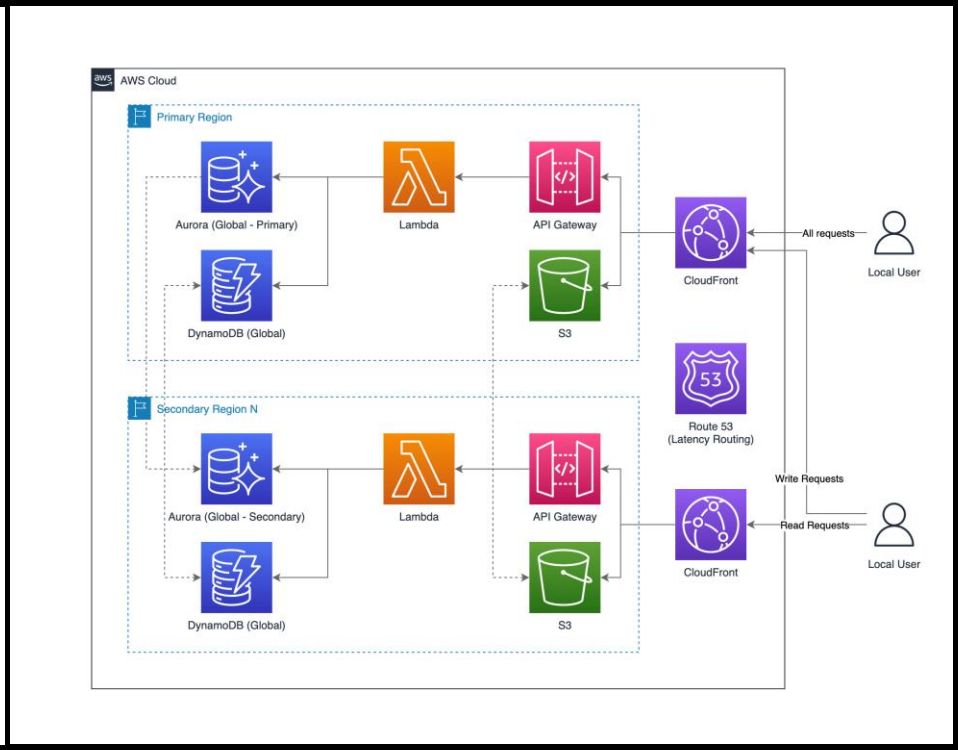
Framework for thinking about DDoS resilience

Framework for thinking about DDoS resilience

Framework for thinking about DDoS resilience

Architect for resilience

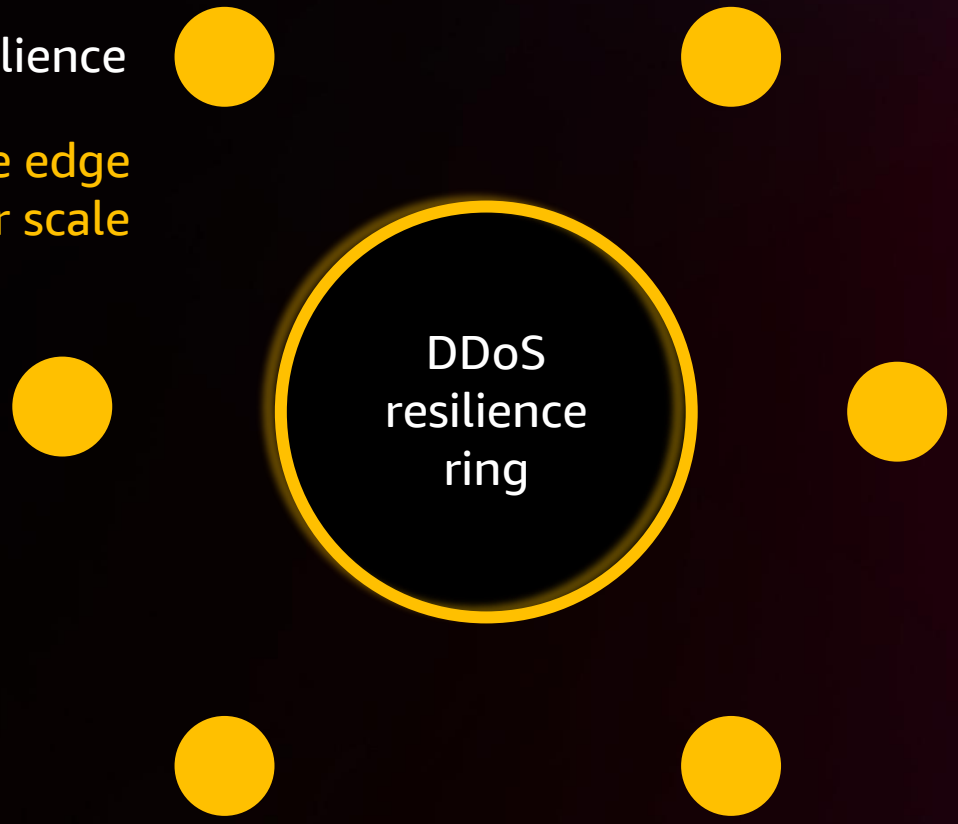




Framework for thinking about DDoS resilience

Architect for resilience

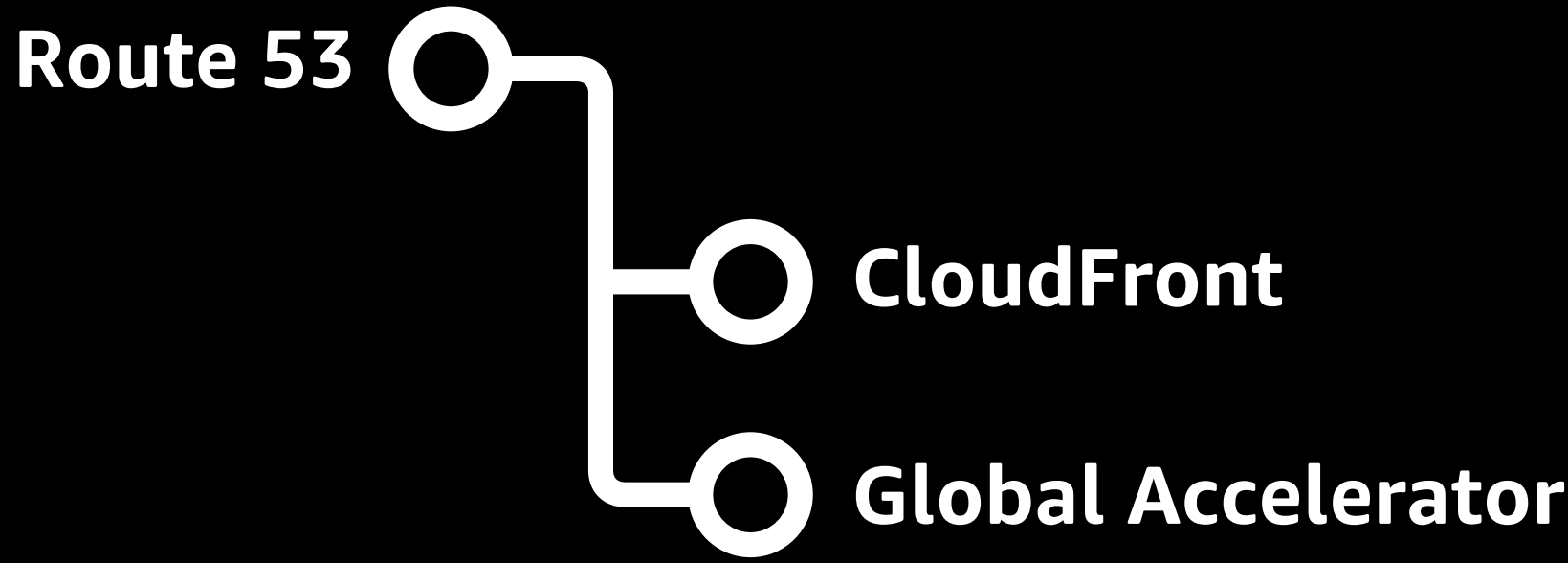
Deploy in multiple AZs; use edge caching and compute for scale



Framework for thinking about DDoS resilience

Distributed network capacity

Use edge services



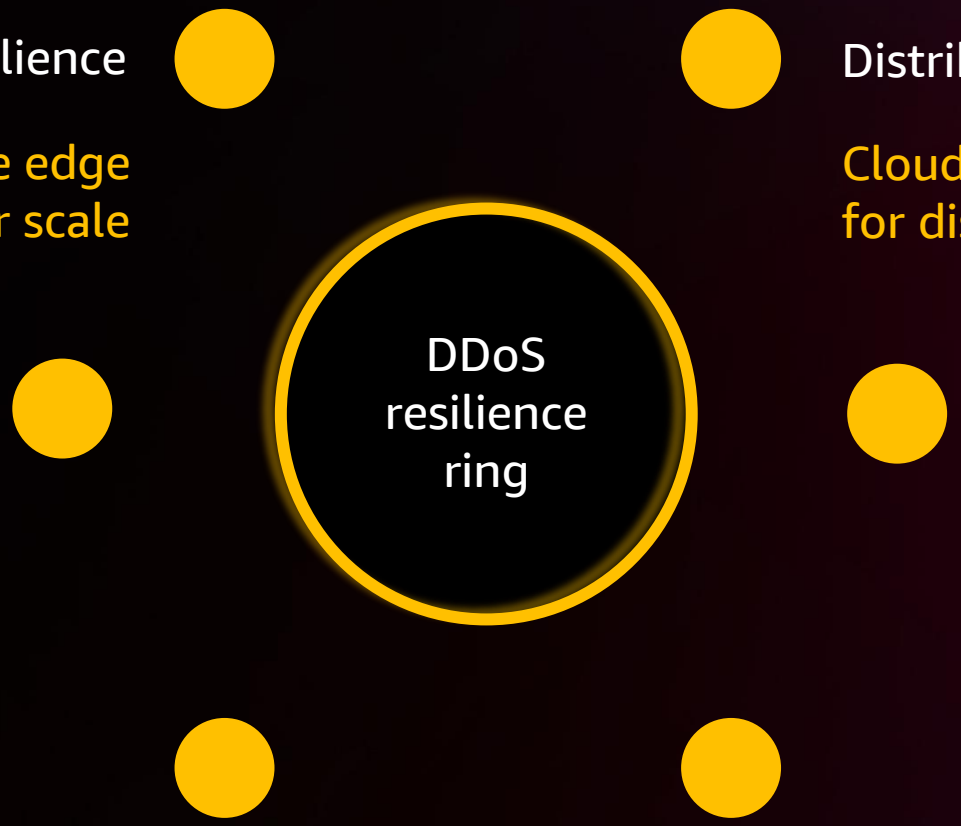
Framework for thinking about DDoS resilience

Architect for resilience

Deploy in multiple AZs; use edge caching and compute for scale

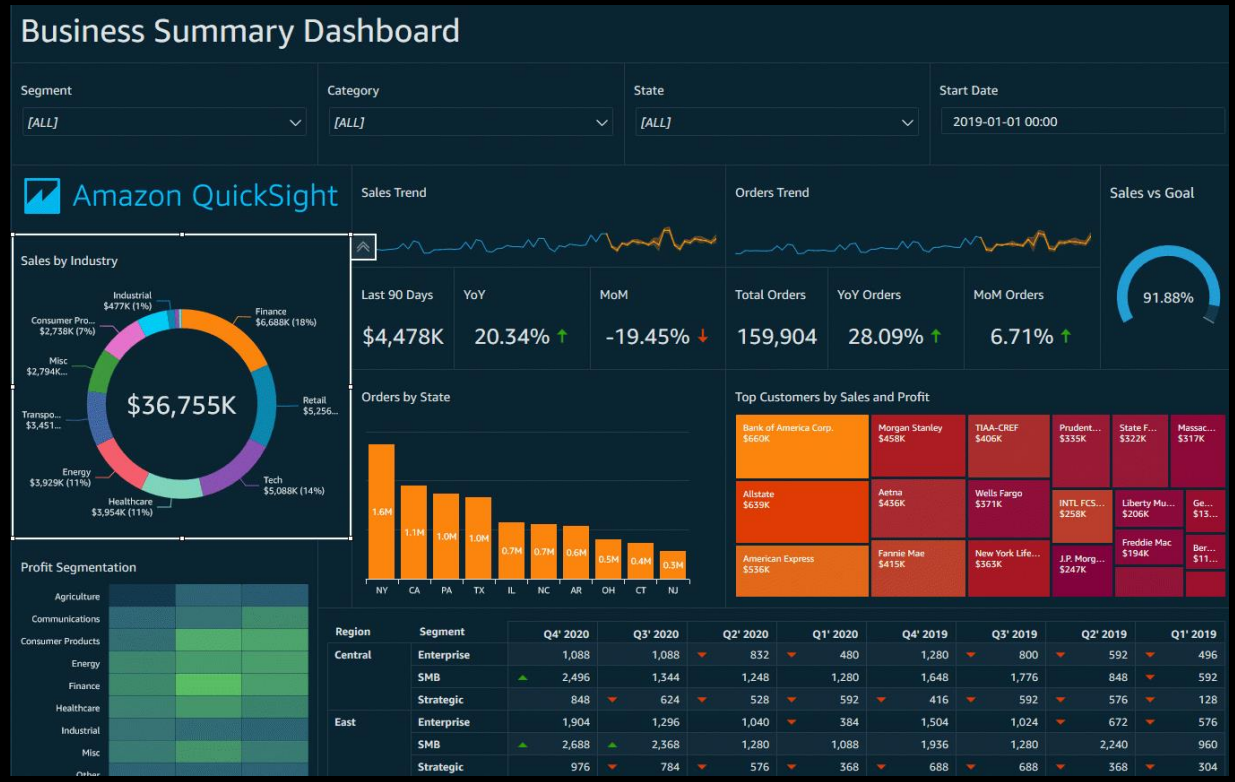
Distributed network capacity

CloudFront or Global Accelerator for distributed networking ingress



Framework for thinking about DDoS resilience

Actively monitor



Framework for thinking about DDoS resilience

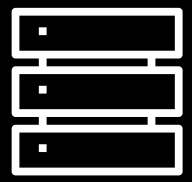
Framework for thinking about DDoS resilience

Scalable applications

Elastic Load Balancing (ELB)

Amazon EC2 Auto Scaling

Amazon DynamoDB



Scale the whole stack

Framework for thinking about DDoS resilience

Architect for resilience

Deploy in multiple AZs; use edge caching and compute for scale

Distributed network capacity

CloudFront or Global Accelerator for distributed networking ingress

Actively monitor

Monitor metrics and alarms for impact; know which resources are impacted

Scalable applications

ELB scales in front of application servers; auto scaling for EC2 instances

Framework for thinking about DDoS resilience

Define your security model

Amazon VPC

Network access control list

AWS WAF

Rule

Managed rule

Filtering rule

Labels

Bot control

Bot

Bad bot

AWS Network Firewall

Endpoints

AWS Firewall Manager

Framework for thinking about DDoS resilience

Architect for resilience

Deploy in multiple AZs; use edge caching and compute for scale

Distributed network capacity

CloudFront or Global Accelerator for distributed networking ingress

Actively monitor

Monitor metrics and alarms for impact; know which resources are impacted

Scalable applications

ELB scales in front of application servers; auto scaling for EC2 instances

Define your security model

Configure static and managed firewall rules to allow only wanted traffic

Framework for thinking about DDoS resilience

Collaborate with AWS on security

AWS Shield

Health-based detections

Proactive response

Advanced mitigations

Framework for thinking about DDoS resilience

Architect for resilience

Deploy in multiple AZs; use edge caching and compute for scale

Distributed network capacity

CloudFront or Global Accelerator for distributed networking ingress

Actively monitor

Monitor metrics and alarms for impact; know which resources are impacted

Scalable applications

ELB scales in front of application servers; auto scaling for EC2 instances

Define your security model

Configure static and managed firewall rules to allow only wanted traffic

Collaborate with AWS on security

Configure health checks; provide contact details for a proactive response

Thank you!

Oliver Sturrock
ossturro@amazon.com

Paul Bodmer
bodmerpb@amazon.com

Please complete the session survey in the **mobile app**