Cloud Services I
Networking II

AWS Cloud Practitioner Essentials (Second Edition): AWS Networking Services

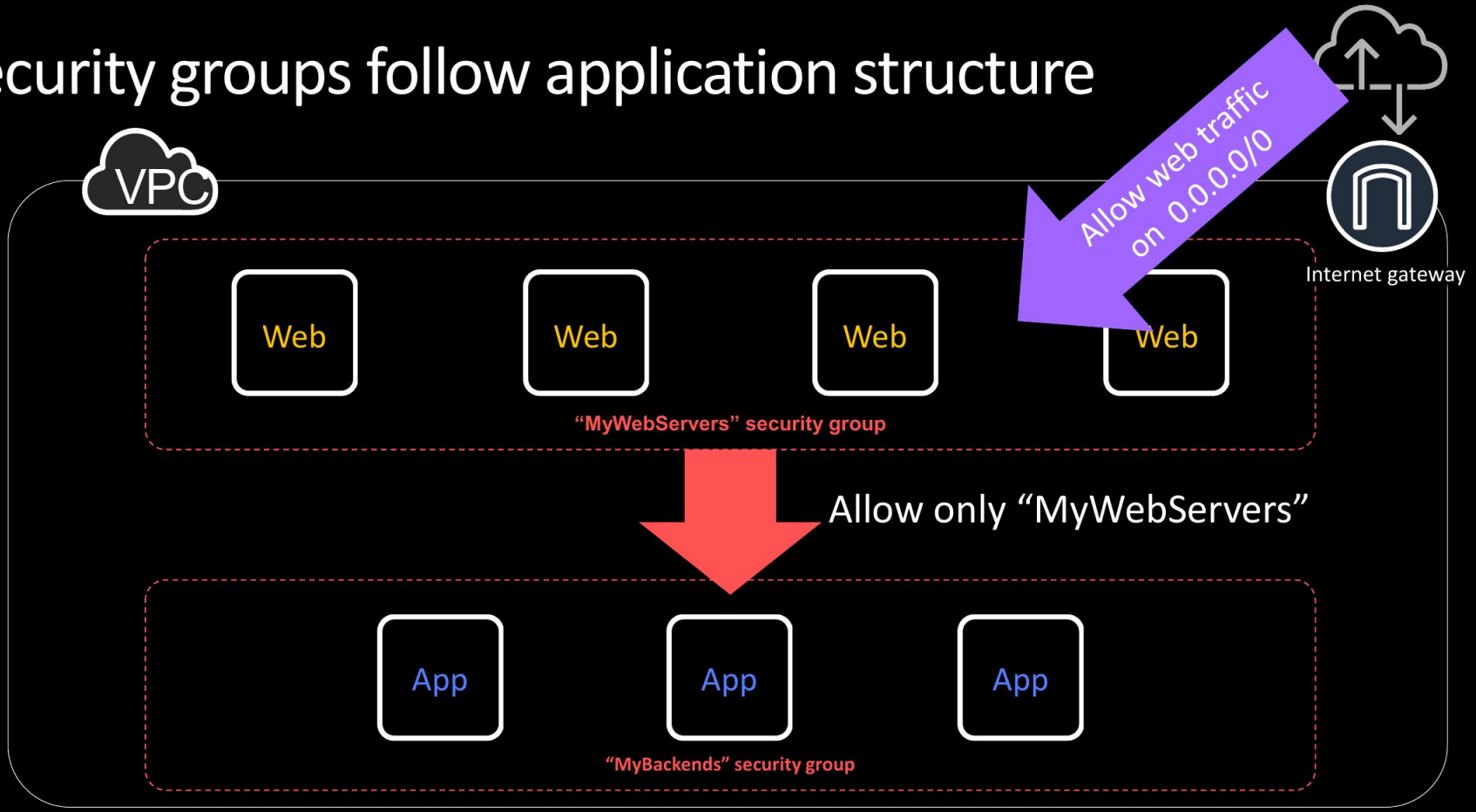
Security groups

Network access control list

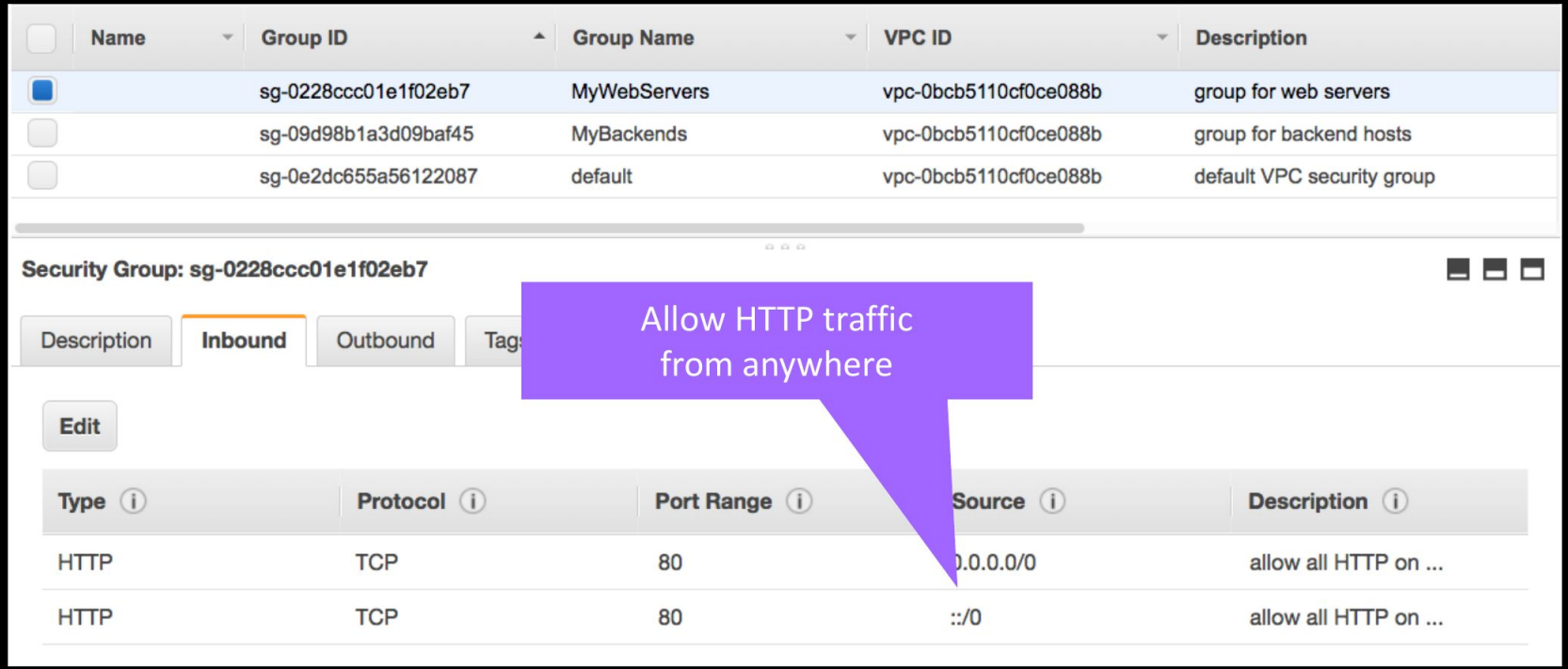
Flow logs

Network security

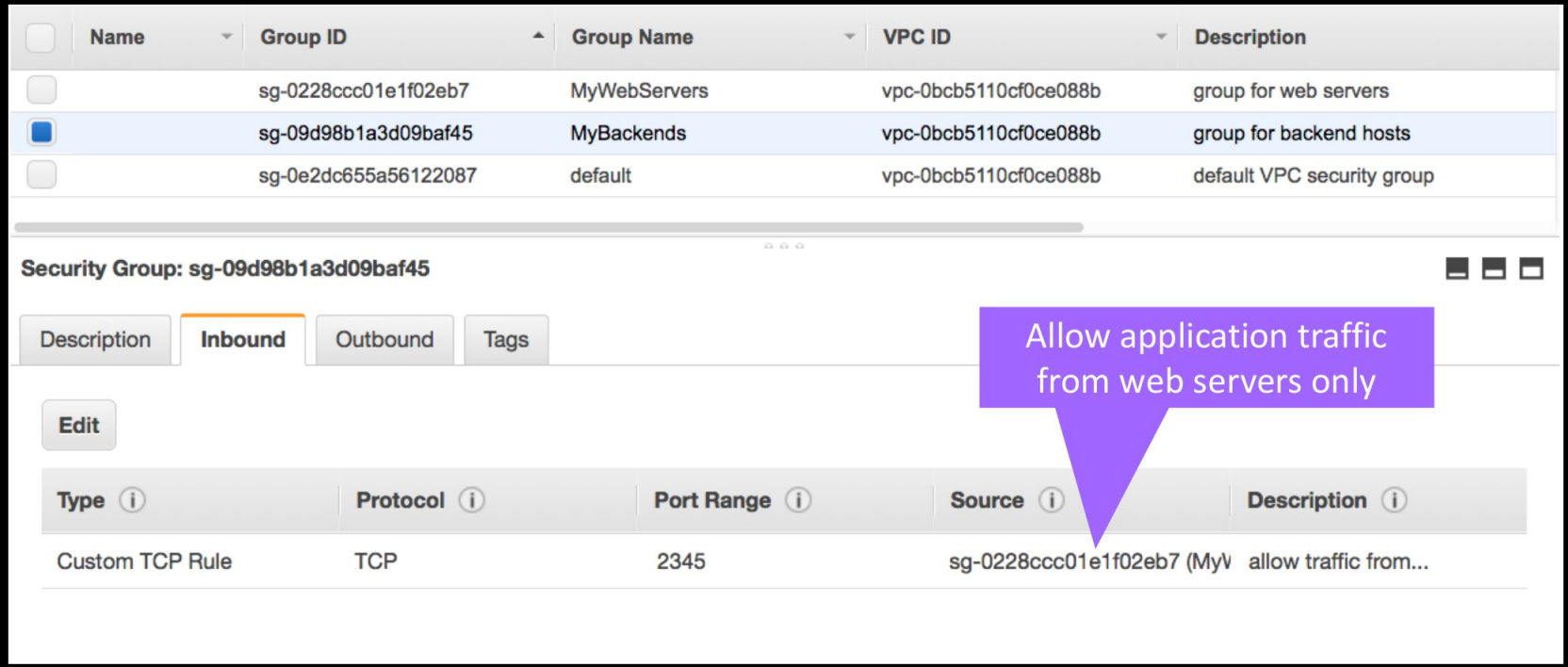
Security groups follow application structure



Security groups example: Web servers



Security groups example: Backends



Security groups

Network access control list

Flow logs

Network security

Security groups vs. NACLs

Security group	Network ACL
Operates at instance level	Operates at subnet level
Supports allow rules only	Supports allow and deny rules
Is stateful: return traffic is automatically allowed regardless of any rules	Is stateless: return traffic must be explicitly allowed by rules
All rules evaluated before deciding whether to allow traffic	Rules evaluated in order when deciding whether to allow traffic
Applies only to instances explicitly associated with the security group	Automatically applies to all instances launched into associated subnets
Doesn’t filter traffic to or from link-local addresses (169.254.0.0/16) or AWS-reserved IPv4 addresses; these are the first four IPv4 addresses of the subnet (including the Amazon VPC DNS server)	

Security groups

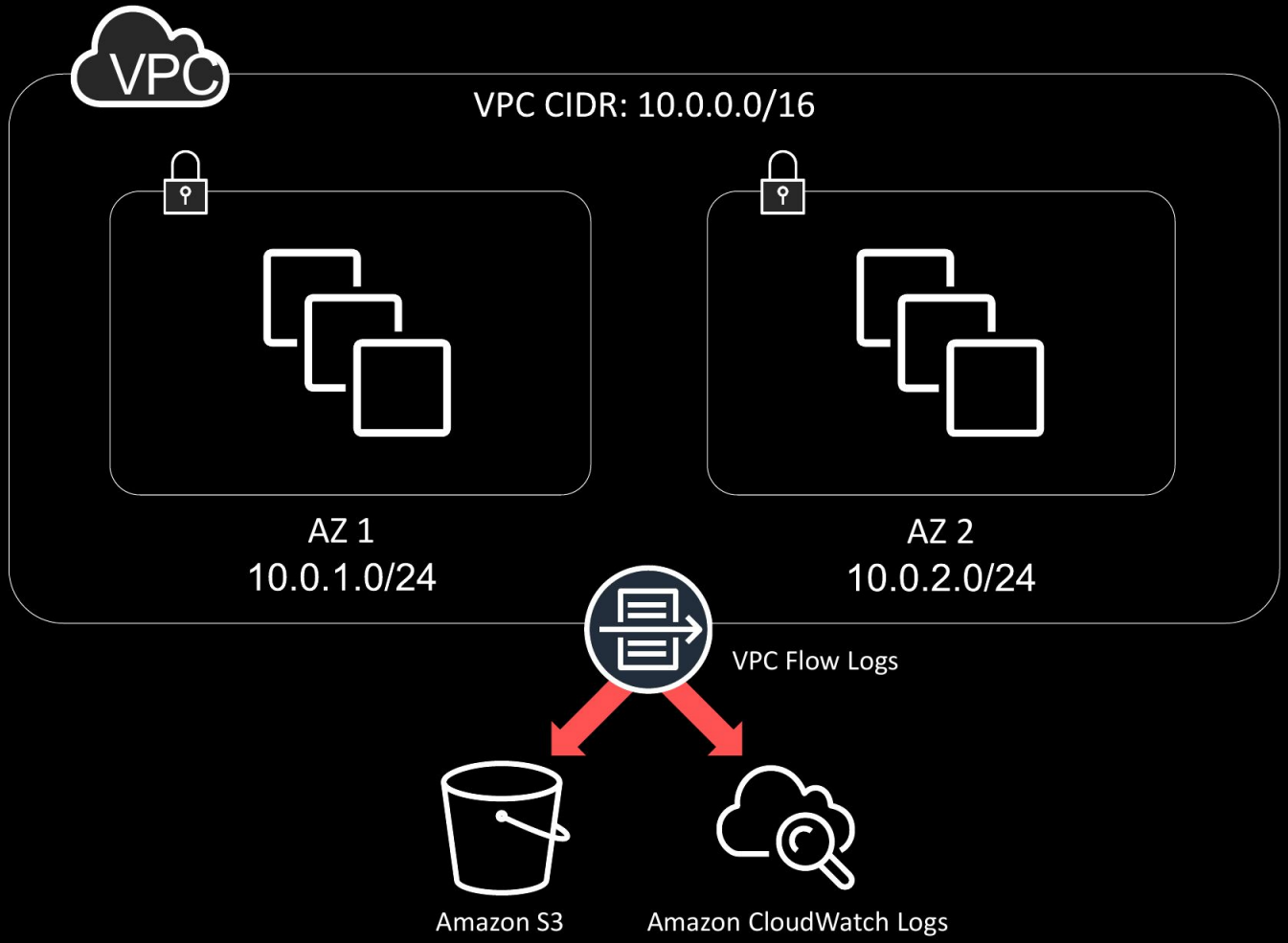
Network access control list

Flow logs

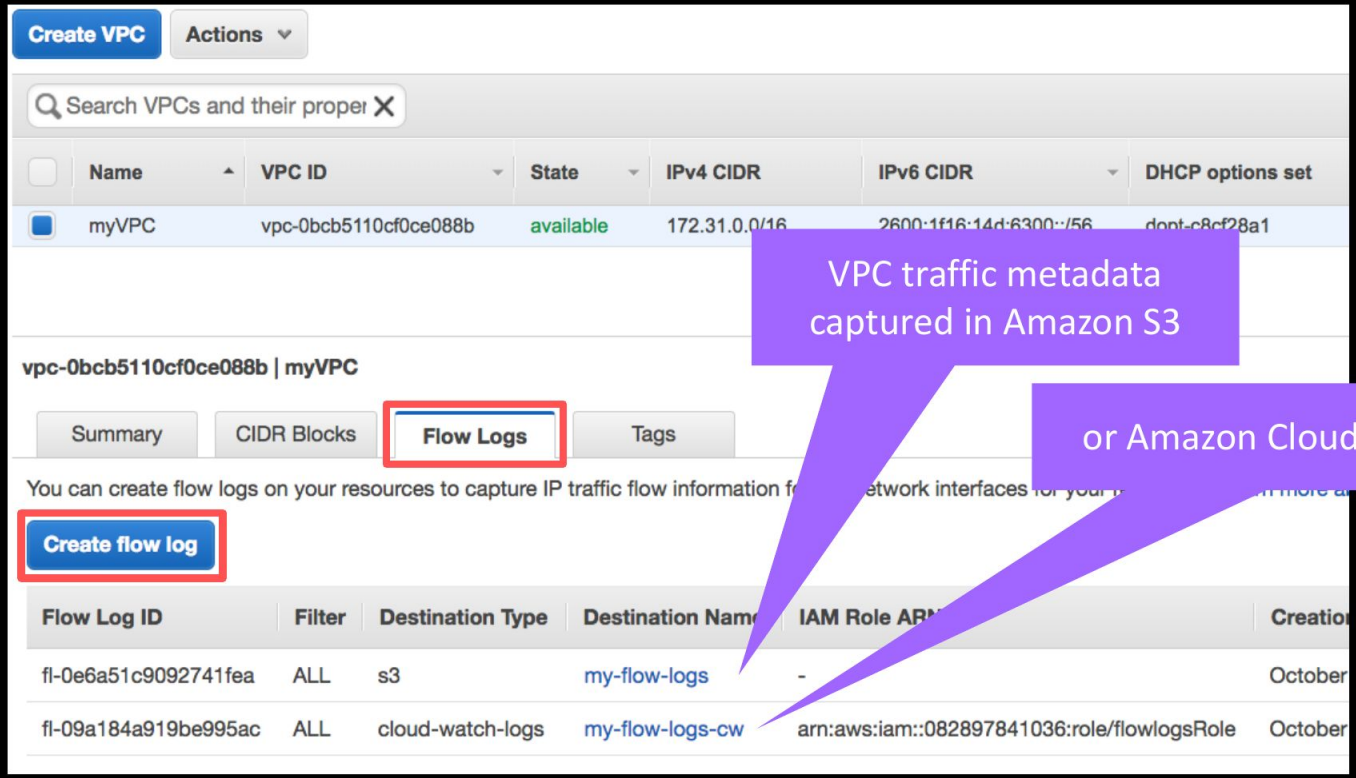
Network security

VPC Flow Logs

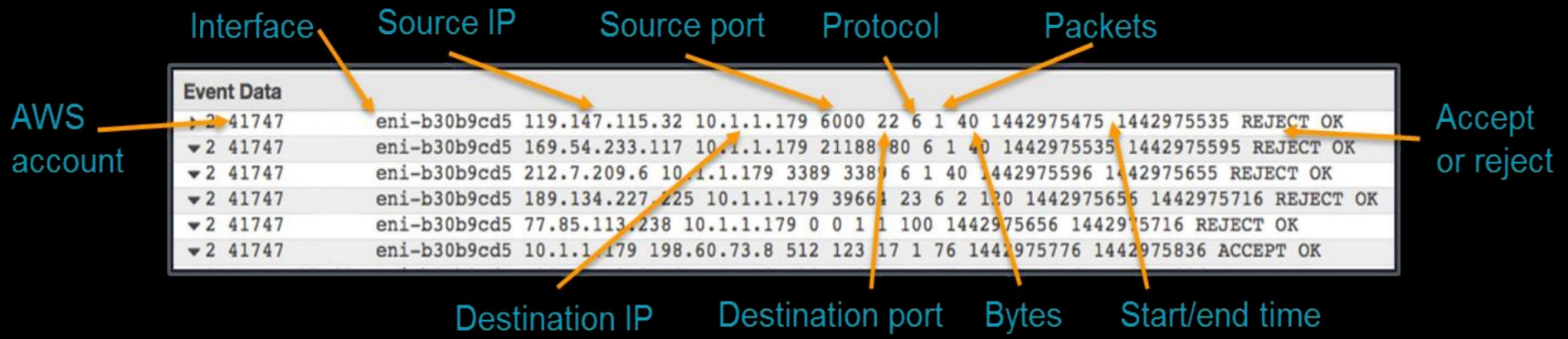
- Visibility
- Troubleshooting
- Analyze traffic



VPC Flow Logs: Setup



VPC Flow Logs format



The Elastic Load Balancing Family

Application Load Balancer

HTTP & HTTPS (VPC)

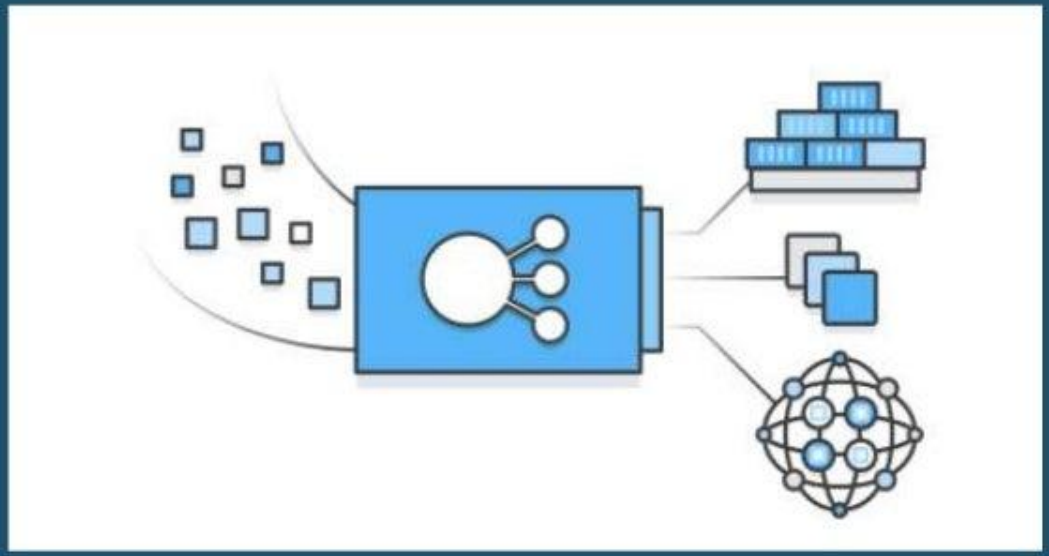
Network Load Balancer

TCP Workloads (VPC)

Classic Load Balancer

Previous Generation
for HTTP, HTTPS, TCP
(Classic Network)

aws



Application Load Balancer

Advanced request routing with support for microservices and container-based applications.

aws

Application Load Balancer

New, feature rich, layer 7 load-balanced platform

Content-based routing allows requests to be routed to different applications behind a single load balancer

Support for microservices and container-based applications, including deep integration with Elastic Container Service

aws

Application Load Balancer

Support for WebSockets and HTTP/2

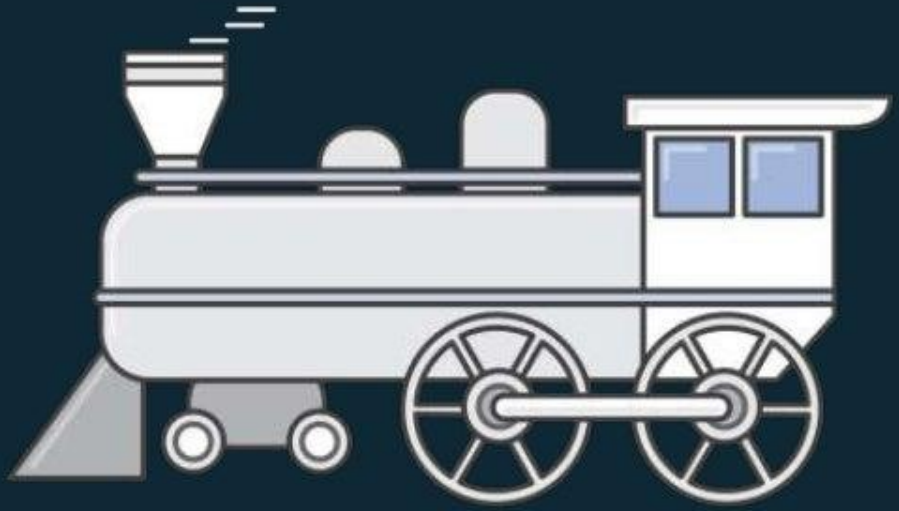
Path and Host Based Routing

Improved health checks and additional CloudWatch metrics

Improved performance for real-time and streaming applications

Improved Elastic Load Balancing API

Load balancer API deletion protection



aws

Listeners

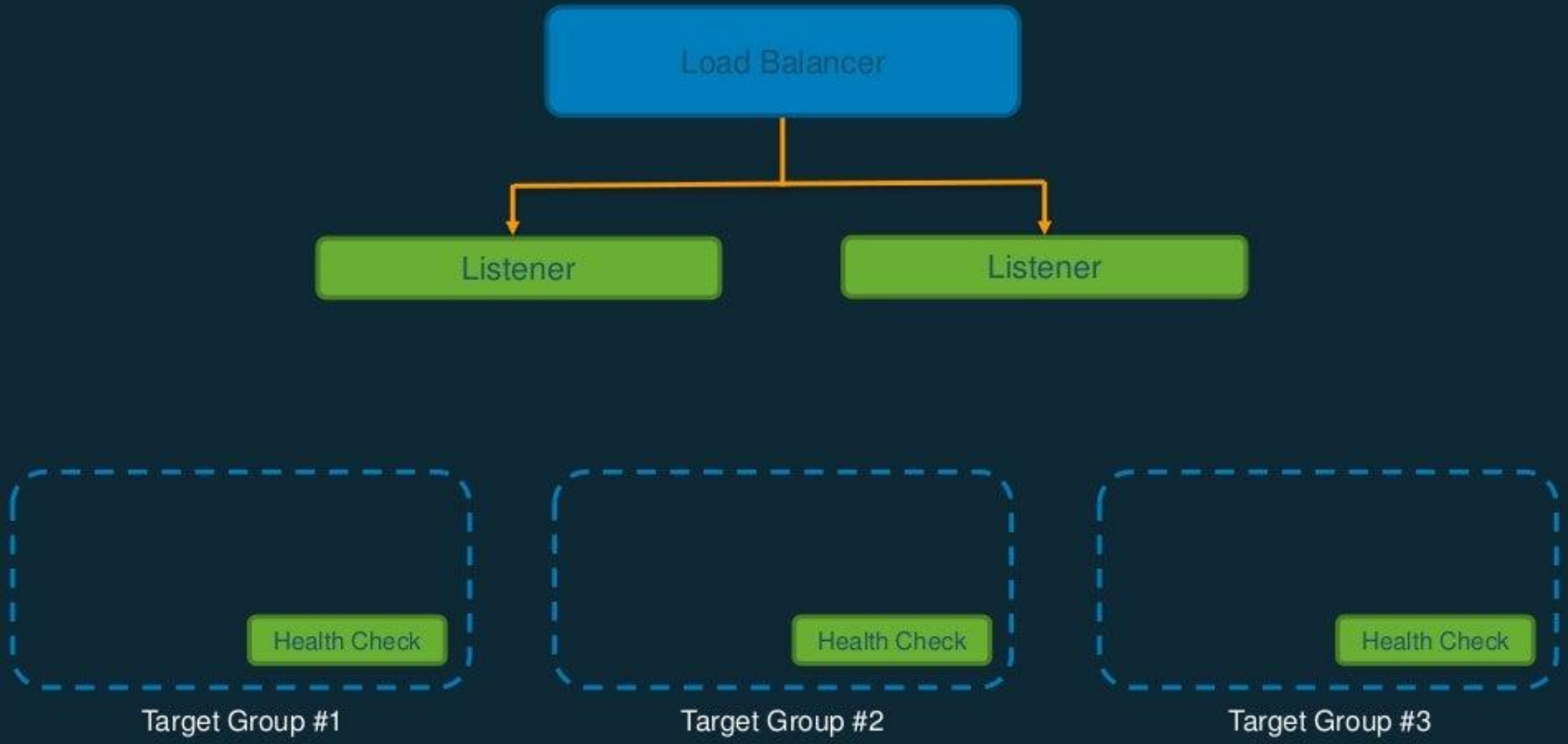
Define the port and protocol which the load balancer must listen on

Each Application Load Balancer needs at least one listener to accept traffic

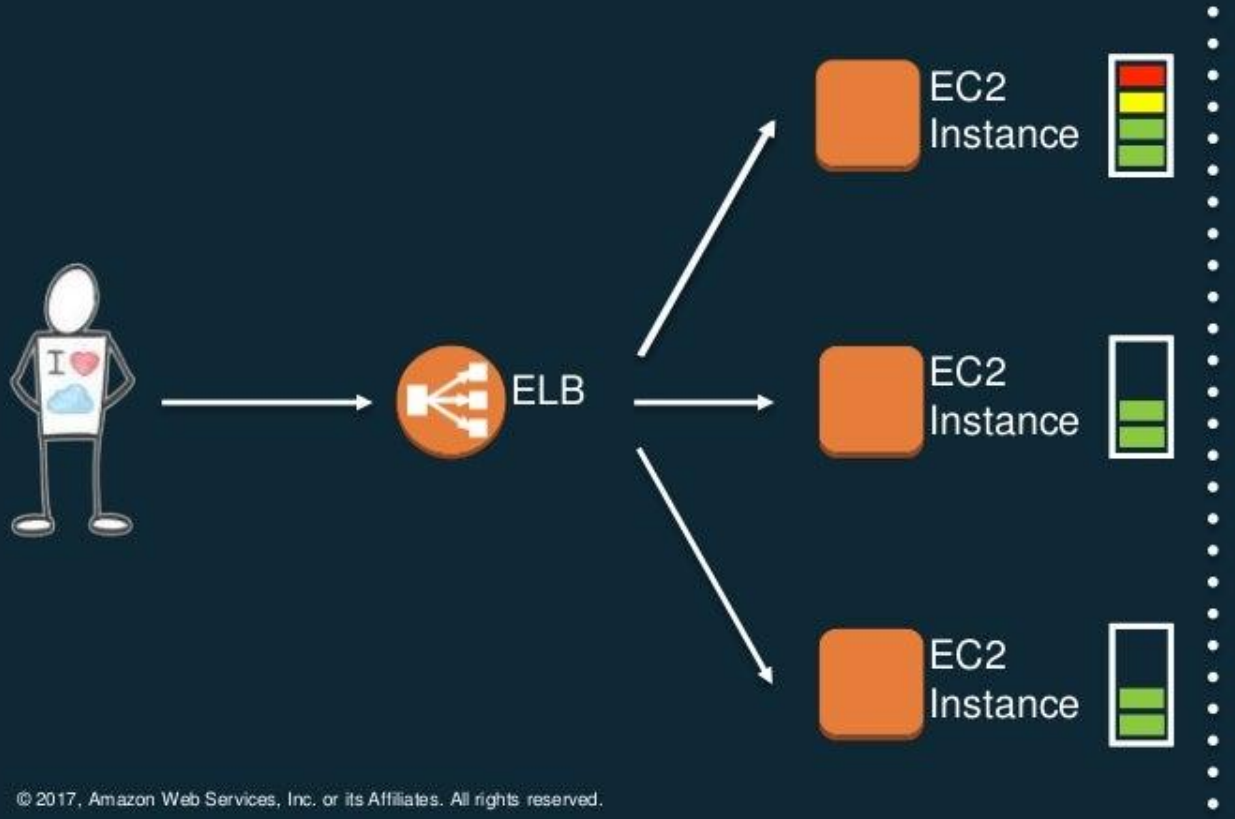
Each Application Load Balancer can have up to 50 listeners

Routing rules are defined on listeners

aws



Health checks



Health checks ensure that request traffic is shifted away from a failed instance.

aws

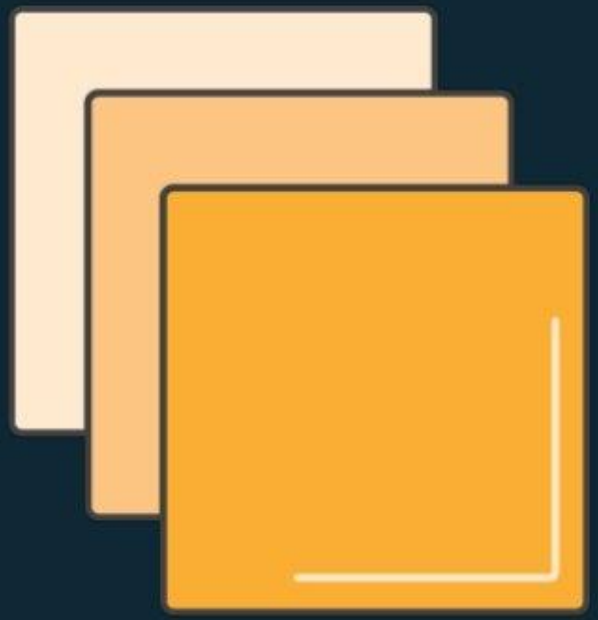
Target groups

Logical grouping of targets behind the load balancer

Target groups can exist independently from the load balancer

Regional construct that can be associated with an Auto Scaling group

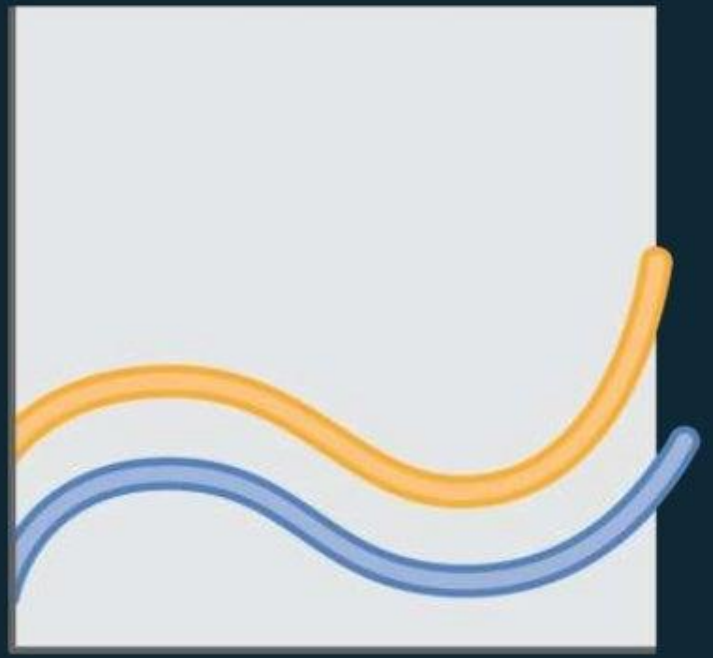
Target groups can contain up to 1,000 targets



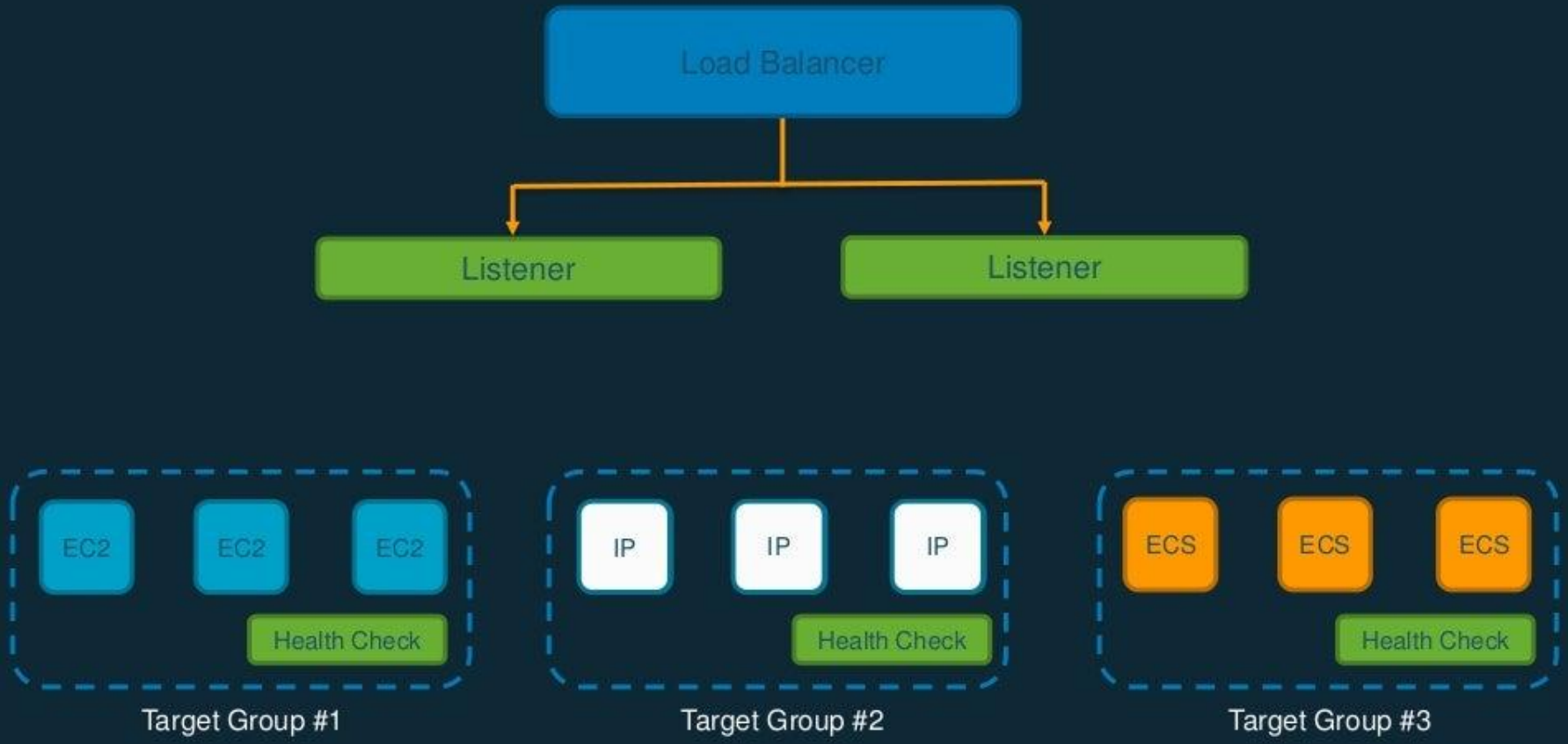
Auto Scaling integration

Auto Scaling can now scale targets within a target group

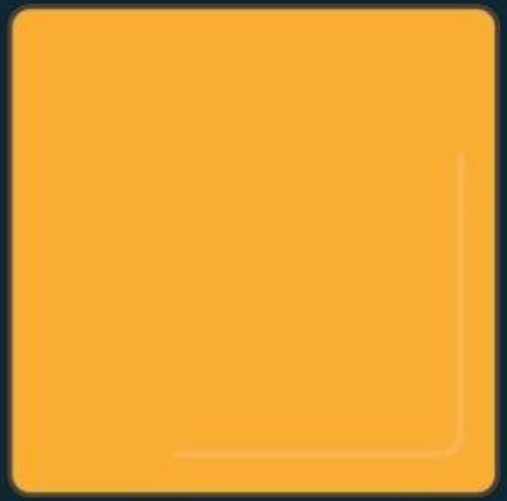
Allows for applications to be scaled independently behind the Application Load Balancer



aws



Targets



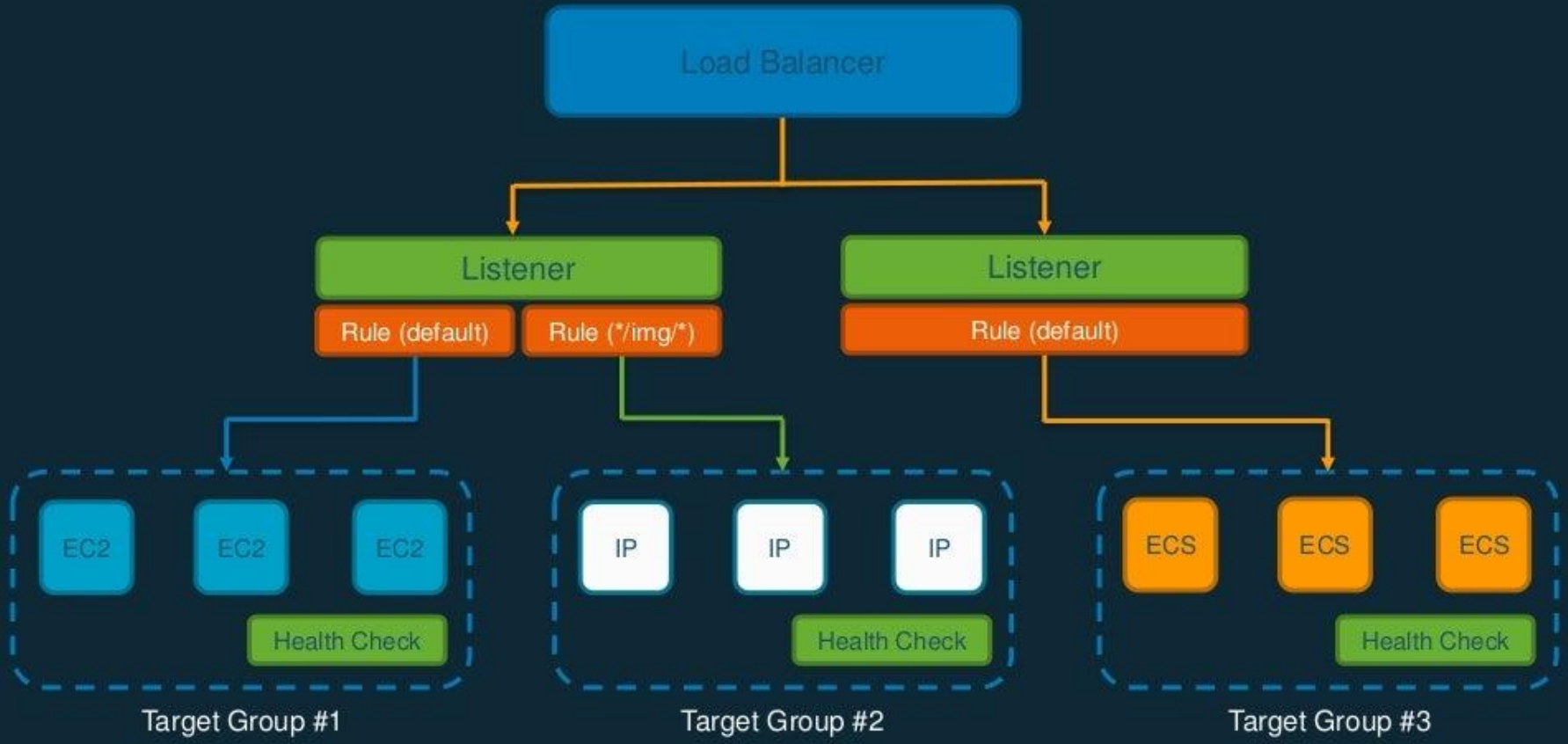
Support for EC2 instances and ECS containers, and IP Addresses.

EC2 instances can be registered with the same target group using multiple ports

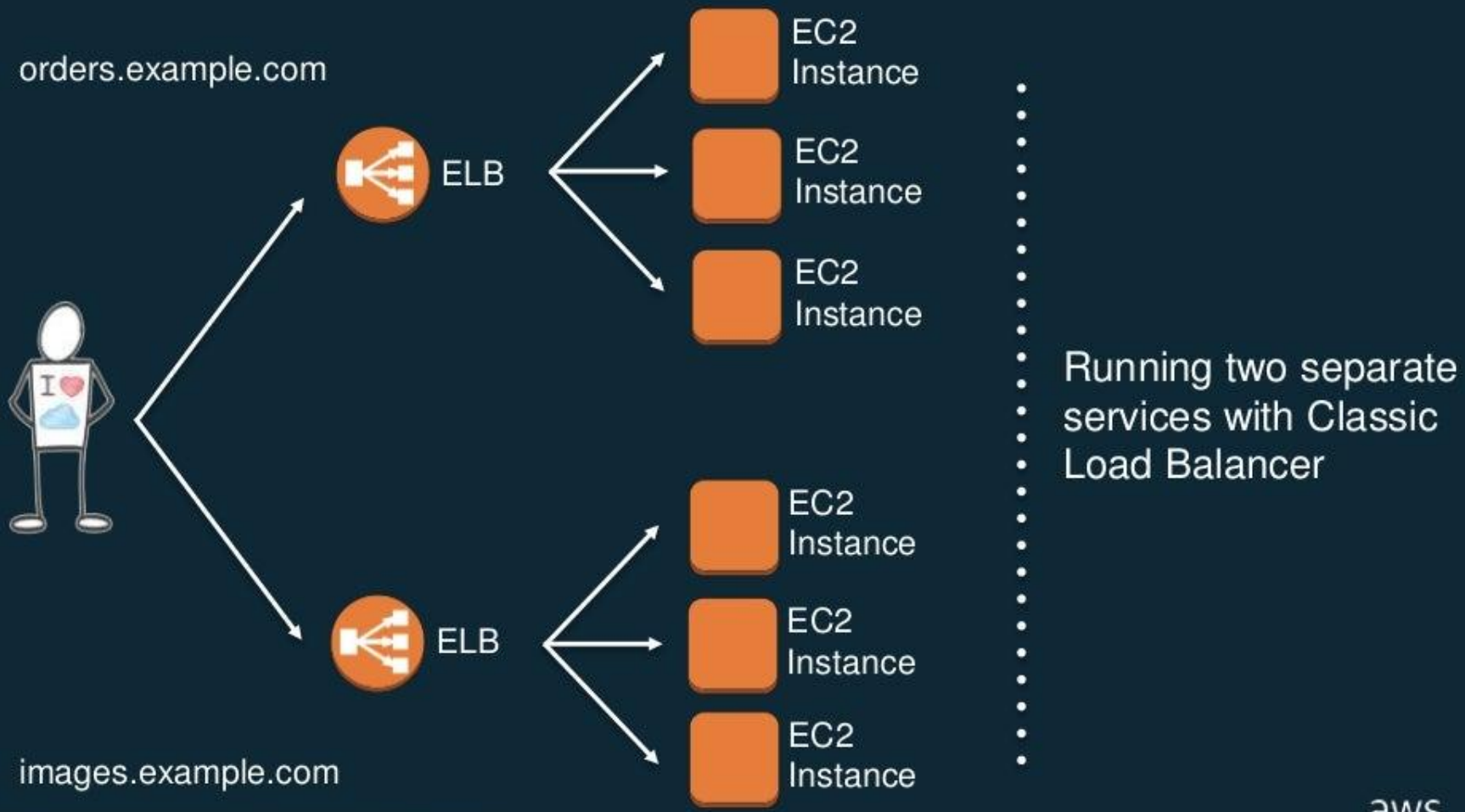
A single target can be registered with multiple target groups

IP Addresses both accessible within your VPC or via DX and VPN

aws

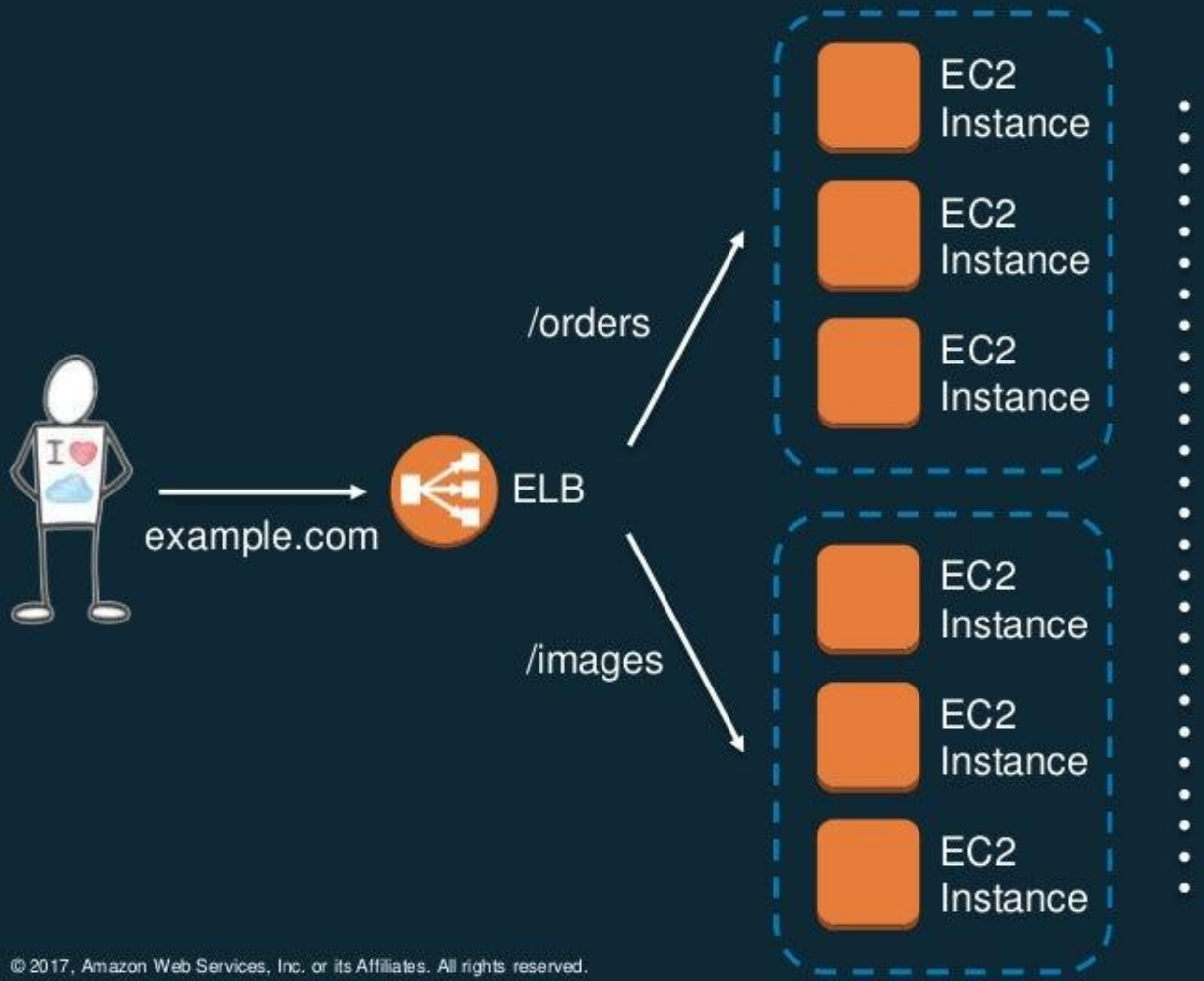


aws



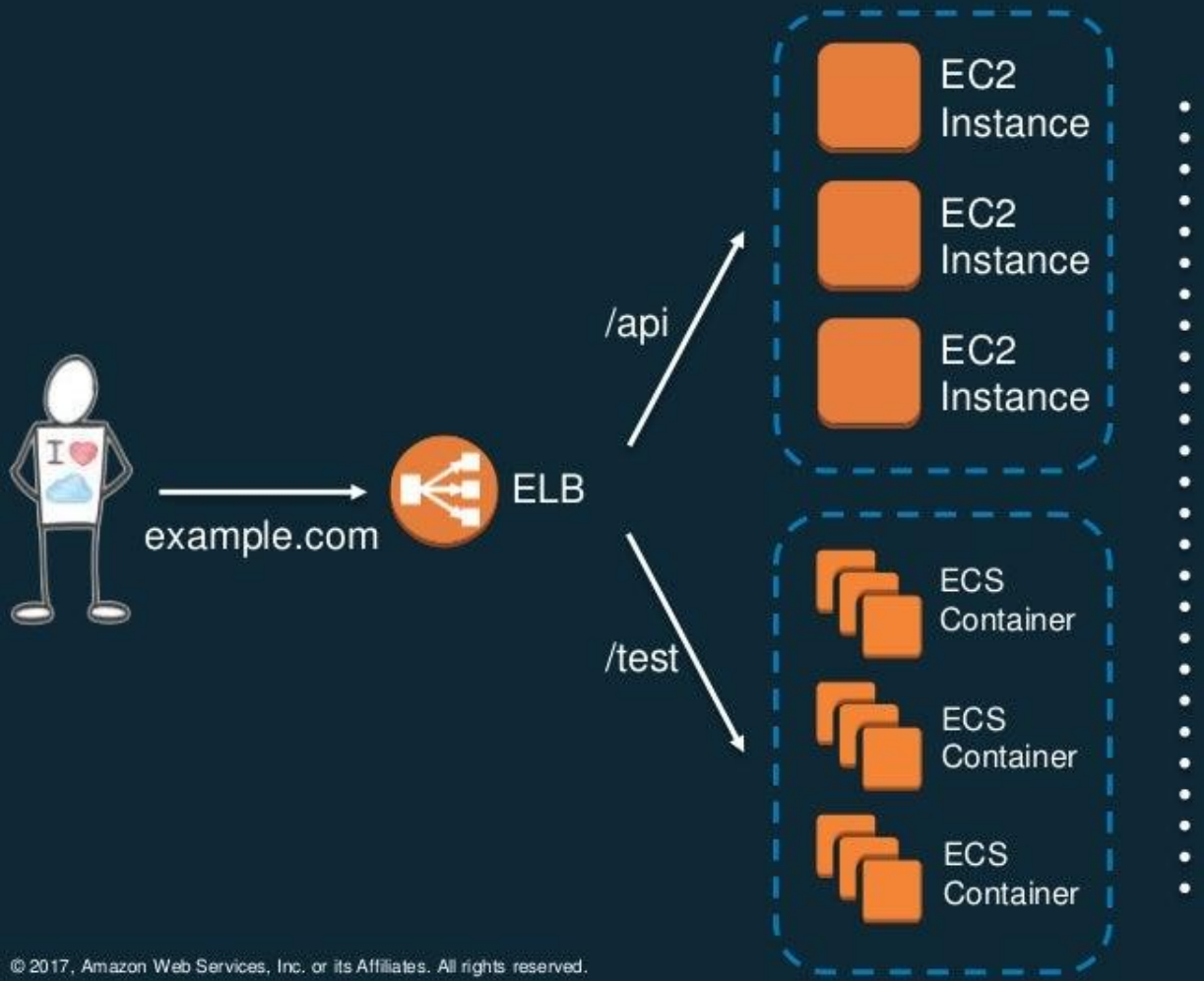
Running two separate services with Classic Load Balancer

aws



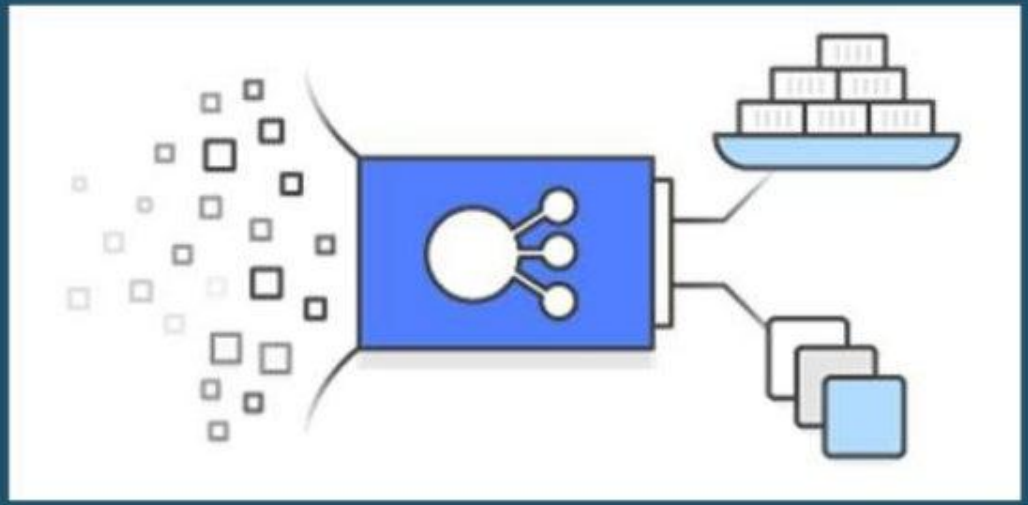
Application Load Balancer allows for multiple services to be hosted behind a single load balancer

aws



Application Load Balancer allows containers to be included in the target group

aws



Network Load Balancer

aws

Network Load Balancer

New, layer 4 load-balancing platform
- Connection-based load balancing
- TCP protocol

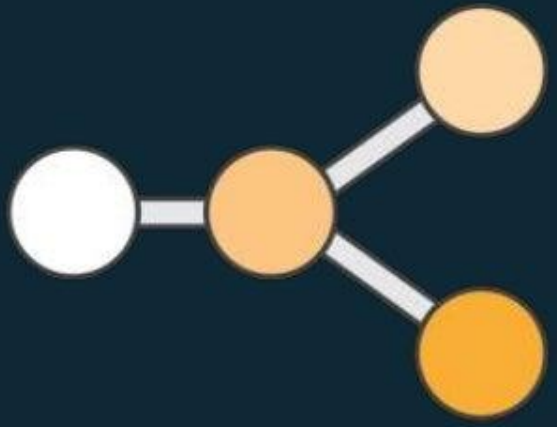
High Performance
- Can handle millions of requests per sec

Static IP Support

Ideal for applications with long running connections

aws

Static IP



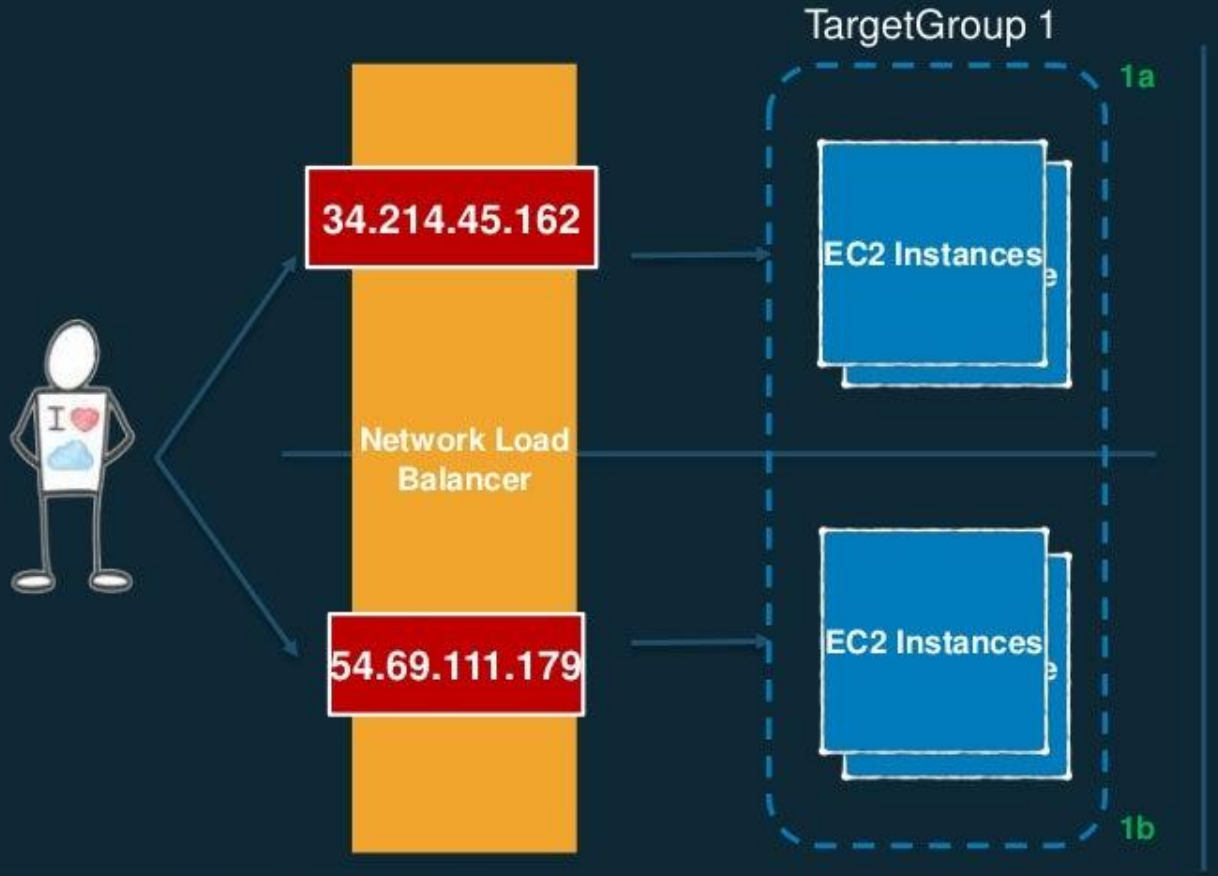
Automatically gets assigned a single IP per Availability Zone

Assign an EIP per AZ to get Static IP

Helps with white-listing for firewalls and zero dollar billing use cases

aws

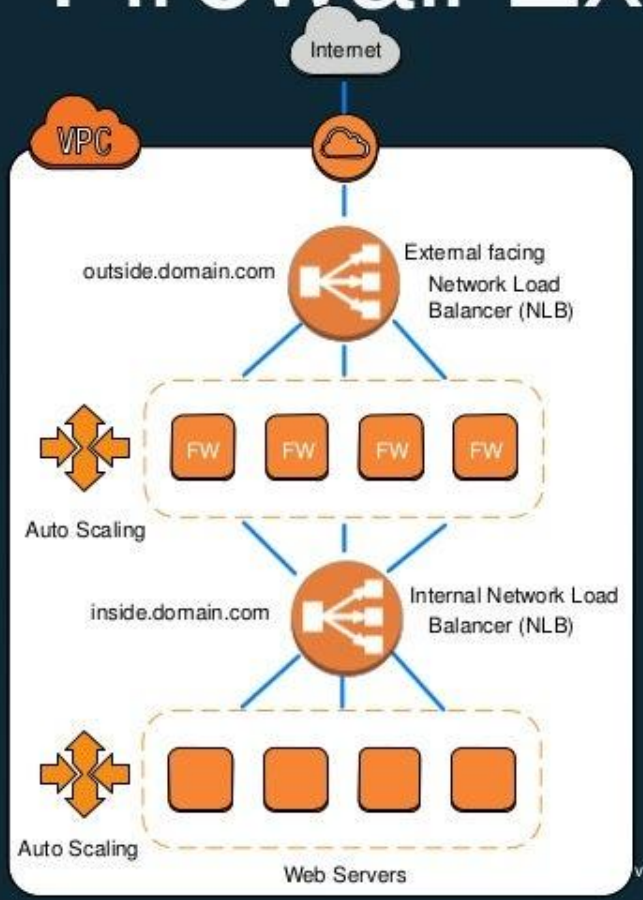
Assign Elastic IP Addresses



Assigning Elastic IP provides a single IP address per Availability Zone per load balancer that will not change.

aws

Firewall Example with NLB



External facing NLB uses less addresses
- Used for Firewalls, proxies or 3rd party load balancers

Preserves source IP helping firewalls with features like Geo-IP blocking

Internal NLB doesn't change IPs
- Allows Firewalls, WAFs and proxies to maintain a single addresses for NAT

aws

	Application Load Balancer	Network Load Balancer	Classic Load Balancer
Protocol	HTTP, HTTPS,HTTP/2	TCP	TCP, SSL, HTTP, HTTPS
SSL offloading	✓		✓
IP as Target	✓	✓	
Path-based routing, Host-based routing	✓		
Static IP		✓	
WebSockets	✓	✓	
Container Support	✓	✓	

aws

Networking II labs

PXL DIGITAL

- Online lab platform
  - AWSGen (networking lab part 2)
  - Configure a NACL for AWS VPC
  - Configure VPC Flow logs to CloudWatch logs groups
  - Build an Amazon EC2 Auto Scalin group with Load balancing
  - Create an Application load balancer with an HTTP Listener