

# Cloud Services I

## Networking II





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



Security groups



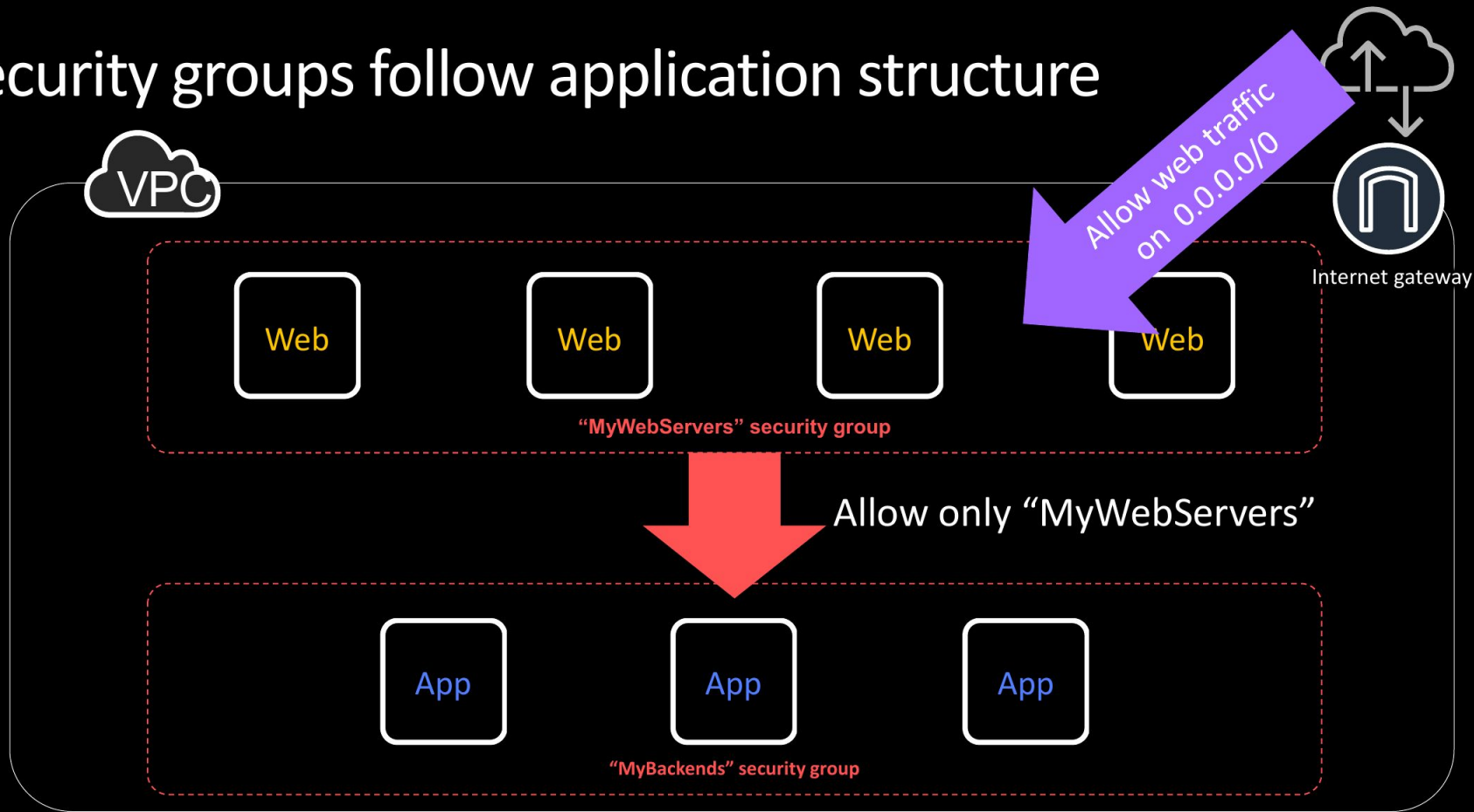
Network access  
control list



Flow logs

# Network security

# Security groups follow application structure



# Security groups example: Web servers

<input type="checkbox"/>	Name	Group ID	Group Name	VPC ID	Description
<input checked="" type="checkbox"/>		sg-0228ccc01e1f02eb7	MyWebServers	vpc-0bcb5110cf0ce088b	group for web servers
<input type="checkbox"/>		sg-09d98b1a3d09baf45	MyBackends	vpc-0bcb5110cf0ce088b	group for backend hosts
<input type="checkbox"/>		sg-0e2dc655a56122087	default	vpc-0bcb5110cf0ce088b	default VPC security group

Security Group: sg-0228ccc01e1f02eb7

Description Inbound Outbound Tags

Edit

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	allow all HTTP on ...
HTTP	TCP	80	:::0	allow all HTTP on ...

Allow HTTP traffic from anywhere

# Security groups example: Backends

<input type="checkbox"/>	Name	Group ID	Group Name	VPC ID	Description
<input type="checkbox"/>		sg-0228ccc01e1f02eb7	MyWebServers	vpc-0bcb5110cf0ce088b	group for web servers
<input checked="" type="checkbox"/>		sg-09d98b1a3d09baf45	MyBackends	vpc-0bcb5110cf0ce088b	group for backend hosts
<input type="checkbox"/>		sg-0e2dc655a56122087	default	vpc-0bcb5110cf0ce088b	default VPC security group

Security Group: sg-09d98b1a3d09baf45

Description Inbound Outbound Tags

Edit

Type	Protocol	Port Range	Source	Description
Custom TCP Rule	TCP	2345	sg-0228ccc01e1f02eb7 (MyV	allow traffic from...

Allow application traffic from web servers only



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

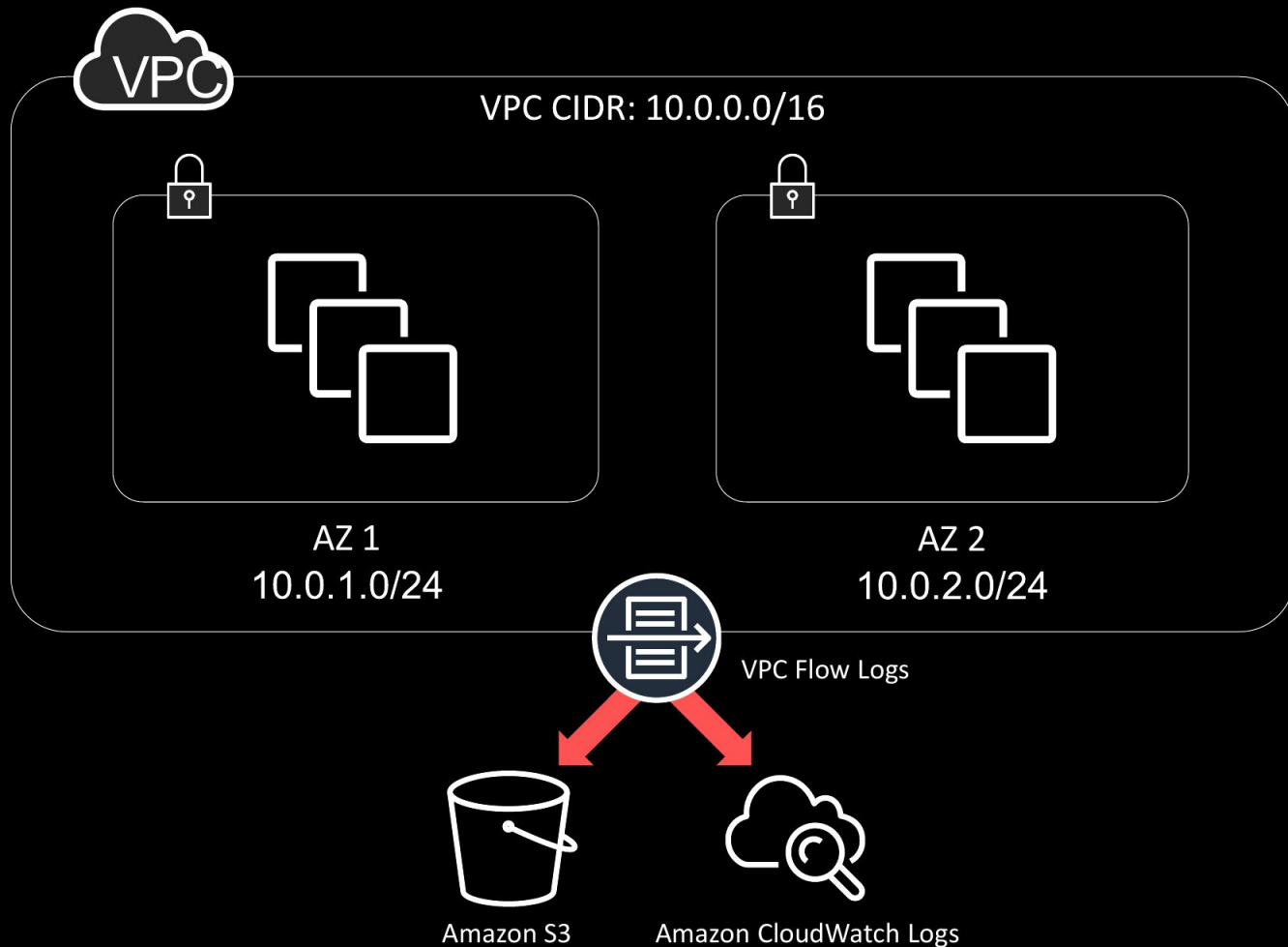


Flow logs

# Network security

# VPC Flow Logs

- Visibility
- Troubleshooting
- Analyze traffic



# VPC Flow Logs: Setup

The screenshot shows the AWS Management Console interface for VPCs. At the top, there's a 'Create VPC' button and an 'Actions' dropdown. Below is a search bar 'Search VPCs and their proper X'. A table lists VPCs, with 'myVPC' (vpc-0bcb5110cf0ce088b) in an 'available' state, having IPv4 CIDR 172.31.0.0/16 and IPv6 CIDR 2600:1f16:14d:6300::/56. Below the table, the details for 'vpc-0bcb5110cf0ce088b | myVPC' are shown. There are tabs for 'Summary', 'CIDR Blocks', 'Flow Logs' (highlighted with a red box), and 'Tags'. A message states: 'You can create flow logs on your resources to capture IP traffic flow information from network interfaces for your VPC. For more information, see the VPC Flow Logs documentation.' Below this message is a 'Create flow log' button (highlighted with a red box). A table lists existing flow logs:

Flow Log ID	Filter	Destination Type	Destination Name	IAM Role ARN	Creation
fl-0e6a51c9092741fea	ALL	s3	my-flow-logs	-	October
fl-09a184a919be995ac	ALL	cloud-watch-logs	my-flow-logs-cw	arn:aws:iam::082897841036:role/flowlogsRole	October

Two purple callout boxes provide additional context:

- A callout pointing to the 'my-flow-logs' entry in the table: 'VPC traffic metadata captured in Amazon S3'
- A callout pointing to the 'my-flow-logs-cw' entry in the table: 'or Amazon CloudWatch Logs'

# VPC Flow Logs format

Interface	Source IP	Source port	Protocol	Packets
Event Data				
2 41747	eni-b30b9cd5	119.147.115.32	10.1.1.179	6000 22 6 1 40 1442975475 1442975535 REJECT OK
2 41747	eni-b30b9cd5	169.54.233.117	10.1.1.179	21188 80 6 1 40 1442975535 1442975595 REJECT OK
2 41747	eni-b30b9cd5	212.7.209.6	10.1.1.179	3389 3389 6 1 40 1442975596 1442975655 REJECT OK
2 41747	eni-b30b9cd5	189.134.227.225	10.1.1.179	39664 23 6 2 120 1442975656 1442975716 REJECT OK
2 41747	eni-b30b9cd5	77.85.113.238	10.1.1.179	0 0 1 1 100 1442975656 1442975716 REJECT OK
2 41747	eni-b30b9cd5	10.1.1.179	198.60.73.8	512 123 17 1 76 1442975776 1442975836 ACCEPT OK

Accept  
or reject

AWS account

Destination IP

## Destination port

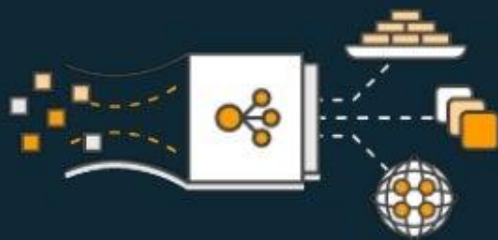
## Bytes

## Start/end time

# The Elastic Load Balancing Family

## Application Load Balancer

HTTP & HTTPS (VPC)



## Network Load Balancer

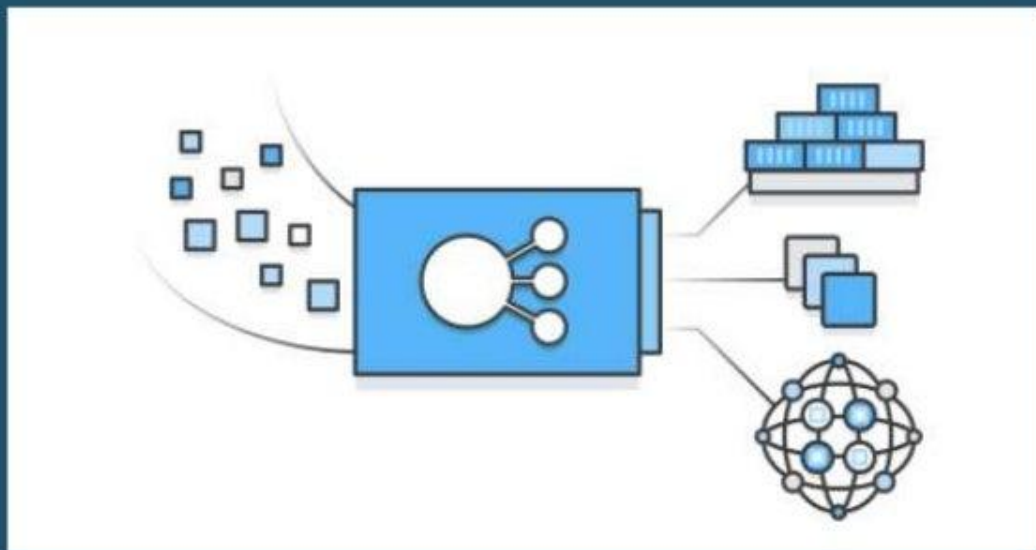
TCP Workloads (VPC)



## Classic Load Balancer

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





# Application Load Balancer

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



# 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

# Application Load Balancer

Support for **WebSockets** and **HTTP/2**

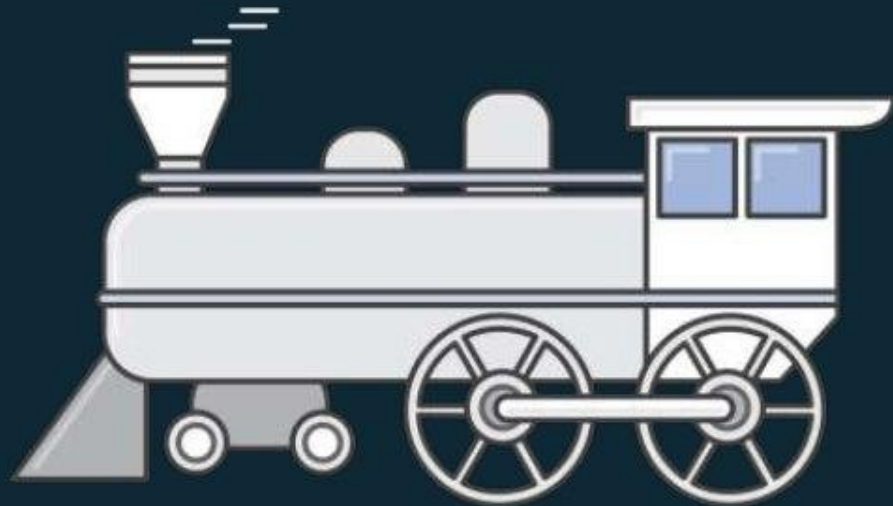
Path and Host Based Routing

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





# Listeners



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

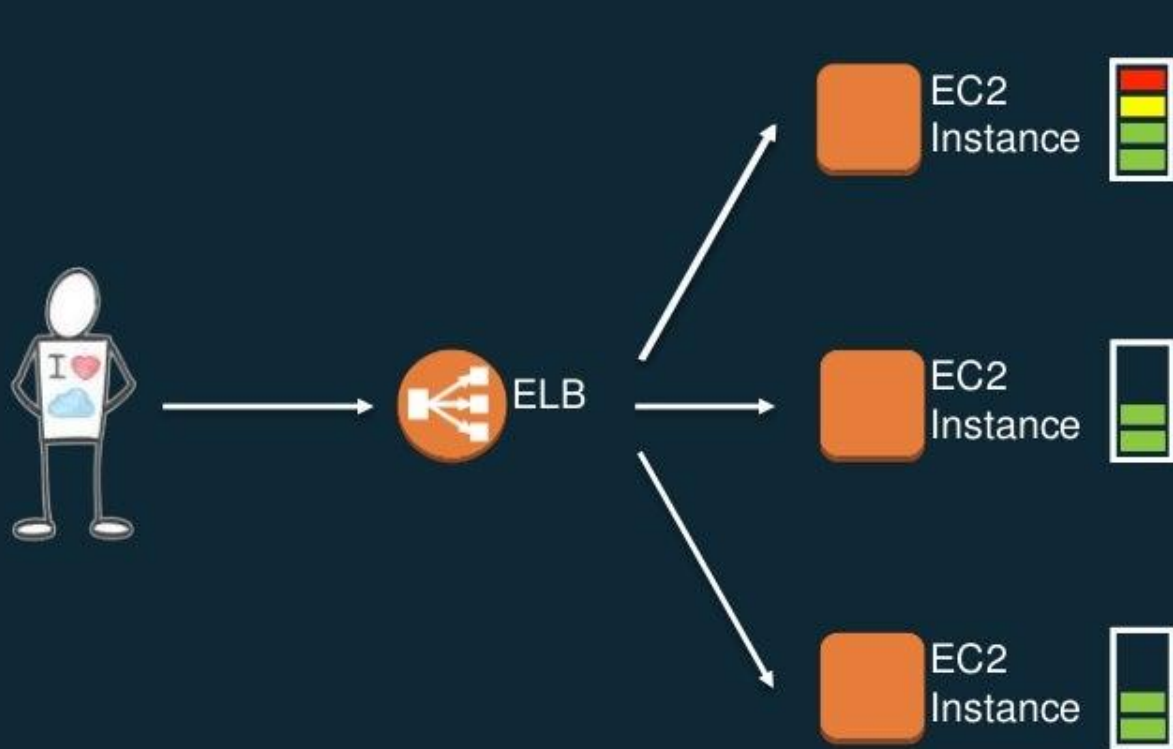
Each Application Load Balancer needs **at least one listener to accept traffic**

Each Application Load Balancer can have **up to 50 listeners**

**Routing rules** are defined on listeners



# Health checks



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

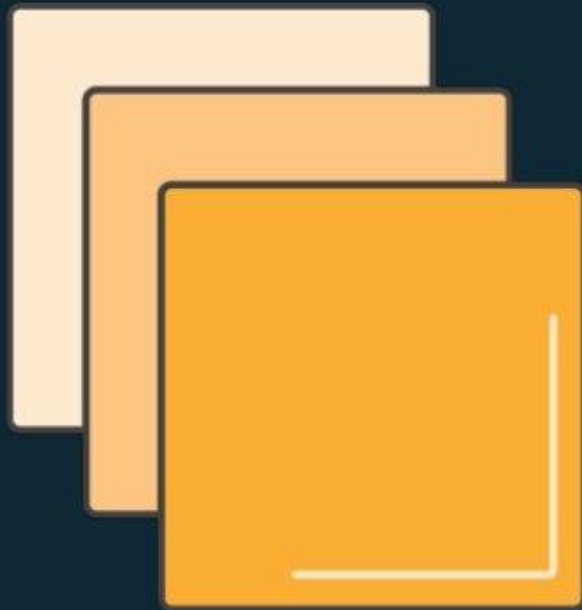
# Target groups

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

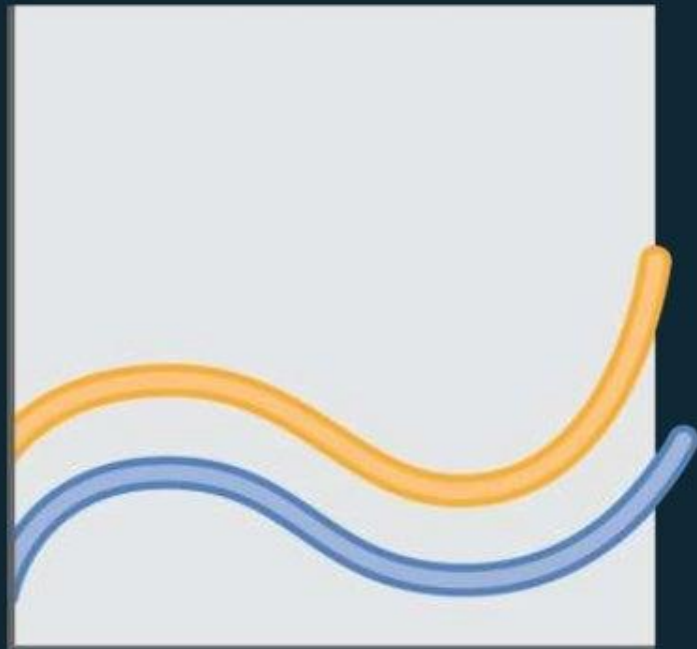
Target groups can contain up to 1,000 targets



# Auto Scaling integration

Auto Scaling can now scale targets within a target group

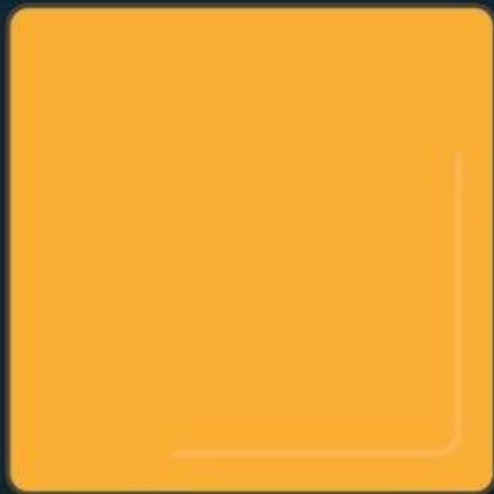
Allows for applications to be scaled independently behind the Application Load Balancer







# Targets

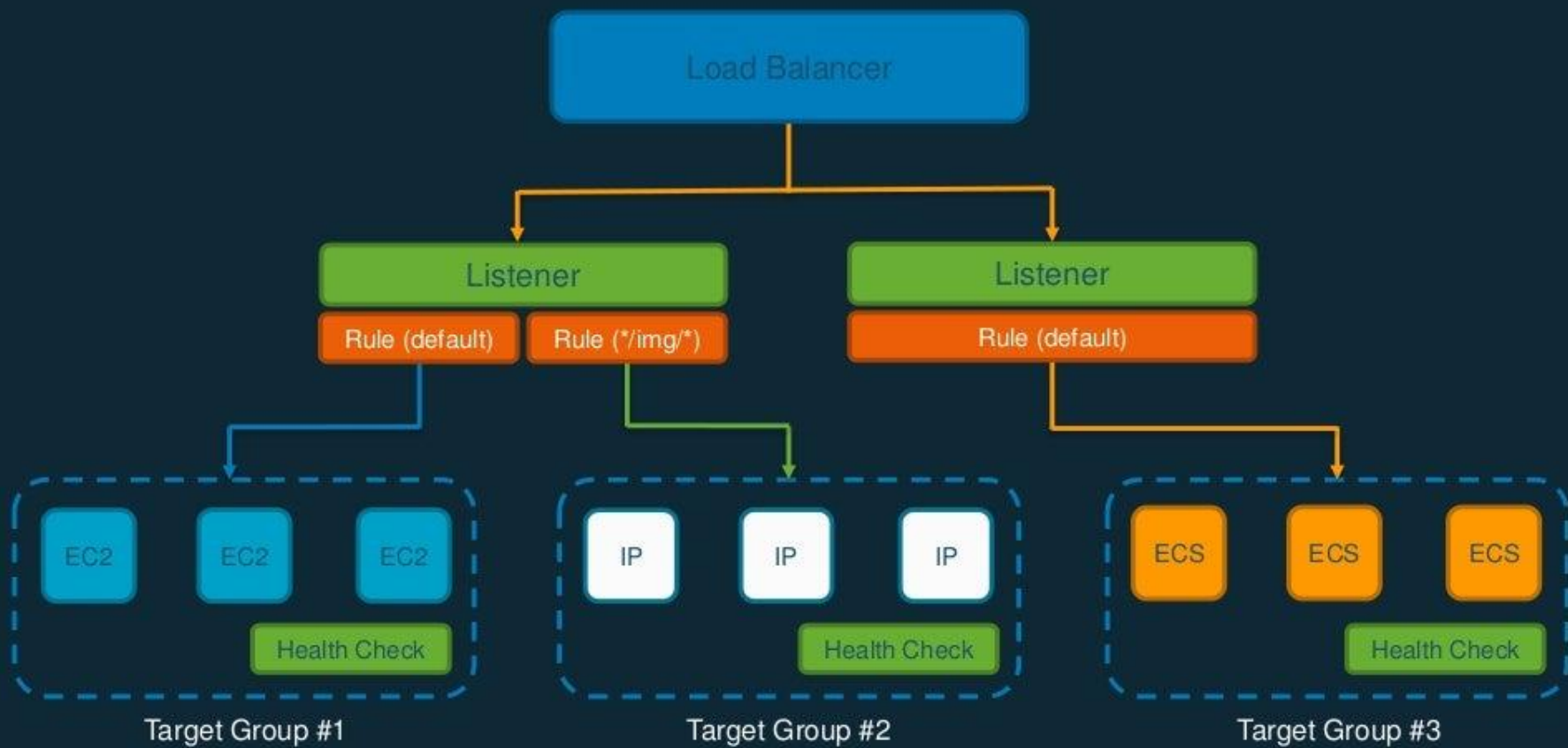


Support for **EC2 instances** and **ECS containers**, and **IP Addresses**.

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





orders.example.com



ELB



EC2  
Instance



EC2  
Instance



EC2  
Instance



ELB



EC2  
Instance



EC2  
Instance



EC2  
Instance

images.example.com

Running two separate  
services with Classic  
Load Balancer



example.com



ELB

/orders

/images



EC2  
Instance



EC2  
Instance



EC2  
Instance



EC2  
Instance



EC2  
Instance



EC2  
Instance

.....

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



example.com



ELB

/api

/test



EC2  
Instance



EC2  
Instance



EC2  
Instance



ECS  
Container

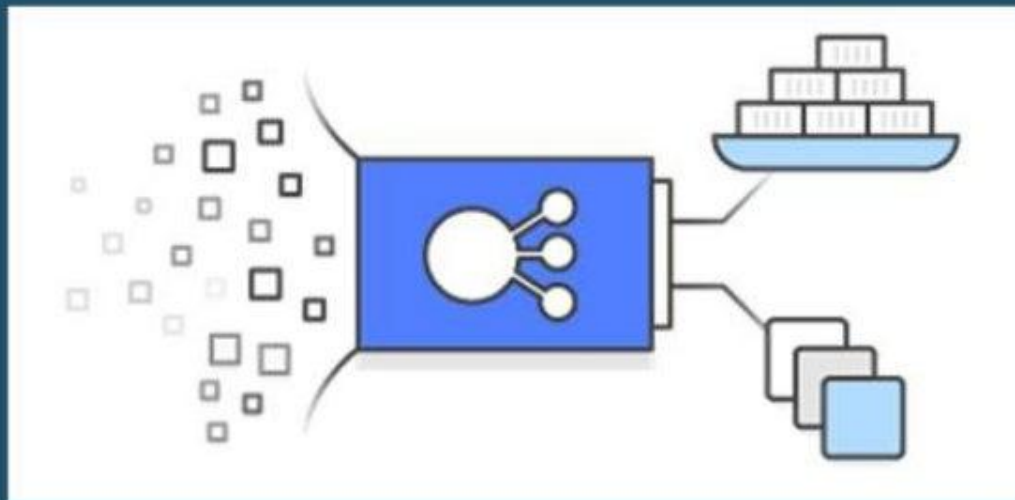


ECS  
Container



ECS  
Container

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



# Network Load Balancer

# Network Load Balancer



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

**High Performance**

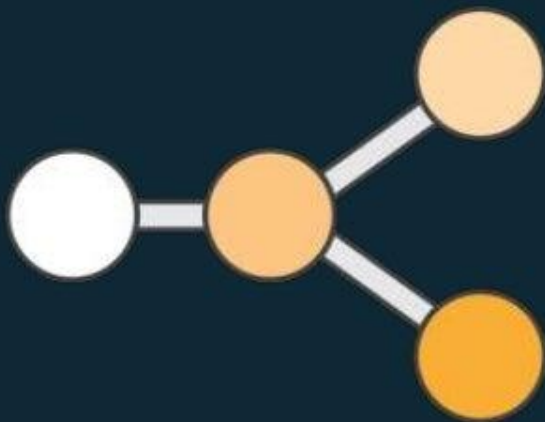
Can handle millions of requests per sec

**Static IP** Support

Ideal for applications with long running  
**connections**



# Static IP

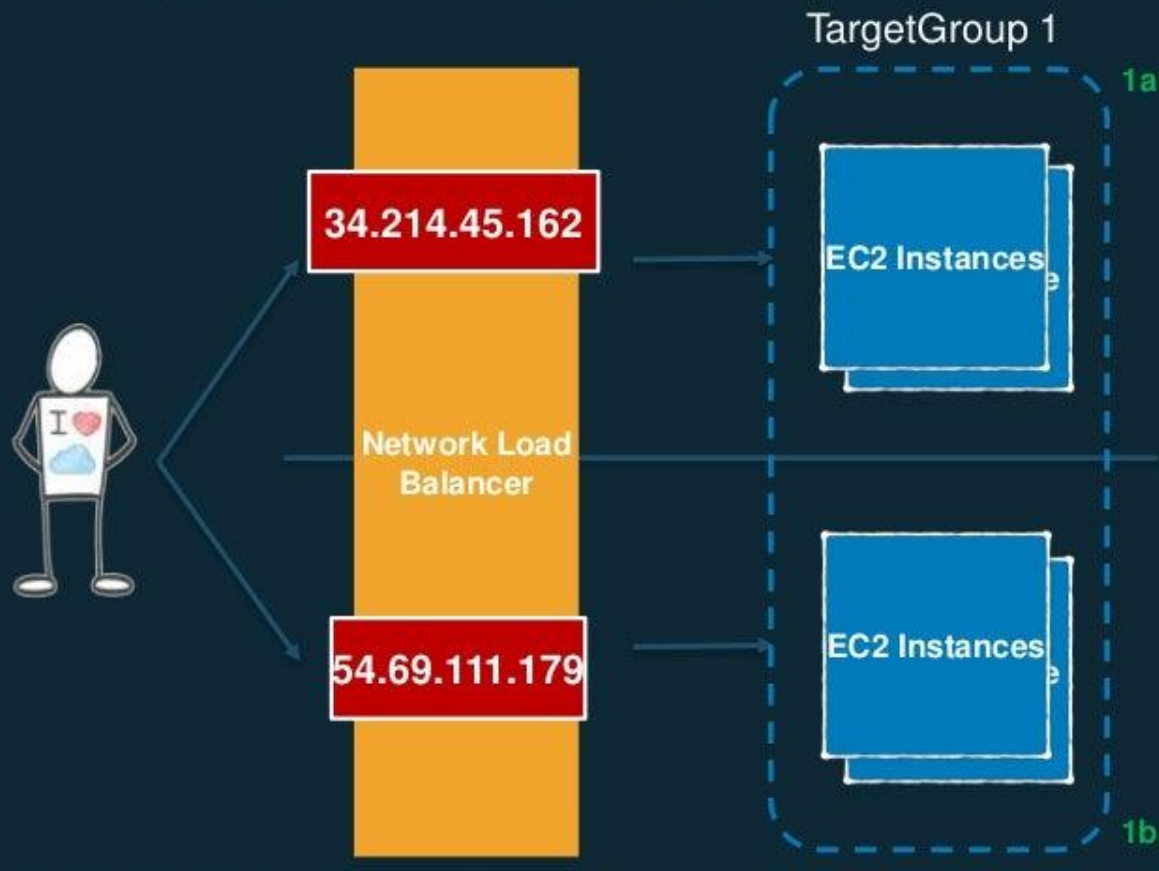


Automatically gets assigned a single IP per Availability Zone

Assign an EIP per AZ to get Static IP

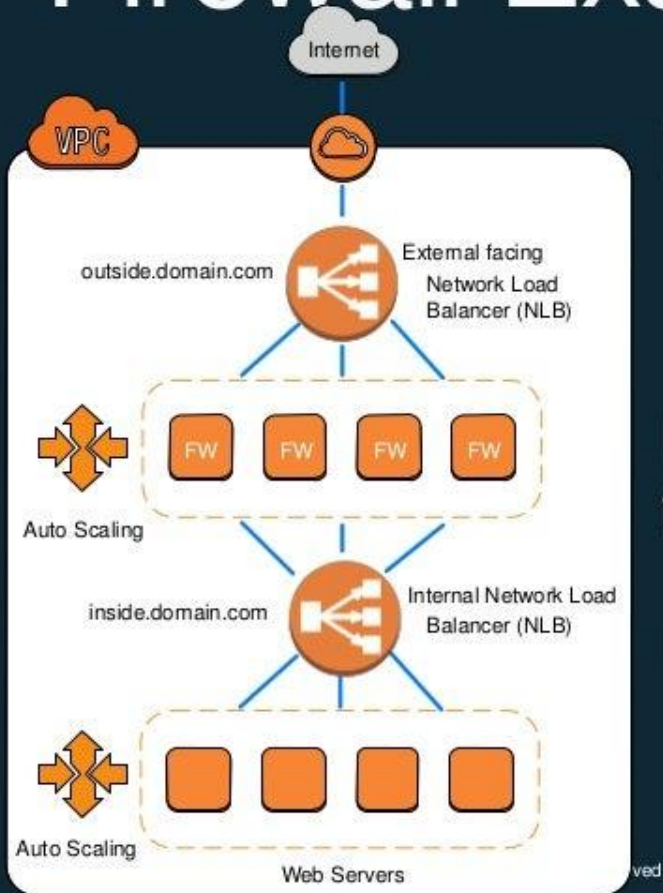
Helps with white-listing for firewalls and zero dollar billing use cases

# Assign Elastic IP Addresses



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

# Firewall Example with NLB



External facing NLB uses less addresses  
Used for Firewalls, proxies or 3<sup>rd</sup> 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



## 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



# Networking II labs



- [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 Scaling group with Load balancing
  - Create an Application load balancer with an HTTP Listener

