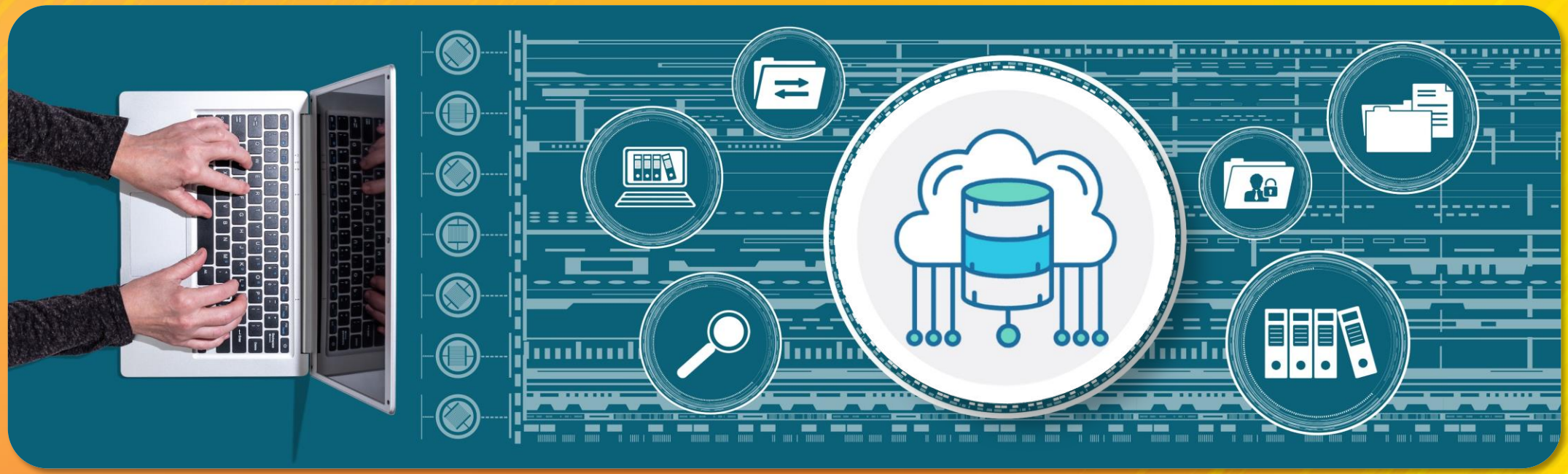
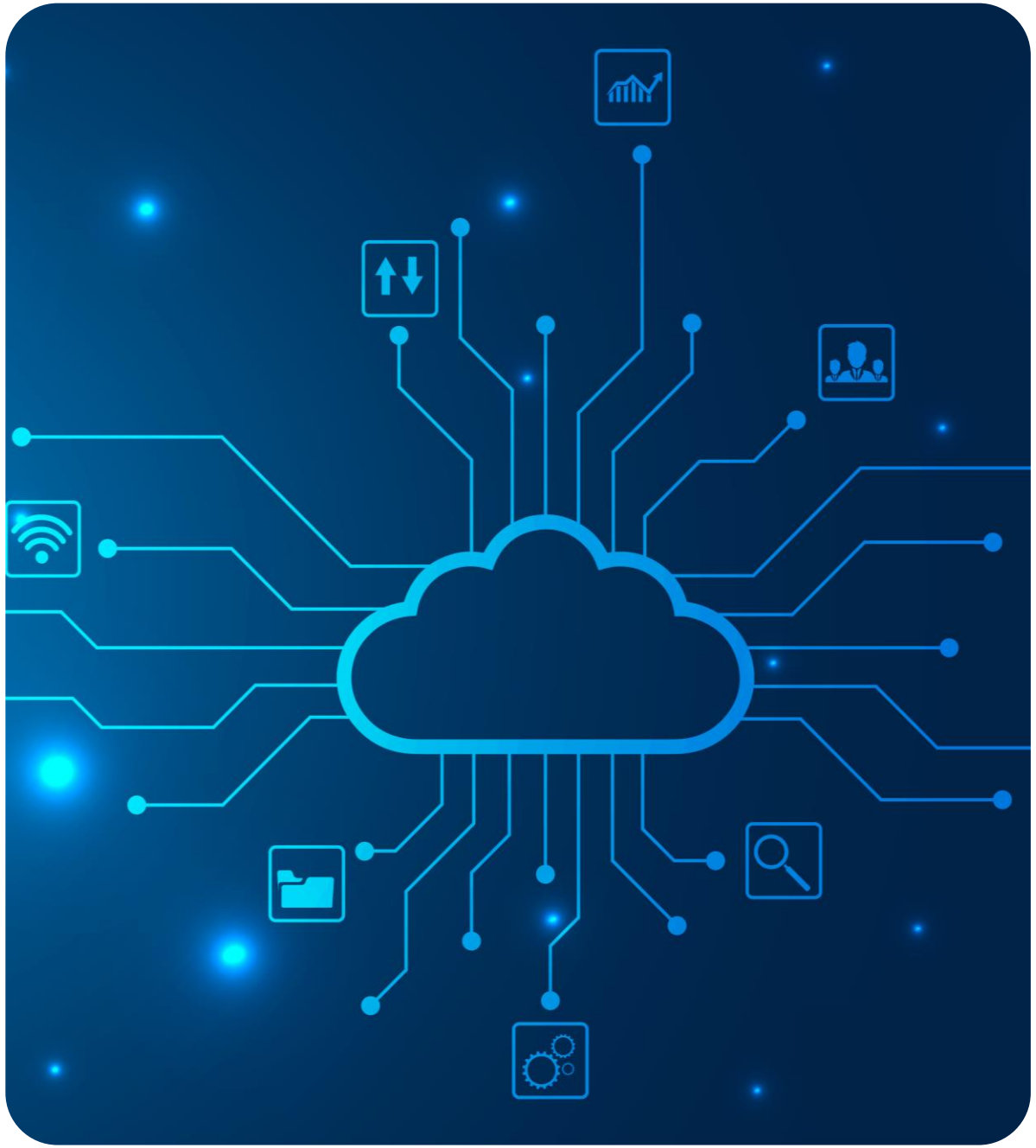
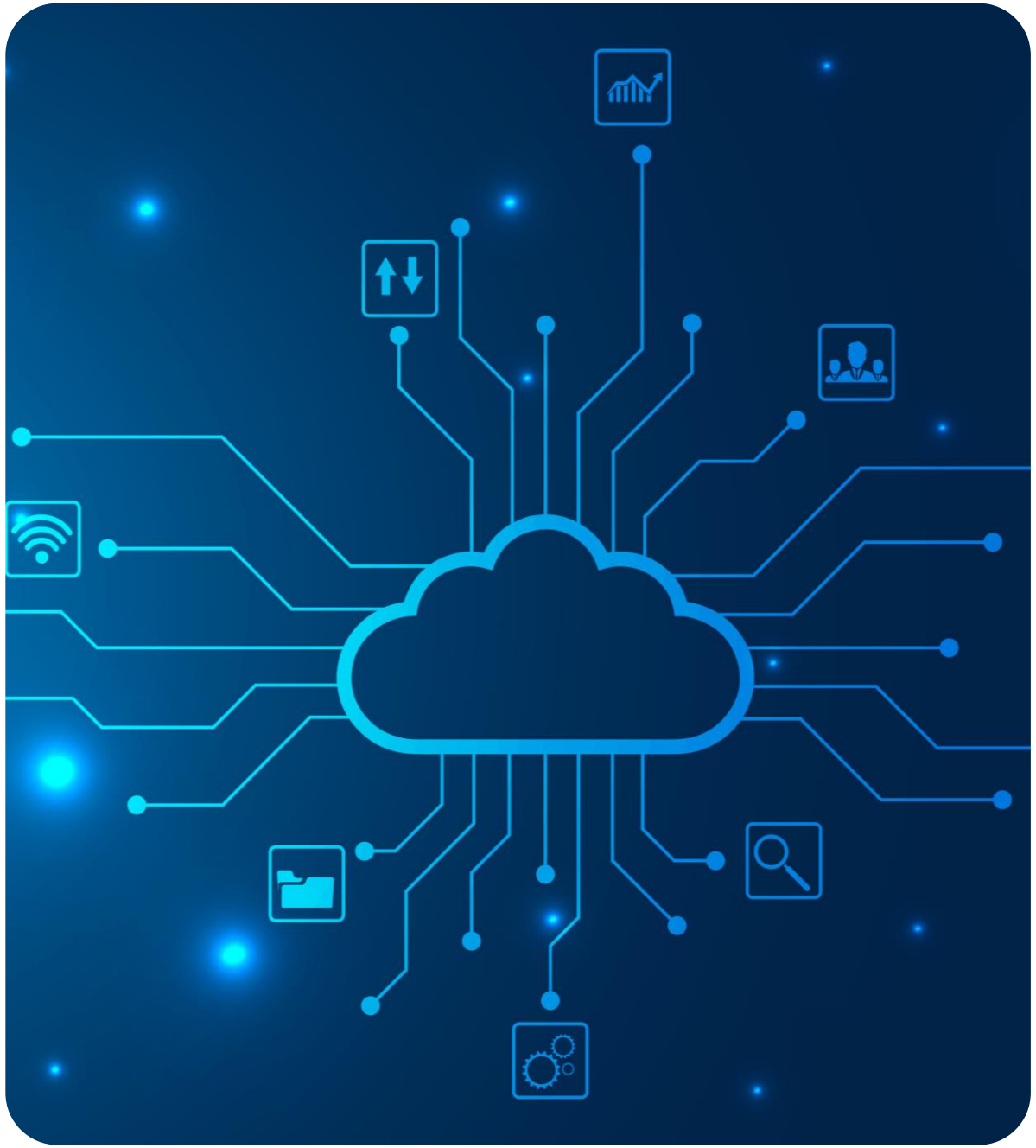
Networking in AWS – Part 2

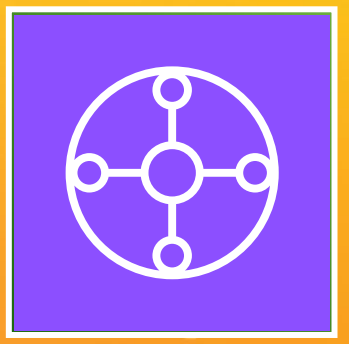




Agenda

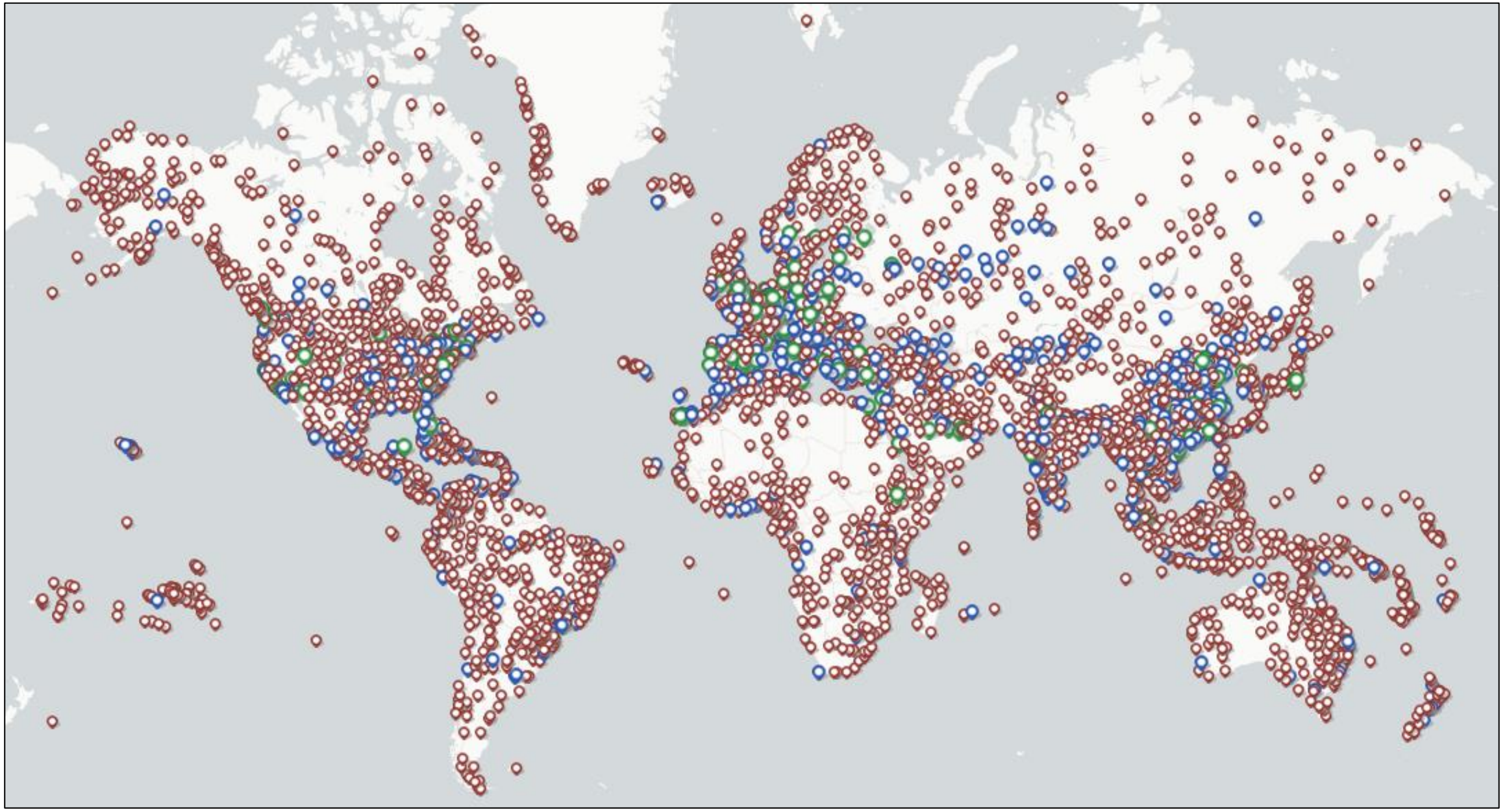
- AWS Transit Gateway
- AWS Global Accelerator
- Network Observability
  - VPC Flow Logs
  - VPC Traffic Mirroring
  - Reachability Analyzer



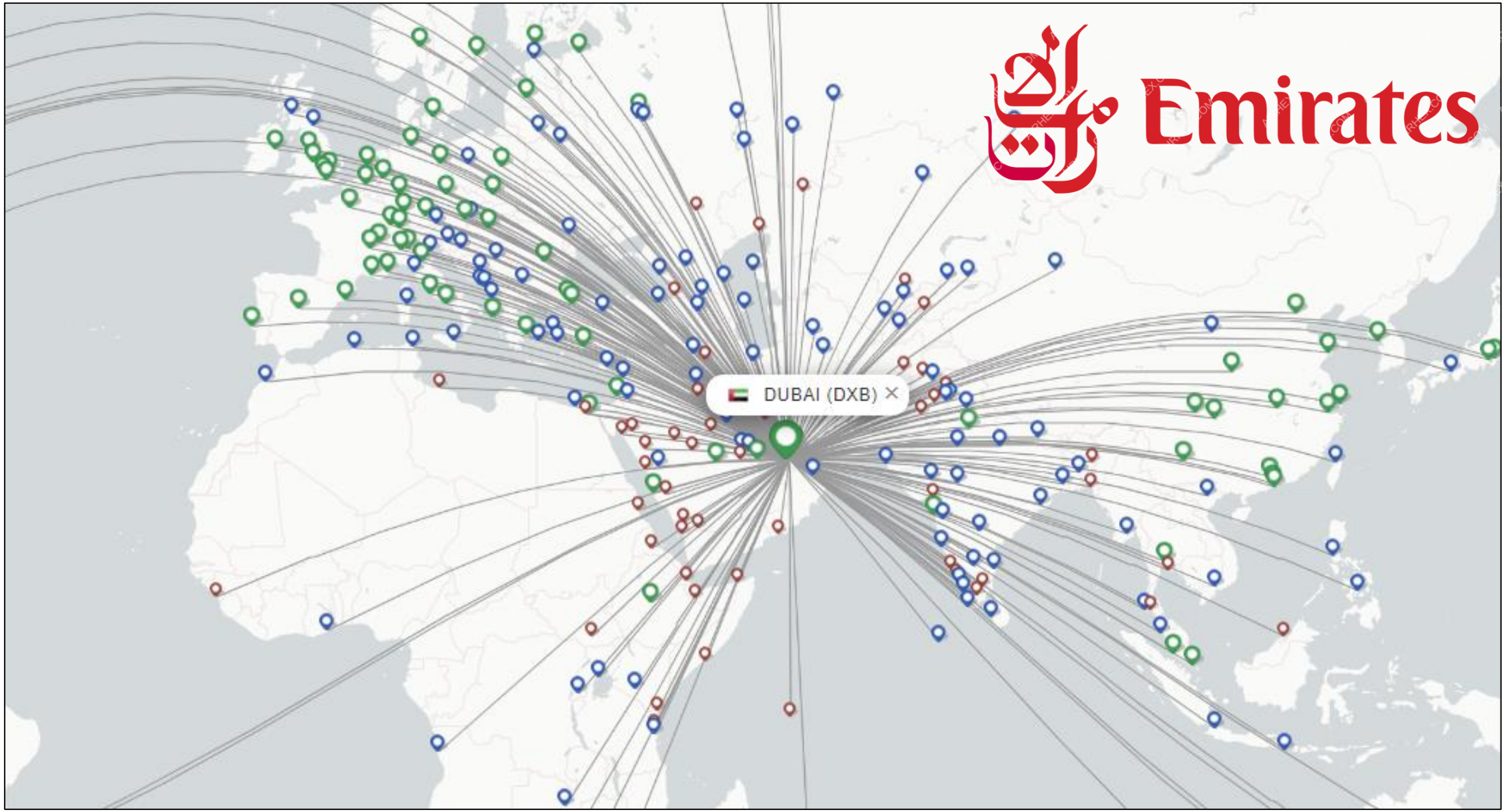


AWS Transit Gateway

Airports in the world



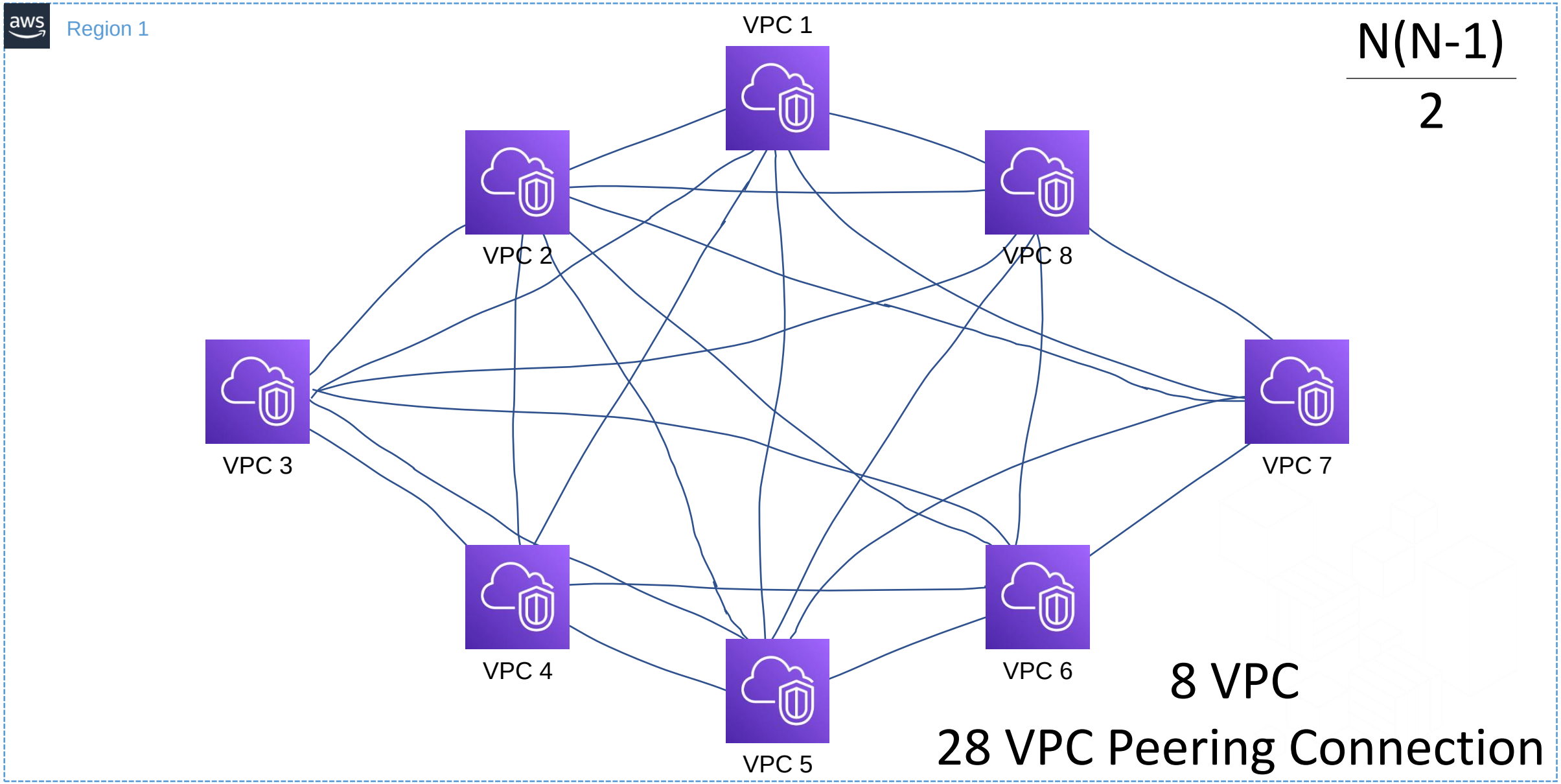
Airline Hub and Spoke Model



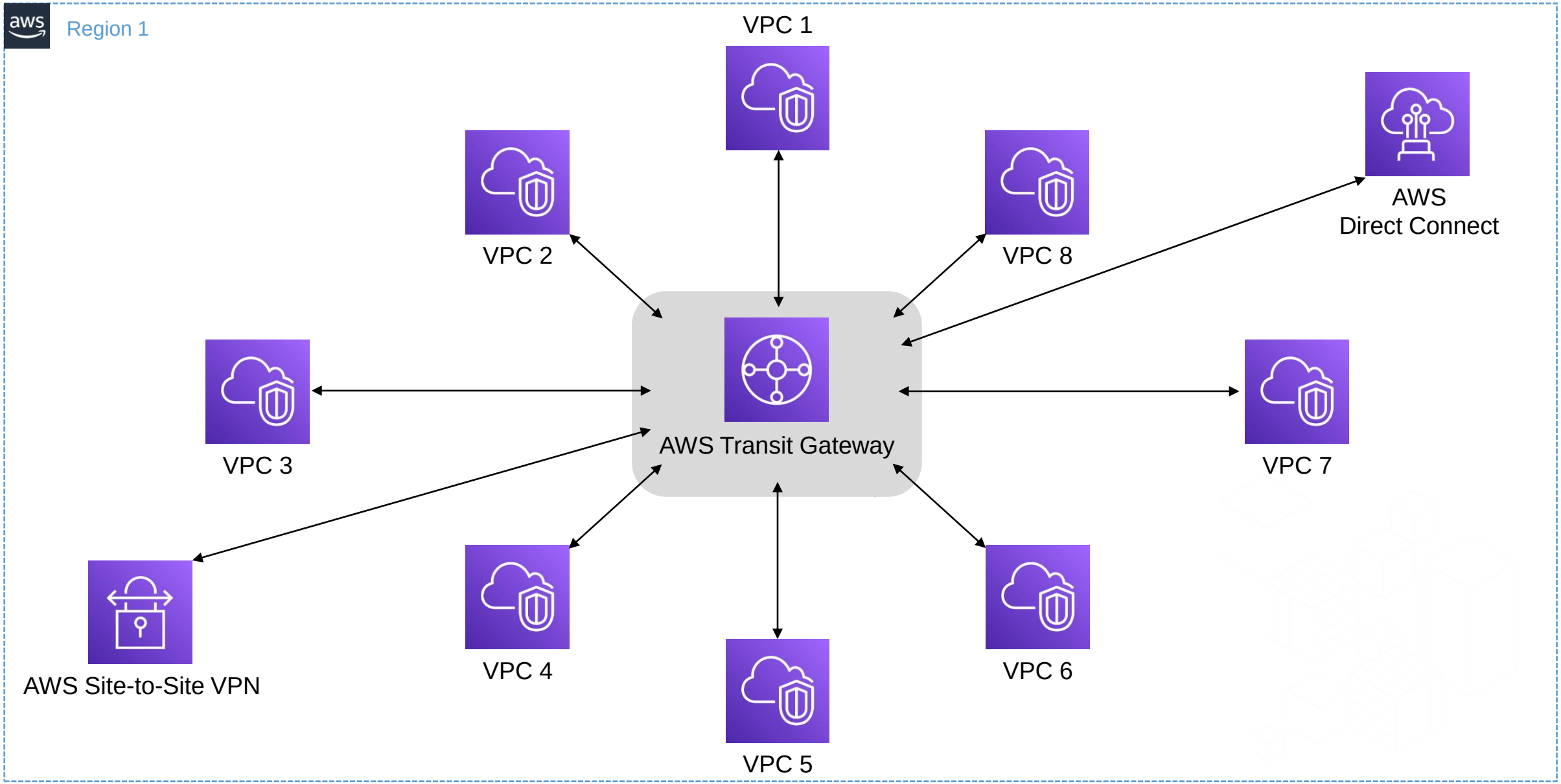
Airline Hub and Spoke Model

Airline Hub and Spoke Model

Peering Multiple VPC



Transit Gateway



AWS Transit Gateway in Action

Networking Workshop 0.2

VPCs, Subnets, Peering, Transit Gateways, VPNs and Traffic Mirroring

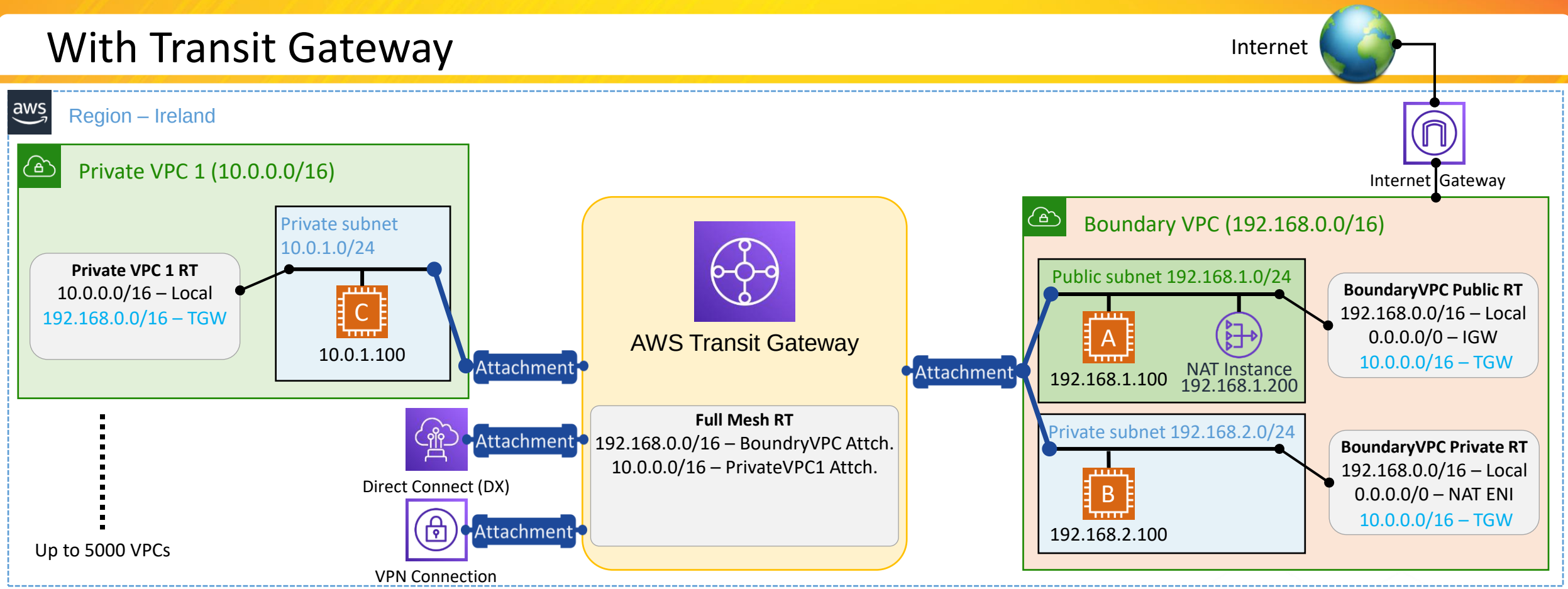
Labs and Instructions

Transit Gateway

https://tgw.networking-workshop.com/#/

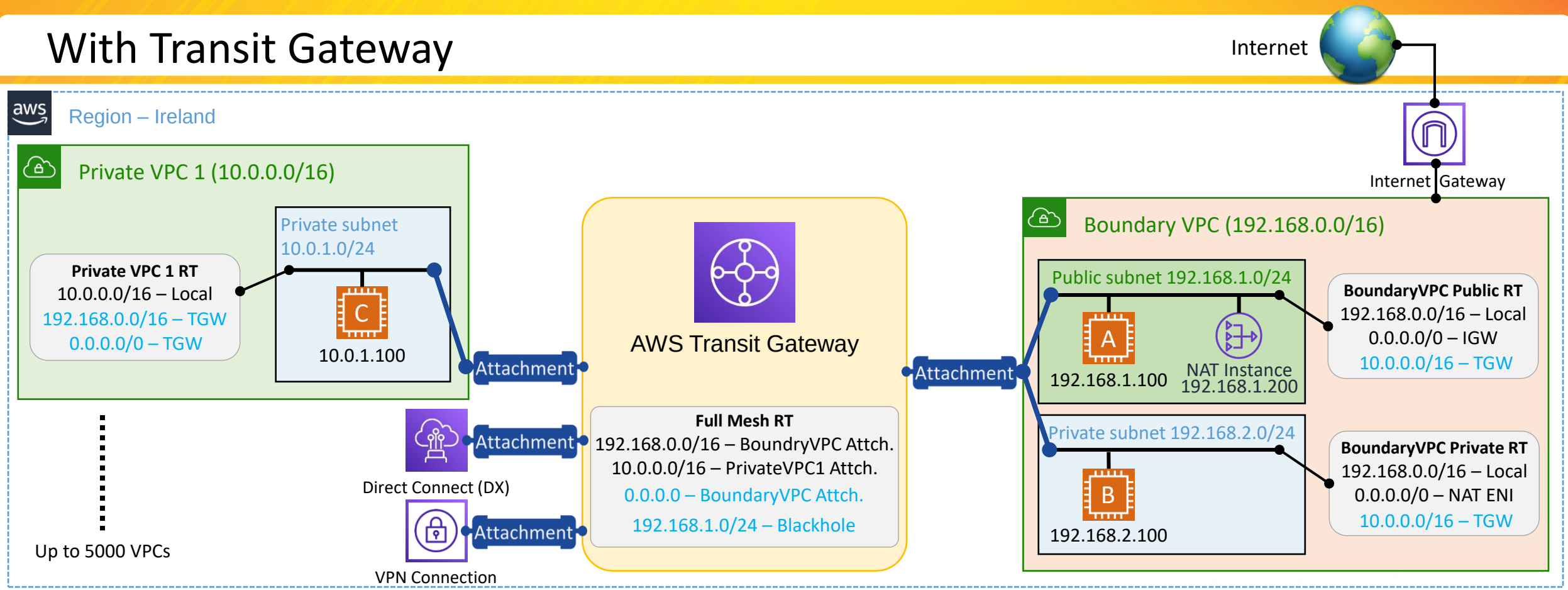
Before Transit Gateway

With Transit Gateway



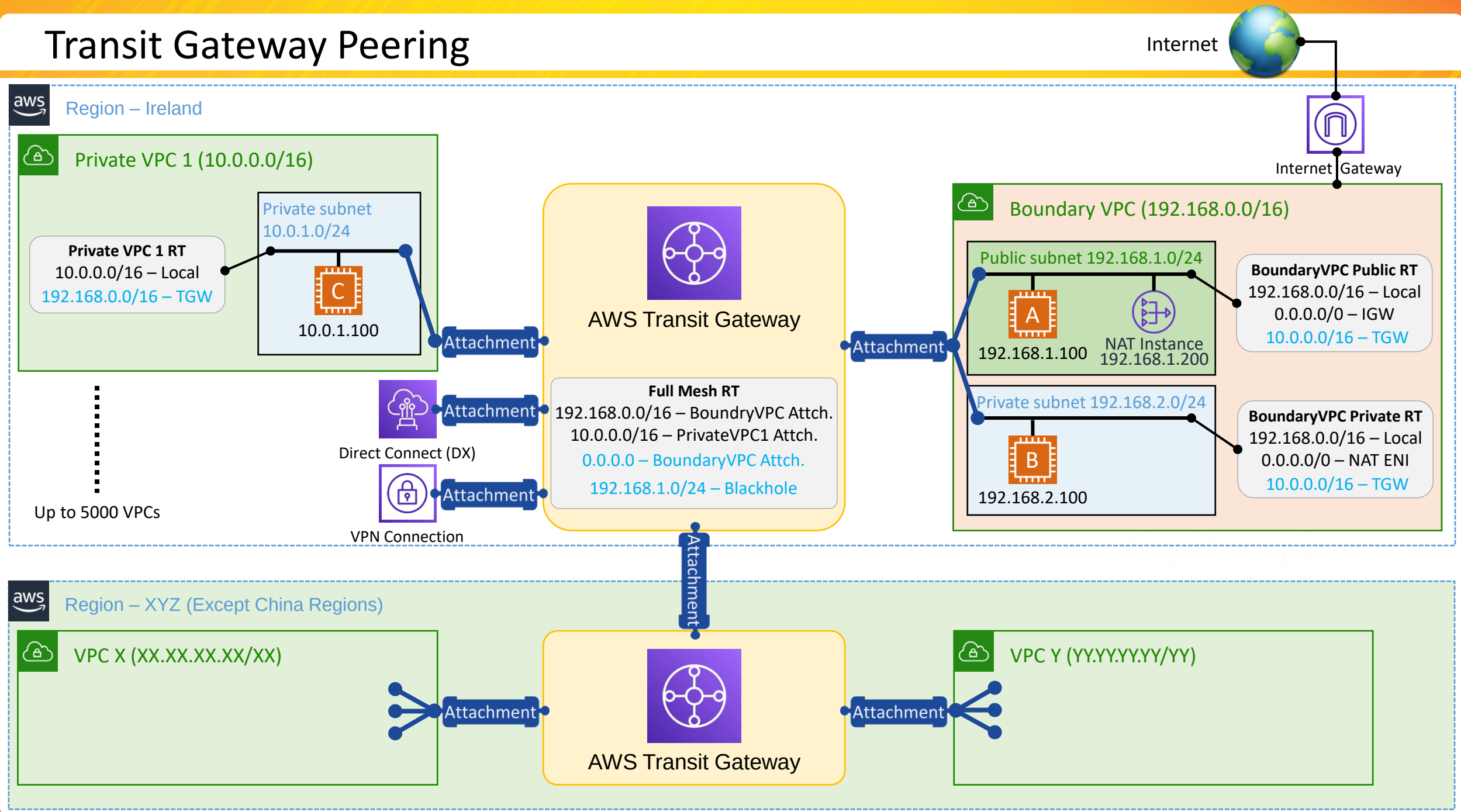
- An attachment is BOTH a source AND destination of packets (next hop, Layer 3 routing)
- One attachment (with “crows foot”) per VPC
- Attachment Type : VPC, VPN, Direct Connect, TGW Peering
- Single or multiple Route Tables, only one Route Table association per attachment

With Transit Gateway

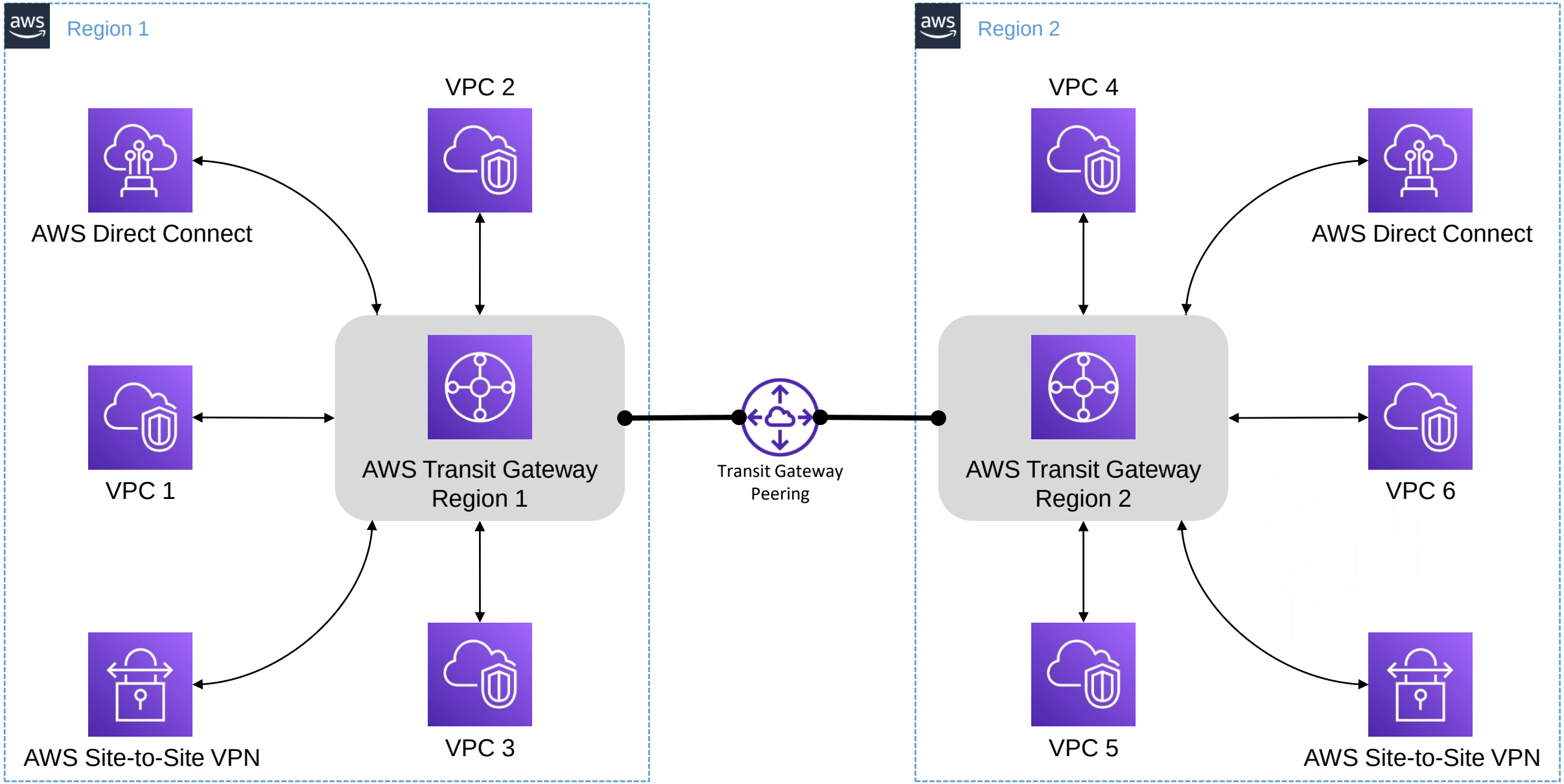


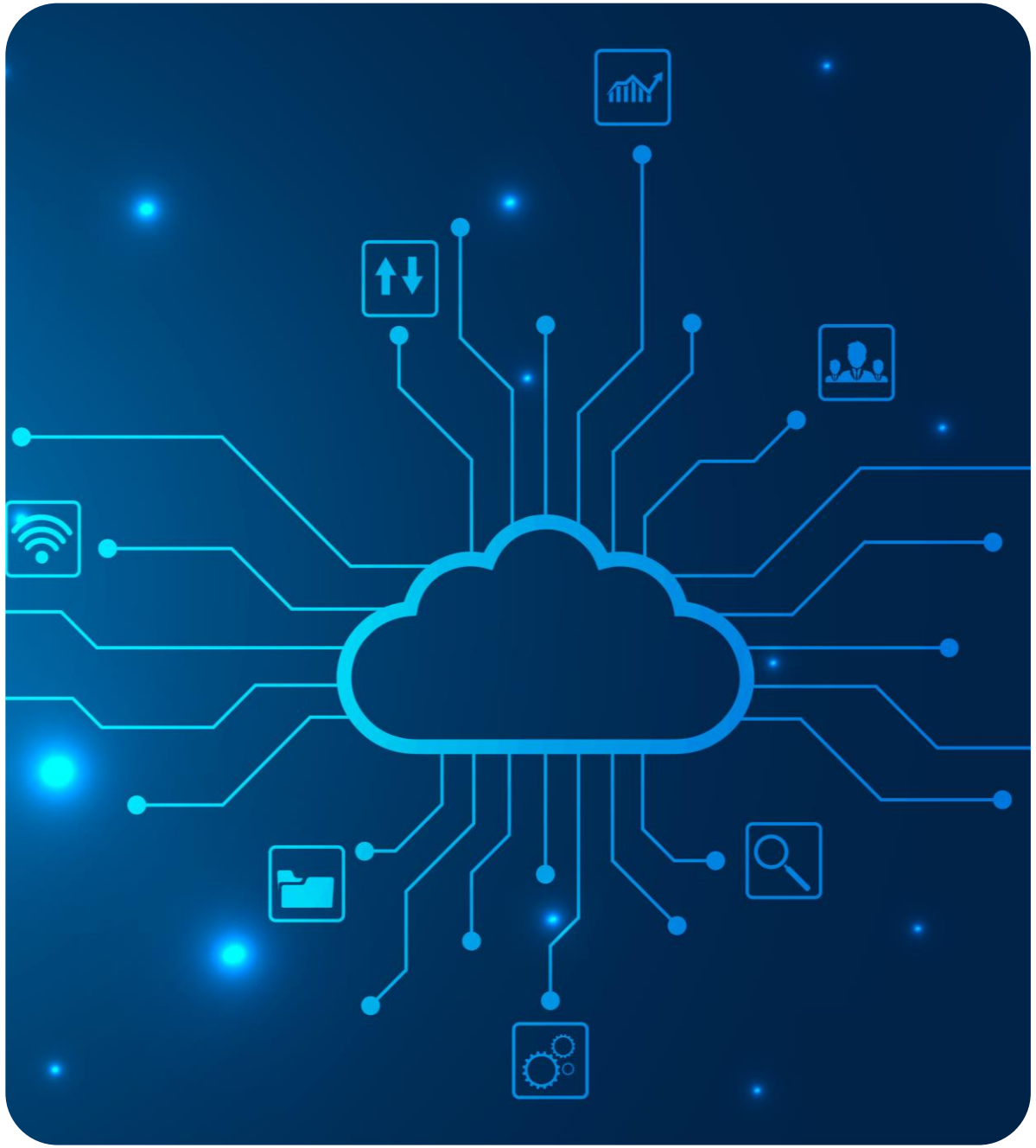
- An attachment is BOTH a source AND destination of packets (next hop, Layer 3 routing)
- One attachment (with “crows foot”) per VPC
- Attachment Type : VPC, VPN, Direct Connect, TGW Peering
- Single or multiple Route Tables, only one Route Table association per attachment

Transit Gateway Peering



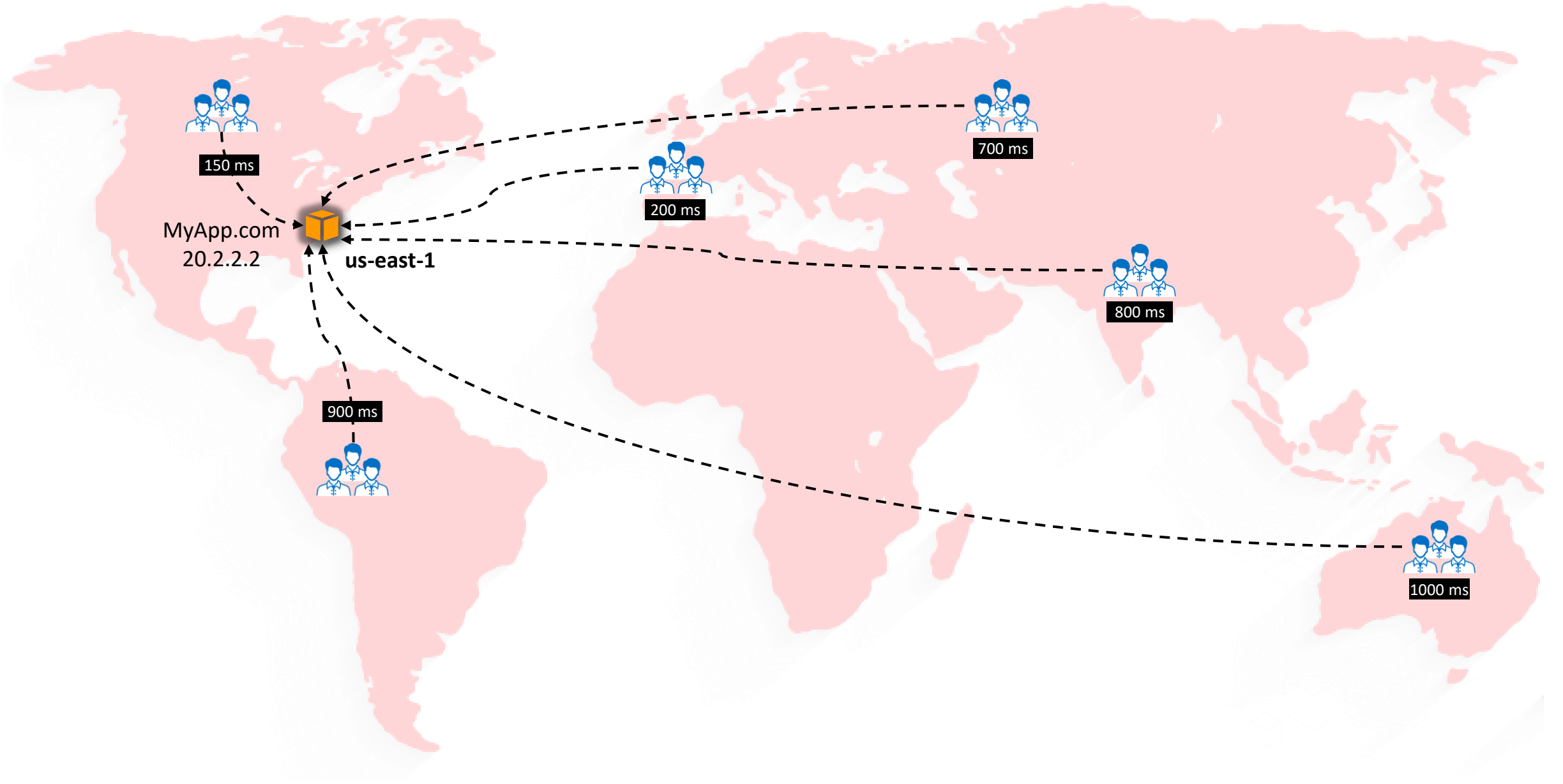
Transit Gateway





AWS Global Accelerator

A typical Workload in AWS

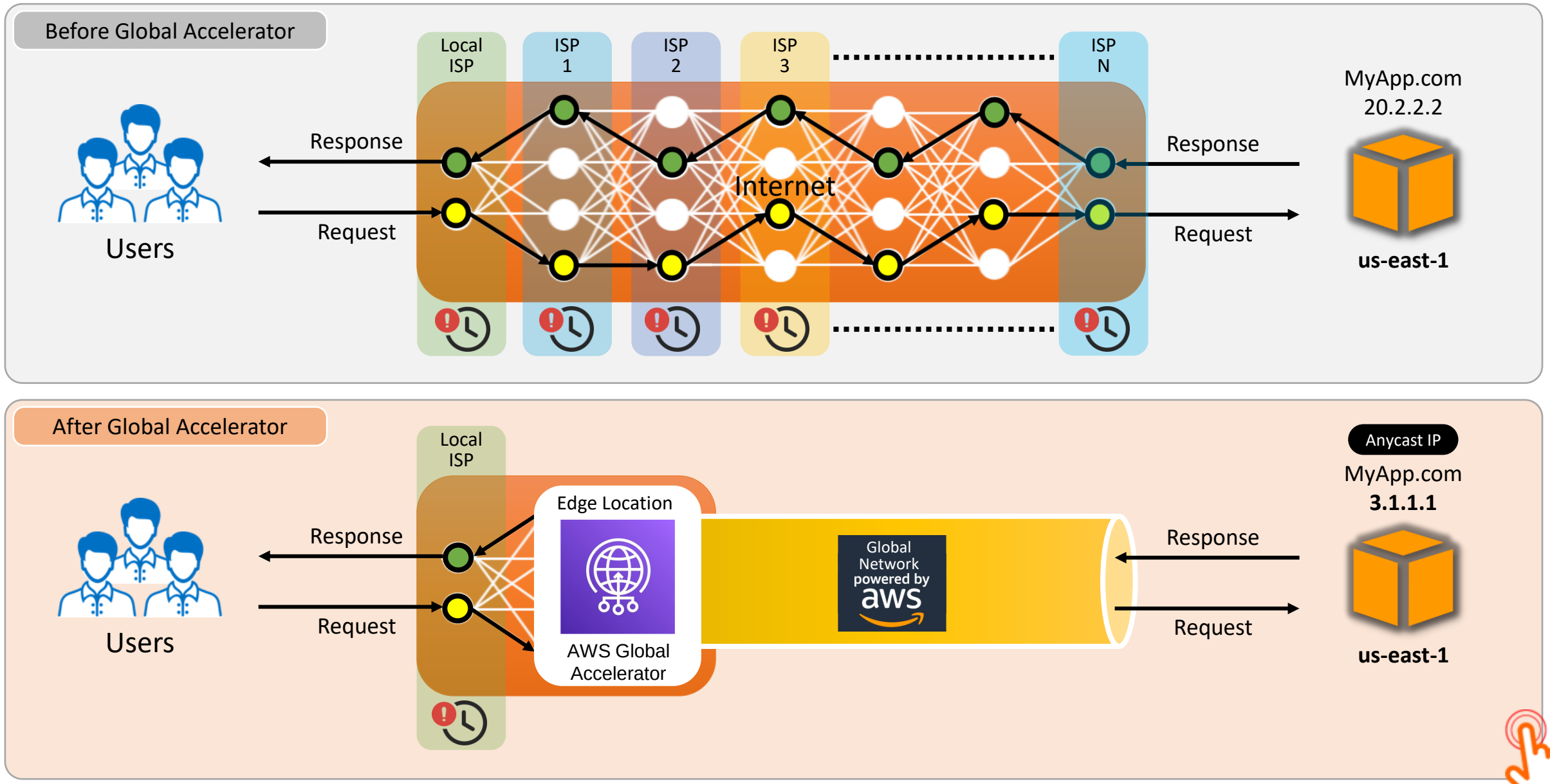


AWS Global Accelerator

AWS Global Accelerator

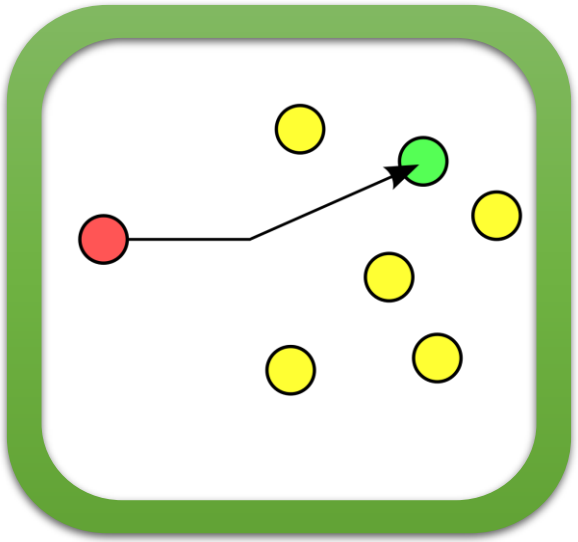
- A network layer service that you can deploy in front of your Internet facing applications to improve availability and performance for your globally distributed users.
- Features
  - Continuous availability monitoring
  - Avoid DNS caching issues
  - Simplified global traffic management
  - Uses Anycast IP address
  - Easy to setup and manage

Traffic Flow – Before and after AWS Global Accelerator



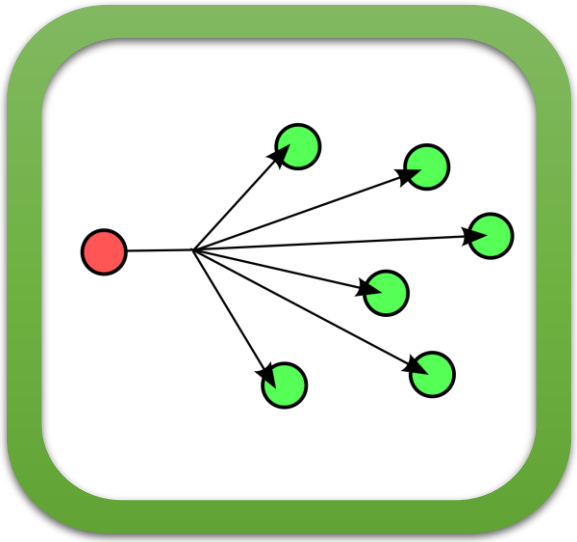
AWS Global Accelerator uses Anycast Communication

Unicast



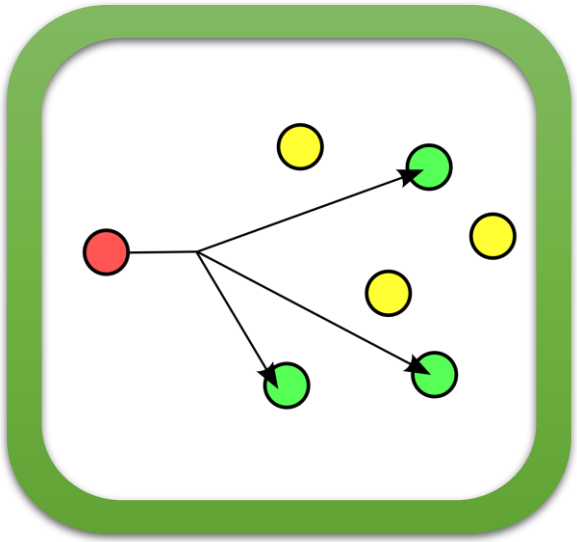
One-to-One Communication

Broadcast



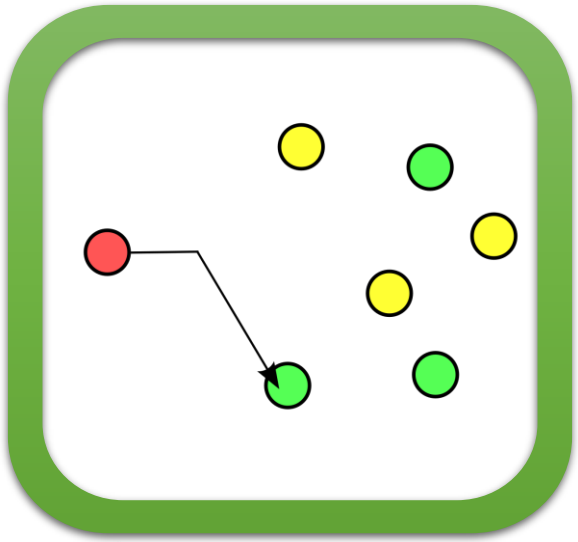
One-to-All Communication

Multicast



One-to-Many Communication

Anycast



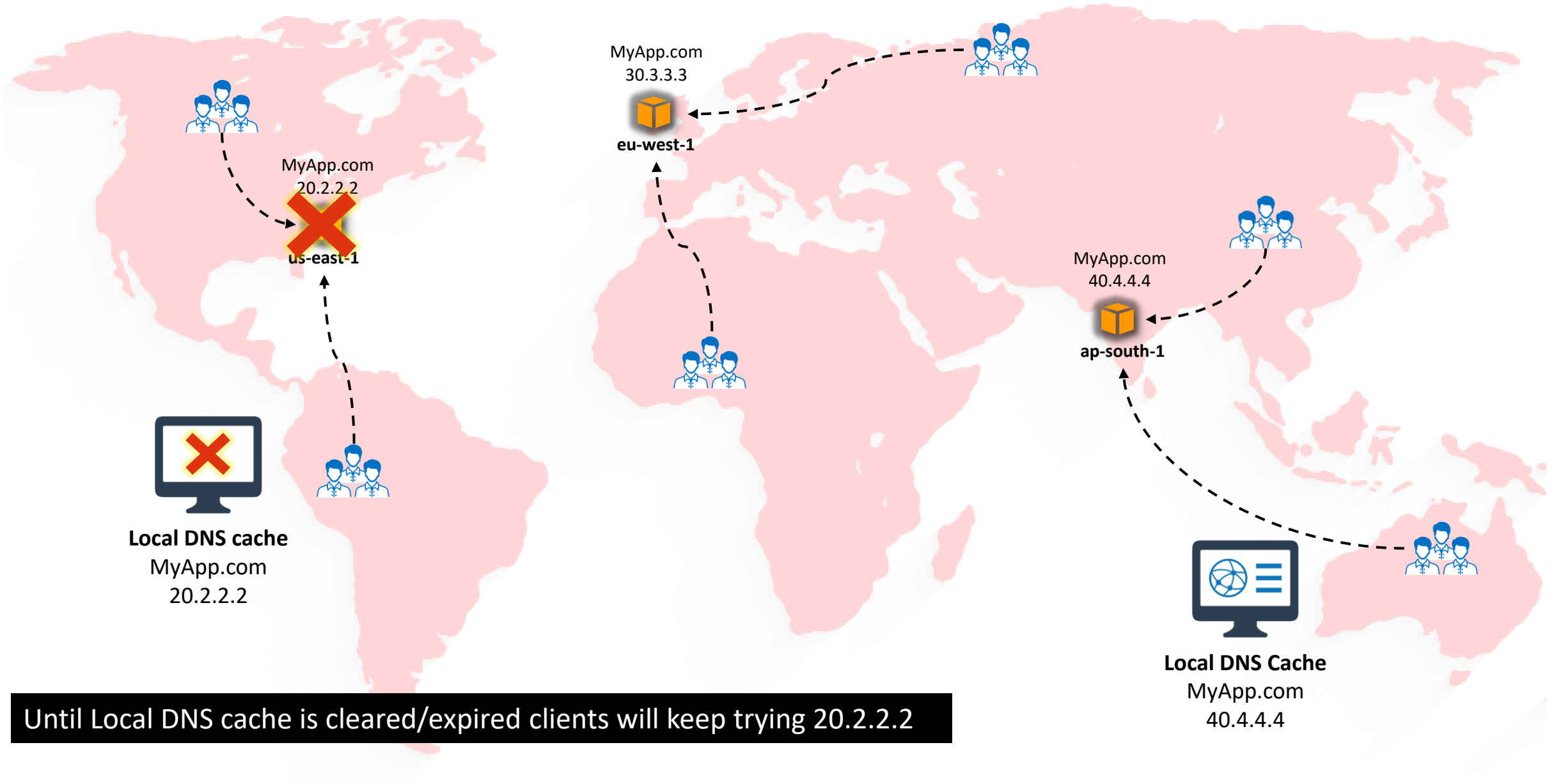
One-to-nearest Communication

Anycast - Requests are routed to the nearest member of an anycast group.

A Multi-Region Application without AWS Global Accelerator

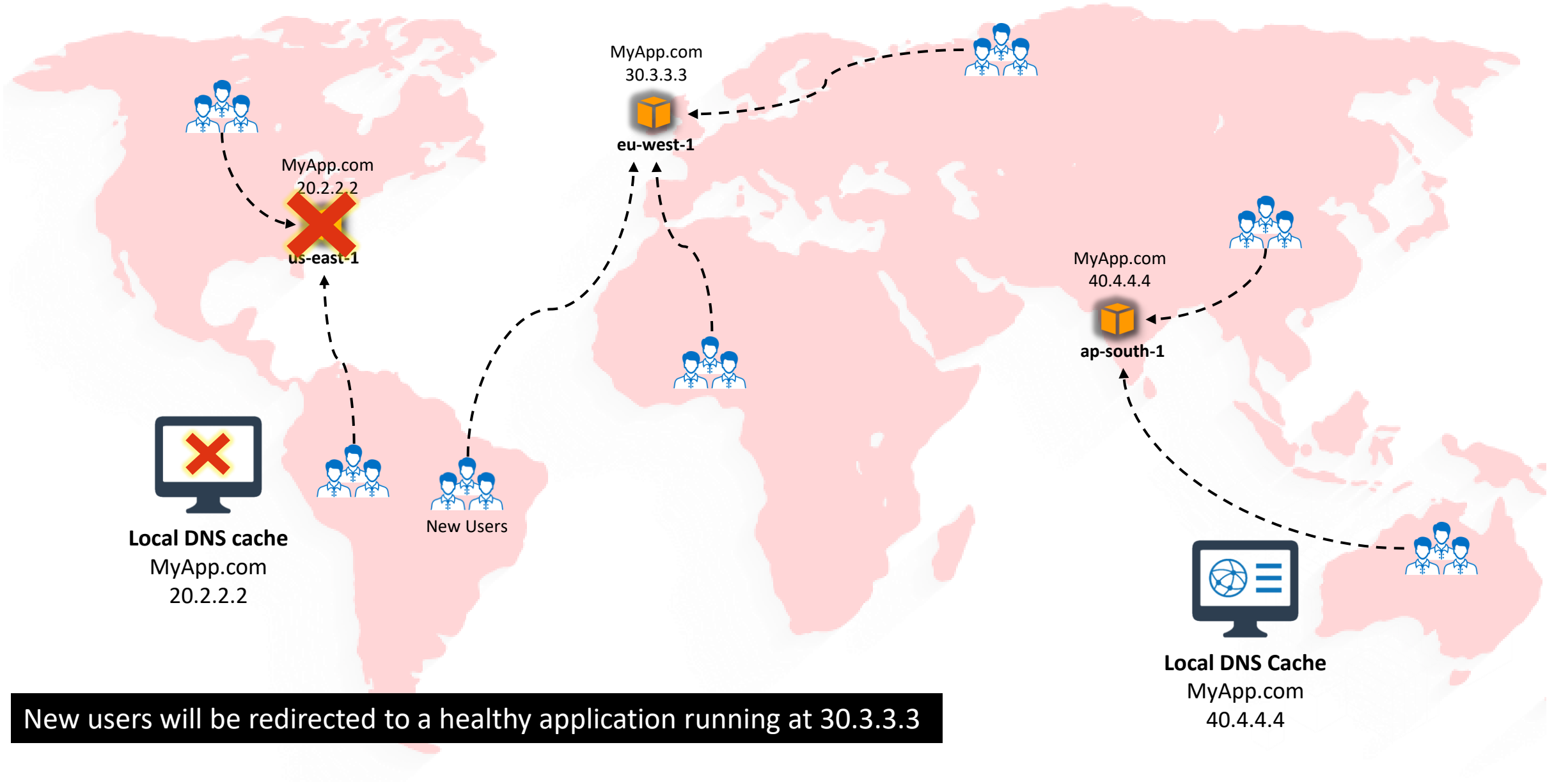
MyApp.com gets a different IP address in each Region.

A Multi-Region Application without AWS Global Accelerator – Region Failure



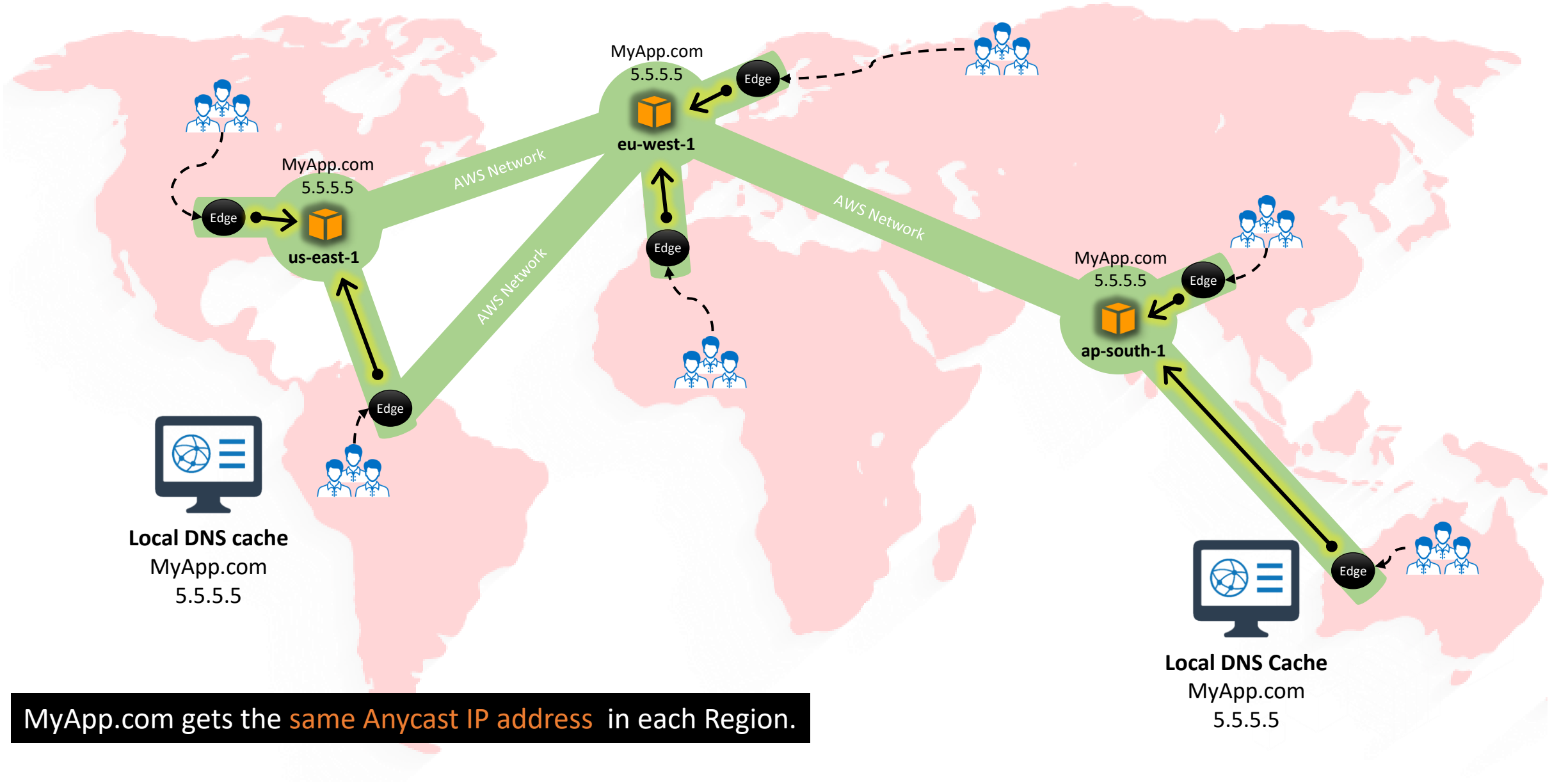
Until Local DNS cache is cleared/expired clients will keep trying 20.2.2.2

A Multi-Region Application without AWS Global Accelerator – Region Failure



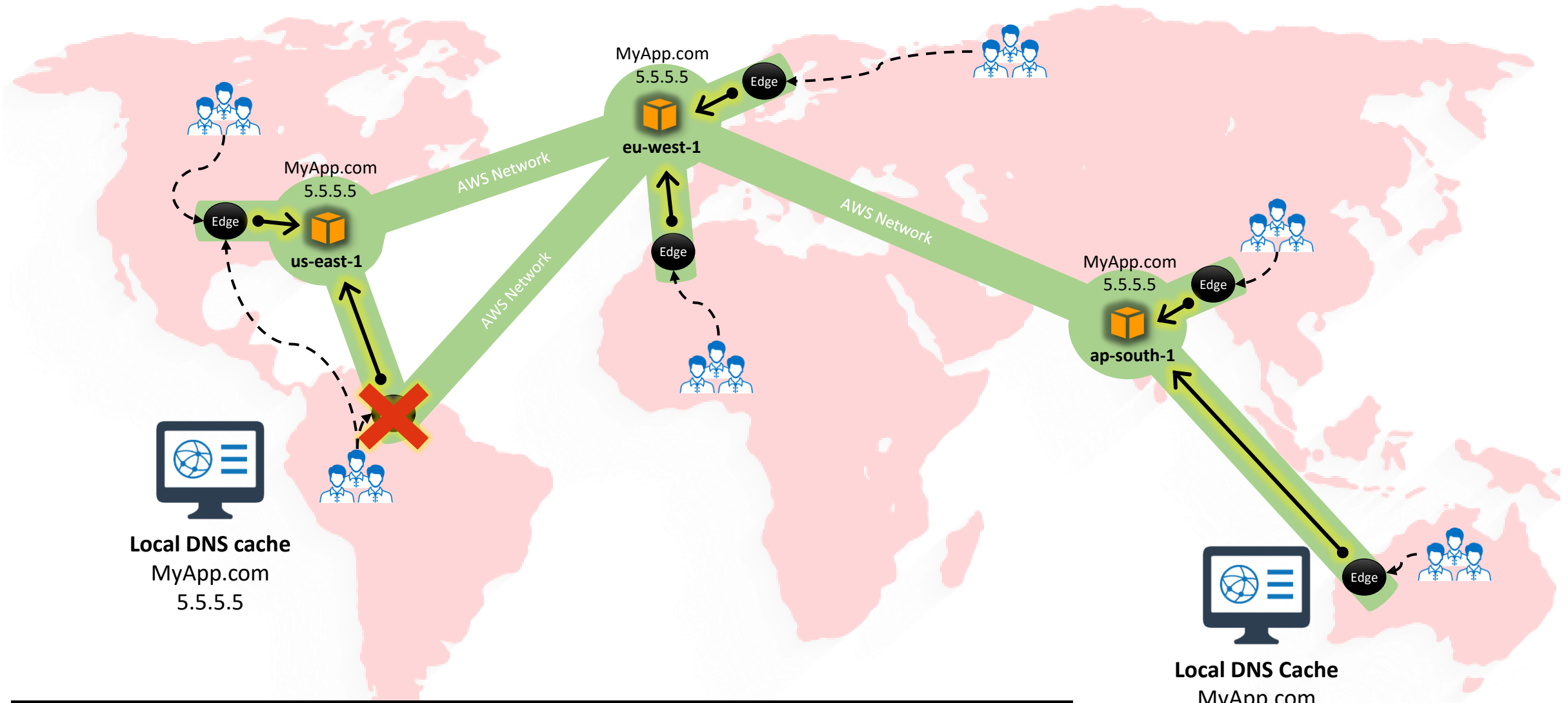
New users will be redirected to a healthy application running at 30.3.3.3

A Multi-Region Application with AWS Global Accelerator



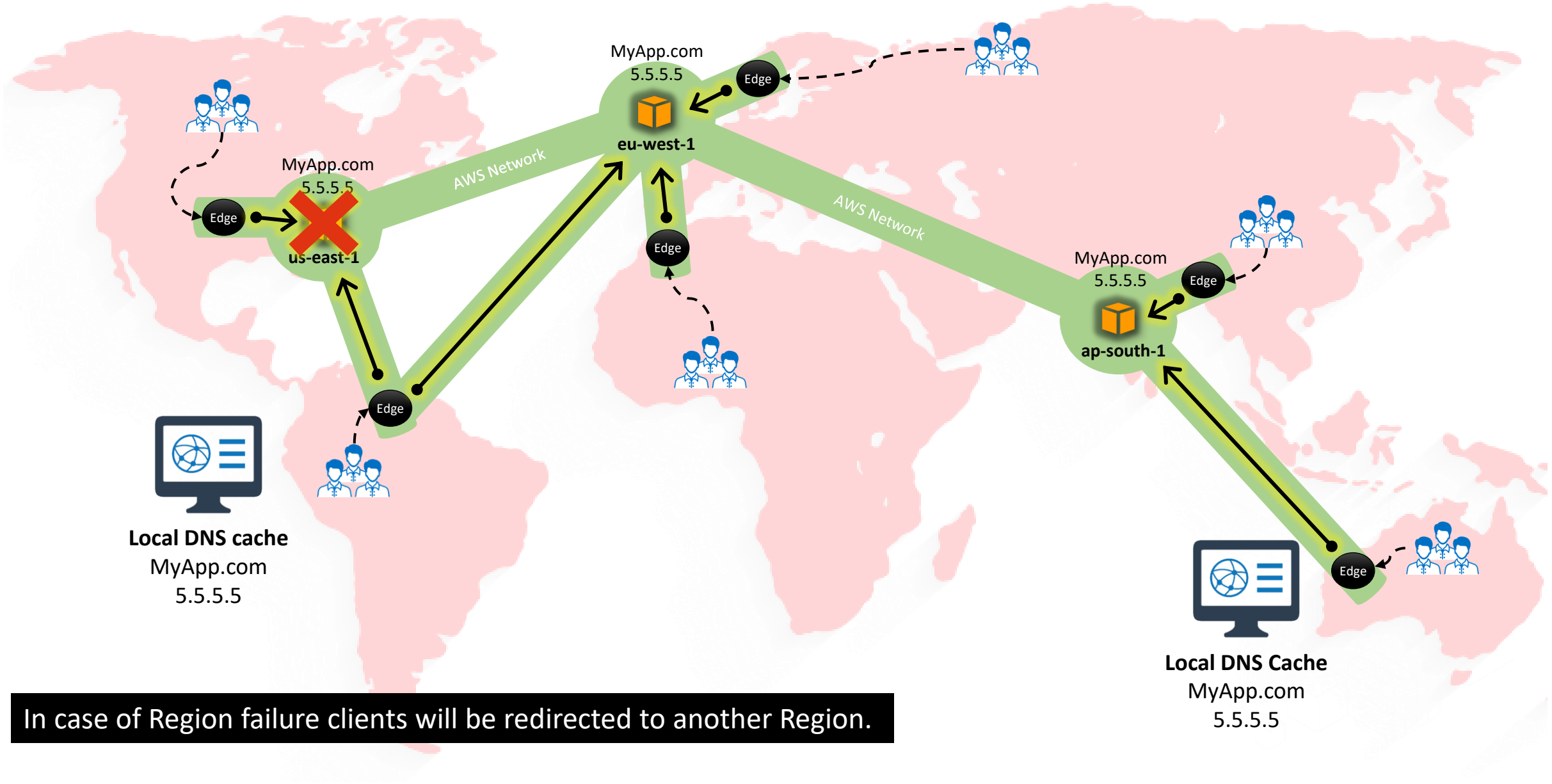
MyApp.com gets the same Anycast IP address in each Region.

A Multi-Region Application with AWS Global Accelerator – Edge Failure



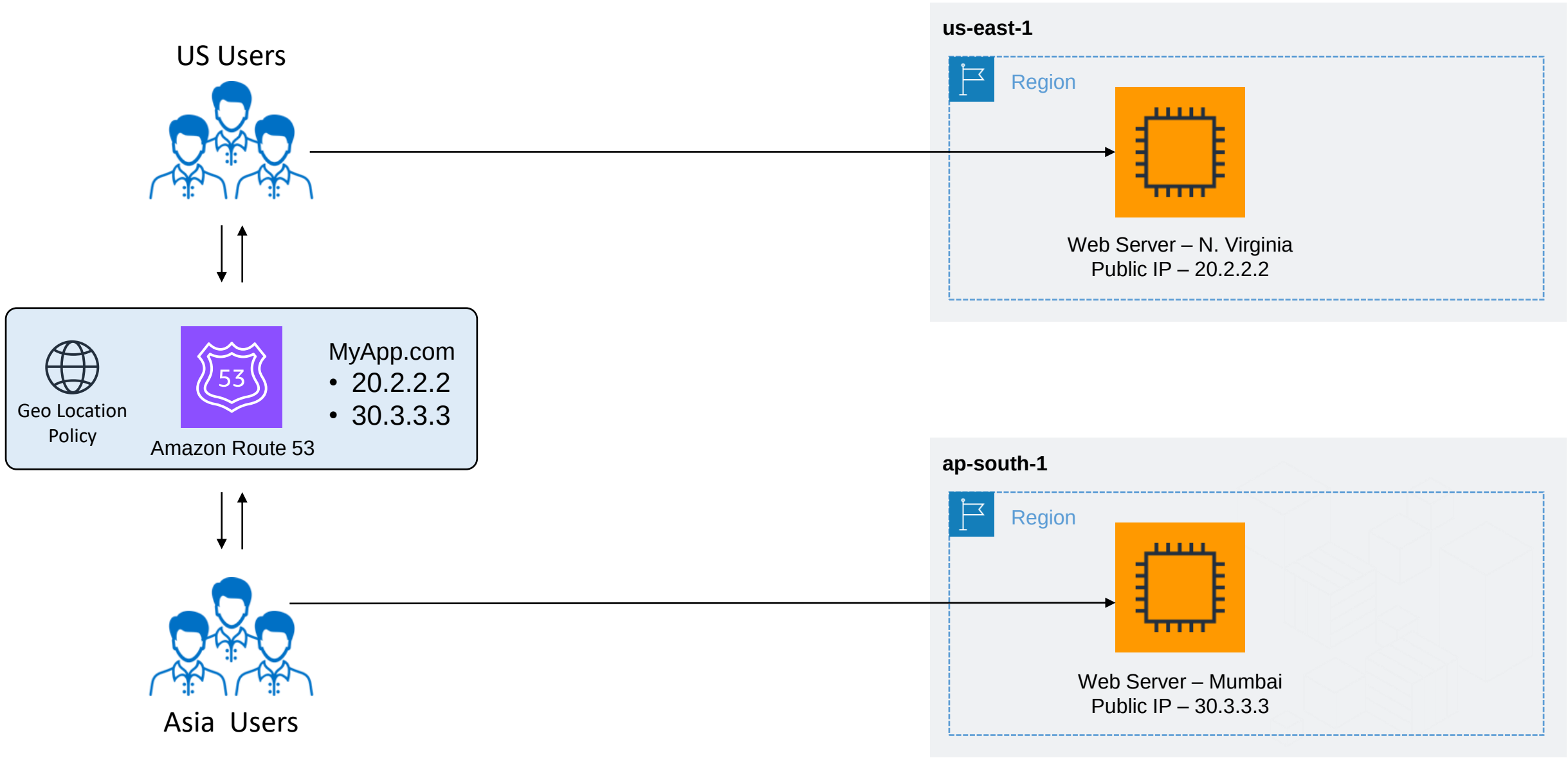
In case of Edge Location failure clients will be redirected to another Edge Location.

A Multi-Region Application with AWS Global Accelerator – Region Failure

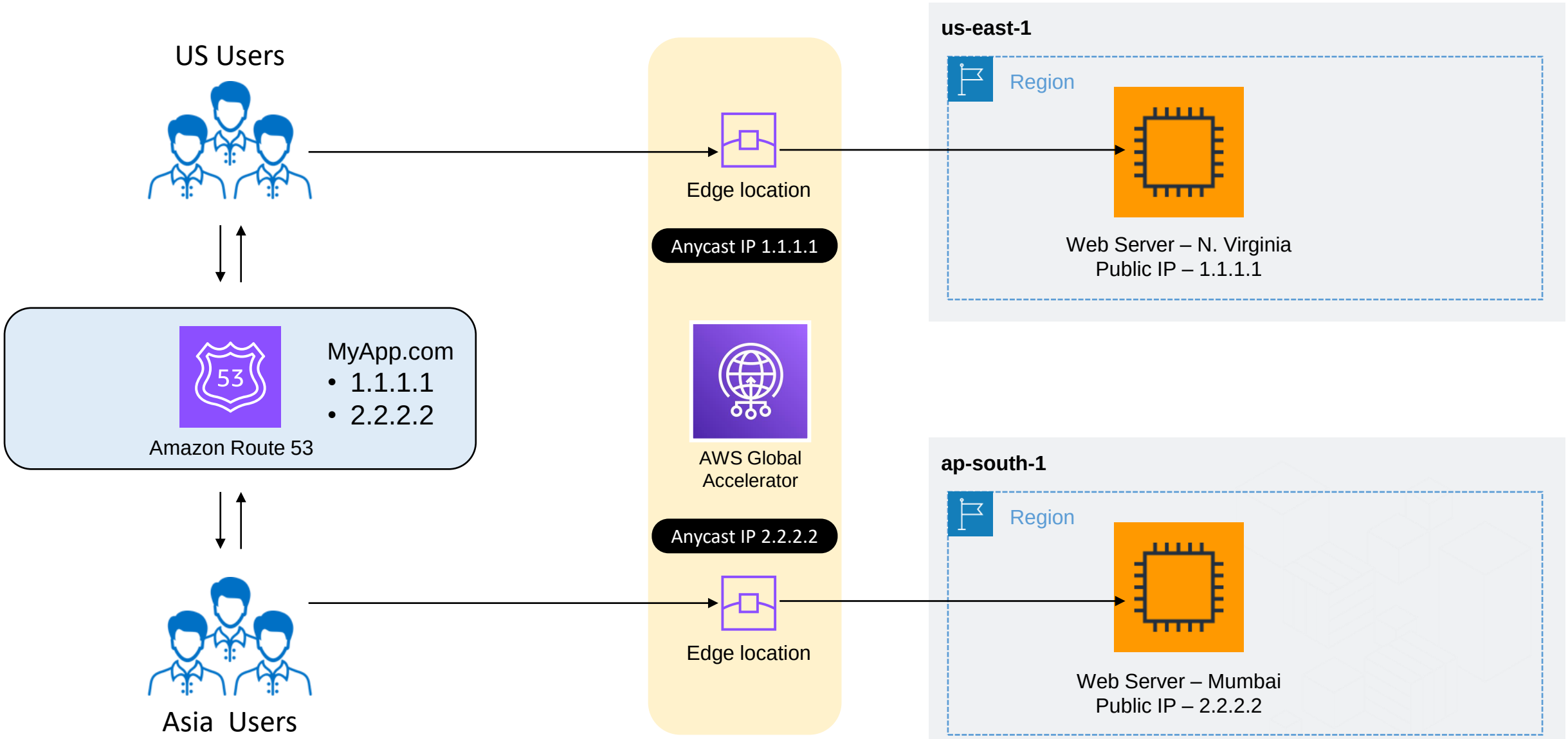


In case of Region failure clients will be redirected to another Region.

Demo – Without Global Accelerator

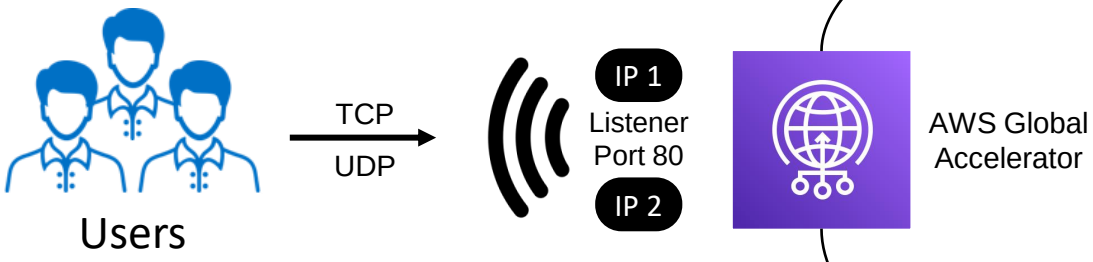


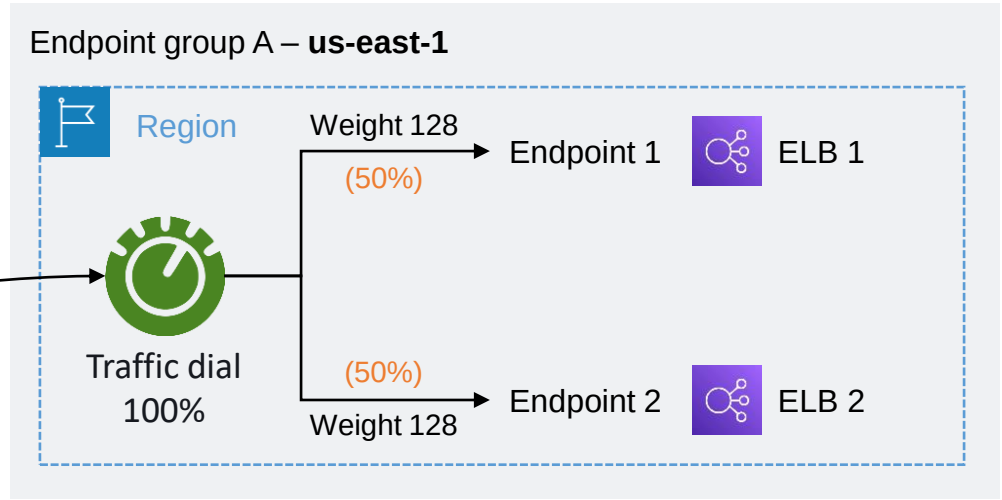
Demo – With Global Accelerator

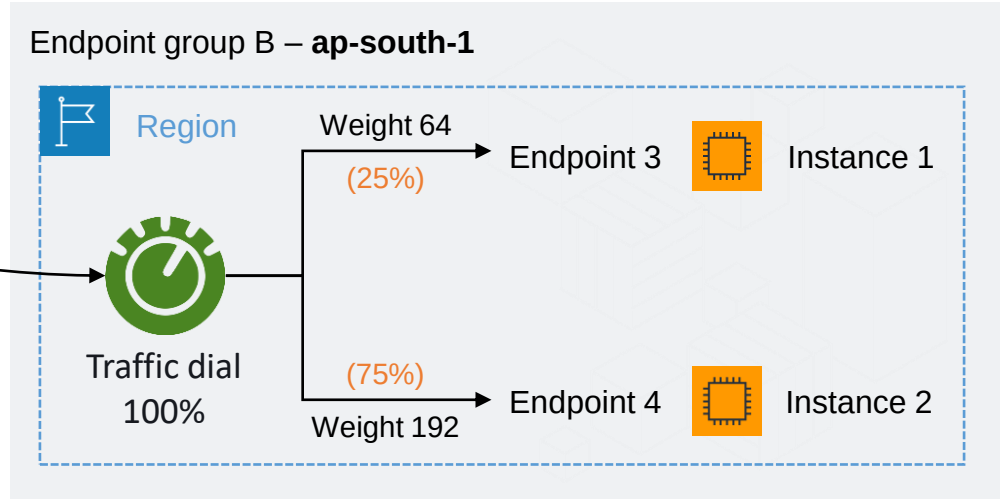


Traffic Distribution

- The **traffic dial** lets you cut off a percentage of **traffic**—or all **traffic**—to the group, by "**dialing** down" **traffic** that the **accelerator** has already directed to it based on other factors, such as proximity.
- You use weights, on the other hand, to set values for individual endpoints within an endpoint group.



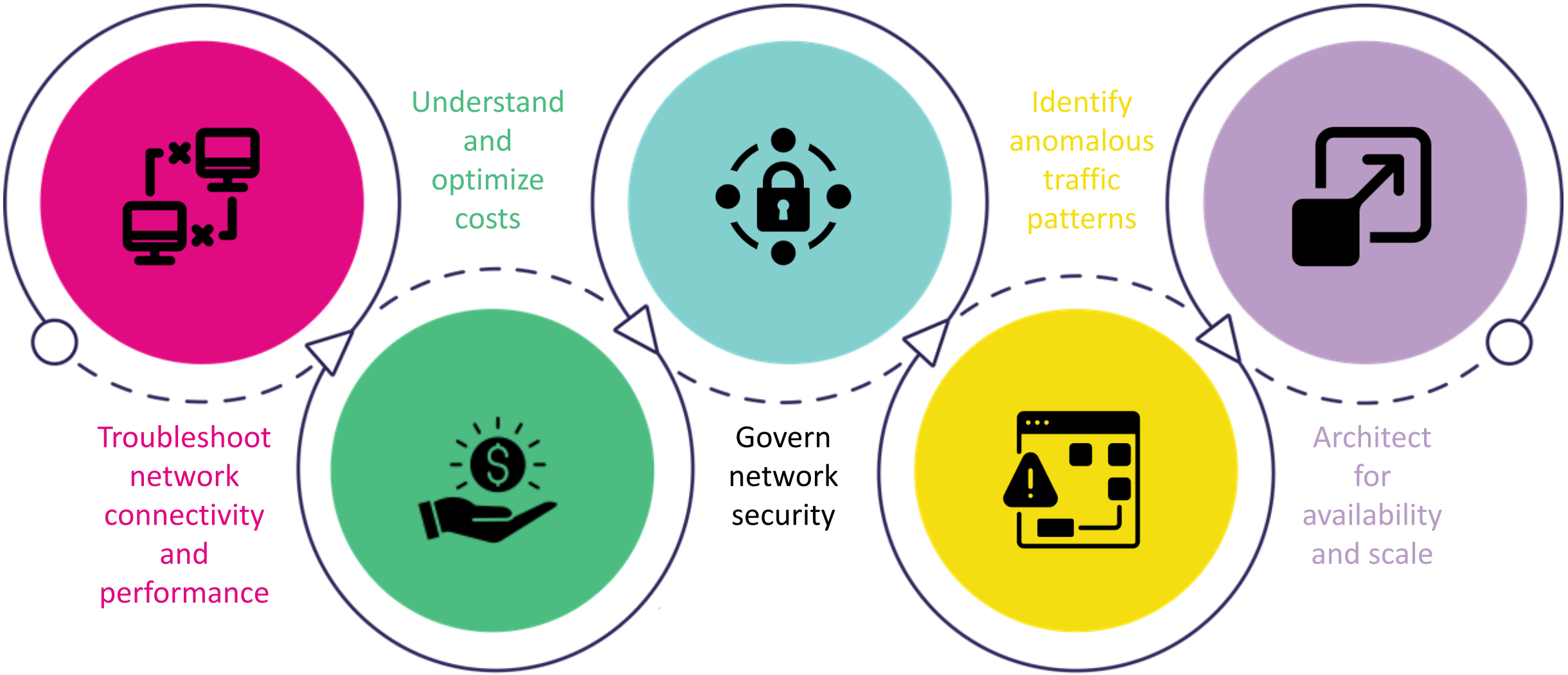




	Traffic Dial Values	Weight Values
Default	100%	128
Min	0%	0
Max	100%	255

Network Observability

Why observe your network?



Overview of network observability

Collect

- Metrics
- Logs

Monitor

- Alarms
- Flow Logs
- CloudWatch dashboards
- CloudWatch metric filter

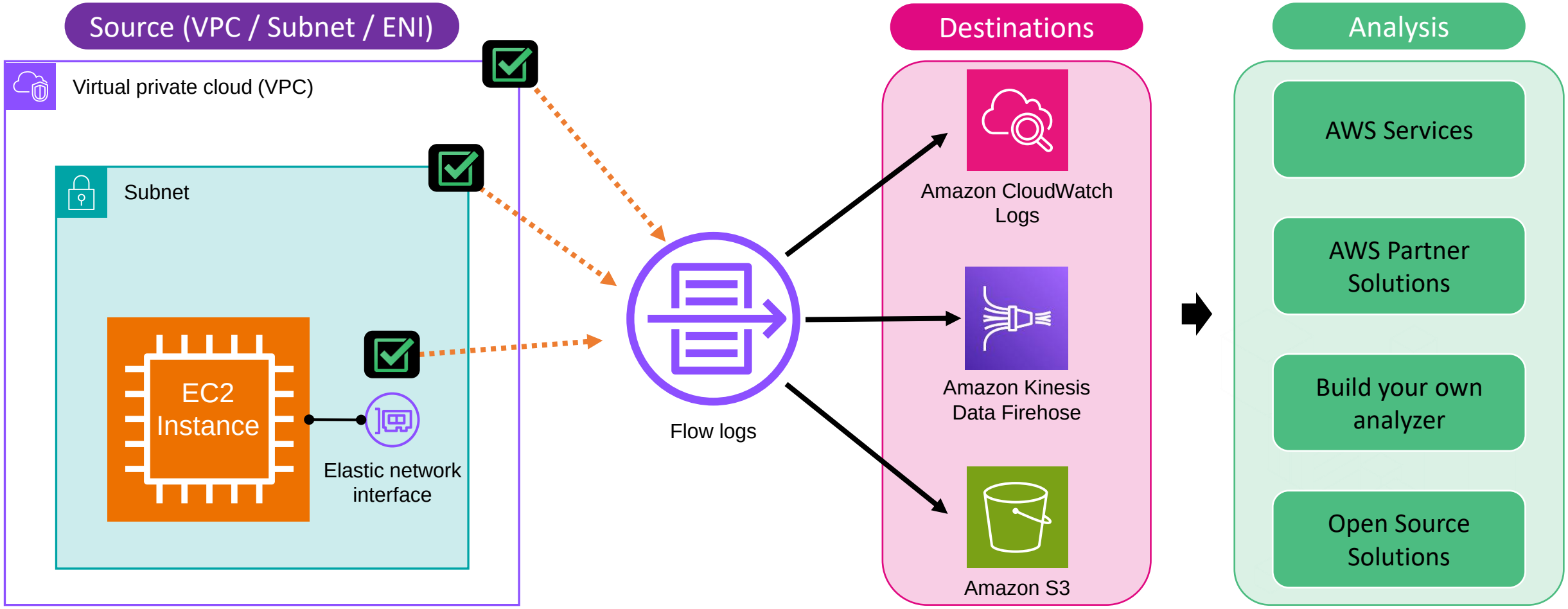
Analyze

- Traffic Mirroring
- Reachability Analyzer
- Amazon CloudWatch Contributor Insights
- CloudWatch Log Insights
- Network Access Analyzer
- Third-party solution

VPC Flow Logs

VPC Flow Logs

- VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC.



Key Facts

Doesn't affect performance

Flow log data is collected outside of the path of your network traffic, and therefore does not affect network throughput or latency.

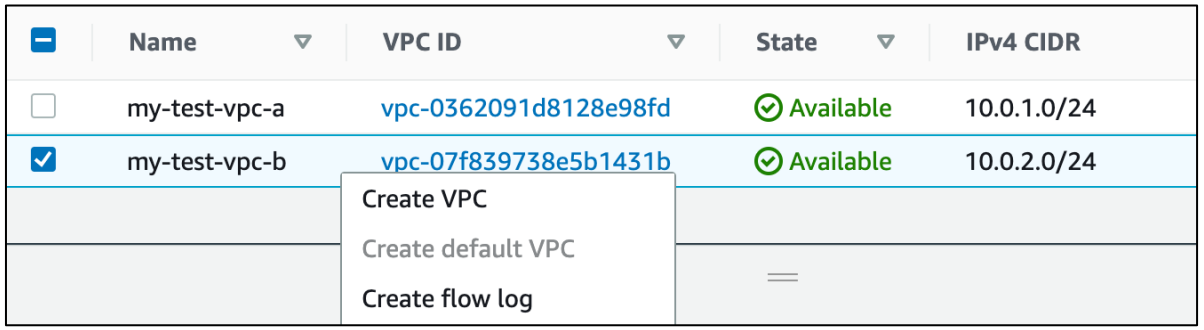
Not real-time

After you create a flow log, it can take several minutes to begin collecting and publishing data to the chosen destinations. Flow logs do not capture real-time log streams.

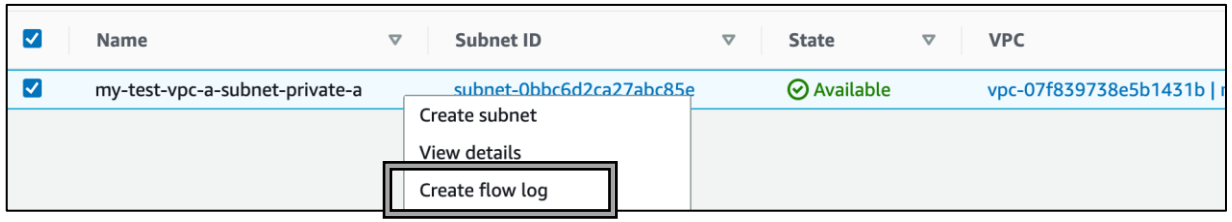
Choice of Format

When you create a flow log, you can use the default format for the flow log record, or you can specify a custom format.

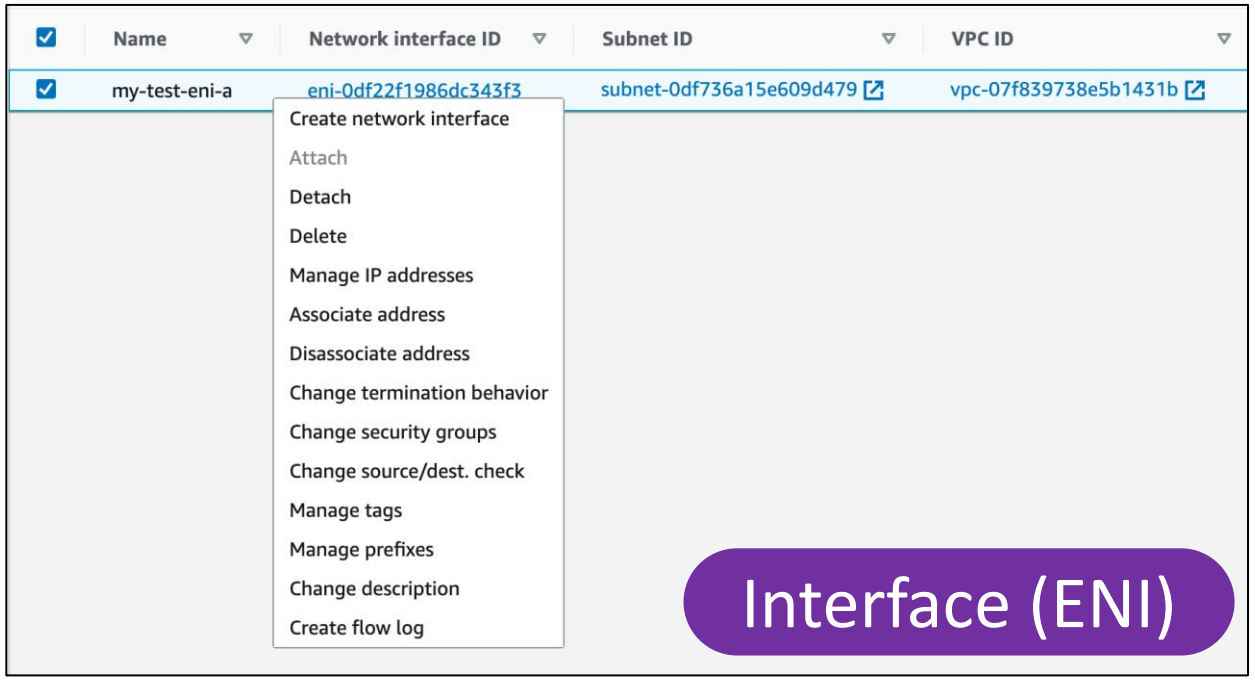
Capturing Flow logs



VPC

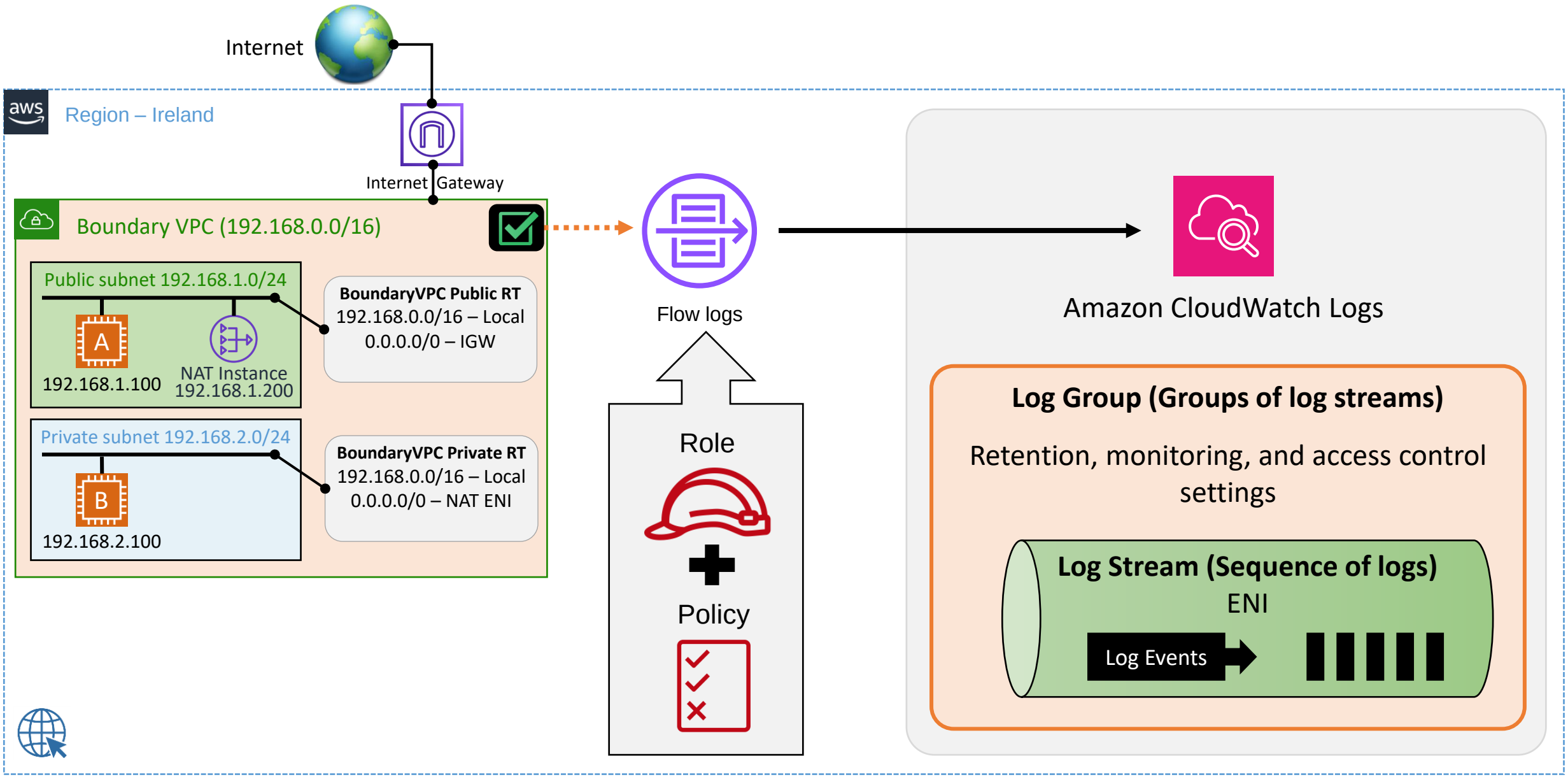


Subnet



Interface (ENI)

Demo Environment



Flow Log Fields

Default flow log fields

Log record format

Specify the fields to include in the flow log record.

- (•) AWS default format
- ( ) Custom format

Format preview

```
${version} ${account-id} ${interface-id} ${srcaddr} ${dstaddr} ${srcport} ${dstport}
${protocol} ${packets} ${bytes} ${start} ${end} ${action} ${log-status}
```

Custom flow log fields

Log record format

Specify the fields to include in the flow log record.

- ( ) AWS default format
- (•) Custom format

Log format

Specify the fields to include in the flow log record.

Select an attribute...

- [ ] account-id
- [ ] action
- [ ] az-id
- [ ] bytes
- [ ] dstaddr
- [ ] dstport
- [ ] end
- [ ] flow-direction
- [ ] instance-id
- [ ] interface-id
- [ ] log-status
- [ ] packets
- [ ] pkt-dst-aws-service
- [ ] pkt-dstaddr

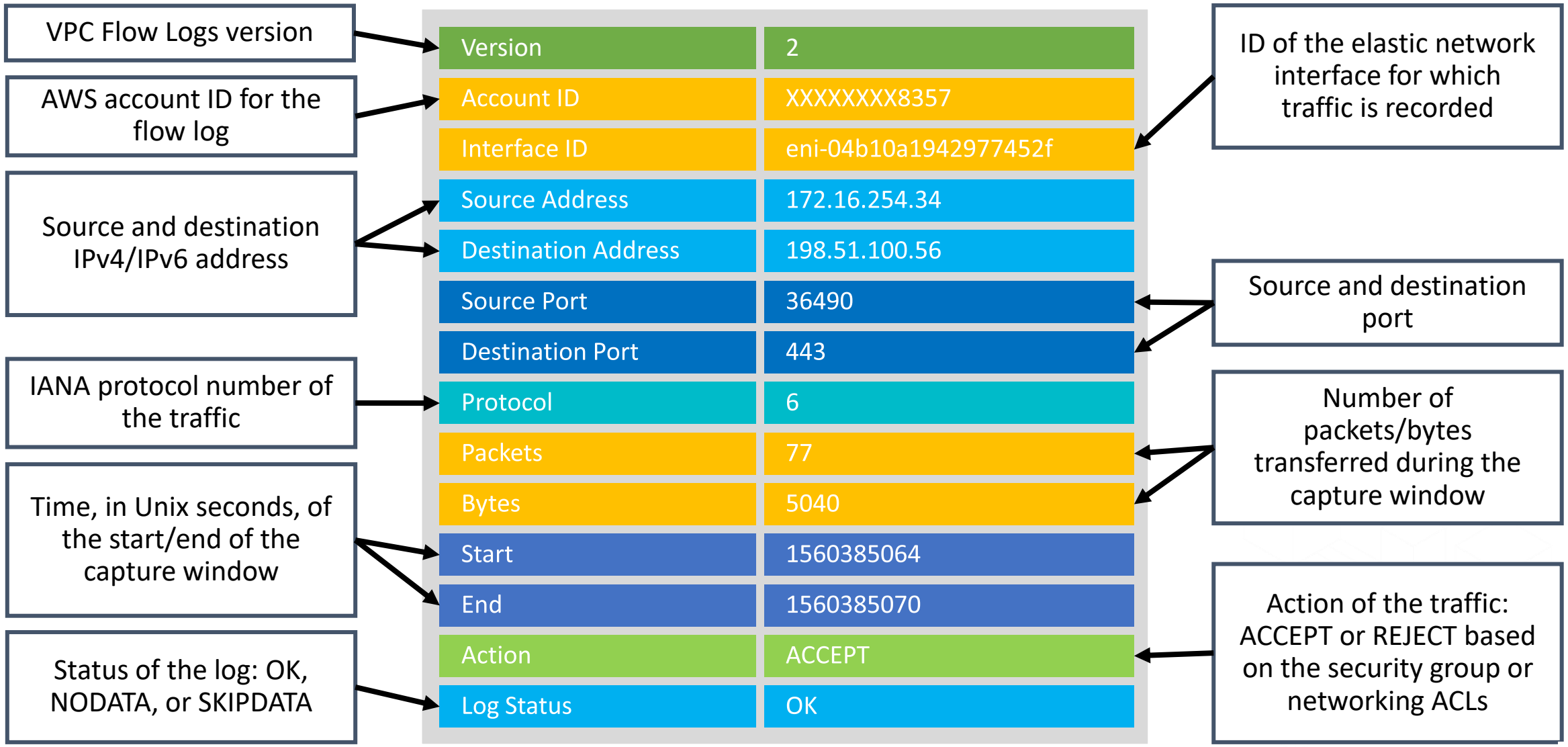
Additional Flow Log Fields that can be captured with a custom format:

VPC Flow Log Fields	Version
VPC id	3
Subnet id	3
Instance id	3
TCP Flags (e.g. SYN, ACK, FIN)	3
Type (IPv4, IPv6)	3
Packet Source Address	3
Packet Destination Address	3

VPC Flow Log Fields	Version
Region	4
Availability Zone ID	4
Sublocation-type	4
Sublocation-id	4

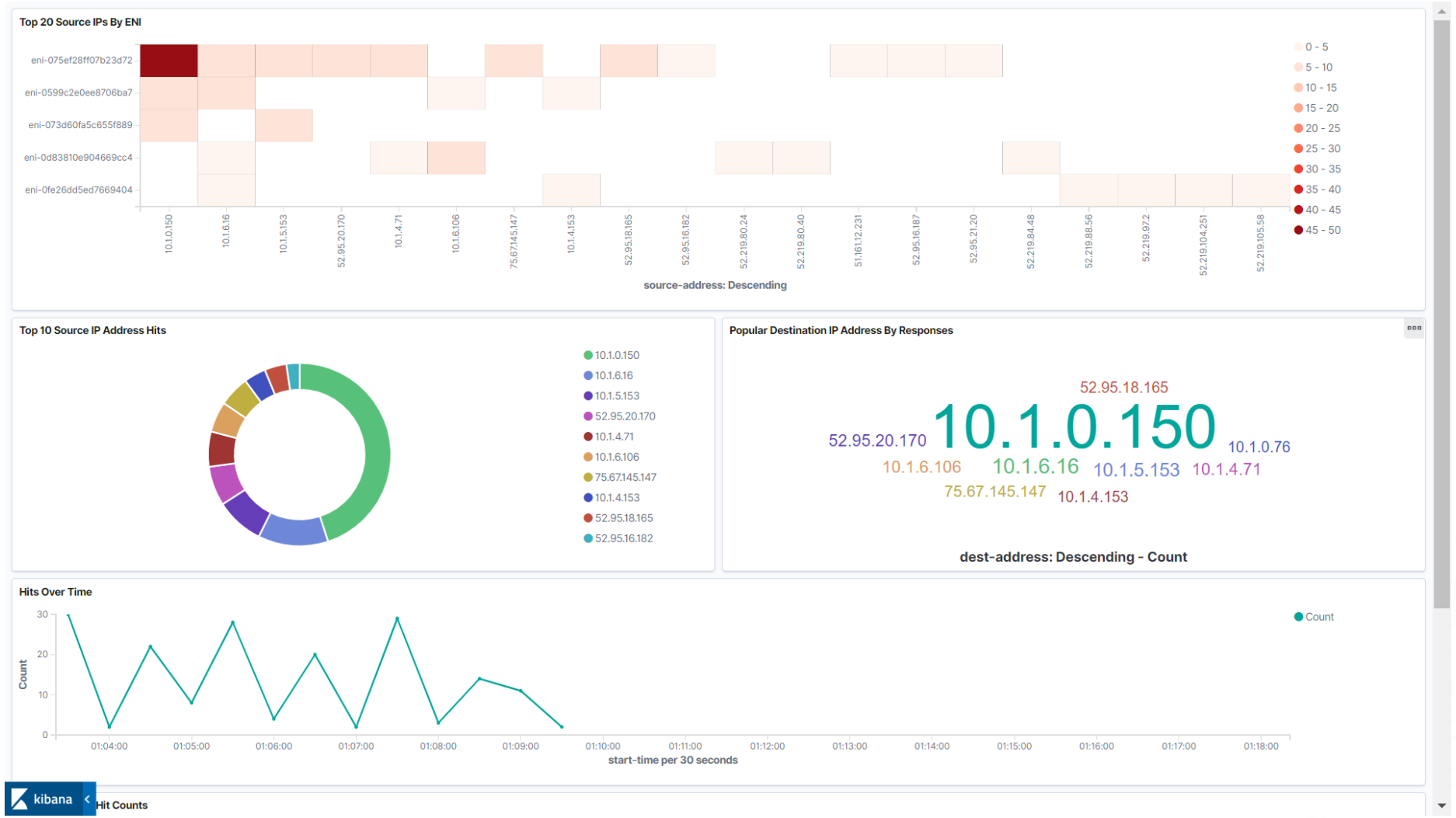
VPC Flow Log Fields	Version
Pkt-src-aws-service	5
Pkt-dst-aws-service	5
Flow-direction	5
Traffic-path	5

Anatomy of a Flow Log



VPC Flow logs analysis using Amazon Elasticsearch service

- https://vpc-flowlogs.aesworkshops.com/



VPC Traffic Mirroring

VPC Traffic Mirroring – Use-cases

Content Inspection

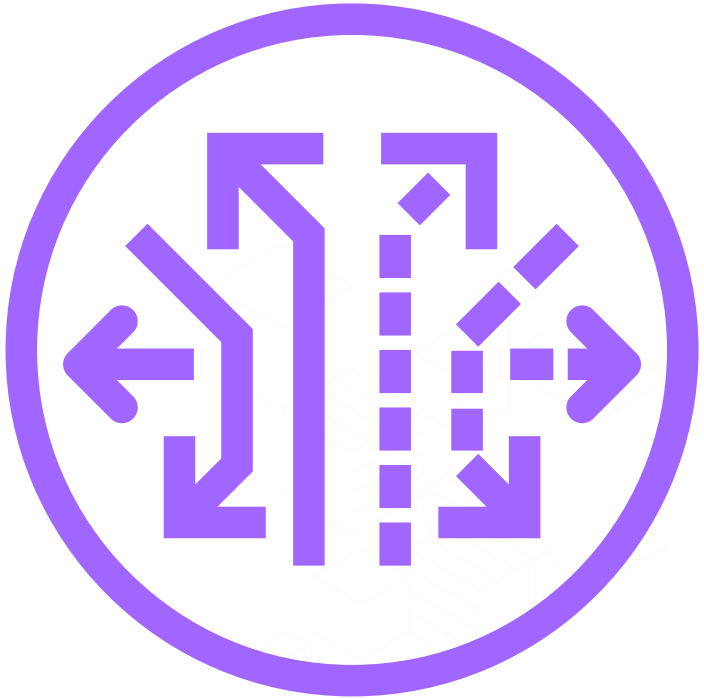
Threat Monitoring

Troubleshooting

- Traffic Mirroring is an Amazon VPC feature that you can use to copy network traffic from an elastic network interface (ENI).
- You can then send the traffic to out-of-band security and monitoring appliances

VPC Traffic Mirroring

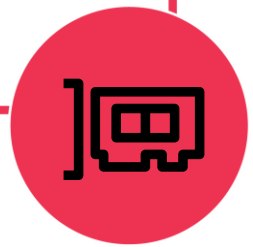
- Amazon VPC traffic mirroring replicates network traffic to and from an Amazon EC2 instance and forward it to security and monitoring appliances.
- These appliances can be deployed on an individual EC2 instance or a fleet of instances behind a Network Load Balancer (NLB) with User Datagram Protocol (UDP) listener.
- Traffic mirroring supports network packet captures at the Elastic Network Interface (ENI) level for EC2 instances.
- Customers can either use open source tools or choose from a wide-range of monitoring solution available on AWS Marketplace.



Traffic Mirroring concepts

Source

The network interface to monitor



Target

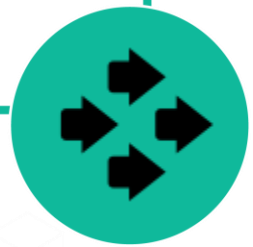
The destination for mirrored traffic

Filter

A set of rules that defines which traffic is mirrored

Session

Establishes a relationship between a source, a filter, and a target



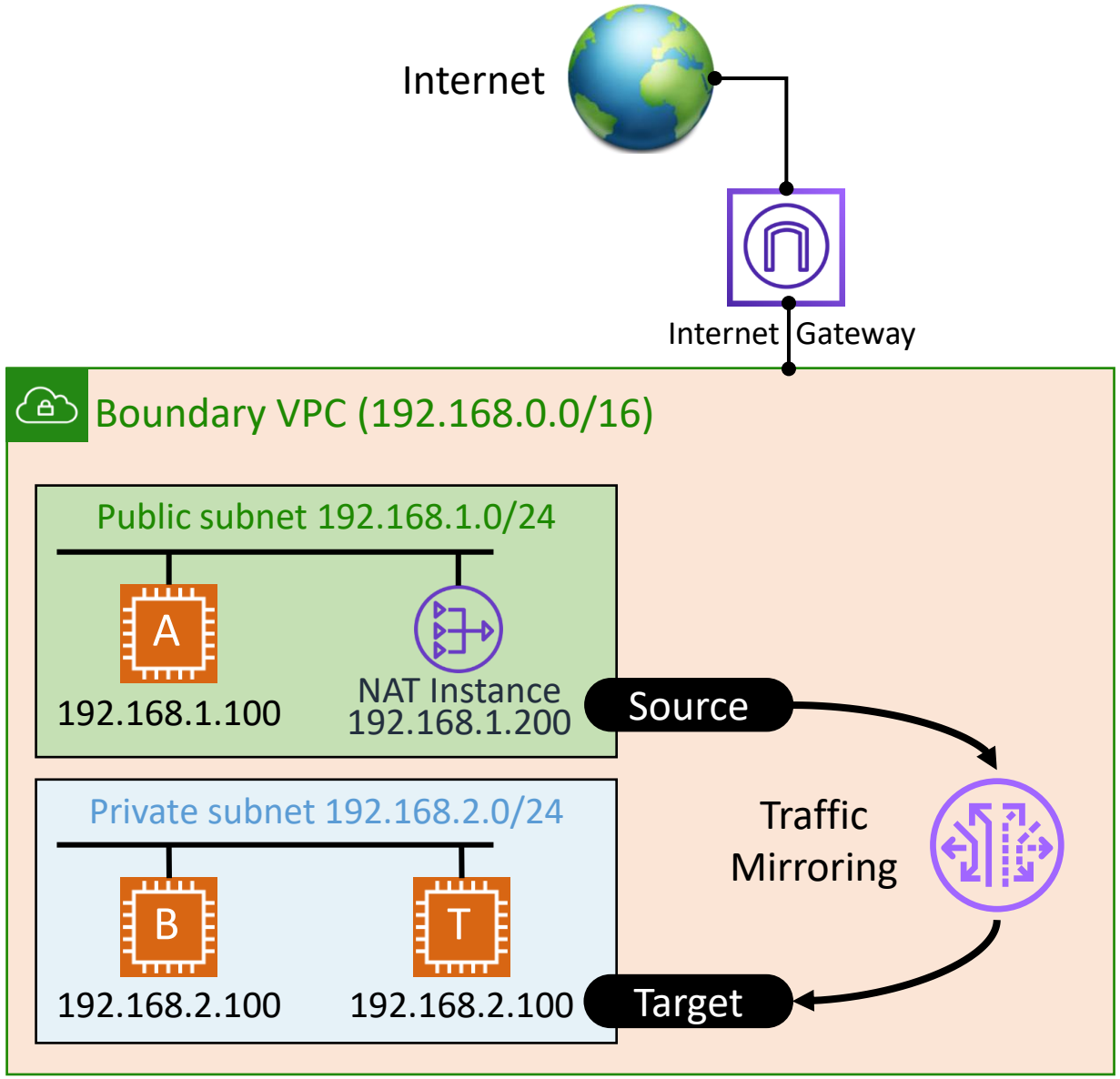
- Mirrored traffic is encapsulated with a VXLAN header.
- Virtual Extensible LAN (VXLAN) is a network virtualization technology that attempts to address the scalability problems associated with large cloud computing deployments.

Setting up traffic mirroring

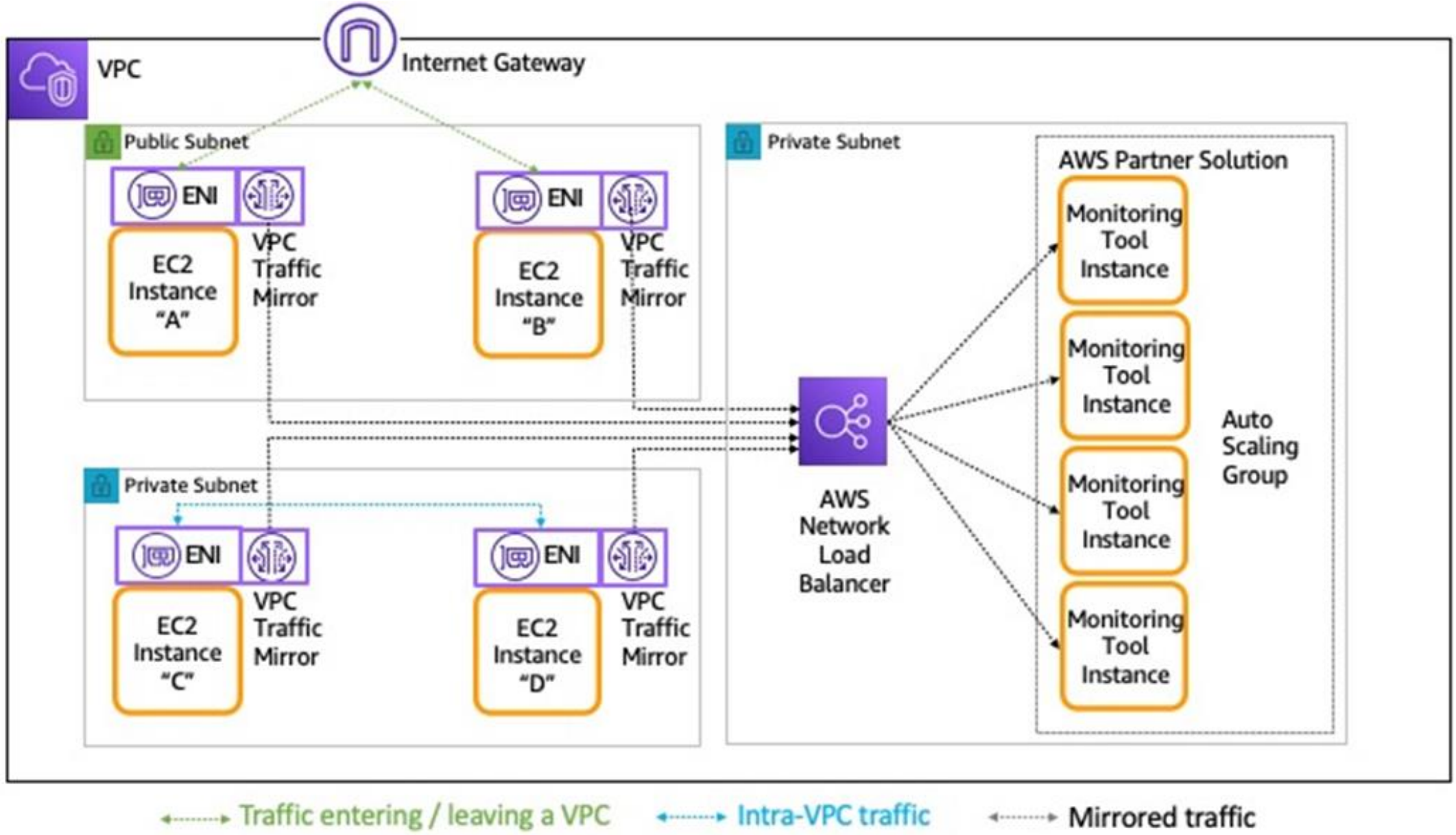
1. Creating the mirror target
2. Creating the mirror filter
3. Setting up the mirror session

Testing the traffic mirroring

- sudo tcpdump -nni eth1



NLB as Target



Comparison

VPC Flow Logs

Captures information about the IP traffic in your VPC

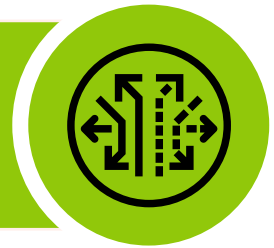
Can be enabled for:
- VPC, Subnet or ENI

Target:
- CW Logs, Kinesis Firehose, Amazon S3

Captures:
- Header of the packet, Metadata

Use-cases: Troubleshoot connectivity and security issues

VPC Traffic Mirroring



Streams a copy of the network traffic from an ENI to a target

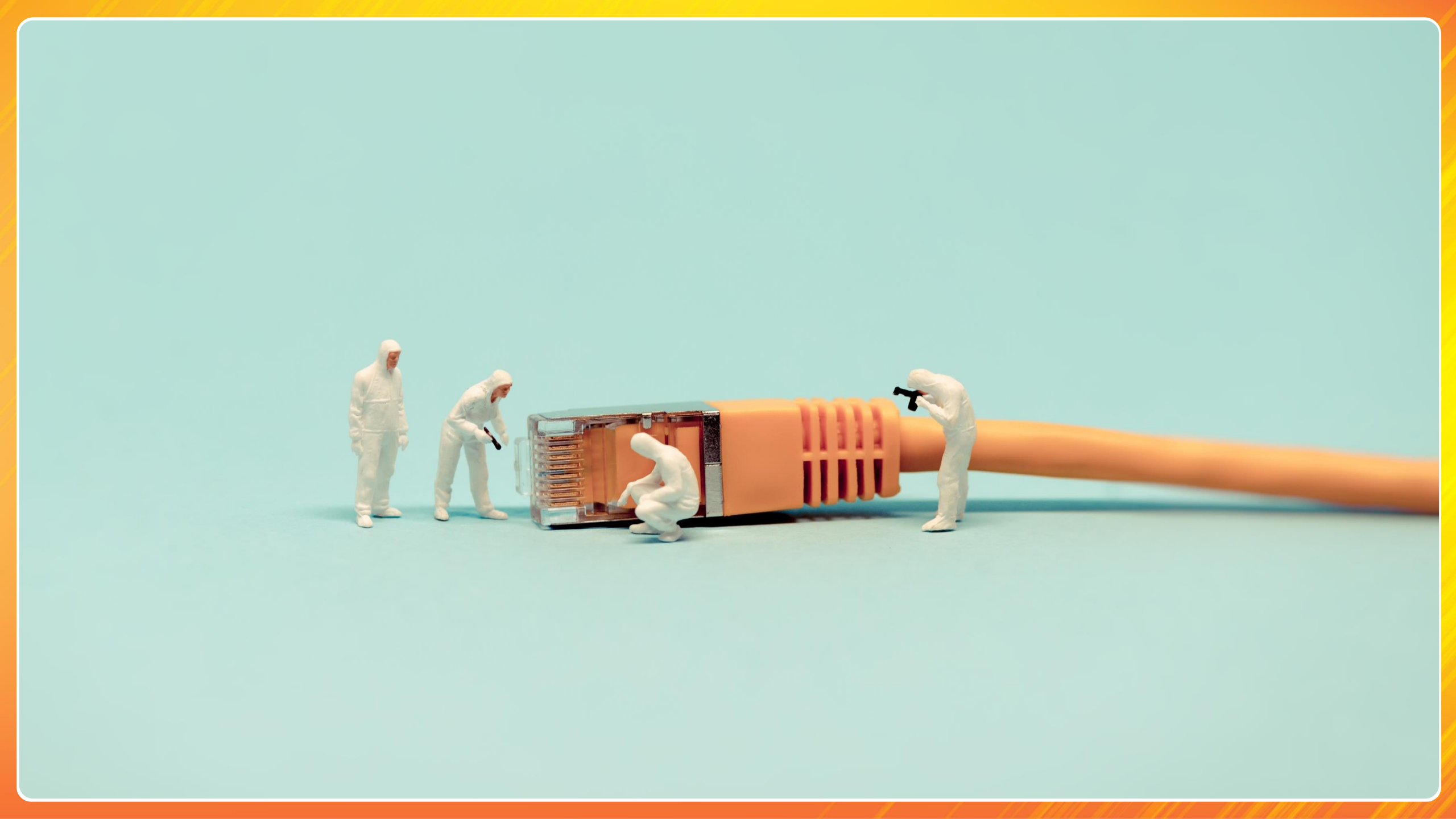
Can be captured from:
- ENI

Target:
- ENI of an instance, NLB, GWLB

Mirros:
- Actual packet (including payload)

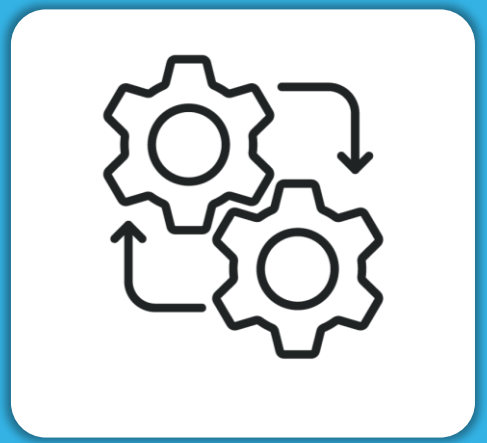
Use-cases: Content inspection, Threat monitoring, Network troubleshooting

Reachability Analyzer

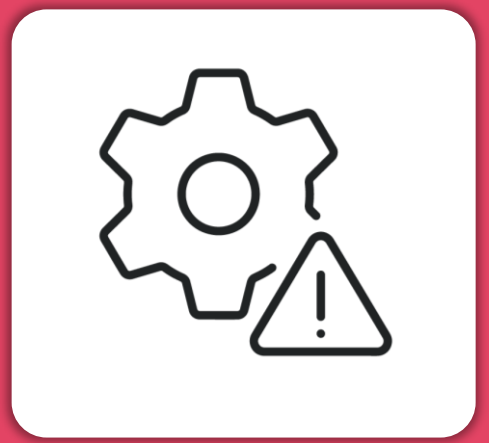


Reachability Analyzer

A configuration analysis tool



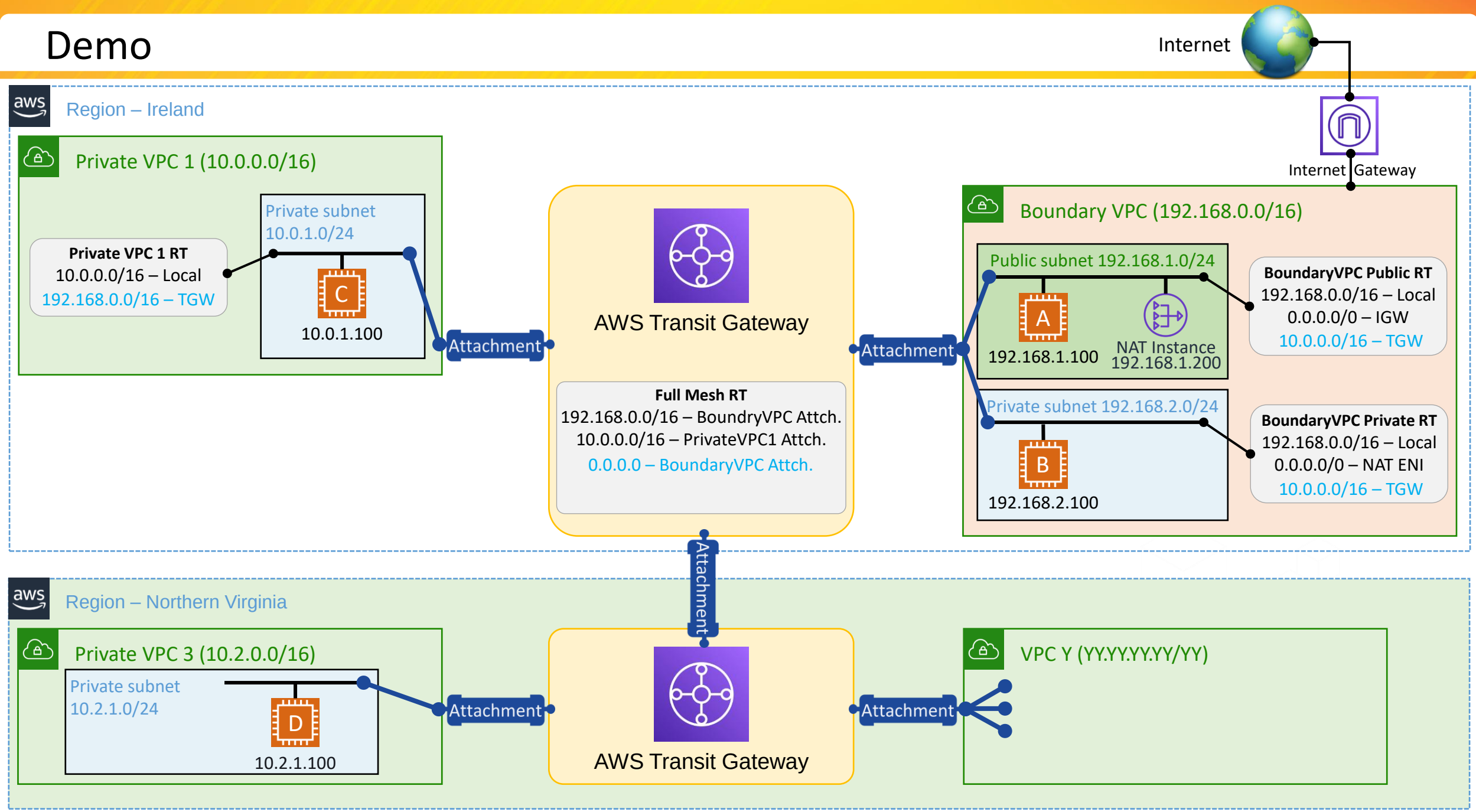
Verifies connectivity between two components



Also provides explanation of the issue

Can be used for automated validation

Demo


Internet
Internet Gateway
Region – Ireland
Private VPC 1 (10.0.0.0/16)
Private subnet
10.0.1.0/24
Private VPC 1 RT
10.0.0.0/16 – Local
192.168.0.0/16 – TGW
C
10.0.1.100
Attachment
AWS Transit Gateway
Full Mesh RT
192.168.0.0/16 – BoundryVPC Attch.
10.0.0.0/16 – PrivateVPC1 Attch.
0.0.0.0 – BoundaryVPC Attch.
Attachment
Boundary VPC (192.168.0.0/16)
Public subnet 192.168.1.0/24
A
192.168.1.100
NAT Instance
192.168.1.200
BoundaryVPC Public RT
192.168.0.0/16 – Local
0.0.0.0/0 – IGW
10.0.0.0/16 – TGW
Private subnet 192.168.2.0/24
B
192.168.2.100
BoundaryVPC Private RT
192.168.0.0/16 – Local
0.0.0.0/0 – NAT ENI
10.0.0.0/16 – TGW
Attachment
Region – Northern Virginia
Private VPC 3 (10.2.0.0/16)
Private subnet
10.2.1.0/24
D
10.2.1.100
Attachment
AWS Transit Gateway
Attachment
VPC Y (YY.YY.YY.YY/YY)