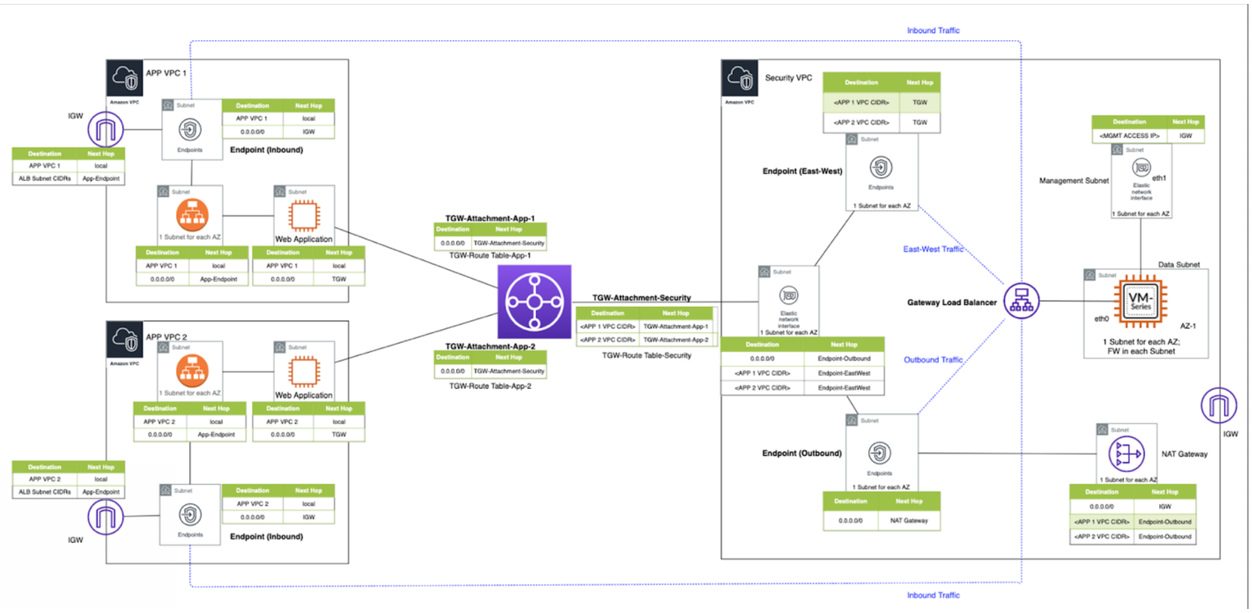
Packet Flow in the AWS Gateway Load Balancer - Inbound
By Patrick GlynnMgr, Consulting Engineering
Published on February 14, 2021

Introduction

With the introduction of the Gateway Load Balancer (GWLB) in mid-November 2020, AWS provided its customers with any port, load-balancing router. Prior to that, Azure and GCP were the only public clouds that had such a construct. Customers use these to provide a security layer that is scalable, resilient, and adaptable. In the AWS implementation, endpoints are an integral part of the solution but are not a new concept in AWS. They connect elastic network interfaces (ENIs) to targets (e.g. GWLB) via "worm holes" in the fabric and and have been used with network load balancers (NLBs) for some time. These worm holes in the fabric bypass the usual routing constructs and can perforce result in some difficulty when troubleshooting. In this blog post, we will trace the flow of a request originating from a client on the internet to a server in the AWS infrastructure. The infrastructure was deployed using the following TerraForm template:

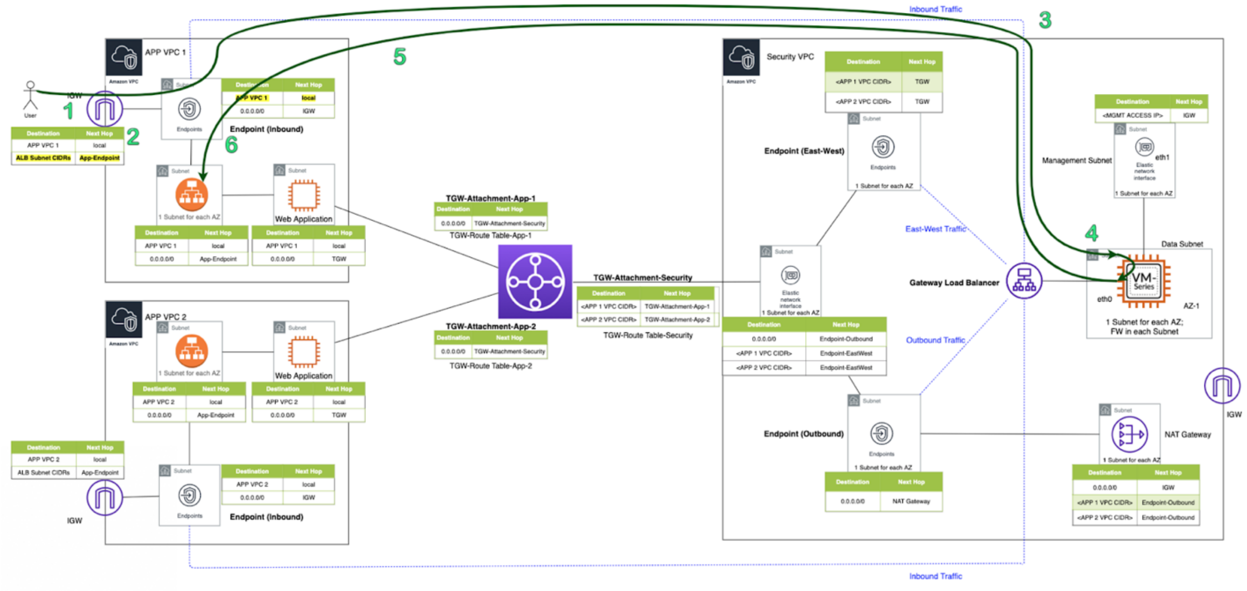
https://github.com/wwce/terraform/tree/master/aws/GWLB-Demo

and follows current best practices regarding architecture:



This architecture also supports east-west and outbound traffic flows, although they will be treated separately in subsequent blog posts. Today, we will focus on the following request flow:

Packet Flow in the AWS Gateway Load Balancer - Inbound
By Patrick GlynnMgr, Consulting Engineering
Published on February 14, 2021



Destination	Next Hop
APP VPC 1	local
ALB Subnet CIDRs	App-Endpoint

Destination	Next Hop
APP VPC 1	local
0.0.0.0/0	IGW

Destination	Next Hop
APP VPC 1	local
0.0.0.0/0	App-Endpoint

Destination	Next Hop
APP VPC 1	local
0.0.0.0/0	TGW

Destination	Next Hop
0.0.0.0/0	TGW-Attachment-Security

Destination	Next Hop
0.0.0.0/0	TGW-Attachment-Security

Destination	Next Hop
APP VPC 2	local
0.0.0.0/0	App-Endpoint

Destination	Next Hop
APP VPC 2	local
0.0.0.0/0	TGW

Destination	Next Hop
APP VPC 2	local
ALB Subnet CIDRs	App-Endpoint

Destination	Next Hop
APP VPC 2	local
0.0.0.0/0	IGW

Destination	Next Hop
<APP 1 VPC CIDR>	TGW-Attachment-App-1
<APP 2 VPC CIDR>	TGW-Attachment-App-2

Destination	Next Hop
<APP 1 VPC CIDR>	TGW
<APP 2 VPC CIDR>	TGW

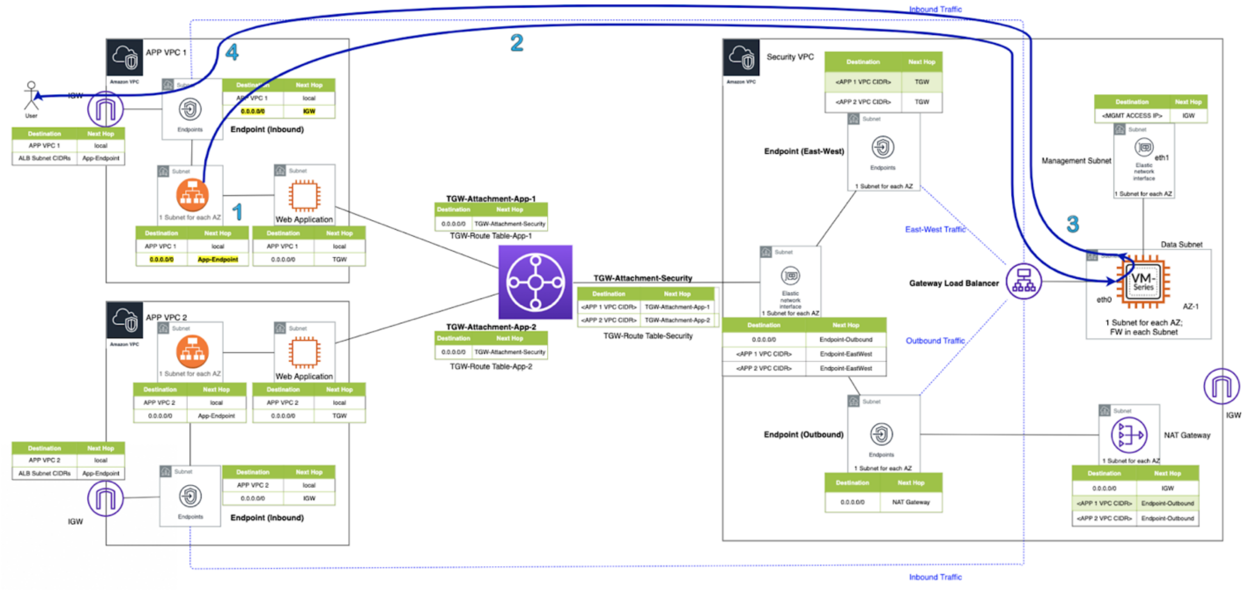
Destination	Next Hop
0.0.0.0/0	Endpoint-Outbound
<APP 1 VPC CIDR>	Endpoint-EastWest
<APP 2 VPC CIDR>	Endpoint-EastWest

Destination	Next Hop
0.0.0.0/0	NAT Gateway

Destination	Next Hop
<MGMT ACCESS IP>	IGW

Destination	Next Hop
0.0.0.0/0	IGW
<APP 1 VPC CIDR>	Endpoint-Outbound
<APP 2 VPC CIDR>	Endpoint-Outbound

And the corresponding response flow:



Destination	Next Hop
APP VPC 1	local
ALB Subnet CIDRs	App-Endpoint

Destination	Next Hop
APP VPC 1	local
0.0.0.0/0	IGW

Destination	Next Hop
APP VPC 1	local
0.0.0.0/0	App-Endpoint

Destination	Next Hop
APP VPC 1	local
0.0.0.0/0	TGW

Destination	Next Hop
0.0.0.0/0	TGW-Attachment-Security

Destination	Next Hop
0.0.0.0/0	TGW-Attachment-Security

Destination	Next Hop
APP VPC 2	local
0.0.0.0/0	App-Endpoint

Destination	Next Hop
APP VPC 2	local
0.0.0.0/0	TGW

Destination	Next Hop
APP VPC 2	local
ALB Subnet CIDRs	App-Endpoint

Destination	Next Hop
APP VPC 2	local
0.0.0.0/0	IGW

Destination	Next Hop
<APP 1 VPC CIDR>	TGW-Attachment-App-1
<APP 2 VPC CIDR>	TGW-Attachment-App-2

Destination	Next Hop
<APP 1 VPC CIDR>	TGW
<APP 2 VPC CIDR>	TGW

Destination	Next Hop
0.0.0.0/0	Endpoint-Outbound
<APP 1 VPC CIDR>	Endpoint-EastWest
<APP 2 VPC CIDR>	Endpoint-EastWest

Destination	Next Hop
0.0.0.0/0	NAT Gateway

Destination	Next Hop
<MGMT ACCESS IP>	IGW

Destination	Next Hop
0.0.0.0/0	IGW
<APP 1 VPC CIDR>	Endpoint-Outbound
<APP 2 VPC CIDR>	Endpoint-Outbound

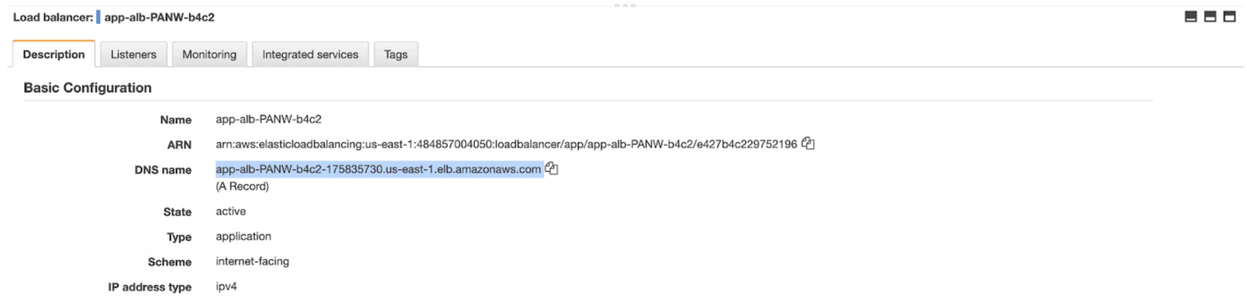
Note that AWS assigns unique resource identifiers to each resource in the environment. Examples include tgw-attach-0b86ac38ab82dfff9 or subnet-0e1119f6fc333ea6d. Every resource created is assigned one of these unique identifiers. This means that although the template creates the environment using identical resources, the individual resource identifiers will be different.

Packet Flow in the AWS Gateway Load Balancer - Inbound
By Patrick GlynnMgr, Consulting Engineering
Published on February 14, 2021

N.B. - Routes to the 104.219.136.0/21 and 107.64.0.0/10 subnets pointing to the internet gateway (IGW) in the APP VPCs are the author's primary/secondary ISP subnets and were added post-deployment to facilitate direct access to the hosts in the VPCs for troubleshooting. They do not exist in the publicly-available templates and can be ignored.

Request Step 1 - Can We Talk?

The process begins when a user wishes to connect to our web server. The FQDN (or Alias or CNAME) of the application load balancer (ALB) is resolved to the relevant public IP address and the browser initiates the connection.



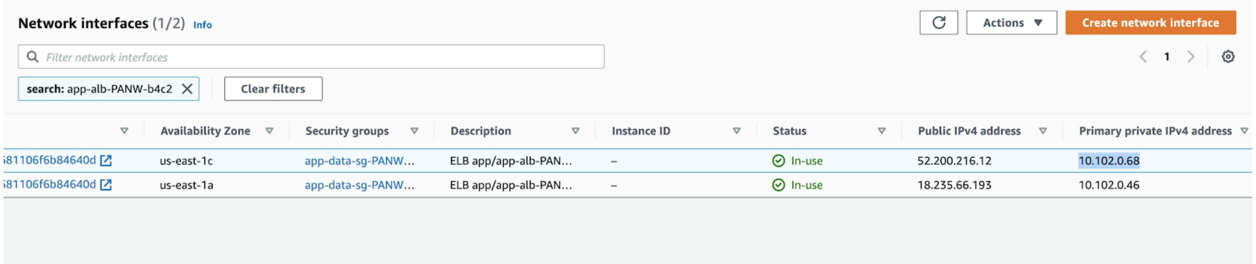
Load balancer: app-alb-PANW-b4c2

Basic Configuration

Name app-alb-PANW-b4c2
ARN arn:aws:elasticloadbalancing:us-east-1:484857004050:loadbalancer/app/app-alb-PANW-b4c2/e427b4c229752196
DNS name app-alb-PANW-b4c2-175835730.us-east-1.elb.amazonaws.com
(A Record)
State active
Type application
Scheme internet-facing
IP address type ipv4

Request Step 2 - Internet Gateway (IGW)

The request is arrives at the IGW, which translates the public IP address of the load balancer (LB) to the corresponding private IP address. Although it is possible to use the AWS CLI to see this mapping, searching for the LB name in the Network Interfaces section of the GUI is somewhat easier:



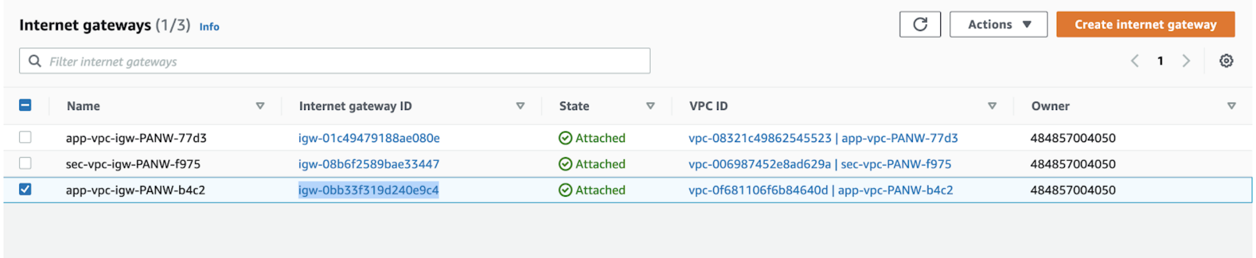
Network interfaces (1/2) Info

search: app-alb-PANW-b4c2

	Availability Zone	Security groups	Description	Instance ID	Status	Public IPv4 address	Primary private IPv4 address
81106f6b84640d	us-east-1c	app-data-sg-PANW...	ELB app/app-alb-PAN...	–	In-use	52.200.216.12	10.102.0.68
81106f6b84640d	us-east-1a	app-data-sg-PANW...	ELB app/app-alb-PAN...	–	In-use	18.235.66.193	10.102.0.46

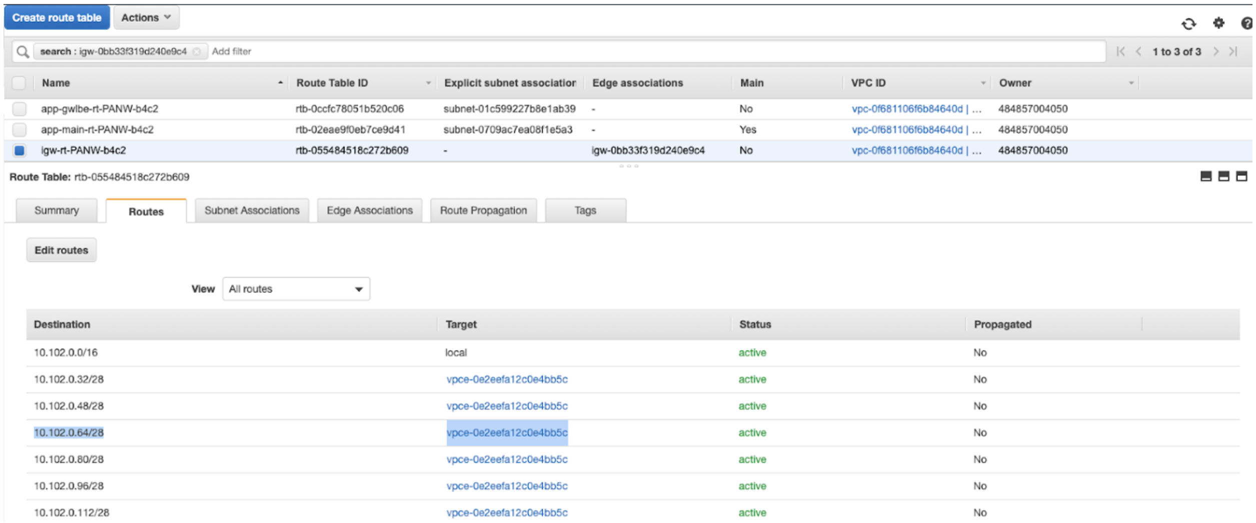
There may be multiple IP address combinations present. This is because it is possible (and best practice) to use multiple availability zones for resiliency.

Once the address translation is complete, the IGW uses ingress routing to send the request to the local GWLB endpoint. The easiest way to see this is to copy the Internet gateway ID from the interface:



	Name	Internet gateway ID	State	VPC ID	Owner
□	app-vpc-igw-PANW-77d3	igw-01c49479188ae080e	✓ Attached	vpc-08321c49862545523 | app-vpc-PANW-77d3	484857004050
□	sec-vpc-igw-PANW-f975	igw-08b6f2589bae33447	✓ Attached	vpc-006987452e8ad629a | sec-vpc-PANW-f975	484857004050
☑	app-vpc-igw-PANW-b4c2	igw-0bb33f319d240e9c4	✓ Attached	vpc-0f681106f6b84640d | app-vpc-PANW-b4c2	484857004050

And search for the IGW ID in the VPC route tables. Looking at the routes, we see that the IGW sends the request to an endpoint as the next hop to the target subnet(s):



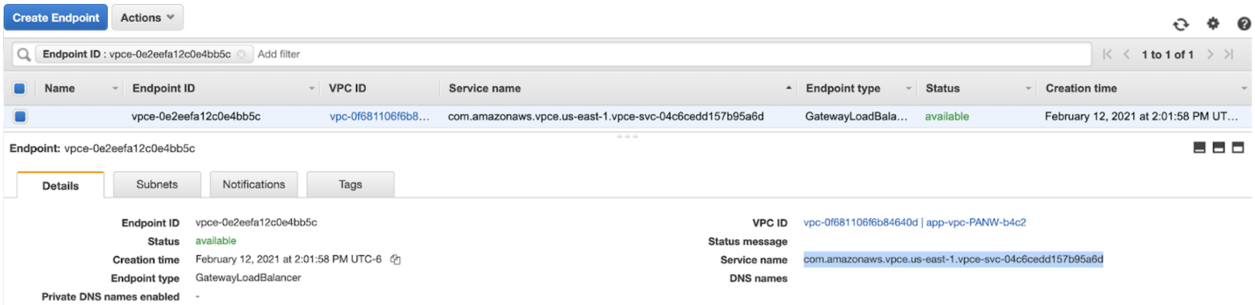
	Name	Route Table ID	Explicit subnet associatior	Edge associations	Main	VPC ID	Owner
□	app-gwlbe-rt-PANW-b4c2	rtb-0ccfc78051b520c06	subnet-01c599227b8e1ab39	-	No	vpc-0f681106f6b84640d | ...	484857004050
□	app-main-rt-PANW-b4c2	rtb-02eae9f0eb7ce9d41	subnet-0709ac7ea08f1e5a3	-	Yes	vpc-0f681106f6b84640d | ...	484857004050
■	igw-rt-PANW-b4c2	rtb-055484518c272b609	-	igw-0bb33f319d240e9c4	No	vpc-0f681106f6b84640d | ...	484857004050

Route Table: rtb-055484518c272b609

Destination	Target	Status	Propagated
10.102.0.0/16	local	active	No
10.102.0.32/28	vpce-0e2eefa12c0e4bb5c	active	No
10.102.0.48/28	vpce-0e2eefa12c0e4bb5c	active	No
10.102.0.64/28	vpce-0e2eefa12c0e4bb5c	active	No
10.102.0.80/28	vpce-0e2eefa12c0e4bb5c	active	No
10.102.0.96/28	vpce-0e2eefa12c0e4bb5c	active	No
10.102.0.112/28	vpce-0e2eefa12c0e4bb5c	active	No

Request Step 3 - The GWLB Endpoint

Recall that Endpoints are ENIs that provide direct access to services within the VPC. ENIs are AZ-specific constructs and are instantiated in every AZ where service access is required. Clicking on the target (vpce-0e2eefa12c0e4bb5c) we can see additional information about the Endpoint, including the associated Endpoint Service:

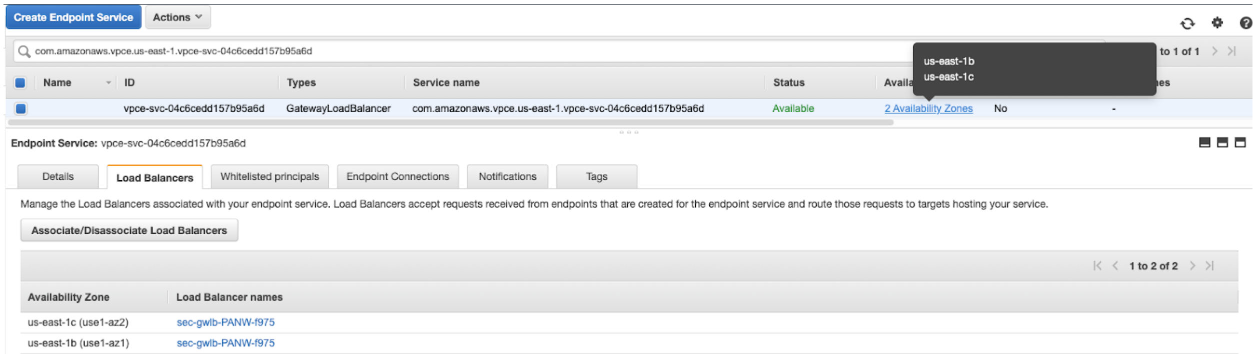


Name	Endpoint ID	VPC ID	Service name	Endpoint type	Status	Creation time
	vpce-0e2eefa12c0e4bb5c	vpc-0f681106f6b8...	com.amazonaws.vpce.us-east-1.vpce-svc-04c6cedd157b95a6d	GatewayLoadBala...	available	February 12, 2021 at 2:01:58 PM UT...

Endpoint: vpce-0e2eefa12c0e4bb5c

Endpoint ID vpce-0e2eefa12c0e4bb5c
Status available
Creation time February 12, 2021 at 2:01:58 PM UTC-6
Endpoint type GatewayLoadBalancer
Private DNS names enabled -
VPC ID vpc-0f681106f6b84640d | app-vpc-PANW-b4c2
Status message
Service name com.amazonaws.vpce.us-east-1.vpce-svc-04c6cedd157b95a6d
DNS names

If we then look at Endpoint Services, we can see that this service is associated with a multi-AZ load balancer in addition to multiple AZs:



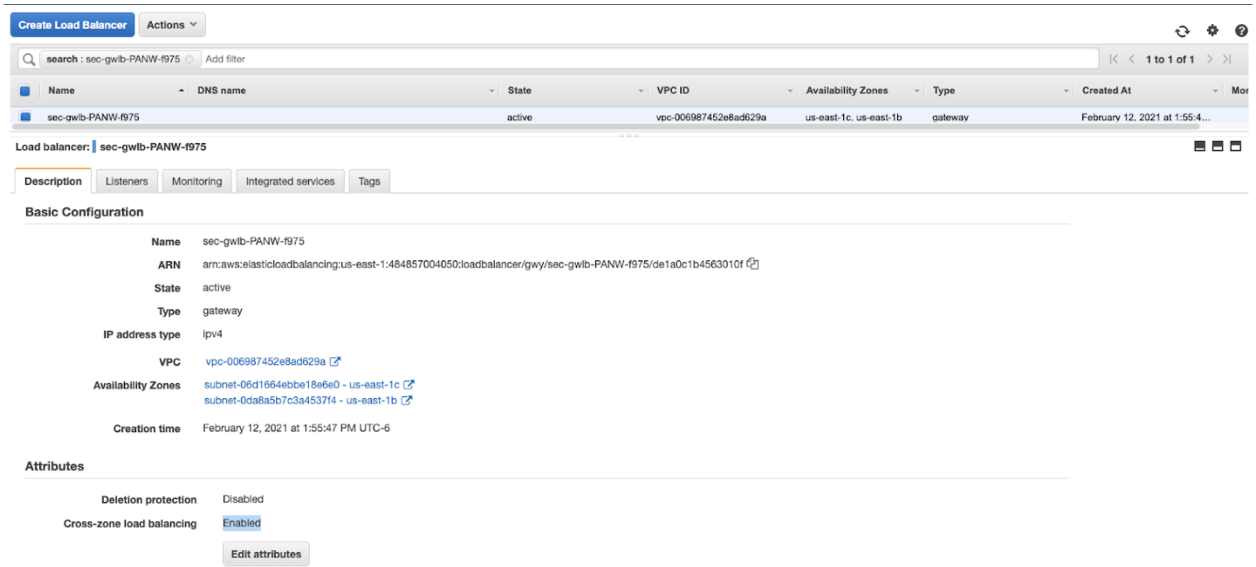
Name	ID	Types	Service name	Status	Availa		es
	vpce-svc-04c6cedd157b95a6d	GatewayLoadBalancer	com.amazonaws.vpce.us-east-1.vpce-svc-04c6cedd157b95a6d	Available	2 Availability Zones	No	-

Endpoint Service: vpce-svc-04c6cedd157b95a6d

Manage the Load Balancers associated with your endpoint service. Load Balancers accept requests received from endpoints that are created for the endpoint service and route those requests to targets hosting your service.

Availability Zone	Load Balancer names
us-east-1c (use1-az2)	sec-gwlb-PANW-f975
us-east-1b (use1-az1)	sec-gwlb-PANW-f975

Clicking on the loadbalancer, we can see more detailed information:



Name	DNS name	State	VPC ID	Availability Zones	Type	Created At	Mor
sec-gwlb-PANW-f975		active	vpc-006987452e8ad629a	us-east-1c, us-east-1b	gateway	February 12, 2021 at 1:55:4...	

Load balancer: sec-gwlb-PANW-f975

Basic Configuration

Name sec-gwlb-PANW-f975
ARN arn:aws:elasticloadbalancing:us-east-1:484857004050:loadbalancer/gwy/sec-gwlb-PANW-f975/de1a0c1b4563010f
State active
Type gateway
IP address type ipv4
VPC vpc-006987452e8ad629a
Availability Zones subnet-06d1664ebbe18e6e0 - us-east-1c
subnet-0da8a5b7c3a4537f4 - us-east-1b
Creation time February 12, 2021 at 1:55:47 PM UTC-6

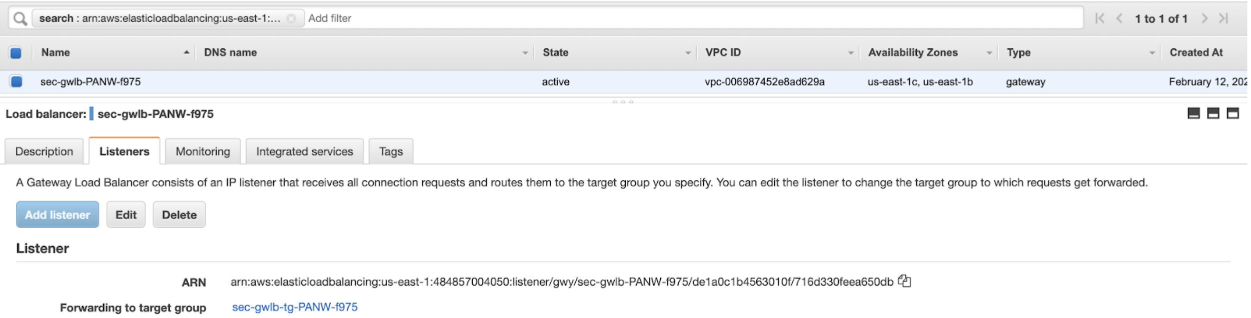
Attributes

Deletion protection Disabled
Cross-zone load balancing Enabled

Pro Tip: If it has not already been done, "Cross-zone load balancing" should be enabled in the attributes. This ensures that the GWLB can use any backend pool member in any availability zone and facilitates resiliency.

Request Step 4 - The Firewalls

The GWLB uses Generic Network Virtualization Encapsulation (GENEVE) to create an overlay network between the load balancer and the firewalls. At present, this overlay network is not connected to the firewalls virtual router, which improves packet handling efficiency but requires that all traffic ingress/egress the FW via the GENEVE tunnel. Under the hood, the GWLB is a souped-up NLB and the configuration is very similar. Once the traffic reaches the GWLB, it is distributed amongst the available backend pool members. Looking at the listeners for the GWLB, we see one of the first differences between the GWLB and a standard NLB:



Name	DNS name	State	VPC ID	Availability Zones	Type	Created At
sec-gwlb-PANW-f975		active	vpc-006987452e8ad629a	us-east-1c, us-east-1b	gateway	February 12, 202

Load balancer: sec-gwlb-PANW-f975

A Gateway Load Balancer consists of an IP listener that receives all connection requests and routes them to the target group you specify. You can edit the listener to change the target group to which requests get forwarded.

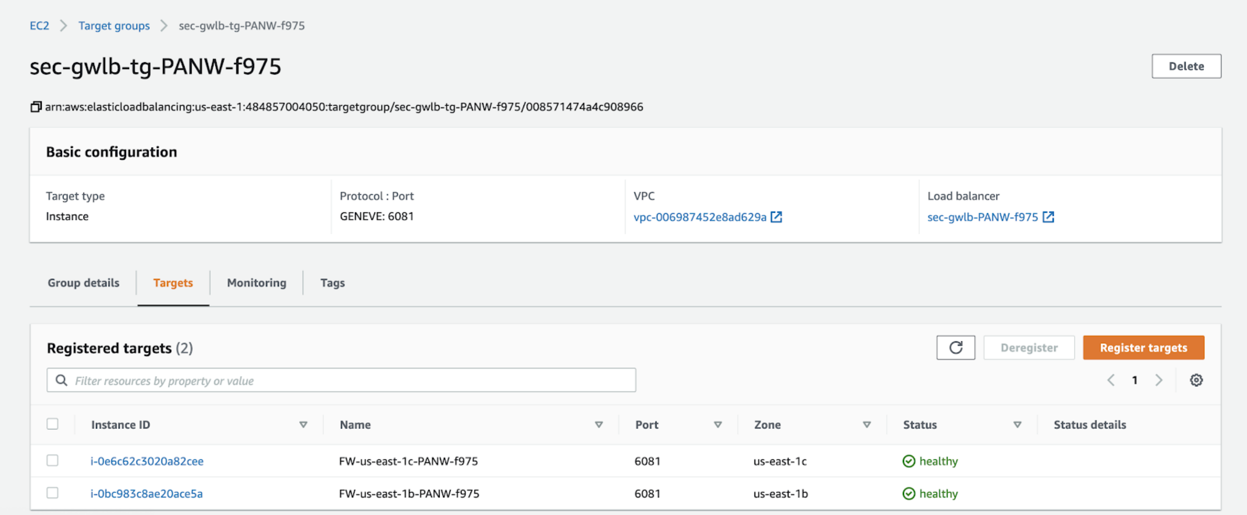
Listener

ARN: arn:aws:elasticloadbalancing:us-east-1:484857004050:listener/gwy/sec-gwlb-PANW-f975/de1a0c1b4563010f/716d330feea650db

Forwarding to target group: sec-gwlb-tg-PANW-f975

The GWLB is an any port load balancer and consequently no port(s)are specified/required. All TCP/UDP traffic is load balanced to the associated target group.

Selecting the target group, we see that it is comprised of the FW in the security VPC:


EC2 > Target groups > sec-gwlb-tg-PANW-f975

sec-gwlb-tg-PANW-f975

arn:aws:elasticloadbalancing:us-east-1:484857004050:targetgroup/sec-gwlb-tg-PANW-f975/008571474a4c908966

Basic configuration

Target type	Protocol : Port	VPC	Load balancer
Instance	GENEVE: 6081	vpc-006987452e8ad629a	sec-gwlb-PANW-f975

Group details
Targets
Monitoring
Tags

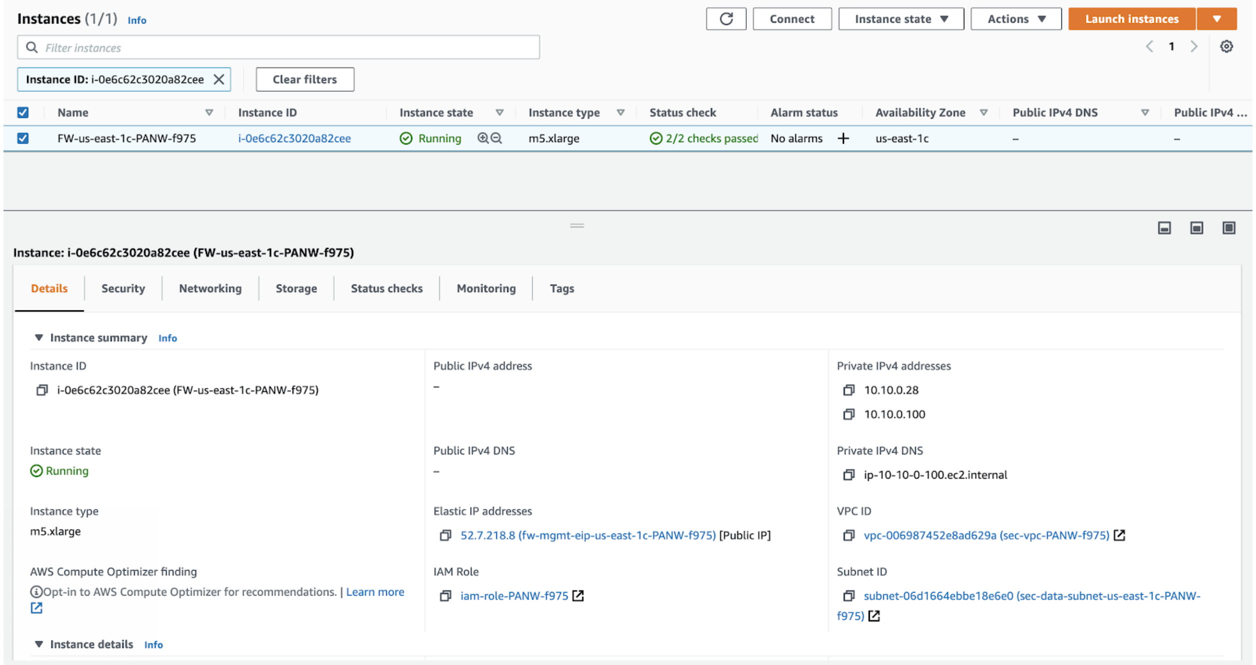
Registered targets (2)

Deregister
Register targets
Filter resources by property or value
1

Instance ID	Name	Port	Zone	Status	Status details
i-0e6c62c3020a82cee	FW-us-east-1c-PANW-f975	6081	us-east-1c	healthy	
i-0bc983c8ae20ace5a	FW-us-east-1b-PANW-f975	6081	us-east-1b	healthy	

The FW are targeted by instance ID, which ensures source IP preservation but requires that the management and first data plane interface be swapped.

Selecting one of the targets, we can see the firewall details:



Instances (1/1) Info

Instance ID: i-0e6c62c3020a82cee

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
FW-us-east-1c-PANW-f975	i-0e6c62c3020a82cee	Running	m5.xlarge	2/2 checks passed	No alarms	us-east-1c	–	–

Instance: i-0e6c62c3020a82cee (FW-us-east-1c-PANW-f975)

Instance summary

Instance ID: i-0e6c62c3020a82cee (FW-us-east-1c-PANW-f975)

Public IPv4 address: –

Private IPv4 addresses: 10.10.0.28
10.10.0.100

Instance state: Running

Public IPv4 DNS: –

Private IPv4 DNS: ip-10-10-0-100.ec2.internal

Instance type: m5.xlarge

Elastic IP addresses: 52.7.218.8 (fw-mgmt-eip-us-east-1c-PANW-f975) [Public IP]

VPC ID: vpc-006987452e8ad629a (sec-vpc-PANW-f975)

AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. | Learn more

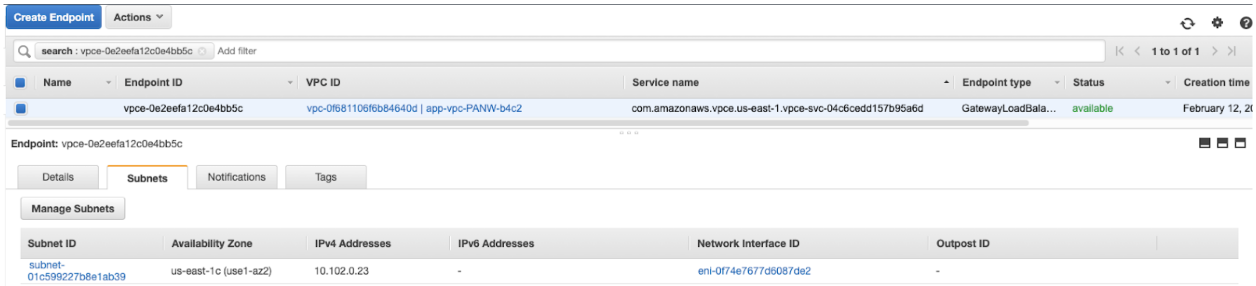
IAM Role: iam-role-PANW-f975

Subnet ID: subnet-06d1664ebbe18e6e0 (sec-data-subnet-us-east-1c-PANW-f975)

Instance details

Request Step 5 - Return to the GWLB Endpoint

The permitted request is returned to the GWLB via the GENEVE tunnel and then back to the Endpoint. Recall that the ID of the Endpoint is vpce-0e2eefa12c0e4bb5c. If we take a closer look at that Endpoint, we can determine the subnet that it resides in:



search : vpce-0e2eefa12c0e4bb5c

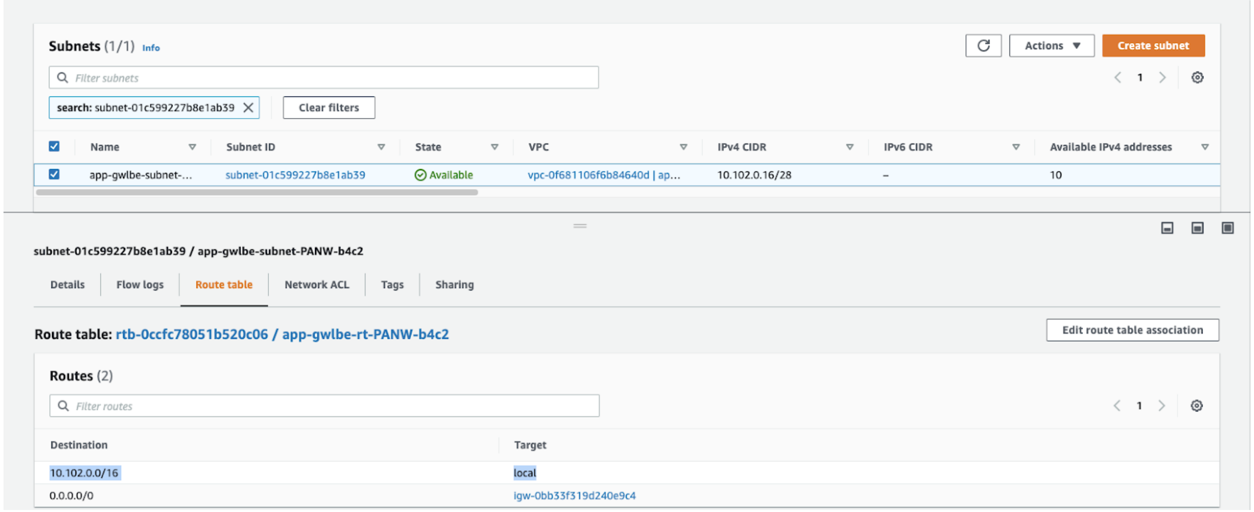
1 to 1 of 1

Name	Endpoint ID	VPC ID	Service name	Endpoint type	Status	Creation time
	vpce-0e2eefa12c0e4bb5c	vpc-0f681106f6b84640d | app-vpc-PANW-b4c2	com.amazonaws.vpce.us-east-1.vpce-svc-04c6cedd157b95a6d	GatewayLoadBala...	available	February 12, 2

Endpoint: vpce-0e2eefa12c0e4bb5c

Subnet ID	Availability Zone	IPv4 Addresses	IPv6 Addresses	Network Interface ID	Outpost ID
subnet-01c599227b8e1ab39	us-east-1c (use1-az2)	10.102.0.23	-	eni-0f74e7677d6087de2	-

The private IP of the LB is on the same subnet and the traffic is delivered directly to the LB:


Subnets (1/1) Info

search: subnet-01c599227b8e1ab39

☑	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses
☑	app-gwlbe-subnet-...	subnet-01c599227b8e1ab39	Available	vpc-0f681106f6b84640d | ap...	10.102.0.16/28	–	10

subnet-01c599227b8e1ab39 / app-gwlbe-subnet-PANW-b4c2

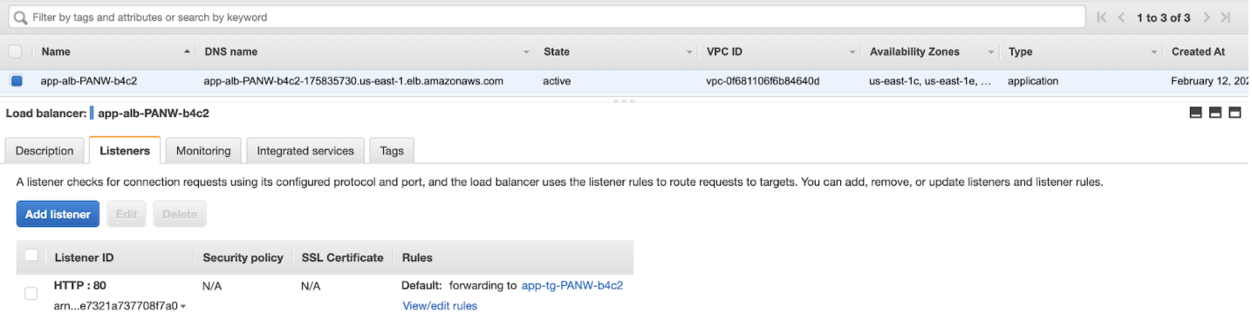
Route table: rtb-0ccfc78051b520c06 / app-gwlbe-rt-PANW-b4c2

Routes (2)

Destination	Target
10.102.0.0/16	local
0.0.0.0/0	igw-0bb33f319d240e9c4

Request Step 6 - The ALB

Once the request arrives at the ALB, it is processed by the local listener:

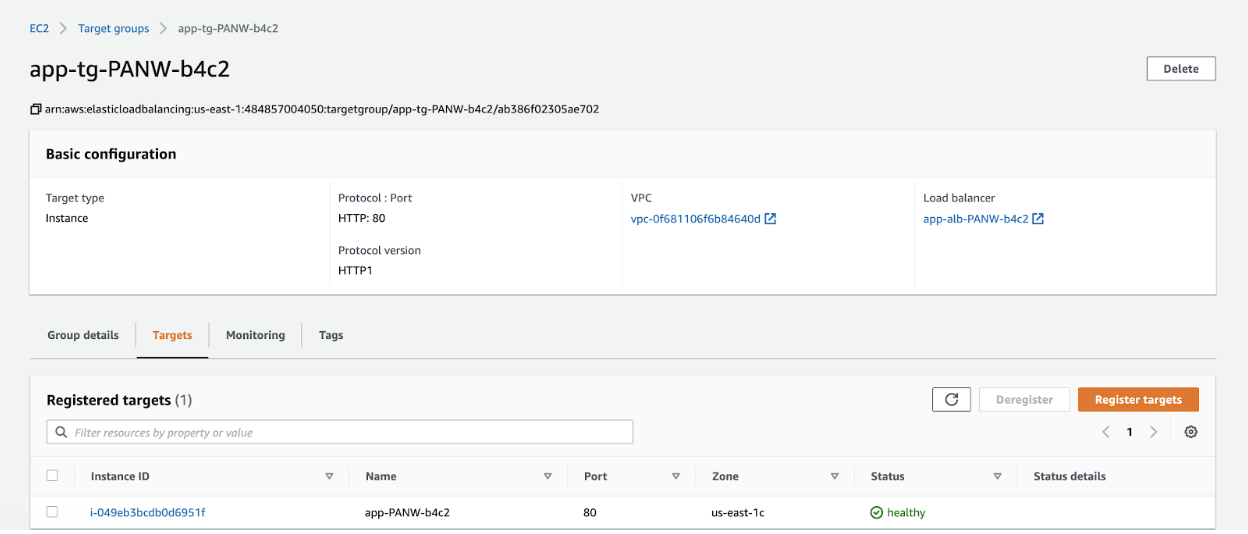

Name	DNS name	State	VPC ID	Availability Zones	Type	Created At
app-alb-PANW-b4c2	app-alb-PANW-b4c2-175835730.us-east-1.elb.amazonaws.com	active	vpc-0f681106f6b84640d	us-east-1c, us-east-1e, ...	application	February 12, 202

Load balancer: app-alb-PANW-b4c2

A listener checks for connection requests using its configured protocol and port, and the load balancer uses the listener rules to route requests to targets. You can add, remove, or update listeners and listener rules.

Listener ID	Security policy	SSL Certificate	Rules
HTTP : 80 arn...e7321a737708f7a0	N/A	N/A	Default: forwarding to app-tg-PANW-b4c2 View/edit rules

And sent to a viable target pool member:



EC2 > Target groups > app-tg-PANW-b4c2

app-tg-PANW-b4c2

arn:aws:elasticloadbalancing:us-east-1:484857004050:targetgroup/app-tg-PANW-b4c2/ab386f02305ae702

Basic configuration

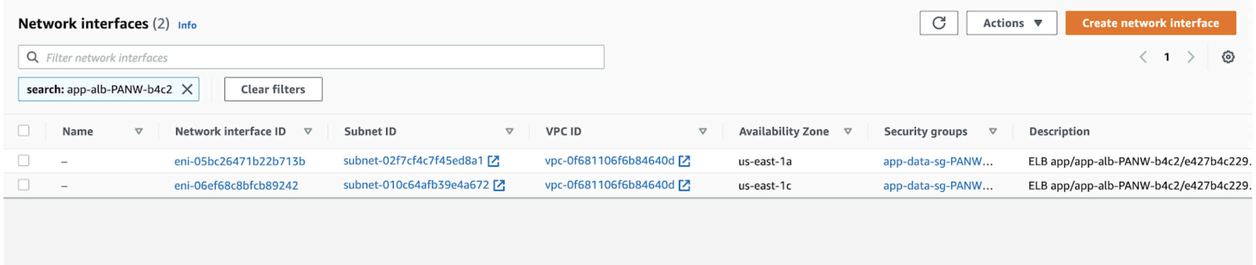
Target type	Protocol : Port	VPC	Load balancer
Instance	HTTP: 80	vpc-0f681106f6b84640d	app-alb-PANW-b4c2
	Protocol version HTTP1		

Registered targets (1)

	Instance ID	Name	Port	Zone	Status	Status details
□	i-049eb3bcdb0d6951f	app-PANW-b4c2	80	us-east-1c	✓ healthy	

Response Step1 - The GWLB Endpoint

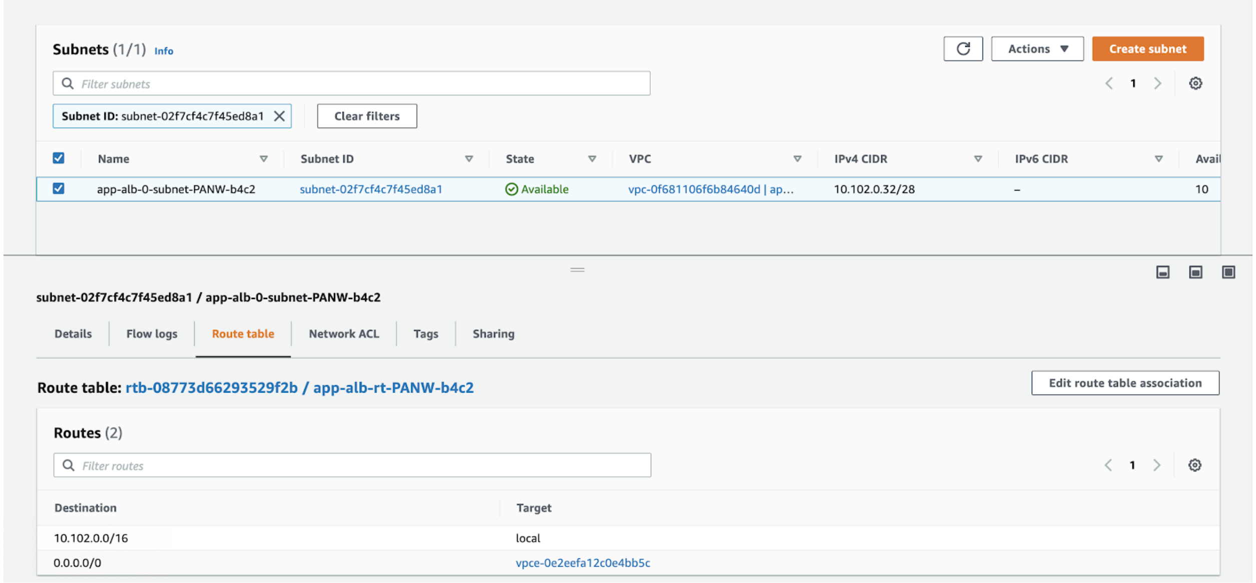
The response from the server is returned to the ALB and then the subnet route table determines where to send the packet. Looking at the ALB, we can see the associated subnets:



Network interfaces (2) Info

	Name	Network interface ID	Subnet ID	VPC ID	Availability Zone	Security groups	Description
□	–	eni-05bc26471b22b713b	subnet-02f7cf4c7f45ed8a1	vpc-0f681106f6b84640d	us-east-1a	app-data-sg-PANW...	ELB app/app-alb-PANW-b4c2/e427b4c229.
□	–	eni-06ef68c8bfcb89242	subnet-010c64afb39e4a672	vpc-0f681106f6b84640d	us-east-1c	app-data-sg-PANW...	ELB app/app-alb-PANW-b4c2/e427b4c229.

Looking at one of the subnets, we can see that the default route sends the response back to the endpoint. The other subnet will show a similar route configuration except the Endpoint ID will be different.



Subnets (1/1) Info

Subnet ID: subnet-02f7cf4c7f45ed8a1 ✕ Clear filters

☑	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Avail
☑	app-alb-0-subnet-PANW-b4c2	subnet-02f7cf4c7f45ed8a1	✓ Available	vpc-0f681106f6b84640d | ap...	10.102.0.32/28	–	10

subnet-02f7cf4c7f45ed8a1 / app-alb-0-subnet-PANW-b4c2

Details | Flow logs | Route table | Network ACL | Tags | Sharing

Route table: rtb-08773d66293529f2b / app-alb-rt-PANW-b4c2

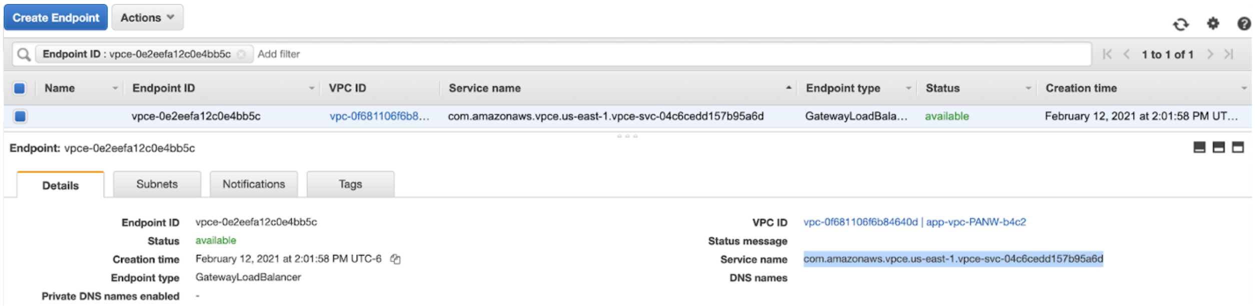
Edit route table association

Routes (2)

Destination	Target
10.102.0.0/16	local
0.0.0.0/0	vpce-0e2eefa12c0e4bb5c

Response Step 2 - The GWLB Endpoint

The traffic arriving at the endpoint is sent on to the GWLB via the associated endpoint service. Clicking on the target (vpce-0e2eefa12c0e4bb5c) we can see additional information about the Endpoint, including the associated Endpoint Service:



Endpoint ID : vpce-0e2eefa12c0e4bb5c Add filter 1 to 1 of 1

■	Name	Endpoint ID	VPC ID	Service name	Endpoint type	Status	Creation time
■		vpce-0e2eefa12c0e4bb5c	vpc-0f681106f6b8...	com.amazonaws.vpce.us-east-1.vpce-svc-04c6cedd157b95a6d	GatewayLoadBala...	available	February 12, 2021 at 2:01:58 PM UT...

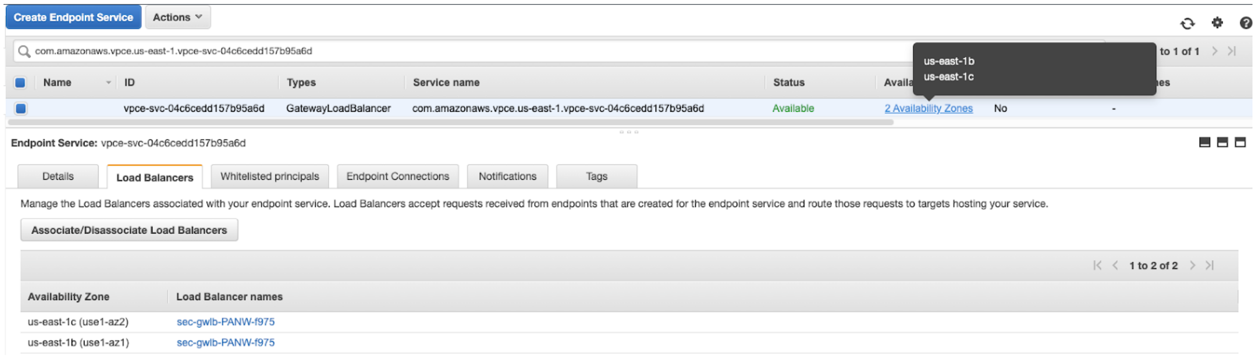
Endpoint: vpce-0e2eefa12c0e4bb5c

Details | Subnets | Notifications | Tags

Endpoint ID vpce-0e2eefa12c0e4bb5c
Status available
Creation time February 12, 2021 at 2:01:58 PM UTC-6
Endpoint type GatewayLoadBalancer
Private DNS names enabled -

VPC ID vpc-0f681106f6b84640d | app-vpc-PANW-b4c2
Status message
Service name com.amazonaws.vpce.us-east-1.vpce-svc-04c6cedd157b95a6d
DNS names

If we then look at Endpoint Services, we can see that this service is associated to a multi-AZ load balancer in addition to multiple AZs:



com.amazonaws.vpce.us-east-1.vpce-svc-04c6cedd157b95a6d

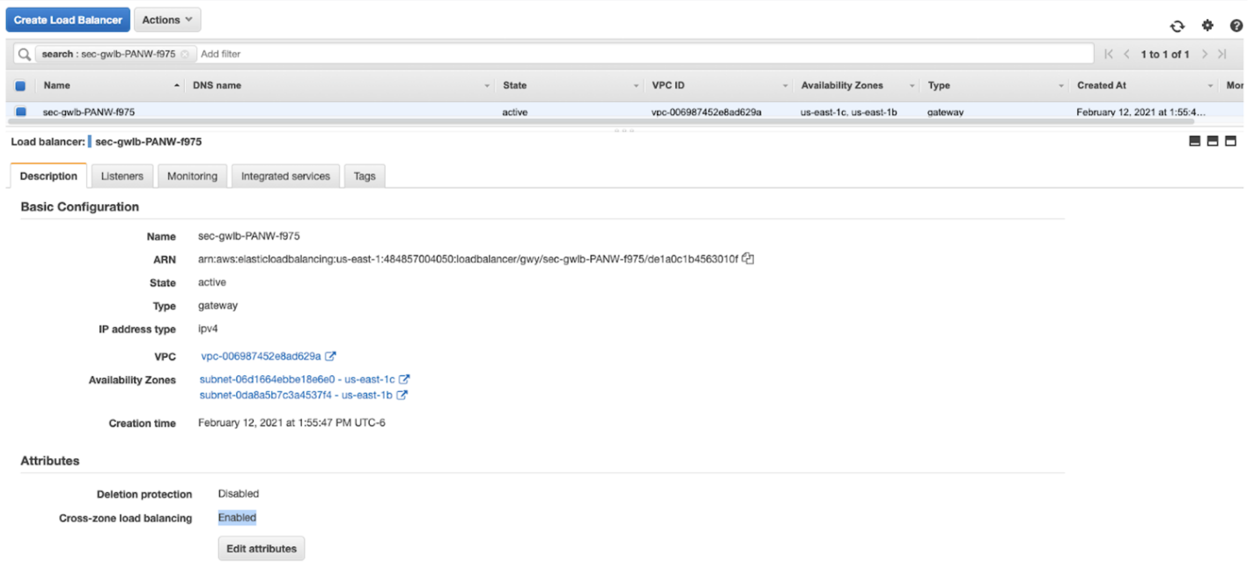
Name	ID	Types	Service name	Status	Availa		es
	vpce-svc-04c6cedd157b95a6d	GatewayLoadBalancer	com.amazonaws.vpce.us-east-1.vpce-svc-04c6cedd157b95a6d	Available	2 Availability Zones	No	-

Endpoint Service: vpce-svc-04c6cedd157b95a6d

Manage the Load Balancers associated with your endpoint service. Load Balancers accept requests received from endpoints that are created for the endpoint service and route those requests to targets hosting your service.

Availability Zone	Load Balancer names
us-east-1c (use1-az2)	sec-gwlb-PANW-f975
us-east-1b (use1-az1)	sec-gwlb-PANW-f975

Clicking on the loadbalancer, we can see more detailed information:



search : sec-gwlb-PANW-f975

Name	DNS name	State	VPC ID	Availability Zones	Type	Created At	Mor
sec-gwlb-PANW-f975		active	vpc-006987452e8ad629a	us-east-1c, us-east-1b	gateway	February 12, 2021 at 1:55:4...	

Load balancer: sec-gwlb-PANW-f975

Basic Configuration

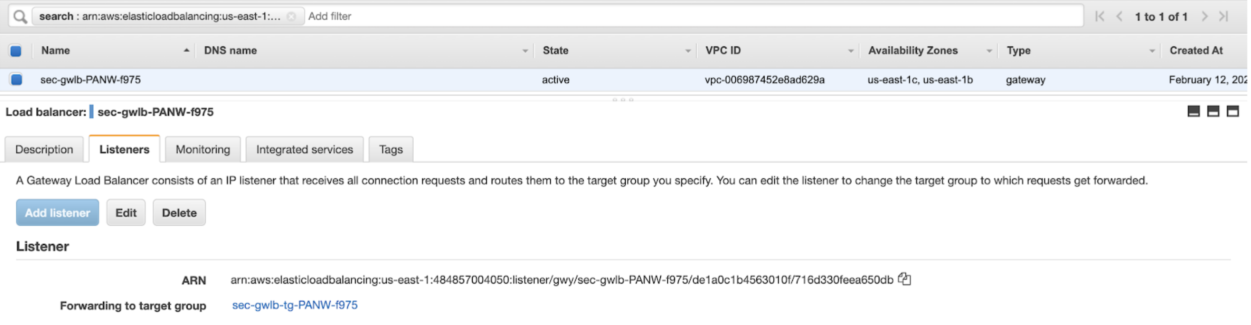
Name	sec-gwlb-PANW-f975
ARN	arn:aws:elasticloadbalancing:us-east-1:484857004050:loadbalancer/gwy/sec-gwlb-PANW-f975/de1a0c1b4563010f
State	active
Type	gateway
IP address type	ipv4
VPC	vpc-006987452e8ad629a
Availability Zones	subnet-06d1664ebbe18e6e0 - us-east-1c subnet-0da8a5b7c3a4537f4 - us-east-1b
Creation time	February 12, 2021 at 1:55:47 PM UTC-6

Attributes

Deletion protection	Disabled
Cross-zone load balancing	Enabled

Response Step 3 - The Firewalls

As mentioned earlier, there is no port associated with the listener on the GWLB. All TCP/UDP traffic is load balanced to the associated target group.



search : arn:aws:elasticloadbalancing:us-east-1:... Add filter 1 to 1 of 1

Name	DNS name	State	VPC ID	Availability Zones	Type	Created At
sec-gwlb-PANW-f975		active	vpc-006987452e8ad629a	us-east-1c, us-east-1b	gateway	February 12, 202

Load balancer: sec-gwlb-PANW-f975

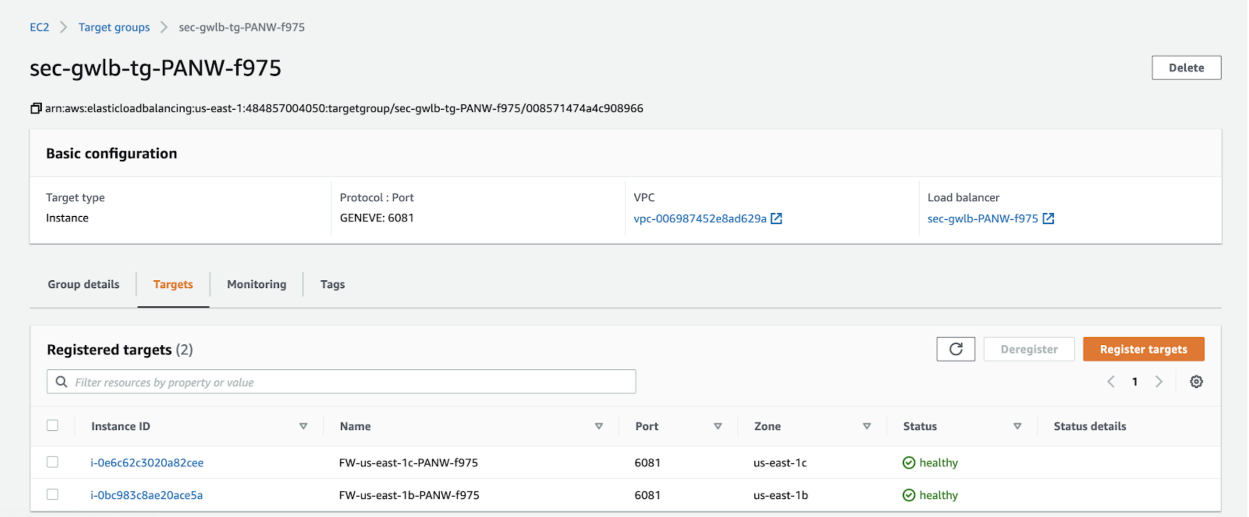
A Gateway Load Balancer consists of an IP listener that receives all connection requests and routes them to the target group you specify. You can edit the listener to change the target group to which requests get forwarded.

Listener

ARN arn:aws:elasticloadbalancing:us-east-1:484857004050:listener/gwy/sec-gwlb-PANW-f975/de1a0c1b4563010f/716d330feea650db

Forwarding to target group sec-gwlb-tg-PANW-f975

Selecting the target group, we see that it is comprised of the FW in the security VPC:



EC2 > Target groups > sec-gwlb-tg-PANW-f975

sec-gwlb-tg-PANW-f975

arn:aws:elasticloadbalancing:us-east-1:484857004050:targetgroup/sec-gwlb-tg-PANW-f975/008571474a4c908966

Basic configuration

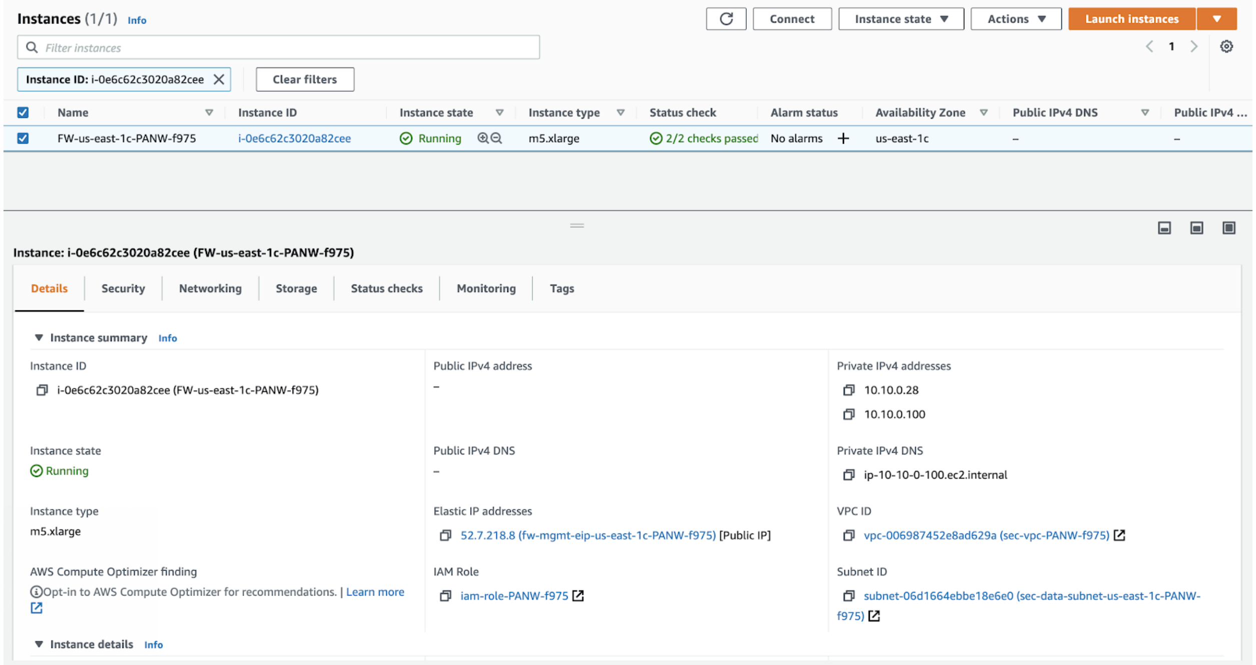
Target type	Protocol : Port	VPC	Load balancer
Instance	GENEVE: 6081	vpc-006987452e8ad629a	sec-gwlb-PANW-f975

Registered targets (2)

Instance ID	Name	Port	Zone	Status	Status details
i-0e6c62c3020a82cee	FW-us-east-1c-PANW-f975	6081	us-east-1c	healthy	
i-0bc983c8ae20ace5a	FW-us-east-1b-PANW-f975	6081	us-east-1b	healthy	

The FW are targeted by instance ID, which ensures source IP preservation but requires that the management and first data plane interface be swapped.

Selecting one of the targets, we can see the firewall details:



Instances (1/1) Info

Filter instances

Instance ID: i-0e6c62c3020a82cee

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
☑	FW-us-east-1c-PANW-f975	i-0e6c62c3020a82cee	✓ Running	m5.xlarge	✓ 2/2 checks passed	No alarms +	us-east-1c	–	–

Instance: i-0e6c62c3020a82cee (FW-us-east-1c-PANW-f975)

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

▼ Instance summary Info

Instance ID
i-0e6c62c3020a82cee (FW-us-east-1c-PANW-f975)

Instance state
✓ Running

Instance type
m5.xlarge

AWS Compute Optimizer finding
ⓘOpt-in to AWS Compute Optimizer for recommendations. | Learn more

Public IPv4 address
–

Public IPv4 DNS
–

Elastic IP addresses
52.7.218.8 (fw-mgmt-eip-us-east-1c-PANW-f975) [Public IP]

IAM Role
iam-role-PANW-f975

Private IPv4 addresses
10.10.0.28
10.10.0.100

Private IPv4 DNS
ip-10-10-0-100.ec2.internal

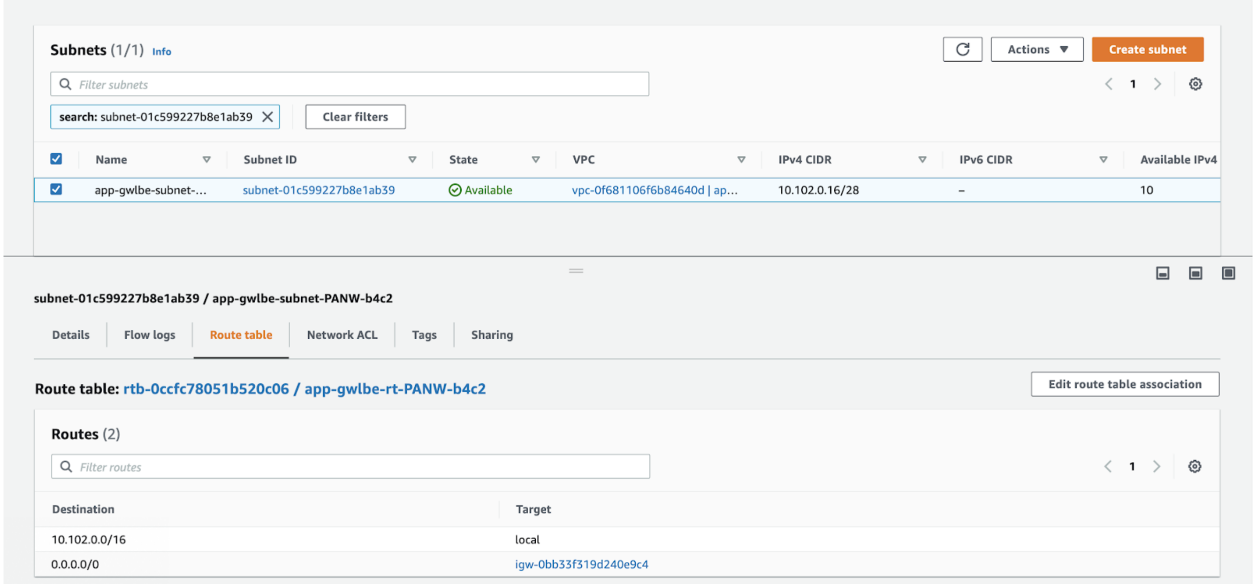
VPC ID
vpc-006987452e8ad629a (sec-vpc-PANW-f975)

Subnet ID
subnet-06d1664ebbe18e6e0 (sec-data-subnet-us-east-1c-PANW-f975)

▼ Instance details Info

Response Step 4 - Return to the GWLB Endpoint

The response is returned to the GWLB via the GENEVE tunnel and then back to the endpoint.Traffic leaving the endpoint is dropped off into the local subnet and based upon the subnet route table is then sent to the IGW as the next hop:



Subnets (1/1) Info

Filter subnets

search: subnet-01c599227b8e1ab39

☑	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4
☑	app-gwlbe-subnet-...	subnet-01c599227b8e1ab39	✓ Available	vpc-0f681106f6b84640d | ap...	10.102.0.16/28	–	10

subnet-01c599227b8e1ab39 / app-gwlbe-subnet-PANW-b4c2

Details | Flow logs | Route table | Network ACL | Tags | Sharing

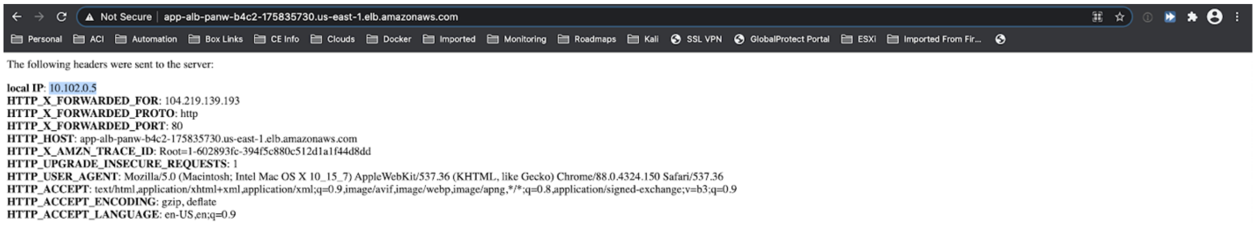
Route table: rtb-0ccfc78051b520c06 / app-gwlbe-rt-PANW-b4c2

Routes (2)

Filter routes

Destination	Target
10.102.0.0/16	local
0.0.0.0/0	igw-0bb33f319d240e9c4

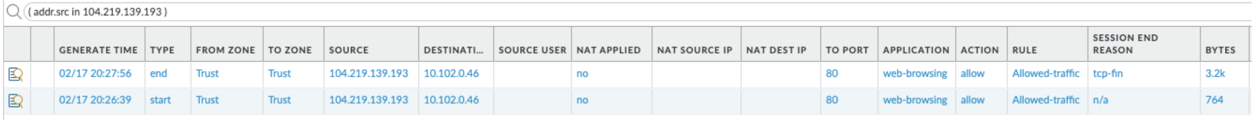
Et violà:



```
The following headers were sent to the server:

local IP: 10.102.0.5
HTTP_X_FORWARDED_FOR: 104.219.139.193
HTTP_X_FORWARDED_PROTO: http
HTTP_X_FORWARDED_PORT: 80
HTTP_HOST: app-alb-panw-b4c2-175835730.us-east-1.elb.amazonaws.com
HTTP_X_AMZN_TRACE_ID: Root=1-602893fc-394f5c880c512d1a1f44d8dd
HTTP_UPGRADE_INSECURE_REQUESTS: 1
HTTP_USER_AGENT: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.150 Safari/537.36
HTTP_ACCEPT: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
HTTP_ACCEPT_ENCODING: gzip, deflate
HTTP_ACCEPT_LANGUAGE: en-US,en;q=0.9
```

Note that the IP of the host matches the host IP. The traffic can be seen at the FW as well:



(addr.src in 104.219.139.193)

		GENERATE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	DESTINATI...	SOURCE USER	NAT APPLIED	NAT SOURCE IP	NAT DEST IP	TO PORT	APPLICATION	ACTION	RULE	SESSION END REASON	BYTES
		02/17 20:27:56	end	Trust	Trust	104.219.139.193	10.102.0.46		no			80	web-browsing	allow	Allowed-traffic	tcp-fin	3.2k
		02/17 20:26:39	start	Trust	Trust	104.219.139.193	10.102.0.46		no			80	web-browsing	allow	Allowed-traffic	n/a	764