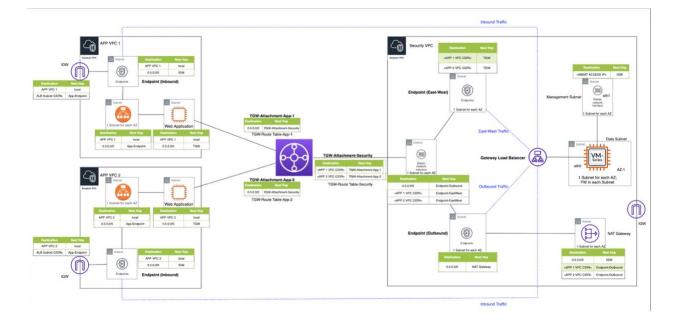
Introduction

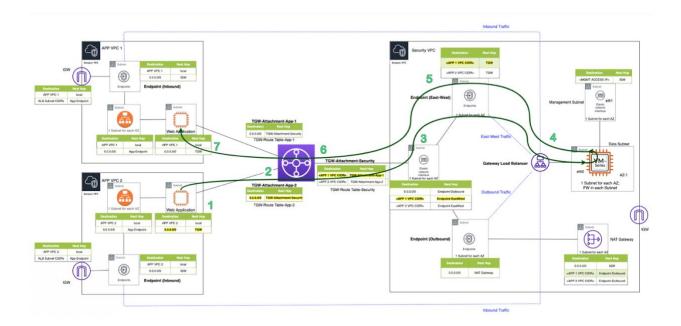
With the introduction of the Gateway Load Balancer (GWLB) in mid-November 2020, AWS provided its customers with any port, load-balancing router . Prior to that, Azure and GCP were the only public clouds that had such a construct. Customers use these to provide a security layer that is scalable, resilient, 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 in one VPC (network 10.102.0.0/16) to a server in another VPC (network 10.101.0.0/16). The infrastructure was deployed using the following TerraForm template:

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

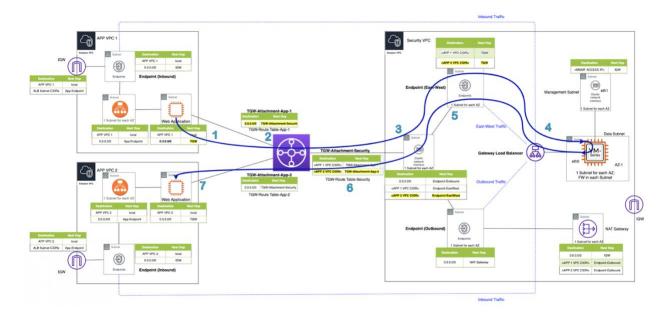


and follows current best practices regarding architecture:

This architecture also supports inbound and outbound traffic flows, which are treated separately in other blog posts. Today, we will focus on the following request flow:



And the corresponding response flow:



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.

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 postdeployment 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/process on a host (IP 10.102.0.5) in APP VPC 2 needs to connect to a host (IP 10.101.0.4) in APP VPC 1. Looking at the EC2 instance, we can see the IP address as well as the subnet membership:

Instances (1/1) Info		C	Connect	Instance state 🔻	Actions 🔻	Launch instances		•
Q Filter instances						< 1	>	۲
search: app-PANW-b4c2 X Clear filters								
Name V Instance ID Instance ID	tance state 🛛 🗸 Instance type	e 🛛 Status check	Alarm status	Availability Zone	♥ Public IPv4 I	DNS V	Public	IPv4 .
app-PANW-b4c2 i-049eb3bcdb0d6951f	Running @@ t2.micro	⊘ 2/2 checks passed	No alarms	us-east-1c	-	3	5.208.2	253.71
Instance: i-049eb3bcdb0d6951f (app-PANW-b4c2) Details Security Networking Storage Status check	Ks Monitoring Tags							
Instance summary Info Instance ID	Public IPv4 address		Р	rivate IPv4 addresses				
i-049eb3bcdb0d6951f (app-PANW-b4c2)	3.208.253.71 (app-mgmt-	eip-PANW-b4c2) open address		D 10.102.0.5				
Instance state	Public IPv4 DNS		D	rivate IPv4 DNS				
⊘ Running	-			p-10-102-0-5.ec2.in	iternal			
Instance type	Elastic IP addresses		v	PC ID				
t2.micro	3.208.253.71 (app-mgmt-	eip-PANW-b4c2) [Public IP]		vpc-0f681106f6b84	640d (app-vpc-PANW	-b4c2) 🔼		
AWS Compute Optimizer finding	IAM Role		s	ubnet ID				
③Opt-in to AWS Compute Optimizer for recommendations. Learn more	-			subnet-0709ac7ea08	3f1e5a3 (app-main-su	bnet-PANW-b4c2)	Z	

The subnet route table has a default route pointing to the transit gateway (TGW) as the next hop.

Q Filter subnets					< 1 > @
Subnet ID: subnet-0709ac7ea08f1e5a3 X	ear filters				
Name V Subnet ID	⊽ State	▽ VPC	IPv4 CIDR	♥ IPv6 CIDR	⊽ Available I
app-main-subnet-P subnet-0709ac7ea08	8f1e5a3 📿 Available	vpc-0f681106f6b84640d ap	10.102.0.0/28	-	9
net-0709ac7ea08f1e5a3 / app-main-subnet-PANW	-b4c2				
onet-0709ac7ea08f1e5a3 / app-main-subnet-PANW Details Flow logs Route table Network					
Details Flow logs Route table Network	k ACL Tags Sharing				Edit route table association
	k ACL Tags Sharing				Edit route table association
Details Flow logs Route table Network	k ACL Tags Sharing				Edit route table association
Details Flow logs Route table Network ute table: rtb-02eae9f0eb7ce9d41 / app-m Routes (3)	k ACL Tags Sharing				
Details Flow logs Route table Network ute table: rtb-02eae9f0eb7ce9d41 / app-m	k ACL Tags Sharing				Edit route table association
Details Flow logs Route table Network ute table: rtb-02eae9f0eb7ce9d41 / app-m Routes (3)	k ACL Tags Sharing	Target			
Details Flow logs Route table Network ute table: rtb-02eae9f0eb7ce9d41 / app-m Routes (3) Q. Filter routes	k ACL Tags Sharing	Target igw-0bb33f319d240e9c4			
Details Flow logs Route table Network ute table: rtb-02eae9f0eb7ce9d41 / app-m Routes (3) Q. Filter routes Destination	k ACL Tags Sharing				

The requester does an internal route lookup and puts the packet out on the wire (local subnet) which has a default route via the TGW.

Request Step 2 - Transit Gateway (TGW)

The TGW is connected to the VPC via a Transit Gateway Attachment. To see this association, we navigate to the Transit Gateway Attachment list and filter on the VPC hosting the requester:

Create Transit Gateway Attachm	Actions V							Ð	• • •
Q search : vpc-0f681106f6b8464	0d 🕥 Add filter						4	< 1 to 1 of	1 > >
Name	 Transit Gateway attachment ID 	+ Transit Gateway ID	· Resource type	· Resource ID		- State	✓ As:	sociated route ta	ble ID
client-server-PANW-b4c2	tgw-attach-07e43a9c4496319b1	tgw-0ad0c9091ead9880f	VPC	vpc-0f681106	f6b84640d	available	tgw	r-rtb-0f89b1da68b	6b5d2c
Petails Tags	-attach-07e43a9c4496319b1								
Details Tags				Transit Gateway owner ID	484857004050				
	tgw-attach-07e43a9c4496319b1			Transit Gateway owner ID Resource owner account ID	484857004050 484857004050				880
Details Tags Transit Gateway attachment ID	tgw-attach-07e43a9c4496319b1 tgw-0ad0c9091ead9880f		I						880
Details Tags Transit Gateway attachment ID Transit Gateway ID	tgw-attach-07e43a9c4496319b1 tgw-0ad0c9091ead9880f VPC		I	Resource owner account ID	484857004050	2			880
Details Tags Transit Gateway attachment ID Transit Gateway ID Resource type	tgw-attach-07e43a9c4496319b1 tgw-0ad0c9091ead9880/f VPC		I	Resource owner account ID State	484857004050 available	2			880

Note that when creating a TGW Attachment, a subnet must be specified and traffic can only be routed to a TGW Attachment in the same availability zone (AZ). In this case, the TGW Attachment and the host exist on the same subnet (and hence same AZ).

Routing within the TGW is handled via route tables associated with the TGW attachment. In the above picture, we can see that the route table associated with the TGW Attachment is tgw-rtb-0f89b1da68b6b5d2c. Clicking on the link to the route table

and inspecting the routes, we can see that the default route points to yet another attachment:

Create Transit Gateway Route Table	Actions *	÷ ÷
Q Transit Gateway route table ID : to	w-rtb-0f89b1da68b6b5d2c 📀 Add filter	< < 1 to 1 of 1 > >
Name	Transit Gateway route table ID * Transit Gateway ID * State * Default association route table * Default	ault propagation route table 🤟
tgw-app-rt-PANW-b4c2	tgw-rtb-0f89b1da68b6b5d2c tgw-0ad0c9091ead9880f available No No	
	tions Prefix list references Routes Tags of 1000 routes. Narrow the filter or use export routes to view more routes. atic route Delete static route	
Q Filter by attributes or search by ke	ywwrd	< 1 to 1 of 1 $>$ >
CIDR	Attachment Resource type Route type I	Route state Prefix List ID
0.0.0/0	tgw-attach-092303149b3633879 vpc-006987452e8ad629a VPC static a	active -

Following the rabbit a little further down the hole, we find that the attachment is associated with two different subnets. Traffic from the requester gets dropped off into one of these subnets when it exits the TGW.

Create Transit Gateway Attachm	Actions *						0 ¢
Q Transit Gateway attachment	ID: tgw-attach-092303149b3633879	Add filter					$ \langle \langle 1 \text{ to 1 of 1} \rangle \rangle $
Name	Transit Gateway attachment ID	Transit Gateway ID	- Resource type	+ Resource ID		- State	- Associated route table ID
security-tgwa-PANW-f975	tgw-attach-092303149b3633879	tgw-0ad0c9091ead9880f	VPC	vpc-0069874	52e8ad629a	available	tgw-rtb-04bf8978d5e84d872
Details Tags	here ethere 0002001 (05-2222020			-	484857004050		
Transit Gateway attachment ID				Transit Gateway owner ID			
Transit Gateway ID			,	lesource owner account ID	484857004050 available		
Resource type				State			
Resource ID				Associated route table	tgw-rtb-04bf8978d5e84d872		
Association state	associated			DNS support	enable		
IPv6 support	disable			Subnet IDs	subnet-0d8d93baf94c3d663		
					subnet-0624e157397d83c5b		

N.B. - The TGW has the ability to load balance across as well as ensure traffic symmetry. More information on traffic symmetry can be found here:

https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-appliance-scenario.html

If we look at the route table of one of the subnets, we can see that the traffic is directed to a GWLB endpoint:

vailable vpc-006987452e8ad629a sec 10.10.1.64/28 - 10	a sec-tgwa-subnet-us subnet-0d8d93baf94c3d663	Name v Subnet ID v State v VPC v IPv4 CIDR v IPv6 CIDR v Available a sec-tgwa-subnet-us subnet-0d8d93baf94c3d663 ② Available vpc-006987452e8ad629a sec 10.10.1.64/28 - 10 a sec-tgwa-subnet-us subnet-0d8d93baf94c3d663 / sec-tgwa-subnet-us-east-1b-PANW-f975 - 10 - 10 betails Flow logs Route table Network ACL Tags Sharing Edit route table association associatio
vailable vpc-006987452e8ad629a sec 10.10.1.64/28 - 10	sec-tgwa-subnet-us subnet-0d8d93baf94c3d663 Petrolog8d93baf94c3d663 / sec-tgwa-subnet-us-east-1b-PANW-f975 Details Flow logs Route table Network ACL Tags Sharing Lite table: rtb-0d94d34e75d135468 / tgwa-rt-us-east-1b-PANW-f975 Edit route table association	sec-tgwa-subnet-us subnet-0d8d93baf94c3d663 Parallable vpc-006987452e8ad629a sec 10.10.1.64/28 10 Inter-0d8d93baf94c3d663 / sec-tgwa-subnet-us-east-1b-PANW-f975 Patalls Flow logs Route table Network ACL Tags Sharing Edit route table association Route table Network ACL Tags Sharing Edit route table association Route table Network ACL Tags Sharing Edit route table association Route table Network ACL Tags Sharing Edit route table association Route table Network ACL Tags Sharing Edit route table association Routes (4)
In In	e e e e e e e e e e e e e e e e e e e	Image: Content of the content of th
Sharing	het-0d8d93baf94c3d663 / sec-tgwa-subnet-us-east-1b-PANW-f975 Details Flow logs Route table Network ACL Tags Sharing ute table: rtb-0d94d34e75d135468 / tgwa-rt-us-east-1b-PANW-f975 Edit route table association	het-0d8d93baf94c3d663 / sec-tgwa-subnet-us-east-1b-PANW-f975 Details Flow logs Route table Network ACL Tags Sharing Ite table: rtb-0d94d34e75d135468 / tgwa-rt-us-east-1b-PANW-f975 Edit route table association Routes (4)
Sharing	het-0d8d93baf94c3d663 / sec-tgwa-subnet-us-east-1b-PANW-f975 Details Flow logs Route table Network ACL Tags Sharing ute table: rtb-0d94d34e75d135468 / tgwa-rt-us-east-1b-PANW-f975 Edit route table association	het-0d8d93baf94c3d663 / sec-tgwa-subnet-us-east-1b-PANW-f975 Details Flow logs Route table Network ACL Tags Sharing Ite table: rtb-0d94d34e75d135468 / tgwa-rt-us-east-1b-PANW-f975 Edit route table association Routes (4)
Sharing	het-0d8d93baf94c3d663 / sec-tgwa-subnet-us-east-1b-PANW-f975 Details Flow logs Route table Network ACL Tags Sharing ute table: rtb-0d94d34e75d135468 / tgwa-rt-us-east-1b-PANW-f975 Edit route table association	het-0d8d93baf94c3d663 / sec-tgwa-subnet-us-east-1b-PANW-f975 Details Flow logs Route table Network ACL Tags Sharing Ite table: rtb-0d94d34e75d135468 / tgwa-rt-us-east-1b-PANW-f975 Edit route table association Routes (4)
-	Flow logs Route table Network ACL Tags Sharing ite table: rtb-0d94d34e75d135468 / tgwa-rt-us-east-1b-PANW-f975 Edit route table association	Plow logs Route table Network ACL Tags Sharing Inte table: rtb-0d94d34e75d135468 / tgwa-rt-us-east-1b-PANW-f975 Edit route table association Routes (4) Edit route table Edit route table
-	Flow logs Route table Network ACL Tags Sharing ite table: rtb-0d94d34e75d135468 / tgwa-rt-us-east-1b-PANW-f975 Edit route table association	Plow logs Route table Network ACL Tags Sharing Inte table: rtb-0d94d34e75d135468 / tgwa-rt-us-east-1b-PANW-f975 Edit route table association Routes (4) Edit route table Edit route table
-	Lite table: rtb-0d94d34e75d135468 / tgwa-rt-us-east-1b-PANW-f975	Lite table: rtb-0d94d34e75d135468 / tgwa-rt-us-east-1b-PANW-f975 Edit route table association toutes (4)
-	ute table: rtb-0d94d34e75d135468 / tgwa-rt-us-east-1b-PANW-f975	Lite table: rtb-0d94d34e75d135468 / tgwa-rt-us-east-1b-PANW-f975 Edit route table association Routes (4)
NW-F075 Edit route table associatio	re table: rtu-uu940340/30153400 / tywa-rt-us-east- ID-PARW-1973	toutes (4)
Edit route table associatio	re table: rtu-uu940340/30153400 / tywa-rt-us-east- ID-PARW-1973	toutes (4)
Edit route table associatio	re table: rtu-uu940340/30153400 / tywa-rt-us-east- ID-PARW-1973	toutes (4)
	toutes (A)	
	outes (4)	Q Filter routes
	Q. Filter routes	
< 1 > @	Q. Filter routes	Destination Target
< 1 > @		
	Destination Target	
Target	Destination Target 0.10.0.0/16 local	0.10.0./16 local
		A Interroutes
< 1 > €	Q, Filter routes	

The route table associated with the other subnet looks similar (note that the endpoint ID is different):

Q. Filter subnets search: subnet-0624e157397d83c5b X Clear filters			< 1 > 0
2 Name ∇ Subnet ID ∇ State	▽ VPC ▽ IPv4 CIDR	▽ IPv6 CIDR	
sec-tgwa-subnet-us subnet-0624e157397d83c5b O Available	vpc-006987452e8ad629a sec 10.10.1.80/28	-	10
Details Flow logs Route table Network ACL Tags Sharing ute table: rtb-07f9337931eb34245 / tgwa-rt-us-east-1c-PANW-f9			Edit route table associatio
			Edit route table associatio
ute table: rtb-07f9337931eb34245 / tgwa-rt-us-east-1c-PANW-f9 Routes (4)			
ute table: rtb-07f9337931eb34245 / tgwa-rt-us-east-1c-PANW-f9 Routes (4) Q. Filter routes	75		
ute table: rtb-07f9337931eb34245 / tgwa-rt-us-east-1c-PANW-f9 Routes (4) Q. Filter routes Destination	75 Target		

In this case, the traffic is sent to the same Endpoint irrespective of whether we are attempting to reach APP VPC 1 or APP VPC 2.

Request Step 3 - The GWLB Endpoint

Recall that endpoints are ENIs that provide direct access to services within the VPC. They are AZ-specific constructs and are instantiated in every AZ where service access is required. The Endpoint is connected to the GWLB via an Endpoint Service.

Clicking on one of the targets associated with either APP VPC 1 (10.101.0.0/16) or APP VPC 2 (10.102.0.0/16), we can see additional information about the endpoint, including the associated Endpoint Service:

Create Endpoint Actions 👻						÷	٥	0
Q search : vpce-03223b31fbd790	0492 🔿 Add filter				K < -	to 1 of 1	>>	1
Name - Endpoint II	D ~	VPC ID	Service name		Endpoint type	Status		
vpce-03223	b31fbd790492	vpc-006987452e8ad629a sec-vpc-PANW-f975	com.amazonaws.vpce	us-east-1.vpce-svc-04c6cedd157b95a6d	GatewayLoadBala	availabl	e	
Details Subnets	Notifications	Tags						
	vpce-03223b31fbd790492 available		VPC ID Status message	vpc-006987452e8ad629a sec-vpc-PANW-f9				
Creation time	February 12, 2021 at 1:59:2	23 PM UTC-6	Service name	com.amazonaws.vpce.us-east-1.vpce-svc-04	4c6cedd157b95a6d (ඵු			
Endpoint type Private DNS names enabled	GatewayLoadBalancer -		DNS names					

If we then look at Endpoint Services, we can see that this service is associated with a multi-AZ load balancer (also note that the Endpoint Service is associated with multiple AZs):

	Actions ~						÷	•
Q, com.amazonaws.vpce.us	s-east-1.vpce-svc-04c6cedd15	7b95a6d			us-east-1	ь	1 to 1 of 1	> >
Name - ID		Types	Service name	Statu	s Availa ^{US-east-1}	c	tes	
vpce	e-svc-04c6cedd157b95a6d	GatewayLoadBala	com amazonaws vpce us-east-1.vpce-svc-04	c6cedd157b95a6d Availa	ble 2 Availability Zone	s No		
ndpoint Service: vpce-svc-	:-04c6cedd157b95a6d						1	
Details Load I	Balancers Whitelisted	principals Endpoin	Connections Notifications Tag	8				
Manage the Lond Balance	rs associated with your endp	oint service. Load Balan	cers accept requests received from endpoints t	hat are created for the endpoint service	and route those requests to targets	hosting your service.		
manage the coau balancer								
Associate/Disassociate	e Load Balancers							
	e Load Balancers						$ \langle \langle 1 \text{ to 2 of 2} \rangle \rangle$	×
	e Load Balancers Load Balancer name	15					K < 1 to 2 of 2 $>$	×
Associate/Disassociate							K < 1 to 2 of 2 >	X

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

search : sec-gwlb-PANW-f975	Add filter				K ≤ 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, 2021 at 1:55:4
d balancer: sec-gwlb-PANW-f9	75				88
escription Listeners Mon	toring Integrated services	Tags			
asic Configuration					
Name	sec-gwlb-PANW-1975				
ARN	arn:aws:elasticloadbalancing:us-	s-east-1:484857004050:loadbalancer/gwy	/sec-gwlb-PANW-f975/de1a0c1b4563010f (건		
State	active				
Туре	gateway				
IP address type	ipv4				
VPC	vpc-006987452e8ad629a 🗷				
Availability Zones	subnet-06d1664ebbe18e6e0 - u subnet-0da8a5b7c3a4537f4 - u				
Creation time	February 12, 2021 at 1:55:47 PM	M UTC-6			
ttributes					
Deletion protection	Disabled				
Constant in the local sector	Enabled				
Cross-zone load balancing					

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:

Q search : arn:aws:elasticloadb	alancing:us-east-1: 🕥 Add filter					$ \langle \langle 1 \text{ to 1 of 1} \rangle \rangle $
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, 20
Load balancer: sec-gwlb-PAN	W-f975					880
Description Listeners	Monitoring Integrated services	Tags				
A Gateway Load Balancer consi	ists of an IP listener that receives all co	nnection requests and routes the	nem to the target group you spe	cify. You can edit the listener t	o change the target group to which requests	get forwarded.
Add listener Edit Del	lete					
Listener						
	ARN arn:aws:elasticloadbalancin	g:us-east-1:484857004050:liste	ner/gwy/sec-gwlb-PANW-f975/	de1a0c1b4563010f/716d330fe	eea650db (2)	
Forwarding to target of	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:

Regis	p details Targets Monitorir istered targets (2) Filter resources by property or value Instance ID	g Tags	Port ⊽ Zone ⊽ Statu	C Deregister Register targets < 1 > us v Status details
Regis	istered targets (2)	g Tags		
		g Tags		C Deregister Register targets
Group	p details Targets Monitorin	g Tags		
Instan	nce	GENEVE: 6081	vpc-006987452e8ad629a 🖸	sec-gwlb-PANW-f975 🖸
Target	t type	Protocol : Port	VPC I	Load balancer
Basic	c configuration			
arn:aw	vs:elasticloadbalancing:us-east-1:48485	7004050:targetgroup/sec-gwlb-tg-PANW-f975/008571	08966	
-		7004050:targetgroup/sec-gwlb-tg-PANW-f975/008571	28966	
-	gwlb-tg-PANW-f975 vs:elasticloadbalancing:us-east-1:48485		18966	Det

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:

Istances (1/1) Info	C Connect	
Q Filter instances		< 1 > 6
Instance ID: i-0e6c62c3020a82cee X Clear filters		
Name V Instance ID Inst	ance state \bigtriangledown Instance type \bigtriangledown Status check Alarm st	atus Availability Zone \triangledown Public IPv4 DNS \triangledown Public IPv
FW-us-east-1c-PANW-f975 i-0e6c62c3020a82cee 📀 I	Running 🔍 Q m5.xlarge 🛛 🛇 2/2 checks passed No alarn	is 🕂 us-east-1c – –
stance: i-0e6c62c3020a82cee (FW-us-east-1c-PANW-f975)		
Details Security Networking Storage Status checks	s Monitoring Tags	
▼ Instance summary Info		
Instance summary Info Instance ID	Public IPv4 address	Private IPv4 addresses
	Public IPv4 address -	Private IPv4 addresses
Instance ID		
Instance ID		D 10.10.0.28
Instance ID D I-0e6c62c3020a82cee (FW-us-east-1c-PANW-f975)	-	四 10.10.0.28 四 10.10.0.100
Instance ID Instance ID Instance ID Instance state	- Public IPv4 DNS	 ① 10.10.0.28 ① 10.10.0.100 Private IPV4 DNS
Instance ID ☐ I-0e6c62z3020a82cee (FW-us-east-1c-PANW-f975) Instance state ⊘ Running	- Public IPv4 DNS -	О 10.10.0.28 О 10.10.0.100 Private IPv4 DNS О ip-10-10-0-100.ec2.internal
Instance ID Instance ID Instance state O Running Instance type	- Public IPv4 DNS - Elastic IP addresses	 ☞ 10.10.0.28 ☞ 10.10.0.100 Private IPv4 DNS ☞ ip-10-10-0-100.ec2.internal VPC ID

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-03223b31fbd790492. If we take a closer look at that endpoint, we can determine the subnet that it resides in:

Endpoint ID : vpce-0	03223b31fbd790492 🕥 Add filter					< < 1	to 1 of 1 >	> >
Name E	Endpoint ID	· VPC ID		Service name		+ Endpoint type -	Status	
) vi	pce-03223b31fbd790492	vpc-006987452e8ad	d629a sec-vpc-PANW-f975	com.amazonaws.vpce.us-east-1.vpce-s	vc-04c6cedd157b95a6d	GatewayLoadBala	available	
dpoint: vpce-03223b31	1fbd700492							1000
		Taos						
	Subnets Notifications	Tags						
Details		Tags	IPv6 Addresses	Network Interface ID	Outpost ID			

The subnet route table has the next hop to the destination as the TGW:

Subnets (1/1) Info						< 1 > @
search: subnet-07578	8004463f9443b X Clear filter	-				< 1 > @
search: subnet-07578	Clear filter					
Name		\bigtriangledown State \bigtriangledown	VPC 🗢	IPv4 CIDR	▽ IPv6 CIDR	
sec-gwlbe-ew-	subnet-07578004463f944	3b 🕢 Available	vpc-006987452e8ad629a sec	10.10.0.240/28	-	10
onet-07578004463f9	443b / sec-awlbe-ew-subnet-us-east	-1b-PANW-f975				
	443b / sec-gwlbe-ew-subnet-us-east					
Details Flow log	s Route table Network ACL	Tags Sharing				
Details Flow log		Tags Sharing			E	idit route table association
Details Flow log	s Route table Network ACL	Tags Sharing			E	
Details Flow log	s Route table Network ACL	Tags Sharing			E	
Details Flow log Dute table: rtb-054 Routes (3) Q. Filter routes	s Route table Network ACL	Tags Sharing			E	idit route table association
Details Flow log pute table: rtb-054 Routes (3)	s Route table Network ACL	Tags Sharing			E	idit route table association

Request Step 6 - Return to the TGW

The TGW is connected to the VPC at the subnet level via a Transit Gateway Attachment. To see this association, we navigate to the Transit Gateway Attachment list in the VPC section of the GUI and filter on the security VPC (vpc-006987452e8ad629a in this example):

Q search : vpc-006987452e8ad6	29a 🗇 Add filter						I< < 1 to 1 of 1 ⇒	> >
Name	- Transit Gateway attachment ID	 Transit Gateway ID 	- Resource type	· Resource ID		- State	- Associated route table I	D
security-tgwa-PANW-1975	tgw-attach-092303149b3633879	tgw-0ad0c9091ead9880f	VPC	vpc-0069874	52e8ad629a	available	tgw-rtb-04bf8978d5e84d8	372
	-attach-092303149b3633879							8
				Transit Gateway owner ID	484857004050			-
Details Tags			,	Transit Gateway owner ID lesource owner account ID			-	
Details Tags Transit Gateway attachment ID	tgw-attach-092303149b3633879 tgw-0ad0c9091ead9880f		r				-	
Details Tags Transit Gateway attachment ID Transit Gateway ID	tgw-attach-092303149b3633879 tgw-0ad0c9091ead9880f VPC		,	tesource owner account ID	484857004050		-	
Transit Gateway attachment ID Transit Gateway ID Resource type	tgw-attach-092303149b3633879 tgw-0ad0c9091ead9880f VPC		,	lesource owner account ID State	484857004050 available tgw-rtb-04bf8978d5e84d872		-	

The TGW attachment and the endpoint are both in the same AZ so the packets can be routed as required.

Recall that routing within the TGW is handled via route tables associated with the TGW attachment. In the above picture, we can see that the route table associated with the TGW attachment is tgw-rtb-04bf8978d5e84d872. Clicking on the link to the route table and inspecting the routes, we can see that the route to the target subnet (10.101.0.0/16) points to another attachment (tgw-attach-0b86ac38ab82dff9):

ate Transit Gateway Route Ta	Actions ~						0	÷ •
search : tgw-rtb-04bf8978d5e8	34d872 💿 Add filter						K ≤ 1 to 1 of	1 > >
Name	~ Transit Gateway route table ID	 Transit Gateway ID 	- State - Default associat	tion route table 👻 D	efault propagation	route table ~		
tgw-sec-rt-PANW-f975	tgw-rtb-04bf8978d5e84d872	tgw-0ad0c9091ead9880f	available No	N	0			
nsit Gateway Route Table: tgw	-rtb-04bf8978d5e84d872							
etails Associations Prop	pagations Prefix list references Routes	fags						
ne table below will return a maxi	mum of 1000 routes. Narrow the filter or use export re	outes to view more routes.						
Create static route Replac								
Q Filter by attributes or search b	by keyword						<pre> < 1 to 2 of 2 </pre>	> >
CIDR	Attachment		Resource type	Route type	Route state	Prefix List ID		
10.101.0.0/16	tgw-attach-0b86ac38ab82dfff9 vpc-08321c4986	2545523	VPC	static	active			
10.102.0.0/16	tgw-attach-07e43a9c4496319b1 vpc-0f681106f6	b84640d	VPC	static	active			

Following this rabbit a little further down the rabbit hole, we find that the attachment is associated with a single subnet. Traffic exiting the TGW gets dropped off into this subnet.

Create Transit Gateway Attachme	Actions *							÷	• •	
Q Transit Gateway attachment I	D: tgw-attach-0b86ac38ab82dfff9 💿 A	dd filter						< < 1 to 1 of	f1 >	×
Name	- Transit Gateway attachment ID	Transit Gateway ID	- Resource type	- Resource ID		- State	~	Associated route t	table ID	
client-server-PANW-77d3	tgw-attach-0b86ac38ab82dfff9	tgw-0ad0c9091ead9880f	VPC	vpc-08321c4	9862545523	available		tgw-rtb-08ae6a8fe9	81a354d	1
Details Tags	attach-0b86ac38ab82dfff9									
Details Tags				Transit Gateway owner ID	484857004050					
Details Tags	attach-0b86ac38ab82dff9 tgw-attach-0b86ac38ab82dfff9 tgw-0ad0c5091 ead9880f			Transit Gateway owner ID Resource owner account ID					88	
Details Tags Transit Gateway attachment ID	tgw-attach-0b86ac38ab82dfff9 tgw-0ad0c9091ead9880f									
Details Tags Transit Gateway attachment ID Transit Gateway ID	tgw-attach-0b86ac38ab82dfff9 tgw-0ad0c9091ead9880f			Resource owner account ID	484857004050					
Details Tags Transit Gateway attachment ID Transit Gateway ID Resource type	tgw-attach-0b86ac38ab82cfff9 tgw-0ad0c5091ead9880f VPC			Resource owner account ID State	484857004050 available tgw-rtb-08ae6a8fe981a354d					

Request Step 7 - The Eagle Has Landed

The request exits the TGW and gets dropped off into the subnet. Inspection of the subnet route table reveals that any traffic destined for the VPC network is delivered directly to the target:

Q Filter subnets					< 1 > @
search: subnet-0e1119f6fc333ea6d X	ers				
Name V Subnet ID		VPC \heartsuit	IPv4 CIDR	▽ IPv6 CIDR	
app-main-subnet-P subnet-0e1119f6fc333e	a6d 🛛 📿 Available	vpc-08321c49862545523 ap	10.101.0.0/28	-	9
		_			
net-0e1119f6fc333ea6d / app-main-subnet-PANW-77	d3				
net-0e1119f6fc333ea6d / app-main-subnet-PANW-77	d3				
net-0e1119f6fc333ea6d / app-main-subnet-PANW-770 Details Flow logs Route table Network AC					
Details Flow logs Route table Network AC	L Tags Sharing			Ec	lit route table association
Details Flow logs Route table Network AC	L Tags Sharing			E	lit route table association
Details Flow logs Route table Network AC	L Tags Sharing			Ec	lit route table association
Details Flow logs Route table Network AC ute table: rtb-08cda79410c2378c9 / app-main Routes (3)	L Tags Sharing			Ec	
Details Flow logs Route table Network AC ute table: rtb-08cda79410c2378c9 / app-main Routes (3)	L Tags Sharing			Ec	lit route table association
Details Flow logs Route table Network AC ute table: rtb-08cda79410c2378c9 / app-main Routes (3) Q. Filter routes	L Tags Sharing	Target		Ē	
Details Flow logs Route table Network AC ute table: rtb-08cda79410c2378c9 / app-main Routes (3) Q. Filter routes Destination	L Tags Sharing	Target gw-01c49479188ae080e		Ē	
Details Flow logs Route table Network AC ute table: rtb-08cda79410c2378c9 / app-main Routes (3)	TL Tags Sharing	-		Ē	

Inspection of the target host reveals that it resides on the destination network. This tells us that the traffic exiting the TGW is delivered directly to the target.

Instances (1/1) Info	C Connect	Instance state V Actions V Launch instances V
search: app-PANW-77d3 X Clear filters		
✓ Name ♥ Instance ID Insta	ance state 🗢 Instance type 🗢 Status check Alarm st	atus Availability Zone 🔻 Public IPv4 DNS 🛛 Public IPv4
☑ app-PANW-77d3 i-062abc81e0975ceaa	Running 🔍 Q t2.micro 🤗 2/2 checks passed No alarm	s 🕂 us-east-1b – 35.171.248.18
Instance: i-062abc81e0975ceaa (app-PANW-77d3)		
Details Security Networking Storage Status check Instance summary Info 	s Monitoring Tags	
Instance ID	Public IPv4 address	Private IPv4 addresses
口 i-062abc81e0975ceaa (app-PANW-77d3)	35.171.248.18 (app-mgmt-eip-PANW-77d3) open address 🕻	口 10.101.0.4
Instance state	Public IPv4 DNS	Private IPv4 DNS
⊘ Running	-	D ip-10-101-0-4.ec2.internal
Instance type	Elastic IP addresses	VPC ID
t2.micro	D 35.171.248.18 (app-mgmt-eip-PANW-77d3) [Public IP]	🗇 vpc-08321c49862545523 (app-vpc-PANW-77d3) 🔀
AWS Compute Optimizer finding	IAM Role	Subnet ID
Opt-in to AWS Compute Optimizer for recommendations. Learn more	-	🗗 subnet-0e1119f6fc333ea6d (app-main-subnet-PANW-77d3) 🗹
▼ Instance details Info		

Response Step 1 - The Destination Deigns to Respond

We start with the target host and note the assigned IP address (10.101.0.4) as well as subnet membership:

Filter instances rch: app-PANW-77d3 X Clear filters		< 1 > @
Name II Instance ID In		
Name V Instance ID In	istance state	status Availability Zone 🔻 Public IPv4 DNS 🛛 Public IPv4
app-PANW-77d3 i-062abc81e0975ceaa	Running ⊕⊖ t2.micro	ms + us-east-1b - 35.171.248.
nce: i-062abc81e0975ceaa (app-PANW-77d3)	== tks Monitoring Tags	
Instance summary Info		
tance ID	Public IPv4 address	Private IPv4 addresses
i-062abc81e0975ceaa (app-PANW-77d3)	35.171.248.18 (app-mgmt-eip-PANW-77d3) open address	D 10.101.0.4
tance state	Public IPv4 DNS	Private IPv4 DNS
Running	-	D ip-10-101-0-4.ec2.internal
tance type	Elastic IP addresses	VPC ID
micro	35.171.248.18 (app-mgmt-eip-PANW-77d3) [Public IP]	🗇 vpc-08321c49862545523 (app-vpc-PANW-77d3) 🖸
	IAM Role	Subnet ID
/S Compute Optimizer finding	IAM ROLE	

Clicking on the subnet and looking at the associated routing table, we see that the default route for the subnet points to the transit gateway (TGW) as the next hop.

Subnets (1/1) Info				C Actions	Create subnet
Q. Filter subnets					< 1 > @
Subnet ID: subnet-0e1119f6fc333ea6d X Clear filters					
Name V Subnet ID V	State VPC	∇	IPv4 CIDR	V IPv6 CIDR	
app-main-subnet-P subnet-0e1119f6fc333ea6d	⊘ Available vpc-	08321c49862545523 ap	10.101.0.0/28	-	9
net_0e1119f6fc777ea6d / ann_main_subnet_DANW_77d7					
onet-0e1119f6fc333ea6d / app-main-subnet-PANW-77d3					
	igs Sharing				
	igs Sharing				
Details Flow logs Route table Network ACL Ta					Edit route table association
Details Flow logs Route table Network ACL Ta					Edit route table association
Details Flow logs Route table Network ACL Ta nute table: rtb-08cda79410c2378c9 / app-main-rt-PAN Routes (3)					
Details Flow logs Route table Network ACL Ta					
Details Flow logs Route table Network ACL Ta oute table: rtb-08cda79410c2378c9 / app-main-rt-PAN Routes (3) Q. Filter routes		e			
Details Flow logs Route table Network ACL Ta oute table: rtb-08cda79410c2378c9 / app-main-rt-PAN Routes (3) Q. Filter routes Destination	NW-77d3 Targe	t 1649479188ae080e			
pute table: rtb-08cda79410c2378c9 / app-main-rt-PAN	NW-77d3 Targe				Edit route table association

Assuming a listener on the requested port, the responder does an internal route lookup and puts the packet out on the wire (local subnet) which has a default route via the TGW.

Response Step 2 - Transit Gateway (TGW)

The TGW is connected to the VPC via a Transit Gateway Attachment. To see this association, we navigate to the Transit Gateway Attachment list and filter on the VPC hosting the target (vpc-08321c49862545523):

Create Transit Gateway Attachm	ent Actions *						0 •
Q search : vpc-08321c49862545	523 💿 Add filter						$ \langle \langle 1 \text{ to 1 of 1} \rangle \rangle$
Name	· Transit Gateway attachment ID	 Transit Gateway ID 	~ Resource type	· Resource ID		- State	 Associated route table ID
client-server-PANW-77d3	tgw-attach-0b86ac38ab82dfff9	tgw-0ad0c9091ead9880f	VPC	vpc-08321c4	9862545523	available	tgw-rtb-08ae6a8fe981a354d
ransit Gateway Attachment: tgw	-attach-0b86ac38ab82dfff9						88
Details Tags				Transit Gateway owner ID	484857004050		88
	tgw-attach-0b86ac38ab82dfff9			Transit Gateway owner ID Resource owner account ID	484857004050 484857004050		88
Details Tags Transit Gateway attachment ID	tgw-attach-0b86ac38ab82dfff9 tgw-0ad0c9091oad9880f						88
Details Tags Transit Gateway attachment ID Transit Gateway ID	tgw-attach-0b86ac38ab82dfff9 tgw-0ad0c9091ead9880f VPC			Resource owner account ID	484857004050		
Details Tags Transit Gateway attachment ID Transit Gateway ID Resource type	tgw-attach-0b86ac38ab82dfff9 tgw-0ad0c9091ead9880f VPC			Resource owner account ID State	484857004050 available		

Note that when creating a TGW Attachment, a subnet must be specified and traffic can only be routed to a TGW Attachment in the same availability zone (AZ). In this case, the TGW Attachment and the host exist on the same subnet (and hence same AZ).

Routing within the TGW is handled via route tables associated with the TGW attachment. In the above picture, we can see that the route table associated with the

TGW attachment is tgw-rtb-08ae6a8fe981a354d. Clicking on the link to the route table and inspecting the routes, we can see that the default route points to a different attachment:

Transit Gateway route table ID : tgw-rtb-08ae6a8ie981a354d Ad Mare Image Transit Gateway route table ID Image Image Image Image Image Image Image Image	reate fra	ansit Gateway Rout	te Table Actions	s *								Ð	•
tgw-app-rt-PANW-77d3 tgw-rtb-08ae6a8fe881a354d tgw-0ad0c9991ead9880f available No No ransit Gateway Route Table: tgw-rtb-08ae6a8fe881a354d Free Control of the table tabl	C Trans	sit Gateway route ta	able ID : tgw-rtb-08ae	6a8fe981a354d 🕥 Add filte	r							K < 1 to 1 of 1	1 >
ransit Gateway Route Table: tgw-rtb-08ae6a8fe981a354d E	Nam	ne		- Transit Gateway route ta	ble ID 🔺	Transit Gateway ID	- State	Default associa	tion route table 👻	Default propagation r	oute table ~		
ransit Gateway Route Table: tgw-rtb-08ae6a8te981a354d Details Associations Propagations Prefix list references Routes Tags The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes. Create static route Replace static route Delete static route	tgw-a	app-rt-PANW-77d3		tgw-rtb-08ae6a8fe981a35	4d	tgw-0ad0c9091ead9880f	available	No		No			
Q. Filter by attributes or search by keyword	Details The table	Associations	Propagations I maximum of 1000 re	Prefix list references Ro outes. Narrow the filter or us	Ū								
CIDR Attachment Resource type Route type Prefix List ID				ent			Resou	rce type	Route type	Route state		< 1 to 1 of 1 >	×

Following the rabbit a little further down the hole, we find that the attachment is associated with two different subnets. Traffic from the requester gets dropped off into one of these subnets when it exits the TGW.

Transit Gateway attachment	ID : tgw-attach-092303149b3633879	Add filter					$ \langle \langle 1 \text{ to 1 of 1} \rangle$
Name	+ Transit Gateway attachment ID	* Transit Gateway ID	- Resource type	+ Resource I	D	- State	- Associated route table ID
security-tgwa-PANW-f975	tgw-attach-092303149b3633879	tgw-0ad0c9091ead9880f	VPC	vpc-006987	452e8ad629a	available	tgw-rtb-04bf8978d5e84d872
onsit Gateway Attachment: tgw Details Tags	-attach-092303149b3633879						88
etails Tags	-attach-092303149b3633879 tgw-attach-092303149b3633879			Transit Gateway owner ID	484857004050		88
etails Tags	tgw-attach-092303149b3633879			Transit Gateway owner ID Resource owner account ID			
etails Tags Transit Gateway attachment ID	tgw-attach-092303149b3633879 tgw-0ad0c9091ead9880f				484857004050		
etails Tags Transit Gateway attachment ID Transit Gateway ID	tgw-attach-092303149b3633879 tgw-0ad0c9091ead9880f VPC			Resource owner account ID	484857004050 available		88

N.B. - The TGW has the ability to load balance across as well as ensure traffic symmetry. More information on traffic symmetry can be found here:

https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-appliance-scenario.html

If we look at the route table of one of the subnets, we can see that the traffic is directed to a GWLB endpoint:

Q Filter subnets	af94c3d663 X Clear filters						< 1	>	¢
Name	⊽ Subnet ID	⊽ State	♥ VPC	∇	IPv4 CIDR	V IPv6 CIDR	⊽ А	vailable	e
sec-tgwa-subnet	us subnet-0d8d93baf94c3d66	3 🔗 Availa	ble vpc-0069874	52e8ad629a sec	10.10.1.64/28	-	10)	
	63 / sec-tgwa-subnet-us-east-1b-P. Route table Network ACL	ANW-f975 Tags Shar						-	
Details Flow logs		Tags Shar	ing				Edit route table as		
Details Flow logs ute table: rtb-0d94 Routes (4)	Route table Network ACL	Tags Shar	ing					sociati	io
Details Flow logs ute table: rtb-0d94 Routes (4) Q Filter routes	Route table Network ACL	Tags Shar	ing				Edit route table as	sociati	ioi
Details Flow logs ute table: rtb-0d94 Routes (4)	Route table Network ACL	Tags Shar	ing -f975				Edit route table as	sociati	io

The route table associated with the other subnet looks similar (note that the Endpoint ID is different):

Subnets (1/1) Info		C Actions Create subnet
Q Filter subnets		< 1 > (3)
search: subnet-0624e157397d83c5b X Clear filters		
Name V Subnet ID V State	▽ VPC ▽ IPv4 CIDR ▽	IPv6 CIDR \heartsuit Available IPv4 addresses \bigtriangledown
sec-tgwa-subnet-us subnet-0624e157397d83c5b O Available	vpc-006987452e8ad629a sec 10.10.1.80/28	- 10
	=	
Details Flow logs Route table Network ACL Tags Sharing		Edit route table association
Details Flow logs Route table Network ACL Tags Sharing ute table: rtb-07f9337931eb34245 / tgwa-rt-us-east-1c-PANW-f93 rtb-07f937931eb34245 / tgwa-rt-us-east-1c-PANW-f93 rtb-07f937931eb34245 / tgw		Edit route table association
Details Flow logs Route table Network ACL Tags Sharing ute table: rtb-07f9337931eb34245 / tgwa-rt-us-east-1c-PANW-f93 rtb-07f937931eb34245 / tgwa-rt-us-east-1c-PANW-f93 <tdrdot pa<="" part="" td=""><td></td><td>Edit route table association</td></tdrdot>		Edit route table association
Details Flow logs Route table Network ACL Tags Sharing ute table: rtb-07f9337931eb34245 / tgwa-rt-us-east-1c-PANW-f93 Routes (4) Routes (4) <td></td> <td></td>		
Details Flow logs Route table Network ACL Tags Sharing ute table: rtb-07f9337931eb34245 / tgwa-rt-us-east-1c-PANW-f93 Routes (4) Rou	75	
Details Flow logs Route table Network ACL Tags Sharing ute table: rtb-07f9337931eb34245 / tgwa-rt-us-east-1c-PANW-f97 Routes (4) Q. Filter routes Destination 10.10.0.0/16	75 Target	
ute table: rtb-07f9337931eb34245 / tgwa-rt-us-east-1c-PANW-f9 Routes (4)	75 Target Iocal	

Response 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. An Endpoint is connected to the GWLB via an Endpoint Service. In this case, the traffic is sent to the same Endpoint irrespective of whether we are attempting to reach APP VPC 1 or APP VPC 2. To see more information about this connection,

click on the target associated with either APP VPC 1 (10.101.0.0/16) or APP VPC 2 (10.102.0.0/16). The subsequent page shows additional information about the endpoint, including the associated Endpoint Service:

reate Endpoint	Actions ~									0	• •
ر search : vpce	e-03223b31fbd790	492 🔿 Add filter							1<	\leq 1 to 1 of	1 > >
Name	- Endpoint I	D	- VPC ID		Servi	ice name		Endpoint type	- Status	~ Ci	reation tim
	vpce-03223	b31fbd790492	vpc-0069874	52e8ad629a sec-vpc-PANW-f975	5 com.a	amazonaws.vpce.us-east-1.	vpce-svc-04c6cedd157b95a6d	GatewayLoadBala	available	Fe	bruary 12.
	Subnets		Taos								885
dpoint: vpce-03	Subnets Endpoint ID	Notifications vpce-03223b31fbd790	Tags			VPC ID	vpc-006987452e8ad629a sec-v	vpc-PANW-1975			880
	Subnets Endpoint ID Status	Notifications vpce-03223b31fbd790 available	492			Status message			5860		880
Details	Subnets Endpoint ID	Notifications vpce-03223b31fbd790	492 :59:23 PM UTC-6				vpc-006987452e8ad629a sec-v com.amazonaws.vpce.us-east-1		5a6d		880

If we then look at Endpoint Services, we can see that this service is associated with a multi-AZ load balancer (also note that the Endpoint Service is associated with multiple AZs):

	Actions Y						0	\$
ာ com.amazonaws.vr	pce.us-east-1.vpce-svc-04c6cedd	157b95a6d				us-east-1b	1 to 1 of 1	> >
Name -	ID	Types	Service name		Status	Availa us-east-1c	pes	
r	vpce-svc-04c6cedd157b95a6d	GatewayLoadBala	com amazonaws vpce us-east-1.v	pce-svc-04c6cedd157b95a6d	Available	2 Availability Zones No		
idpoint Service: vpc	e-svc-04c6cedd157b95a6d							880
Details	Load Balancers Whiteliste	d principals Endpoin	nt Connections Notifications	Tags				
Manage the Load Ba	lancers associated with your end	lpoint service. Load Bala	ncers accept requests received from	endpoints that are created for the en	dpoint service and route	those requests to targets hosting your servi	ce.	
	ociate Load Balancers							
Associate/Disass								
Associate/Disass							K ≤ 1 to 2 of 2 >	н
Associate/Disasso	Load Balancer nar	nes					$ \langle \langle 1 \text{ to 2 of 2} \rangle \rangle$	×
							K < 1 to 2 of 2 →	Я

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

	-gwlb-PANW-f975	Add filter							< < 1 to	1 of 1 >	×
Name		DNS name		- State		· VPC ID	 Availability Zones 	- Туре	 Created At 		N
sec-gwlb-PA		Dito name		active		vpc-006987452e8ad629a	us-east-1c, us-east-1b	gateway	February 12, 2021 a		
				acave	0.0.0	4p-00056/45266au625a	us-east- IC, us-east- ID	galeway	rebituary 12, 2021 e		
ad balancer:	sec-gwlb-PANW-f	75									1 6
Description	Listeners Mor	itoring Integrated services	Tags								
Basic Config	uration										
	Name	sec-gwlb-PANW-f975									
	ARN	arn:aws:elasticloadbalancing:	ue-onet-1-494957	7004050-loadbalancer/a	unione auto DANBN 60	75/do1a0a1b4563010f (D)					
	State	arti.aws.elasticioadbalaricing.	12-6921-11404021	roo-oso.ioaubaiancer/g	ny/560-9wib-FANN-15/	and race re-second re-					
	Type	gateway									
	IP address type	ipv4									
		vpc-006987452e8ad629a 🗗									
	VPC										
A1	VPC		- us-east-1c 🕅								
A	VPC wailability Zones	subnet-06d1664ebbe18e6e0 subnet-06d8a5b7c3a4537f4 -									
A		subnet-06d1664ebbe18e6e0	us-east-1b 🗗								
	vailability Zones	subnet-06d1664ebbe18e6e0 subnet-0da8a5b7c3a4537f4 -	us-east-1b 🗗								
Ar Attributes	vailability Zones	subnet-06d1664ebbe18e6e0 subnet-0da8a5b7c3a4537f4 -	us-east-1b 🗗								
Attributes	vailability Zones	subnet-06d1864ebbe18e6e0 subnet-0da8a5b7c3a4537f4 - February 12, 2021 at 1:55:47 I	us-east-1b 🗗								

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.

Response Step 4 - 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.

Q search : arn:aws:elasticloadbalancing	us-east-1: 🔘 Add filter					$ \langle \langle 1 \text{ to 1 of 1} \rangle \rangle $
Name + DN	S name	v	State	- VPC ID	 Availability Zones Type 	- Created At
sec-gwlb-PANW-1975			active	vpc-006987452e8ad629a	us-east-1c, us-east-1b gateway	February 12, 20
.oad balancer: sec-gwlb-PANW-f975						888
Description Listeners Monitori	Integrated services	Tags				
A Gateway Load Balancer consists of a	IP listener that receives all c	onnection requests and routes th	em to the target group you	specify. You can edit the listene	er to change the target group to which request	ts get forwarded.
Add listener Edit Delete						
Listener						
ARN	arn:aws:elasticloadbalancir	ng:us-east-1:484857004050:liste	ner/gwy/sec-gwlb-PANW-f9	75/de1a0c1b4563010f/716d33	Ofeea650db අ	
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:

2 > Target groups > sec-gwlb-tg-PA					
ec-gwlb-tg-PANW-f9	75				Delet
arn:aws:elasticloadbalancing:us-east-1:48	4857004050:targetgroup/sec-gwlb-tg-PA	ANW-f975/008571474a4c908966			
Basic configuration					
Target type Instance	Protocol : Port GENEVE: 6081	VPC	52e8ad629a 🔀		Load balancer sec-gwlb-PANW-f975 🔀
	GENEVE. 0001	vpc-00698745	5268a0629a 🔽		Sec-gwid-FARW-1973
Group details Targets Monit		vpc-00698745	2669900739 [2]		30-980-1907-1972 E
Group details Targets Monit		vpc-00698743	2269900739 [7]		C Deregister Register targets
		vpc-00698743	5269405734 [2]		
Group details Targets Monit		vpc-00698743	v Zone Zone	⊽ Sta	C Deregister Register targets < 1 > 6
Group details Targets Monit Registered targets (2) Q. Filter resources by property or value	oring Tags	v Port		500	C Deregister Register targets

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:

Q Filter instances		< 1 >
Instance ID: i-0e6c62c3020a82cee X Clear filters		
Name V Instance ID Inst	ance state 🛛 Instance type 🔍 Status check Alarm s	tatus Availability Zone 🗵 Public IPv4 DNS 🛛 Public IF
FW-us-east-1c-PANW-f975 i-0e6c62c3020a82cee 📀	Running 🔍 Q m5.xlarge 🥥 2/2 checks passed No alar	ns 🕂 us-east-1c – –
	=	
tance: i-0e6c62c3020a82cee (FW-us-east-1c-PANW-f975)		
Details Security Networking Storage Status check	s Monitoring Tags	
Details Security Networking Storage Status check	s Monitoring Tags	
▼ Instance summary Info		
Instance ID	Public IPv4 address	Private IPv4 addresses
i-0e6c62c3020a82cee (FW-us-east-1c-PANW-f975)	-	☐ 10.10.0.28
		□ 10.10.0.100
Instance state	Public IPv4 DNS	Private IPv4 DNS
⊘ Running	-	D ip-10-10-0-100.ec2.internal
Instance type	Elastic IP addresses	VPC ID
m5.xlarge	52.7.218.8 (fw-mgmt-eip-us-east-1c-PANW-f975) [Public IP]	vpc-006987452e8ad629a (sec-vpc-PANW-f975) ☑
	Er senterete (in nyme ep us ease te thermosis) (i ubien j	
AWS Compute Optimizer finding	IAM Role	Subnet ID
Opt-in to AWS Compute Optimizer for recommendations. Learn more 2	🗇 iam-role-PANW-f975 🗹	🗗 subnet-06d1664ebbe18e6e0 (sec-data-subnet-us-east-1c-PANW- f975) 🖸

Response 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-03223b31fbd790492. If we take a closer look at that endpoint, we can determine the subnet that it resides in:

Create Endpoint Activ	ons 👻						÷	• •
Q Endpoint ID : vpce-0	3223b31fbd790492					IK K	to 1 of 1	> >
Name - Er	ndpoint ID	· VPC ID		Service name		Endpoint type	Status	
vp	oce-03223b31fbd790492	vpc-006987452e8a	d629a sec-vpc-PANW-f975	com.amazonaws.vpce.us-east-1.vpce-s	vc-04c6cedd157b95a6d	GatewayLoadBala	availabl	е
ndpoint: vpce-03223b31	fbd790492	Tags						
Manage Subnets		lago						
Subnet ID	Availability Zone	IPv4 Addresses	IPv6 Addresses	Network Interface ID	Outpost ID			
subnet- 07578004463f9443b	us-east-1b (use1-az1)	10.10.0.252	*	eni-03fae688ac27a4185	-			

The subnet route table points has the next hop to the destination as the TGW:

Q Filter subnets						< 1 >
search: subnet-07578	Clear filter	5				
Name		⊽ State ⊽	7 VPC	▽ IPv4 CIDR		
sec-gwlbe-ew-	subn subnet-07578004463f9443	5b 🕢 Available	vpc-006987452e8ad629	a sec 10.10.0.240/28	-	10
			—			=
	443b / sec-gwlbe-ew-subnet-us-east s Route table Network ACL	Tags Sharing				
etails Flow log	s Route table Network ACL	Tags Sharing	975			Edit route table assoc
retails Flow log		Tags Sharing	975			Edit route table assoc
Details Flow log	s Route table Network ACL	Tags Sharing	975			Edit route table assoc
tte table: rtb-054	s Route table Network ACL	Tags Sharing	975			Edit route table assoc
Petails Flow log ute table: rtb-054 Routes (3) Q Filter routes	s Route table Network ACL	Tags Sharing	1975 Target			
Details Flow log ute table: rtb-054 Routes (3) Q. Filter routes Destination	s Route table Network ACL	Tags Sharing				
Details Flow log ute table: rtb-057 Routes (3)	s Route table Network ACL	Tags Sharing	Target			

Response Step 6 - Return to the TGW

The TGW is connected to the VPC at the subnet level via a Transit Gateway Attachment. To see this association, we navigate to the Transit Gateway Attachment list in the VPC section of the GUI and filter on the security VPC (vpc-006987452e8ad629a in this example):

								•
Q search : vpc-006987452e8ad6	29a 🔿 Add filter						K < 1 to 1 of 1	1 >>>
Name	- Transit Gateway attachment ID	 Transit Gateway ID 	- Resource type	· Resource I	D	- State	- Associated route tab	ble ID
security-tgwa-PANW-f975	tgw-attach-092303149b3633879	tgw-0ad0c9091ead9880f	VPC	vpc-006987	452e8ad629a	available	tgw-rtb-04bf8978d5e8	84d872
ansit Gateway Attachment: tgw Details Tags	attach-092303149b3633879							88
Details Tags				Transit Gateway owner ID	484857004050			88
				Transit Gateway owner ID				88
etails Tags Transit Gateway attachment ID	tgw-attach-092303149b3633879 tgw-0ad0c9091ead9880f				484857004050			
etails Tags Transit Gateway attachment ID Transit Gateway ID	tgw-attach-092303149b3633879 tgw-0ad0c9091ead9880f			esource owner account ID	484857004050 available			
transit Gateway attachment ID Transit Gateway ID Resource type	tgw-attach-092303149b3633879 tgw-0ad0c9091ead9880f VPC			esource owner account ID State	484857004050 available tgw-rtb-04bf8978d5e84d872			

The TGW attachment and the endpoint are both on the same subnet (same AZ).

Recall that routing within the TGW is handled via route tables associated with the TGW attachment. In the above picture, we can see that the route table associated with the TGW attachment is tgw-rtb-04bf8978d5e84d872. Clicking on the link to the route table and inspecting the routes, we can see that the route to the requester subnet (10.102.0.0/16) points to another attachment (tgw-attach-07e43a9c4496319b1):

	ansit Gateway Ro	Acut	ons *									0	•
C, Tran	sit Gateway route	table ID : tgw-rtb-04	bf8978d5e84d872 🔿 Ad	ld filter									> >
Nam	10		- Transit Gateway ros	ute table ID		Transit Gateway ID	- State	- Default as	ssociation route table -	Default propagation	n route table ~		
tgw-r	sec-rt-PANW-f975		tgw-rtb-04bf8978d5e	84d872		tgw-0ad0c9091ead9880f	available	No		No			
ansit Gal	teway Route Tab	le: tgw-rtb-04bf897	8d5e84d872										880
Details	Associations	Propagations	Prefix list references	Routes	Tags								
The table	below will return	a maximum of 1000	o routes. Narrow the filter	or use expo	rt routes	to view more routes.							
Create	static route	Replace static rout	e Delete static route	•									
Q, Filt	ter by attributes or t	search by keyword										$ \langle \langle 1 \text{ to 2 of 2} \rangle \rangle$	>1
0	CIDR	Attach	ument				Reso	urce type	Route type	Route state	Prefix List ID		
1	0.101.0.0/16	tgw-at	tach-Ob86ac38ab82dff9	vpc-08321c4	862545	523	VPC		static	active			

Following this rabbit a little further down the hole, we find that the attachment is associated with a single subnet. Traffic exiting the TGW gets dropped off into this subnet.

Create Transit Gateway Attachme	Actions Y						0 ¢ (
Q Transit Gateway attachment I	D : tgw-attach-07e43a9c4496319b1	Add filter				IK K	< 1 to 1 of 1 > >
Name	- Transit Gateway attachment ID	Transit Gateway ID	- Resource type	- Resource ID	~ State	 Associated route table ID 	- Association s
client-server-PANW-b4c2	tgw-attach-07e43a9c4496319b1	tgw-0ad0c9091ead9880f	VPC	vpc-0f681106f6b84640d	available	tow-rtb-0f89b1da68b6b5d2c	associated
ransit Gateway Attachment: tgw-	attach-07e43a9c4496319b1						
Details Tags					48-165-700-1050		880
Details Tags Transit Gateway attachment ID	tgw-attach-07e43a9c4496319b1			Transit Gateway owner ID	484857004050 494857004050		
Details Tags Transit Gateway attachment ID Transit Gateway ID	tgw-attach-07e43a9c4496319b1 tgw-0ad0c9091ead9880f			Transit Gateway owner ID	484857004050 484857004050 available		880
Details Tags Transit Gateway attachment ID Transit Gateway ID Resource type	tgw-attach-07e43a9c4496319b1			Transit Gateway owner ID Resource owner account ID	484857004050		885
Details Tags Transit Gateway attachment ID Transit Gateway ID Resource type	tgw-attach-07e43a9c4496319b1 tgw-0ad0c9091ead9880f VPC			Transit Gateway owner ID Resource owner account ID State Associated route table	484857004050 available		885

Response Step 7 - At Last

Inspection of the subnet route table reveals that any traffic destined for the network is delivered locally:

Subnets (1/1) Info			C Actions Create subr	net
Q Filter subnets			< 1 >	6
search: subnet-0709ac7ea08f1e5a3 × Clear filters				
🖸 Name 🔻 Subnet ID 🗢 State 🗢	VPC v IPv4 CIDR	V IPv6 CIDR		
app-main-subnet-P subnet-0709ac7ea08f1e5a3 O Available	vpc-0f681106f6b84640d ap 10.102.0.0/28	-	9	
bnet-0709ac7ea08f1e5a3 / app-main-subnet-PANW-b4c2 Details Flow logs Route table Network ACL Tags Sharing				
Details Flow logs Route table Network ACL Tags Sharing			Edit route table associ	iatio
Details Flow logs Route table Network ACL Tags Sharing			Edit route table associ	iatio
Details Flow logs Route table Network ACL Tags Sharing pute table: rtb-02eae9f0eb7ce9d41 / app-main-rt-PANW-b4c2			Edit route table associ	
Details Flow logs Route table Network ACL Tags Sharing oute table: rtb-02eae9f0eb7ce9d41 / app-main-rt-PANW-b4c2 Routes (4) Q. Filter routes	Target			
Details Flow logs Route table Network ACL Tags Sharing oute table: rtb-02eae9f0eb7ce9d41 / app-main-rt-PANW-b4c2 Routes (4) Q. Filter routes Destination	Target igw-0bb33f319d240e9c4			
oute table: rtb-02eae9f0eb7ce9d41 / app-main-rt-PANW-b4c2 Routes (4)	-			

Inspection of the target host reveals that it resides on the destination network. This tells us that the traffic exiting the TGW is delivered directly to the target.

Instances (1/1) Info	C	Connect Instance state V Actions V Launch instance	es	
Q. Filter Instances		< -	1 >	۲
search: app-PANW-b4c2 X Clear filters				
☑ Name ♥ Instance ID Instan	ce state 🛛 Instance type 🔍 Status check 🛛 Alarm status	Availability Zone 🗵 Public IPv4 DNS 🛛 🗸 Public IPv4	•	Elastic IF
app-PANW-b4c2 i-049eb3bcdb0d6951f	nning @@ t2.micro	us-east-1c - 3.208.253.71		3.208.25
	=		E	
Instance: i-049eb3bcdb0d6951f (app-PANW-b4c2)			-	
Details Security Networking Storage Status checks	Monitoring Tags			
▼ Instance summary Info				
Instance ID	Public IPv4 address	Private IPv4 addresses		
I-049eb3bcdb0d6951f (app-PANW-b4c2)	🗇 3.208.253.71 (app-mgmt-eip-PANW-b4c2) open address 🖸	D 10.102.0.5		
Instance state	Public IPv4 DNS	Private IPv4 DNS		
⊘ Running	-	ip-10-102-0-5.ec2.internal		
Instance type	Elastic IP addresses	VPC ID		
t2.micro	3.208.253.71 (app-mgmt-eip-PANW-b4c2) [Public IP]	D vpc-0f681106f6b84640d (app-vpc-PANW-b4c2)		
AWS Compute Optimizer finding	IAM Role	Subnet ID		

Et violà:

ubuntu@admin-appliance: ~ (com.docker.cli)	\$1	ubuntu@ip-10-101-0-4: ~ (ssh)	ж2								
ubuntu@ip-10-102-0-5:~\$!ssh											
ssh 10.101.0.4											
ubuntu@10.101.0.4's password:											
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1037-aws	x86_64)										
<pre>* Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/advantage</pre>											
System information as of Mon Feb 15 22:02:05 UTC 2021											
System load: 0.0 Processes:	103										
Usage of /: 20.1% of 7.69GB Users logged in:											
Memory usage: 20% IP address for eth0:	10.101.0.4										
Swap usage: 0%											
 * Introducing self-healing high availability clusters Simple, hardened, Kubernetes for production, from Ra 											
https://microk8s.io/high-availability											
* Canonical Livepatch is available for installation.											
- Reduce system reboots and improve kernel security.	Activate at:										
https://ubuntu.com/livepatch											
1 package can be updated.											
0 of these updates are security updates.											
To see these additional updates run: apt listupgrada	ble										
New release '20.04.2 LTS' available.											
Run 'do-release-upgrade' to upgrade to it.											
Aun do rerease apgrade to apgrade to re.											
Last login: Mon Feb 15 22:01:05 2021 from 104.219.139.1	93										
ubuntu@ip-10-101-0-4:~\$											
Looking at the FW logs, we can see both	original source a	nd original destination:									

 \mathbb{Q} (addr in 10.101.0.0/16) and (app eq ssh)

		GENERATE TIME	түре	FROM ZONE	TO ZONE	SOURCE	DESTINATI	SOURCE USER	NAT APPLIED	NAT SOURCE IP	NAT DEST IP	TO PORT	APPLICATI	ACTION	RULE	SESSION END REASON	BYTES	ł.
Ľ	2	02/15 22:01:55	start	Trust	Trust	10.102.0.5	10.101.0.4		no			22	ssh	allow	Allowed-traffic	n/a	321	¢
K	2	02/15 19:19:27	end	Trust	Trust	10.102.0.5	10.101.0.4		no			22	ssh	allow	Allowed-traffic	tcp-fin	5.0k	(
K	2	02/15 19:19:09	start	Trust	Trust	10.102.0.5	10.101.0.4		no			22	ssh	allow	Allowed-traffic	n/a	321	¢