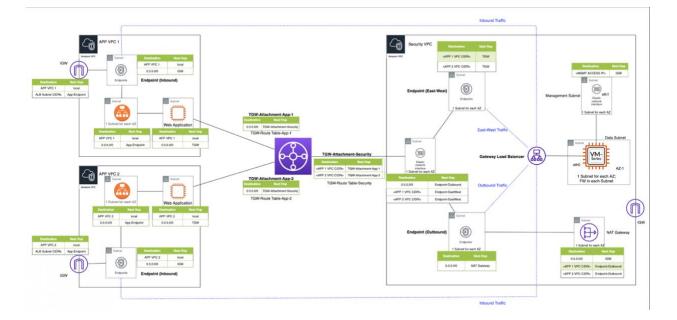
Introduction

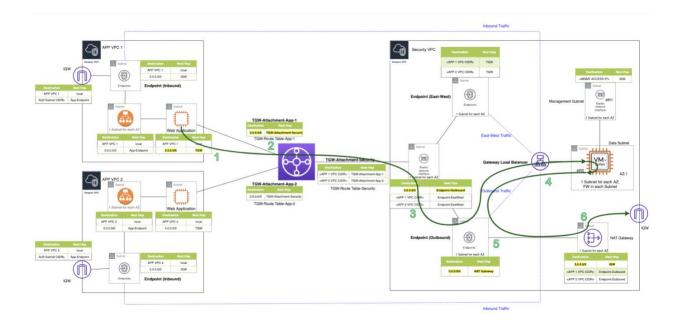
With the introduction of the Gateway Load Balancer (GWLB) in mid-November 2020, AWS provided its customers with any port, load-balancing router . Prior to that, Azure and GCP were the only public clouds that had such a construct. Customers use these to provide a security layer that is scalable, resilient,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

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

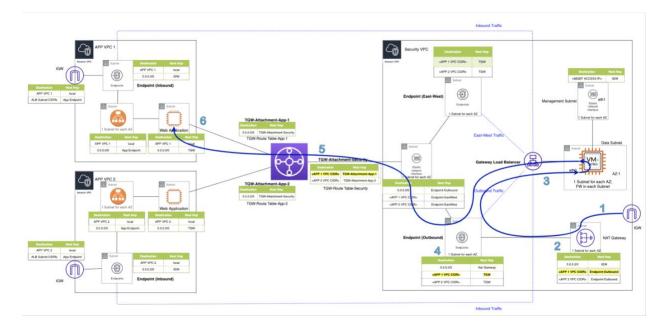


and follows current best practices regarding architecture:

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



And the corresponding response flow:

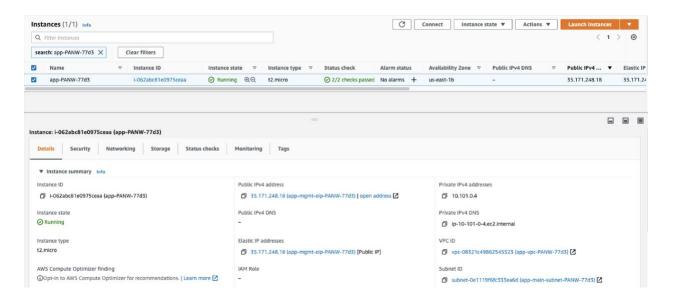


Note that AWS assigns unique resource identifiers to each resource in the environment. Examples include tgw-attach-0b86ac38ab82dff9 or subnet-0e1119f6fc333ea6d. Every resource created is assigned one of these unique identifiers. This means that although the template creates the environment using identical 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 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/process on a host (IP 10.101.0.4) in APP VPC 1 needs to connect to the internet. Looking at the EC2 instance, we can see the IP address as well as the subnet membership:



The route table associated with the subnet shows that the default route for the subnet points to the transit gateway (TGW) as the next hop.

Q Filter subnets			< 1 > @
Subnet ID: subnet-0e1119f6fc333ea6d X Clear filters			
Name ▼ Subnet ID ▼ State ▼	VPC VPC VPV4 CIDR	▽ IPv6 CIDR	
app-main-subnet-P subnet-0e1119f6fc333ea6d O Available	vpc-08321c49862545523 ap 10.101.0.0/28	-	9
net-0e1119f6fc333ea6d / app-main-subnet-PANW-77d3			
net-0e1119f6fc333ea6d / app-main-subnet-PANW-77d3 Details Flow logs <u>Route table</u> Network ACL Tags Sharing			
		Ec	iit route table associatio
Details Flow logs Route table Network ACL Tags Sharing		Ec	lit route table association
Details Flow logs Route table Network ACL Tags Sharing ute table: rtb-08cda79410c2378c9 / app-main-rt-PANW-77d3		Ed	lit route table association < 1 > @
Details Flow logs Route table Network ACL Tags Sharing ute table: rtb-08cda79410c2378c9 / app-main-rt-PANW-77d3 Routes (4) Q Filter routes	Target	Ec	
Poteialis Flow logs Route table Network ACL Tags Sharing ute table: rtb-08cda79410c2378c9 / app-main-rt-PANW-77d3 Routes (4) Q. Filter routes Destination	Target Igw-01c49479188ae080e	Ec	

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:

reate Transit Gateway Attachme	Actions V						0 •
Q search : vpc-08321c49862545	523 💿 Add filter						< < 1 to 1 of 1 > >
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-0ad0c9091ead9880	Of VPC	vpc-08321c49	9862545523	available	tgw-rtb-08ae6a8fe981a354d
	-attach-0b86ac38ab82dfff9						
Details Tags							
Details Tags Transit Gateway attachment ID	tgw-attach-0b86ac38ab82dfff9			ansit Gateway owner ID	484857004050		
Details Tags Transit Gateway attachment ID Transit Gateway ID	tgw-attach-0b86ac38ab82dfff9 tgw-0ad0c9091ead9880f		Tra	ansit Gateway owner ID ource owner account ID	484857004050 484857004050		
Transit Gateway attachment ID	tgw-attach-0b86ac38ab82dfff9 tgw-0ad0c9091ead9880f		Tra	-			
Details Tags Transit Gateway attachment ID Transit Gateway ID	tgw-attach-0b86ac38ab82dfff9 tgw-0ad0c9091ead9880f VPC		Tra	ource owner account ID	484857004050		
Details Tags Transit Gateway attachment ID Transit Gateway ID Resource type	tgw-attach-0b86ac38ab82dfff9 tgw-0ad0c9091ead9880f VPC		Tra	ource owner account ID State Associated route table	484857004050 available tgw-rtb-08ae6a8fe981a354d		

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) as the source. 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 yet another attachment:

Actions *	÷ (
Q search : tgw-rtb-08ae6a8/e991a354d 💿 Add filter	K < 1 to 1 of 1 ⇒
Name v Transit Gateway route table ID * Transit Gateway ID v State v Default association route table v Default propagation route table	*
tgw-app-rt-PANW-77d3 tgw-rtb-08ae6a8fe981a354d tgw-0ad0c9091ead9880f available No No	
ransit Gateway Route Table: tgw-rtb-08ae6a8fe981a354d 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 Delete static route Delete static route Delete static route	
Q. Filter by attributes or search by keyword	$ \langle \langle 1 \text{ to 1 of 1} \rangle \rangle$
CIDR Attachment Resource type Route type Route state Prefix L	ist ID
0.0.0/0 tgw-attach-092303149b3633879 vpc-006987452e8ad629a VPC static 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	ent Actions *						0 ¢
Q Transit Gateway attachment	ID: tgw-attach-092303149b3633879	Add filter					< < 1 to 1 of 1 > >
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-00698745	2e8ad629a	available	tgw-rtb-04bf8978d5e84d872
Details Tags Transit Gateway attachment ID	tgw-attach-092303149b3633879		Ter	nsit Gateway owner ID	484857004050		
Transit Gateway attachment ID				urce owner account ID	484857004050		
Resource type			neso	State	available		
Resource ID				Associated route table	tgw-rtb-04bf8978d5e84d872		
Association state	associated			DNS support	enable		
IPv6 support	disable			Subnet IDs	subnet-0d8d93baf94c3d663		
					subpet-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

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.

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							< 1 >	Q
search: subnet-0d8d93baf94c3d66	3 X Clear filters							
Name \bigtriangledown	Subnet ID	⊽ State	▽ VPC	∇	IPv4 CIDR		⊽ Available	le
sec-tgwa-subnet-us	subnet-0d8d93baf94c3d663	⊘ Availat	ble vpc-006987	452e8ad629a sec	10.10.1.64/28	-	10	
								_
								E.
			—					l
iet-0d8d93baf94c3d663 / sec-tg	jwa-subnet-us-east-1b-PAN	NW-f975	—				_	l
net-0d8d93baf94c3d663 / sec-tg	jwa-subnet-us-east-1b-PAN	NW-f975	—					I
								I
		NW-f975 Tags Shari						[
etails Flow logs Route	table Network ACL	Tags Shari	ng				Edit route table associati	
etails Flow logs Route	table Network ACL	Tags Shari	ng					
Details Flow logs Route	table Network ACL	Tags Shari	ng					
Details Flow logs Route	table Network ACL	Tags Shari	ng					
retails Flow logs Route ret table: rtb-0d94d34e75c Routes (4)	table Network ACL	Tags Shari	ng				Edit route table associati	i
retails Flow logs Route ret table: rtb-0d94d34e75c Routes (4)	table Network ACL	Tags Shari	ng				Edit route table associati	tic
etails Flow logs Route te table: rtb-0d94d34e75c toutes (4) Q. Filter routes	table Network ACL	Tags Shari	ng				Edit route table associati	tic
etails Flow logs Route rte table: rtb-0d94d34e75c Routes (4) Q. Filter routes Destination	table Network ACL	Tags Shari	ng f975				Edit route table associati	tic
net-Od8d93baf94c3d663 / sec-tg Details Flow logs Route ute table: rtb-Od94d34e75c Routes (4) Q. Filter routes Destination 0.100.00/16 0.101.00/16	table Network ACL	Tags Shari	ng f975 Target	2			Edit route table associati	E tio

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

Q Filter subnets						< 1	>
search: subnet-0624e1	Subnet ID Subnet ID		♥ VPC	♥ IPv4 CIDR	♥ IPv6 CIDR		es
sec-tgwa-subne	t-us subnet-0624e157397d8	3c5b 🔗 Available	vpc-006987452e8a	d629a sec 10.10.1.80/28	-	10	
* 06240157707497		DANIM 6075	—				=
	C5b / sec-tgwa-subnet-us-east-1c Route table Network AC						
etails Flow logs		L Tags Sharing				Edit route table ass	ociati
retails Flow logs te table: rtb-07fs toutes (4)	Route table Network AC	L Tags Sharing				Edit route table ass	
Petails Flow logs ite table: rtb-07fs Routes (4) Q Filter routes	Route table Network AC	L Tags Sharing	Target				
Details Flow logs	Route table Network AC	L Tags Sharing	Target				
Details Flow logs ute table: rtb-07fs Routes (4) Q. <i>Filter routes</i> Destination	Route table Network AC	L Tags Sharing		м			

The Endpoint is connected to the GWLB via an Endpoint Service. In this case, the traffic is routed out the Endpoint associated with the default gateway (vpce-

000ae0168a8c692c3). To see more information about this connection, click on the target. The subsequent page shows additional information about the Endpoint, including the associated Endpoint Service:

Create Endpoint	Actions V					0	• 0
Q Endpoint ID	: vpce-000ae0168	a8c692c3 🔿 Add filter			I< <	1 to 1 of 1	> >
Name	- Endpoint I	D *	VPC ID	Service name * Endpoint	type	- Status	
	vpce-000ae	0168a8c692c3	vpc-0069874	2e8ad629a sec-vpc-PANW-1975 com.amazonaws.vpce.us-east-1.vpce-svc-04c6cedd157b95a6d GatewayL	oadBala	. availat	le
Endpoint: vpce-0	00ae0168a8c692 Subnets	Notifications	Tags				
	Endpoint ID	vpce-000ae0168a8c692c3		VPC ID vpc-006987452e8ad629a sec-vpc-PANW-f975			
	Status	available		Status message			
	Creation time	February 12, 2021 at 1:57:	0 PM UTC-6	Service name com.amazonaws.vpce.us-east-1.vpce-svc-04c6cedd157b95i	a6d		
	Endpoint type	GatewayLoadBalancer		DNS names			
Private DNS	names enabled	÷					

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 *						0	¢
Ĵ com.amazonaws.vpce.us	s-east-1.vpce-svc-04c6cedd15	57b95a6d				us-east-1b	1 to 1 of 1	1 > >
Name - ID		Types	Service name		Status	Availa us-east-1c	nes	
vpc	e-svc-04c6cedd157b95a6d	GatewayLoadBala	com amazonaws vpce us-east-1.	vpce-svc-04c6cedd157b95a6d	Available	2 Availability Zones No		
dpoint Service: vpce-svc	c-04c6cedd157b95a6d							
Details Load	Balancers Whitelisted	principals Endpoi	nt Connections Notifications	Tags				
Manage the Load Balance	ers associated with your ends	point service. Load Bala	ncers accept requests received from	endpoints that are created for the er	ndpoint service and route	those requests to targets hosting your servi	ce.	
	and and Balance							
Associate/Disassociat	te Load Balancers							
Associate/Disassociat	te Load Balancers						< < 1 to 2 of 2 →	>
Associate/Disassociat	Load Balancers	es					$ \langle \langle 1 to 2 of 2 \rangle \rangle$	×
							< < 1 to 2 of 2 >	×

Clicking on the loadbalancer, we see more detailed information:

Q search : se	ec-gwlb-PANW-f975	Add filter										< < 1 t	o 1 of 1	> >
Name		DNS name			State	*	VPC ID	~ A1	ailability Zones	Туре	*	Created At		-
sec-gwlb-P	PANW-f975				active		vpc-006987452e8ad629a	us	east-1c, us-east-1b	gateway		February 12, 2021	at 1:55:4	l
ad balancer:	sec-gwlb-PANW-f9	75												
Description	Listeners Mon	itoring Integrated services	Tags											
Basic Confi	iguration													
	Name	sec-gwlb-PANW-f975												
	ARN	arn:aws:elasticloadbalancing:	us-east-1:4848	57004050:loadbal	lancer/gwy/sec-gwlb-	PANW-f975	/de1a0c1b4563010f (건							
	State	active												
	Туре	gateway												
	IP address type	ipv4												
	VPC	vpc-006987452e8ad629a 🗷												
	Availability Zones	subnet-06d1664ebbe18e6e0 subnet-0da8a5b7c3a4537f4 -												
	Creation time	February 12, 2021 at 1:55:47 F	PM UTC-6											
	Creation time	February 12, 2021 at 1:55:47 l	PM UTC-6											
Attributes	Creation time		PM UTC-6											
Attributes		n Disabled	PM UTC-6											

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:elasticloadbaland	sing: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, 2
oad balancer: sec-gwlb-PANW-f9	75				880
Description Listeners Monit	toring Integrated services Tags				
A Gateway Load Balancer consists of	f an IP listener that receives all connection requests and rout	ites them to the target group you	specify. You can edit the listener	to change the target group to which requests g	et forwarded.
Add listener Edit Delete					
Listener					
ARM	arn:aws:elasticloadbalancing:us-east-1:484857004050	D:listener/gwy/sec-gwlb-PANW-1	975/de1a0c1b4563010f/716d330	feea650db	
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:

2 > Target groups > sec-gwlb-tg-PANW-F975							
ec-gwlb-tg-PANW-f975							
arn:aws:elasticloadbalancing:us-east-1:484857004050:targetgroup/sec-gwlb-tg-PANW-f975/008571474a4c908966							
Basic configuration							
Target type	Protocol : Port GENEVE: 6081	VPC	Load balancer				
Instance	GENEVE: 6081	vpc-006987452e8ad629a 🔀	sec-gwlb-PANW-f975 🔀				
Group details Targets Monit		vpc-00698745288ad629a	sec-gwlb-PANW-1975				
		vpc-00698745288ad629a	sec-gwlb-PANW-1975				
Group details Targets Monit		vpc-00698745268ad629a					
Group details Targets Monit		vpc-00698745288ad629a [2] ▼ Port ▼ Zone	C Deregister Register targets				
Group details Targets Monit Registered targets (2) Q. Filter resources by property or value	oring Tags		C Deregister Register targets < 1 > ③				

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:

	C Connect	,
Instance: i-0e6c62c3020a82cee (FW-us-east-1c-PANW-f975)	=	. M 8
Details Security Networking Storage Status checks	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)
-	S2.7.210.0 (Weinginteep-us-ease terrainers/s) [Fubile in]	■ *Pr-00030743260800238 (360-4Pt-FMRW-1373) ■
AWS Compute Optimizer finding	IAM Role	Subnet ID
Opt-in to AWS Compute Optimizer for recommendations. Learn more	iam-role-PANW-f975	In Subnet-06d1664ebbe18e6e0 (sec-data-subnet-us-east-1c-PANW- 1975)
▼ Instance details Info		

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 in step 3 is vpce-000ae0168a8c692c3. If we take a closer look at that endpoint, we can determine the subnet that it resides in:

search : vpce-000ae	0168a8c692c3 O Add filter					< < 1	to 1 of 1	> >
Name - E	ndpoint ID	- VPC ID		Service name		* Endpoint type ~	Status	
) vj	pce-000ae0168a8c692c3	vpc-006987452e8ad	d629a sec-vpc-PANW-f975	com.amazonaws.vpce.us-east-1.vpce-sv	vc-04c6cedd157b95a6d	GatewayLoadBala	available	
apoint: vpce-uuuaeu ie	58a8c692c3							
dpoint: vpce-000ae016								
Details	Subnets Notifications	Tags					-	
Details		Tags					-	
		Tags IPv4 Addresses	IPv6 Addresses	Network Interface ID	Outpost ID		-	

The subnet default route points to the NAT GW as the next hop:

Subnets (1/1) Info						C Actio	ons Create s	subnet	
Q Filter subnets							< 1	>	0
search: subnet-0471afc10680bfa4c 🗙	Clear filters								
Z Name ⊽ Subne	t ID 🗸	State	♥ VPC	∇	IPv4 CIDR	v IPv6 CIDR		vailable	e I
sec-gwlbe-ob-subn subnet	-0471afc10680bfa4c	⊘ Available	vpc-006987	452e8ad629a sec	10.10.0.160/28	-	10	D	
								-	
net-0471afc10680bfa4c / sec-gwlbe-o	o-subnet-us-east-1b-PAN	NW-f975							
		ww-f975							
						r			
Details Flow logs Route table	Network ACL T	ags Sharing				[Edit route table as:	sociati	or
Details Flow logs Route table	Network ACL T	ags Sharing				[Edit route table as:	sociati	or
Details Flow logs Route table ute table: rtb-008c854b5beb833 Routes (4)	Network ACL T	ags Sharing				[Edit route table as	sociati	or
Details Flow logs Route table ute table: rtb-008c854b5beb833 Routes (4)	Network ACL T	ags Sharing				[
Details Flow logs Route table ute table: rtb-008c854b5beb833	Network ACL T	ags Sharing				[Edit route table as:		
Details Flow logs Route table ute table: rtb-008c854b5beb833 Routes (4) Q Filter routes	Network ACL T	ags Sharing				[
Details Flow logs Route table ute table: rtb-008c854b5beb833 Routes (4) Q. Filter routes Destination	Network ACL T	ags Sharing	W-f975			[
Details Flow logs Route table ute table: rtb-008c854b5beb833 Routes (4)	Network ACL T	ags Sharing	W-f975 Target	sof		[ior

Request Step 6 - Into the Great Wide Open

Clicking on the NAT GW, we can see the subnet it is associated with as well as the associated Elastic IP (EIP):

Q Filter NAT gateways				< 1	> @
NAT gateway ID: nat-0e5d6f99129bcdc9	2 X Clear filters				
Name 🗢 NAT g	ateway ID 🛛 🗸 State	♥ State m	essage 🛛 Elastic IP address 🔍 Private IP	P address v Network interface ID	▽
O – nat-0e	5d6f99129bcdc92 🔗 Avail	able -	107.22.216.234 10.10.1.1	58 eni-04e24015a8303c487	ß
t-0e5d6f99129bcdc92		=			
t- 0e5d6f99129bcdc92 Details Monitoring Tags					
Details Monitoring Tags	State		State message	Elastic IP address	
Details Monitoring Tags	State Ø Available		State message	Elastic IP address 107.22.216.234	
Details Monitoring Tags Details NAT gateway ID					
Details Monitoring Tags Details Image: Comparison of the second sec	⊘ Available		-	107.22.216.234	

Looking at the routes associated with the subnet, we can see that the traffic is routed out via the $\ensuremath{\mathsf{IGW}}$

Q Filter subnets						< 1 > @
Subnet ID: subnet-06184	5de126f7734c X Clear f	filters				
Name	♥ Subnet ID	⊽ State	♥ VPC		V IPv6 CIDR	
sec-natgw-subnet-	subnet-061845de126f77	34c 🛛 🐼 Avai	ilable vpc-006	87452e8ad629a sec 10.10.1.144/28	-	10
1et-061845de126f7734	c / sec-natgw-subnet-us-east-1	b-PANW-f975				
Details Flow logs	Route table Network ACL	. Tags Sh	aring			
Details Flow logs	Route table Network ACL	. Tags Sh	aring			
	Route table Network ACL	1 - 1				Edit route table associatior
		1 - 1				Edit route table associatior
		1 - 1				Edit route table associatior
ute table: rtb-05fe3 Routes (4)		1 - 1				
ute table: rtb-05fe3 Routes (4)		1 - 1				Edit route table association
tte table: rtb-05fe3 toutes (4) Q Filter routes		1 - 1	W-f975			
ute table: rtb-05fe3 Routes (4) Q Filter routes		1 - 1	W-f975 Target			
te table: rtb-05fe3 Routes (4) Q. Filter routes Destination 0.10.0.0/16		1 - 1	W-f975 Target local			
Acutes (4) Q. Filter routes Destination 10.10.0.0/16 10.101.0.0/16		1 - 1	W-f975 Target local vpce-000ae0168a8c6			
Aute table: rtb-05fe3 Routes (4) Q. Filter routes Destination 0.10.0.0/16		1 - 1	W-f975 Target local			

Response Step 1 - The Destination Deigns to Respond

Recall that the requesting host resides on the 10.101.0.0/16 subnet. When the response from the server returns to the IGW, it is sent to the NAT GW, which performs a reverse translation and puts the packet out on the wire where it is handled by the local subnet routing table. Looking at those routes, we see that the route to the destination subnet is via an Endpoint:

Q Filter subnets							< 1 >
Subnet ID: subnet-06	1845de126f7734c X Clear	filters					
Name		⊽ State	♥ VPC	∇	IPv4 CIDR	▽ IPv6 CIDR	
sec-natgw-subr	subnet-061845de126f7	734c 🛛 📿 Availab	le vpc-00698	452e8ad629a sec	10.10.1.144/28	-	10
							=
net-061845de126f77	34c / sec-natgw-subnet-us-east-1	lb-PANW-f975					
	,						
Details Flow logs	Route table Network AC	L Tags Shari	ng				
			-				Edit route table associati
	Route table Network AC		-				Edit route table associati
ute table: rtb-05f			-				Edit route table associati
ute table: rtb-05fe			-				Edit route table associati
ute table: rtb-05fr Routes (4) Q. Filter routes			-				
			f975				
ute table: rtb-05fr Routes (4) Q Filter routes			f975 Target	6			
ute table: rtb-05fr Routes (4) Q Filter routes Destination 10.10.0.0/16			f975 Target local	_			

Response Step 2 - The GWLB Endpoint

The Endpoint is connected to the GWLB via an Endpoint Service. In this case, the traffic is routed out the Endpoint associated with the 10.101.0.0/16 subnet (vpce-000ae0168a8c692c3). To see more information about this connection, click on the target. The subsequent page shows additional information about the Endpoint, including the associated Endpoint Service:

Create Endpoint Actions *			0	¢ 0
Q Endpoint ID : vpce-000ae010	8a8c692c3 Add filter	К	< 1 to 1 of 1	>>1
Name - Endpoint	ID + VPC ID	Service name * Endpoint type	- Status	5
vpce-000	ae0168a8c692c3 vpc-0069874	2e8ad629a sec-vpc-PANW-f975 com.amazonaws.vpce.us-east-1.vpce-svc-04c6cedd157b95a6d GatewayLoadBa	l a availal	ole
Endpoint: vpce-000ae0168a8c69 Details Subnets				880
Endpoint ID	vpce-000ae0168a8c692c3	VPC ID vpc-006987452e8ad629a sec-vpc-PANW-1975		
Status	available	Status message		
Creation time	February 12, 2021 at 1:57:20 PM UTC-6	Service name com.amazonaws.vpce.us-east-1.vpce-svc-04c6cedd157b95a6d		
Endpoint type Private DNS names enabled		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):

							0	
Com.amazonaws.vpc	e.us-east-1.vpce-svc-04c6cedd18	57b95a6d				us-east-1b	1 to 1 of 1	1 > 3
Name - I	D	Types	Service name		Status	Availa us-east-1c	hes	
l v	nce-svc-04c6cedd157b95a6d	GatewayLoadBala	com amazonaws vpce us-east-1.v	pce-svc-04c6cedd157b95a6d	Available	2 Availability Zones No		
dpoint Service: vpce-	svc-04c6cedd157b95a6d							88
Details	ad Balancers Whitelisted	principals Endpoir	t Connections Notifications	Tags				
	ncers associated with your end	ooint service. Load Balar	ncers accept requests received from (endpoints that are created for the en	dpoint service and route	those requests to targets hosting your servi	ce.	
vanage the Load Balar								
	iate Load Balancers							
							K < 1 to 2 of 2 >	×
		es					< 1 to 2 of 2 →	×
Associate/Disassoc	iate Load Balancers Load Balancer nam						< < 1 to 2 of 2 →	×

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

								Ð	
search : sec-gwlb-F	ANW-1975	3 Add filter						K < 1 to 1 of 1	> >
Name		DNS name	*	State	 VPC ID 	 Availability Zones 	- Туре	· Created At	*
sec-gwlb-PANW-f97	5			active	vpc-006987452e8ad629a	us-east-1c, us-east-1b	gateway	February 12, 2021 at 1:55:	:4
ad balancer: sec-gv	/lb-PANW-f	975						1	
Description	ers Mor	hitoring Integrated services	Tags						
Basic Configuration	on								
	Name	sec-gwlb-PANW-f975							
	ARN	arn:aws:elasticloadbalancing:u	us-east-1:484857004050:loadbala	ncer/gwy/sec-gwlb-PANV	/-f975/de1a0c1b4563010f 입				
	State	active							
	Type	gateway							
IP add	Iress type	ipv4							
	VPC	vpc-006987452e8ad629a 🗷							
Availabi	lity Zones	subnet-06d1664ebbe18e6e0 - subnet-0da8a5b7c3a4537f4 -							
Crea	ation time	February 12, 2021 at 1:55:47 P	PM UTC-6						
ttributes									
Deletic	on protectio	n Disabled							
	ad belonein	g Enabled							
Cross-zone lo	ad balancin								

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 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:

Q search : arn:aws:elasticloadbalancing:u	s-east-1: 🔘 Add filter			1	< 1 to 1 of 1 > >
Name	name	- State	v VPC ID v	Availability Zones - Type	~ Created At
sec-gwlb-PANW-f975		active	vpc-006987452e8ad629a	us-east-1c, us-east-1b gateway	February 12, 2
oad balancer: sec-gwlb-PANW-f975					885
Description Listeners Monitoring	Integrated services Tags				
A Gateway Load Balancer consists of an I	² listener that receives all connection req	uests and routes them to the target group	p you specify. You can edit the listener to cha	ange the target group to which requests get fo	orwarded.
Add listener Edit Delete					
Listener					
ARN	arn:aws:elasticloadbalancing:us-east-1:4	84857004050:listener/gwy/sec-gwlb-PA	NW-f975/de1a0c1b4563010f/716d330feea6	50db 🖓	
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-PAN			
ec-gwlb-tg-PANW-f97	/5		Delet
arn:aws:elasticloadbalancing:us-east-1:484	4857004050:targetgroup/sec-gwlb-tg-PANW-f975/00	71474a4c908966	
Basic configuration			
Target type Instance	Protocol : Port GENEVE: 6081	VPC vpc-006987452e8ad629a	Load balancer sec-gwlb-PANW-f975
Group details Targets Monito	oring Tags		
Group details Targets Monito	oring Tags		
Group details Targets Monito	oring Tags		C Deregister Register targets
	oring Tags		
Registered targets (2)	Tags	v Port v Zone	C Deregister Register targets
Registered targets (2) Q. Filter resources by property or value			C Deregister Register targets < 1 > @ v Status v Status details

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 >
Filter instances		
Instance ID: i-0e6c62c3020a82cee X Clear filters		
Name V Instance ID Ins	tance state v Instance type v Status check Alarm st	tatus Availability Zone V Public IPv4 DNS V Public II
FW-us-east-1c-PANW-f975 i-0e6c62c3020a82cee	Running ⊕⊖ m5.xlarge ⊘ 2/2 checks passed No alarm	ns 🕂 us-east-1c – –
	=	
tance: i-0e6c62c3020a82cee (FW-us-east-1c-PANW-f975)		
Details Security Networking Storage Status check	cs Monitoring Tags	
Details Security Networking Storage Status check	is 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
		D 10.10.0.100
Instance state	Public IPv4 DNS	Private IPv4 DNS
⊘ Running		p 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]	D vpc-006987452e8ad629a (sec-vpc-PANW-f975) 🖸
AWS Compute Optimizer finding	IAM Role	Subnet ID
Opt-in to AWS Compute Optimizer for recommendations. Learn more	iam-role-PANW-f975	subnet-06d1664ebbe18e6e0 (sec-data-subnet-us-east-1c-PANW- f975) 2

Response Step 4 - 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-000ae0168a8c692c3. If we take a closer look at that endpoint, we can determine the subnet that it resides in:

Create Endpoint Actions *		·			
Q search : vpce-000ae0168a8c692c3 🕥 Add filter					
Name Endpoint ID VPC ID	Service name	▲ Endpoint type – Status			
vpce-000ae0168a8c692c3 vpc-006987452e8ad629a sec-vpc-PANW-f975	com.amazonaws.vpce.us-east-1.vpce-svc-04c6cedd157b95a6d	GatewayLoadBala available			
Endpoint: vpce-000ae0168a8c692c3		888			
Details Subnets Notifications Tags					
Manage Subnets					
Subnet ID Availability Zone IPv4 Addresses IPv6 Addresses	Network Interface ID Outpost ID				
subnet- 0471afc10680bfa4c us-east-1b (use1-az1) 10.10.0.165 -	eni-0b92b8095ead347ed -				

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

Q Filter subnets		< 1 >
search: subnet-0471afc10680bfa4c X Clear filters]	
✓ Name	▽ State ▽ VPC ▽ IPv4 CIDR	
sec-gwlbe-ob-subn subnet-0471afc10680bfa4c	⊘ Available vpc-006987452e8ad629a sec 10.10.0.160	/28 – 10
	=	-
net-0471afc10680bfa4c / sec-gwlbe-ob-subnet-us-east-1b		
Details Flow logs Route table Network ACL	PANW-F975 Tags Sharing	Edit route table associati
Details Flow logs Route table Network ACL ute table: rtb-008c854b5beb83337 / gwlbe-ob-rt	PANW-F975 Tags Sharing	
Details Flow logs Route table Network ACL ute table: rtb-008c854b5beb83337 / gwlbe-ob-rt	PANW-F975 Tags Sharing	
Details Flow logs Route table Network ACL ute table: rtb-008c854b5beb83337 / gwlbe-ob-rt Routes (4) Q. Filter routes	PANW-F975 Tags Sharing	Edit route table association
ute table: rtb-008c854b5beb83337 / gwlbe-ob-rt Routes (4)	PANW-F975 Tags Sharing -us-east-1b-PANW-F975	Edit route table association

Response Step 5 - Return to the TGW

Recall that 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):

g search : vpc-006987452e8ad6	29a 🔘 Add filter						1< <	0- 1 to 1 of 1	\$
Name	- Transit Gateway attachment ID	▲ Transit Gateway ID	- Resource type	- Resource ID		- State		ted route table	
security-tgwa-PANW-1975	tgw-attach-092303149b3633879	tgw-0ad0c9091ead9880f	VPC	vpc-0069874	52e8ad629a	available	tgw-rtb-0	4bf8978d5e84d	872
ansit Gateway Attachment: tgw	-attach-092303149b3633879								
Details Tags					101072001070				
Details Tags Transit Gateway attachment ID	tgw-attach-092303149b3633879		Tra	nsit Gateway owner ID	484857004050			=	
Details Tags Transit Gateway attachment ID Transit Gateway ID	tgw-attach-092303149b3633879 tgw-0ad0c9091ead9880f		Tra	arce owner account ID	484857004050			-	
tetails Tags Transit Gateway attachment ID Transit Gateway ID Resource type	tgw-attach-092303149b3633879 tgw-0ad0c9091ead9880f VPC		Trai Reso	urce owner account ID State	484857004050 available			-	
Details Tags Transit Gateway attachment ID Transit Gateway ID	tgw-attach-092303149b3633879 tgw-0ad0c9091ead9880f VPC		Trai Reso	arce owner account ID	484857004050			-	

As long as the Endpoint and TGW Attachment are in the same AZ, subnet routing will ensure that the packet is delivered to the TGW.

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 (10.101.0.0/16) points to another attachment (tgw-attach-0b86ac38ab82dfff9):

Create Transit Gateway Route	Table Actions *								÷	۰
Q Transit Gateway route tab	le ID : tgw-rtb-04bf8978d5e84d872 🕥 Ad	ld filter						K	< 1 to 1 of 1	> >
Name	 Transit Gateway room 	ute table ID 🔺	Transit Gateway ID	- State -	Default association route	e table 👻 De	fault propagation	route table ~		
tgw-sec-rt-PANW-f975	tgw-rtb-04bf8978d5e	84d872	tgw-0ad0c9091ead9880f	available	No	No				
ransit Gateway Route Table:	tgw-rtb-04bf8978d5e84d872									
Details Associations	Propagations Prefix list references	Routes Tags								
The table below will return a n	naximum of 1000 routes. Narrow the filter	or use export routes	to view more routes.							
Create static route Rep	Delete static route	,								
Q, Filter by attributes or sear	rch by keyword							K < 1	to 2 of 2 🔿	>
CIDR	Attachment			Resource	type Ro	oute type	Route state	Prefix List ID		
10.101.0.0/16	tgw-attach-0b86ac38ab82dfff9	vpc-08321c498625455	23	VPC	sta	atic	active			
10.102.0.0/16	tgw-attach-07e43a9c4496319b1	vpc-0f681106f6b8464	b0i	VPC	sta	atic	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 Attachm	Actions *						Ŕ	÷ 🗘
Q Transit Gateway attachment	ID : tgw-attach-0b86ac38ab82dfff9 💿 A	dd filter					< < 1 to 1 c	f1 > >
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-08ae6a8fe	981a354d
ransit Gateway Attachment: tgw	r-attach-0b86ac38ab82dfff9							
Details Tags				Cotoway owner ID	484857004050			
Details Tags Transit Gateway attachment ID	tgw-attach-0b86ac38ab82dfff9		Transit	Gateway owner ID	484857004050 484857004050			
Details Tags	tgw-attach-0b86ac38ab82dfff9 tgw-0ad0c9091ead9880f		Transit	Gateway owner ID o owner account ID State				
Details Tags Transit Gateway attachment ID Transit Gateway ID	tgw-attach-0b86ac38ab82dfff9 tgw-0ad0c9091ead9880f VPC		Transit Resource	owner account ID	484857004050			
Transit Gateway attachment ID Transit Gateway ID Resource type	tgw-attach-0b86ac38ab82dfff9 tgw-0ad0c9091ead9880f VPC		Transit Resource	e owner account ID State	484857004050 available tgw-rtb-08ae6a8fe981a354d			

Response Step 6 - At Last

Inspection of the subnet route table reveals that any traffic destined for the VPC network is delivered directly to the target:

>	<				nets
				Clear filters	et-0e1119f6fc333ea6d 🗙
Availab	♥ IPv6 CIDR ♥	▽ IPv4 CIDR	ate 🛛 🖉 VPC	∇	
9	-	49862545523 ap 10.101.0.0/28	Available vpc-083	1119f6fc333ea6d	ain-subnet-P subnet-0
-			Sharing	et-PANW-77d3 Network ACL Tags	6fc333ea6d / app-main-sub
associat	Edit route tab		-	_	tb-08cda79410c2378cs
			-	_	
associat			-	_	
		1188ae080e	rd3 Target	_	
		1188ae080e	rd3 Target	_	tb-08cda79410c2378ct
			rd3 Target	_	tb-08cda79410c2378ct

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.

	C Connect	Instance state Actions Launch instances
Q Filter instances		< 1 > @
search: app-PANW-77d3 X Clear filters		
2 Name ♥ Instance ID Ins	tance state 🛛 🛛 Instance type 🔻 Status check 🔹 Alarm st	atus Availability Zone 🔻 Public IPv4 DNS 🛛 Public IPv4
app-PANW-77d3 i-062abc81e0975ceaa 🥥	Running ⊕⊖ t2.micro ⊘ 2/2 checks passed No alarm	s 🕂 us-east-1b – 35.171.248
	=	
stance: i-062abc81e0975ceaa (app-PANW-77d3)		
Details Security Networking Storage Status check Instance summary info Instance summary info <t< th=""><th>xs Monitoring Tags</th><th></th></t<>	xs Monitoring Tags	
Instance ID	Public IPv4 address	Private IPv4 addresses
Instance ID D i-062abc81e0975ceaa (app-PANW-77d3)	Public IPv4 address 35.171.248.18 (app-mgmt-eip-PANW-77d3) open address	Private IPv4 addresses
D i-062abc81e0975ceaa (app-PANW-77d3)	35.171.248.18 (app-mgmt-eip-PANW-77d3) open address 🗹	D 10.101.0.4
 ☐ i-062abc81e0975ceaa (app-PANW-77d3) Instance state Ø Running 	35.171.248.18 (app-mgmt-eip-PANW-77d3) open address Public IPv4 DNS	년 10.101.0.4 Private IPv4 DNS
① i-062abc81e0975ceaa (app-PANW-77d3) Instance state	35.171.248.18 (app-mgmt-eip-PANW-77d3) open address Public IPv4 DNS -	 ID.101.0.4 Private IPv4 DNS ip-10-101-0-4.ec2.internal
 ☐ i-062abc81e0975ceaa (app-PANW-77d3) Instance state Ø Running Instance type 	35.171.248.18 (app-mgmt-eip-PANW-77d3) open address Public IPv4 DNS - Elastic IP addresses	 D.101.0.4 Private IPv4 DNS ip-10-101-0-4.ec2.internal VPC ID

Et violà:			
ubuntu@admin-appliance: ~ (com.docker.cli)	¥1	ubuntu@ip-10-101-0-4: ~ (ssh)	₩2
<pre>ubuntu@ip-10-101-0-4:~\$ curl -I https://www.keycd</pre>	n.com		
HTTP/2 200			
server: keycdn-engine			
date: Wed, 17 Feb 2021 14:22:49 GMT			
content-type: text/html			
last-modified: Tue, 16 Feb 2021 17:40:33 GMT			
vary: Accept-Encoding			
etag: W/"602c0391-10111"			
expires: Wed, 24 Feb 2021 14:22:49 GMT			
cache-control: max-age=604800			
strict-transport-security: max-age=31536000; incl	· •		
<pre>content-security-policy: default-src 'self' 'unsa x-frame-options: SAMEORIGIN</pre>	re-inline unsa	are-eval' https: data:	
x-irame-options: SAMEORIGIN x-xss-protection: 1; mode=block			
x-content-type-options: nosniff			
referrer-policy: no-referrer-when-downgrade			
x-cache: HIT			
x-edge-location: usda			
access-control-allow-origin: *			
ubuntu@ip-10-101-0-4:~\$			

Looking at the FW logs, we can see both original source and original destination:

-11	(auui																
		GENERATE TIME	TYPE	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
EQ.		02/17 14:23:03	end	Trust	Trust	10.101.0.4	68.70.205.2		no			443	ssl	allow	Allowed-traffic	tcp-fin	7.4k
EQ.		02/17 14:22:58	end	Trust	Trust	10.101.0.4	68.70.205.3		no			443	ssl	allow	Allowed-traffic	tcp-fin	7.4k
EQ.		02/17 14:22:48	start	Trust	Trust	10.101.0.4	68.70.205.2		no			443	ssl	allow	Allowed-traffic	n/a	797
EQ.		02/17 14:22:43	start	Trust	Trust	10.101.0.4	68.70.205.3		no			443	ssl	allow	Allowed-traffic	n/a	797
EQ.		02/17 14:21:04	end	Trust	Trust	10.101.0.4	68.70.205.3		no			443	ssl	allow	Allowed-traffic	tcp-fin	7.5k
EQ.		02/17 14:21:03	end	Trust	Trust	10.101.0.4	68.70.205.3		no			443	ssl	allow	Allowed-traffic	tcp-fin	7.3k
EQ.		02/17 14:20:49	start	Trust	Trust	10.101.0.4	68.70.205.3		no			443	ssl	allow	Allowed-traffic	n/a	797
EQ.		02/17 14:20:48	start	Trust	Trust	10.101.0.4	68.70.205.3		no			443	ssl	allow	Allowed-traffic	n/a	797