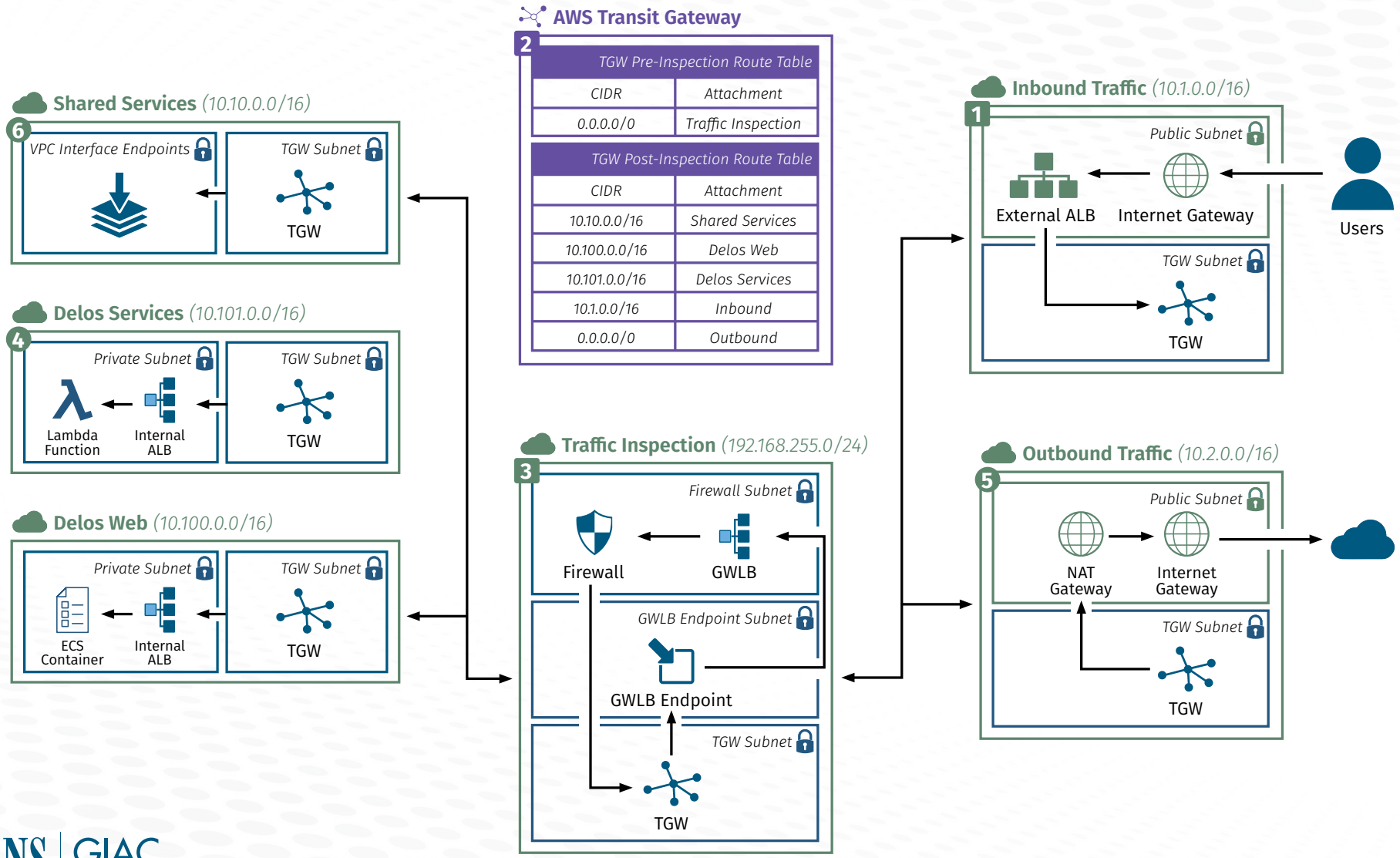
Inspection VPC

CLOUD SECURITY

Created by Kat Traxler and Eric Johnson, co-authors of
SEC549: Enterprise Cloud Security Architecture | *sans.org/sec549*



SANS GIAC CERTIFICATIONS

Inspection VPC

DIAGRAM KEY

The Delos AWS organization uses the Transit Gateway (TGW) resource to perform traffic inspection for all inbound, outbound, and east/west network traffic. The diagram depicts centralized inbound and outbound networks for resources that need internet connectivity. The TGW default route table ensures the next hop for all traffic leaving a spoke VPC is sent to a security VPC for inspection.

1

Manages all inbound traffic to the Delos network. The network team deploys all of the organization's public load balancers in a centralized network. All public IP addresses and internet gateways are hosted in a single public subnet. Organization Service Control Policy (SCP) prevents internet gateways and public IP addresses from being created in non-approved networks.

The load balancer sandwich pattern depicted in the diagram starts with the public load balancer in this network. DNS entries route incoming traffic to the load balancer's public IP address. The load balancer's target group routes traffic through the transit gateway to an application running in the Delos Services private network (10.101.0.0/16).

2

The AWS Transit Gateway (TGW) manages the traffic flow between each micro-network in the Delos organization. Each micro-network contains a small private subnet for its workloads (e.g., virtual machines, containers, or functions) and a transit gateway subnet. Routing is allowed locally within the micro-network's IP address range. Traffic leaving a micro-network reaches the TGW Pre-Inspection route table.

Traffic to the public load balancer routes into the TGW subnet. The TGW Pre-Inspection route table has one default route (0.0.0.0/0) sending all traffic to the traffic inspection network.

3

The traffic inspection network's transit gateway subnet route table has one default route (0.0.0.0/0) sending all traffic to a Gateway Load Balancer endpoint service. The Gateway Load Balancer's target group is a firewall appliance performing stateless and stateful traffic inspection. The firewall subnet route table forwards traffic allowed by firewall policy back to the transit gateway network interface.

The TGW Post-Inspection route table uses the traffic's destination to forward to the correct VPC network.

4

The public load balancer's target group is an internal load balancer running in the Delos Services private network (10.101.0.0/16). After firewall inspection, the TGW Post-Inspection route table forwards the traffic to the internal load balancer. The internal load balancer's target group is a Lambda function running in the private Delos Services subnet.

5

The Lambda function running in the private Delos Services subnet requires outbound network access to a Microsoft identity provider. The function makes an outbound API call to the identity provider, which reaches the TGW Pre-Inspection route table. The TGW Pre-Inspection route table forwards the traffic to the firewall appliance for inspection. Firewall policy validates that the function is permitted to communicate with the identity provider's domain (sts.windows.net), also known as fully qualified domain name (FQDN) filtering.

The firewall subnet routes allowed outbound traffic back to the transit gateway network interface, which reaches the TGW Post-Inspection route table. The TGW Post-Inspection route table's default route (0.0.0.0/0) forwards the traffic to the outbound network (10.2.0.0/16), through a NAT gateway, to the internet gateway, and to the identity provider.

6

The Lambda function running in the private Delos Services subnet requires internal network access to the AWS Secrets Manager API. The function makes an API call to a Secrets Manager private endpoint hosted in the Shared Services network (10.10.0.0/16). The TGW Pre-Inspection route table forwards the traffic to the firewall appliance for east-west traffic inspection. Firewall policy validates that the Lambda function is permitted to communicate with APIs in the Shared Services network.

The firewall subnet routes allowed east-west traffic back to the transit gateway network interface, which reaches the TGW Post-Inspection route table. The TGW Post-Inspection route table sends the traffic into the Shared Services network (10.10.0.0/16) to the Secrets Manger API.