Traffic Control: Network Access Control Lists and Security Groups Part 1

Brock Tubre

TECHNICAL INSTRUCTOR

Parking Garage

Parking Garage

Parking Garage Security

Every car in the garage has the same level of security.

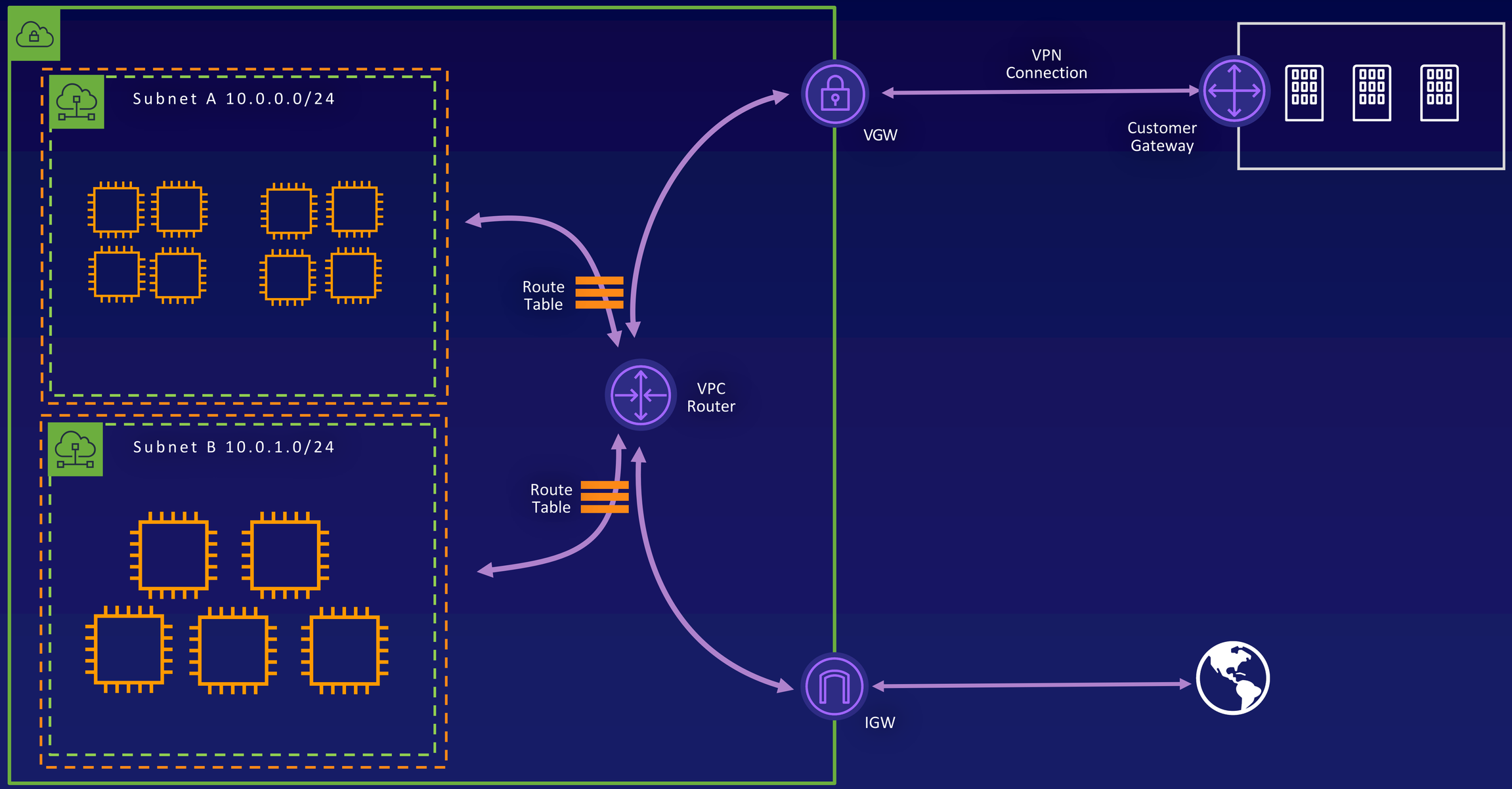
Network Access Control Lists (NACLs) are applied to any resource launched into a subnet.

Car Security

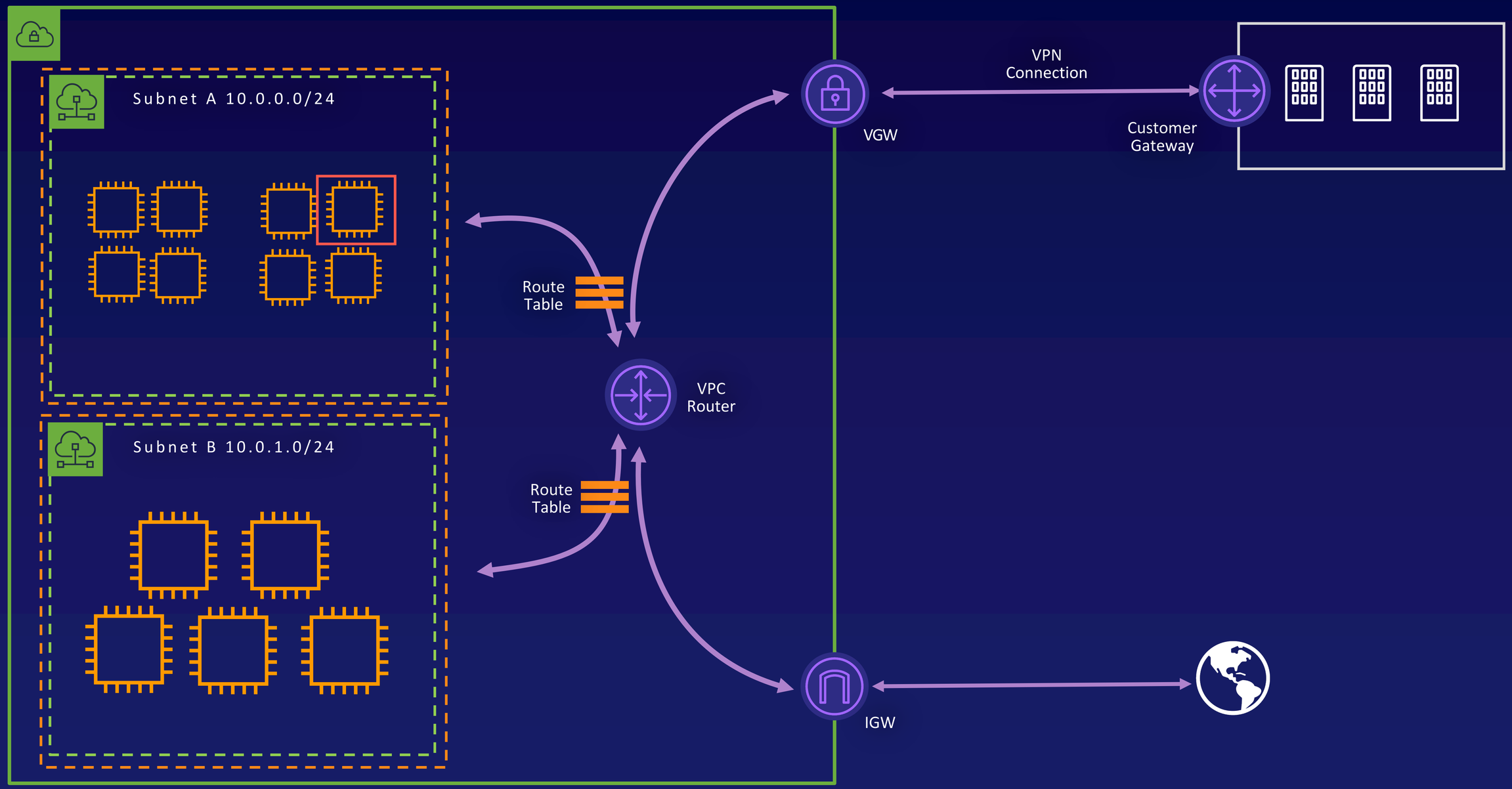
Each car has their own type of security mechanism.

Security Groups (SGs) only apply to those ENIs or resources they are associated with.

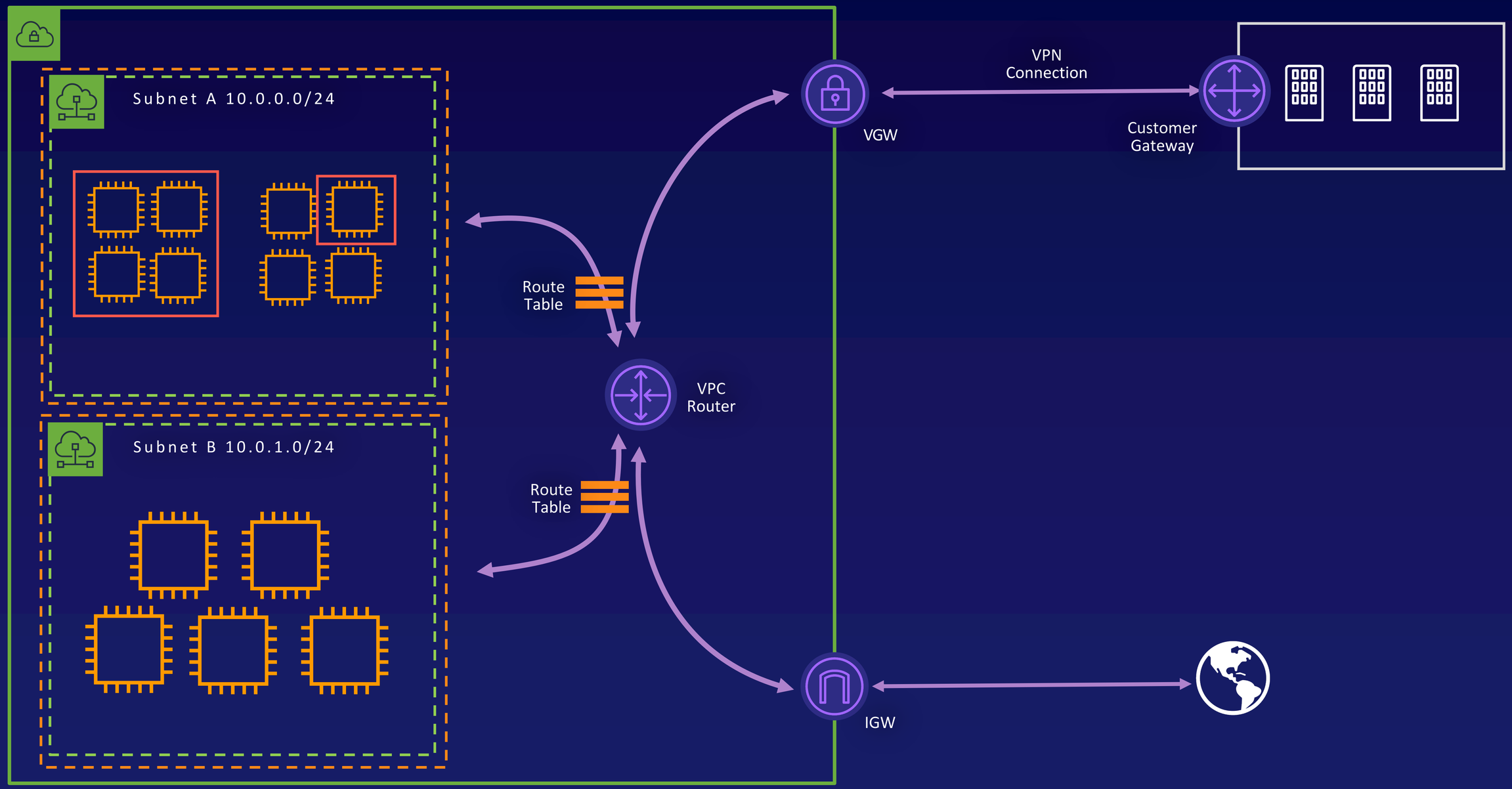
NACLs and SGs in Use



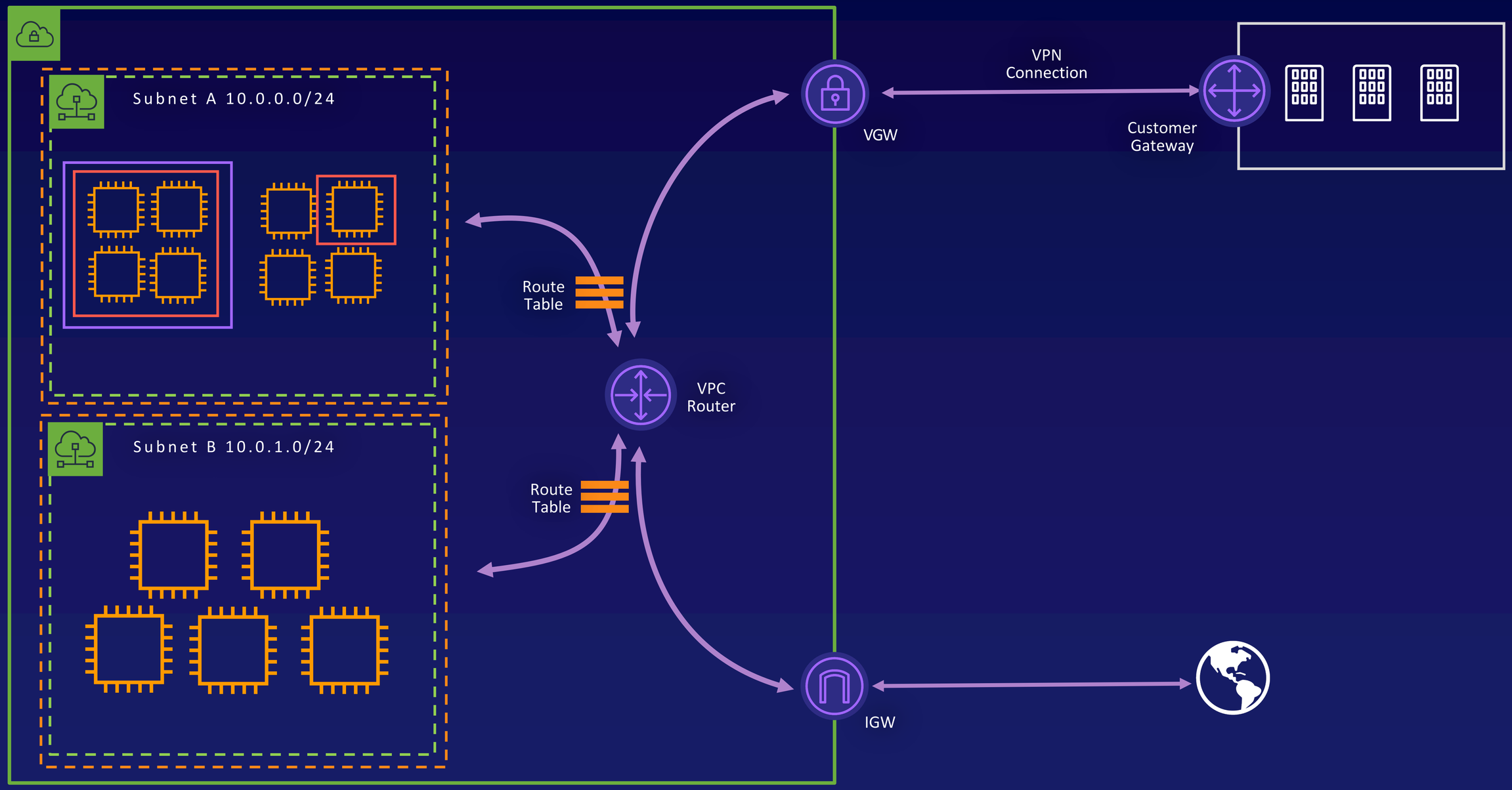
NACLs and SGs in Use



NACLs and SGs in Use

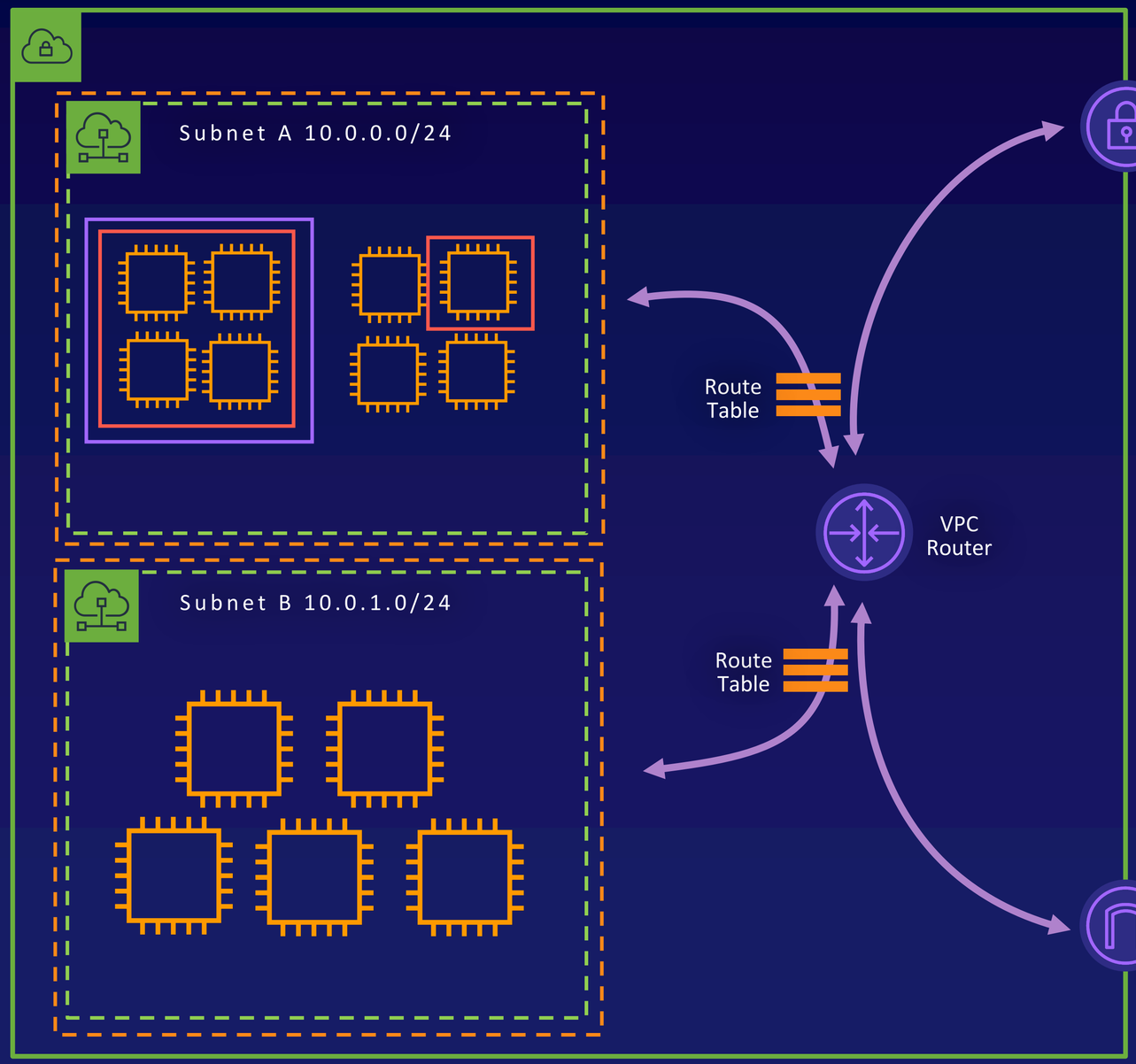


NACLs and SGs in Use



NACLs and SGs in Use

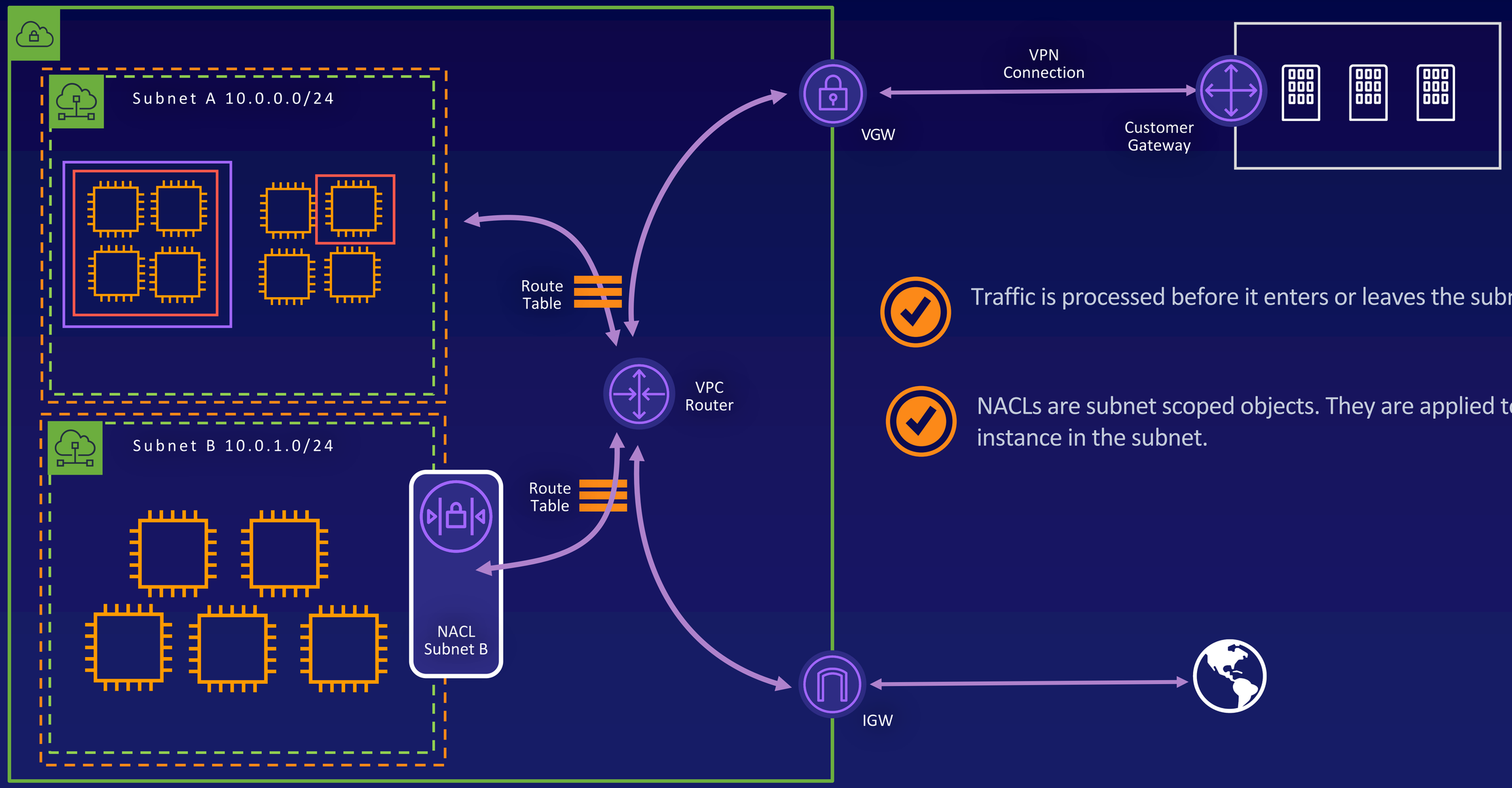
A CLOUD GURU



- The product of rules are applied when multiple Security Groups are attached.
- Security Groups are attached to an object's Elastic Network Interface.

NACLs and SGs in Use

A CLOUD GURU



Traffic is processed before it enters or leaves the subnet.

NACLs are subnet scoped objects. They are applied to any instance in the subnet.

NACLs and SGs

Security Groups	Network Access Control Lists

NACLs and SGs

Security Groups	Network Access Control Lists
Applied at the resource level (applied to ENI).	Applied at the subnet level.

NACLs and SGs

Security Groups	Network Access Control Lists
Applied at the resource level (applied to ENI).	Applied at the subnet level.
Resources can have multiple SGs. The product of rules are used.	A subnet is associated with one NACL, and a NACL can be associated with multiple subnets.

NACLs and SGs

Security Groups	Network Access Control Lists
Applied at the resource level (applied to ENI).	Applied at the subnet level.
Resources can have multiple SGs. The product of rules are used.	A subnet is associated with one NACL, and a NACL can be associated with multiple subnets.
Stateful: Return traffic is automatically allowed, regardless of any rules.	**Stateless**: Return traffic must be explicitly allowed by rules.

NACLs and SGs

Security Groups	Network Access Control Lists
Applied at the resource level (applied to ENI).	Applied at the subnet level.
Resources can have multiple SGs. The product of rules are used.	A subnet is associated with one NACL, and a NACL can be associated with multiple subnets.
Stateful: Return traffic is automatically allowed, regardless of any rules.	**Stateless**: Return traffic must be explicitly allowed by rules.
Can specify allow rules, but not deny rules.	Can specify both allow and deny rules.

NACLs and SGs

Security Groups	Network Access Control Lists
Applied at the resource level (applied to ENI).	Applied at the subnet level.
Resources can have multiple SGs. The product of rules are used.	A subnet is associated with one NACL, and a NACL can be associated with multiple subnets.
Stateful: Return traffic is automatically allowed, regardless of any rules.	**Stateless**: Return traffic must be explicitly allowed by rules.
Can specify allow rules, but not deny rules.	Can specify both allow and deny rules.
AWS evaluates all rules, in any order, to decide whether to allow traffic.	Rules are evaluated in order to decide whether to allow traffic.

Ingress and Egress

Ingress traffic = inbound traffic

Egress traffic = outbound traffic