

The diagram illustrates the flow of traffic through AWS network components. An orange arrow at the top points down to a central router icon (a dark blue circle with four white arrows pointing outwards). To the left of the router is a 'Route Table' box. An orange arrow points from the router down to a yellow padlock icon labeled 'NACL'. Below the router are two VPC subnets. 'VPC subnet 1' (10.0.1.0/24) contains two orange squares, each labeled 'security group'. 'VPC subnet 2' (10.0.2.0/24) also contains two orange squares labeled 'security group'. An orange arrow points from the 'NACL' padlock down to the first 'security group' in 'VPC subnet 2'.

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-1e72d67b



security group



security group

VPC subnet 1  
10.0.1.0/24



security group



security group

VPC subnet 2  
10.0.2.0/24

## Security Groups

Every instance needs at least one

Up to 5

- per network interface

Manage traffic flow

- explicit ALLOW
- implicit DENY

Security Group: sg-e46e6781

Description

Inbound

Outbound

Tags

Edit

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
HTTP	TCP	80	0.0.0.0/0
Custom TCP Rule	TCP	2375	10.0.3.0/24
HTTPS	TCP	443	0.0.0.0/0

Security Groups

Every instance needs at least one

Up to 5

- per network interface

Manage traffic flow

- explicit ALLOW
- implicit DENY
- inbound traffic
- outbound traffic

Rules comprise

- protocol
- port
- source/dest

All rules get evaluated

## Security Group: sg-e46e6781

Description

Inbound

Outbound

Tags

Edit

Type ⓘ

Protocol ⓘ

Port Range ⓘ

Destination ⓘ

All traffic

All

All

0.0.0.0/0

## Security Groups

Every instance needs at least one

Up to 5

- per network interface

Manage traffic flow

- explicit ALLOW
- implicit DENY
- inbound traffic
- outbound traffic

Rules comprise

- protocol
- port
- source/dest

All rules get evaluated

Stateful

Dynamic

## Security Group: sg-e46e6781

Description

Inbound

Outbound

Tags

Edit

Type ⓘ

Protocol ⓘ

Port Range ⓘ

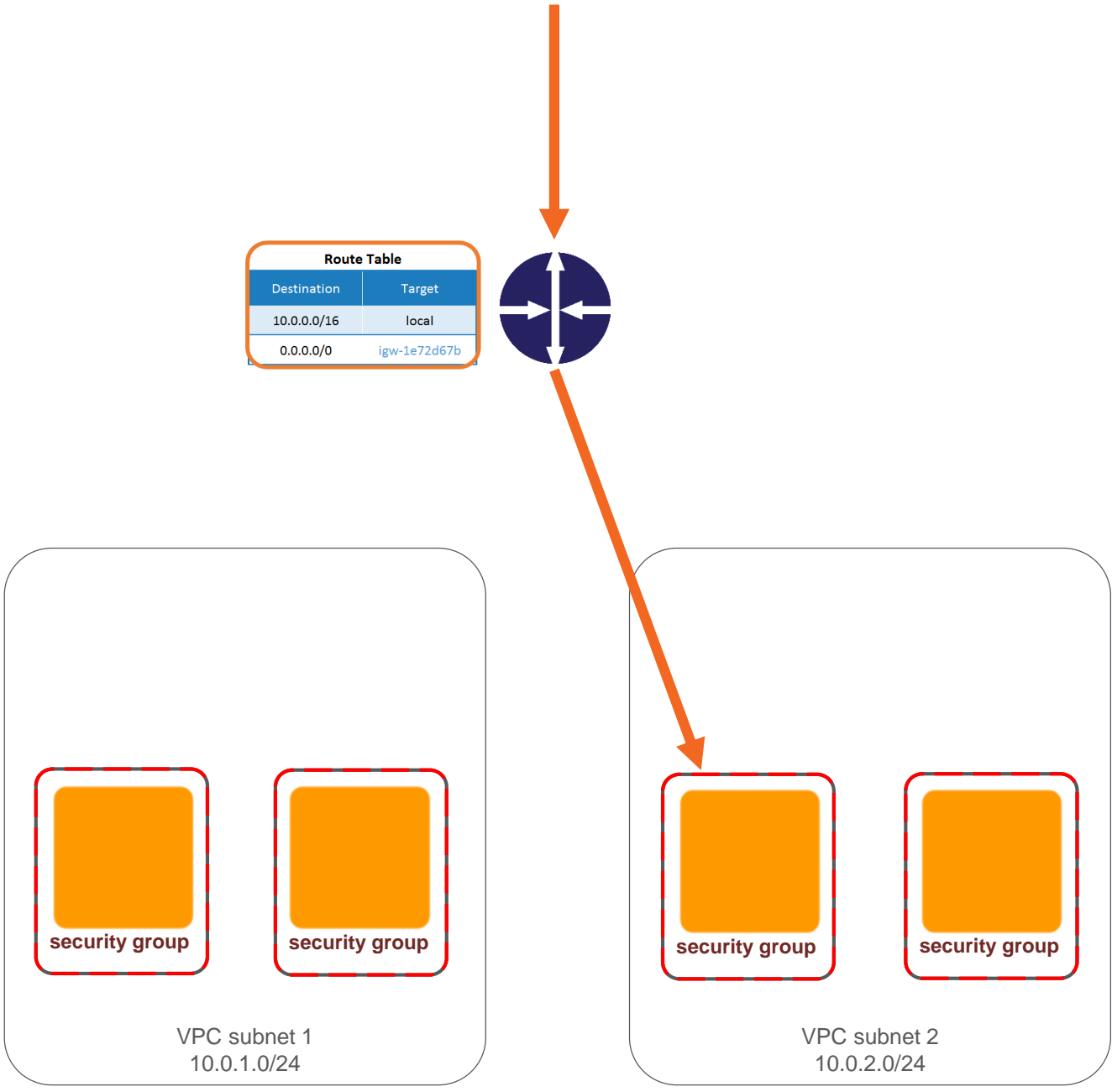
Destination ⓘ

All traffic

All

All

0.0.0.0/0



Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-1e72d67b



security group



security group

VPC subnet 1  
10.0.1.0/24



security group



security group

VPC subnet 2  
10.0.2.0/24

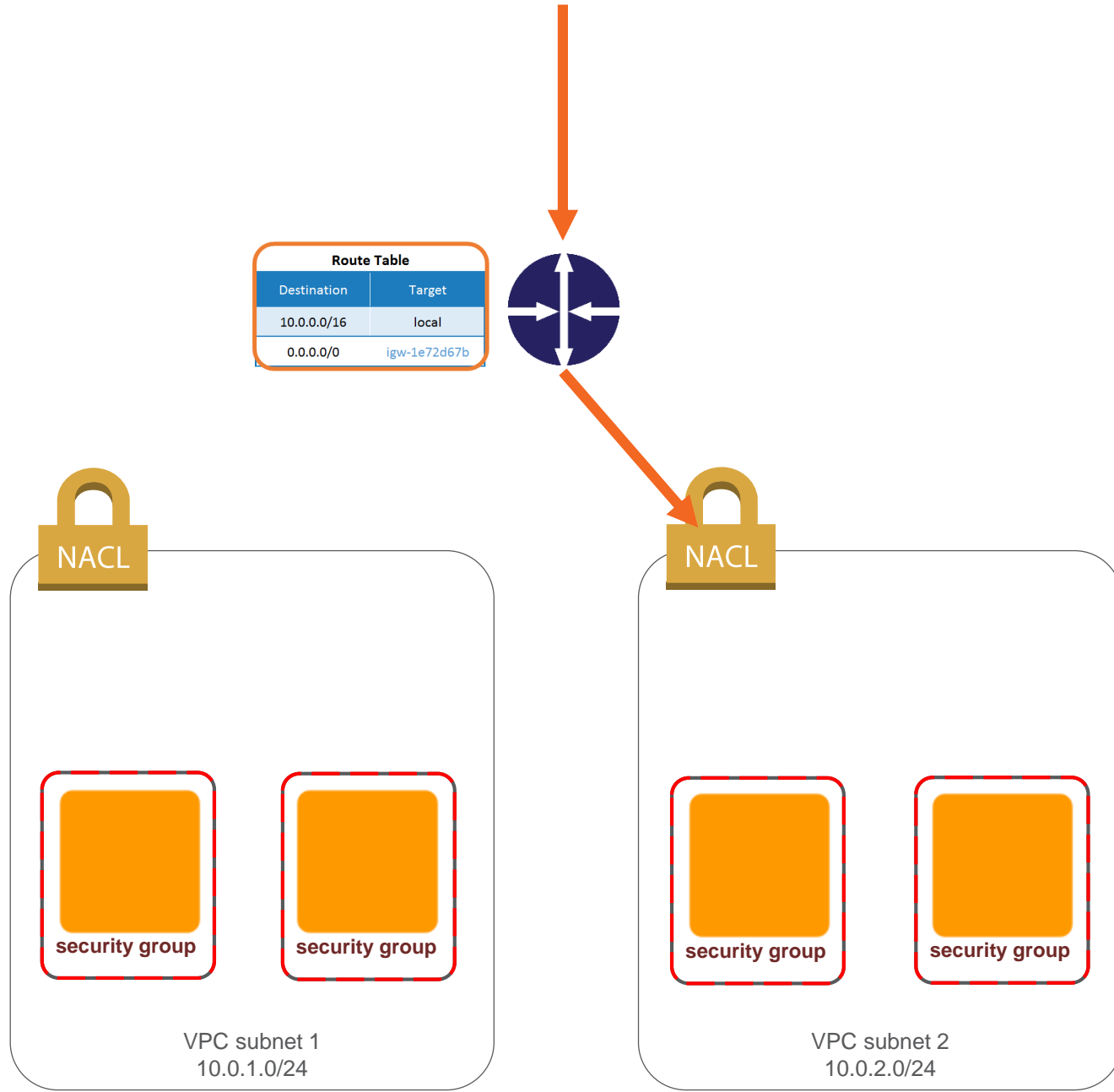
## Security Groups

Inbound rules

Outbound rules

Explicit ALLOW | Implicit DENY

Stateful



## Security Groups

Inbound rules

Outbound rules

Explicit ALLOW | Implicit DENY

Stateful

## Network ACLs

Inbound rules

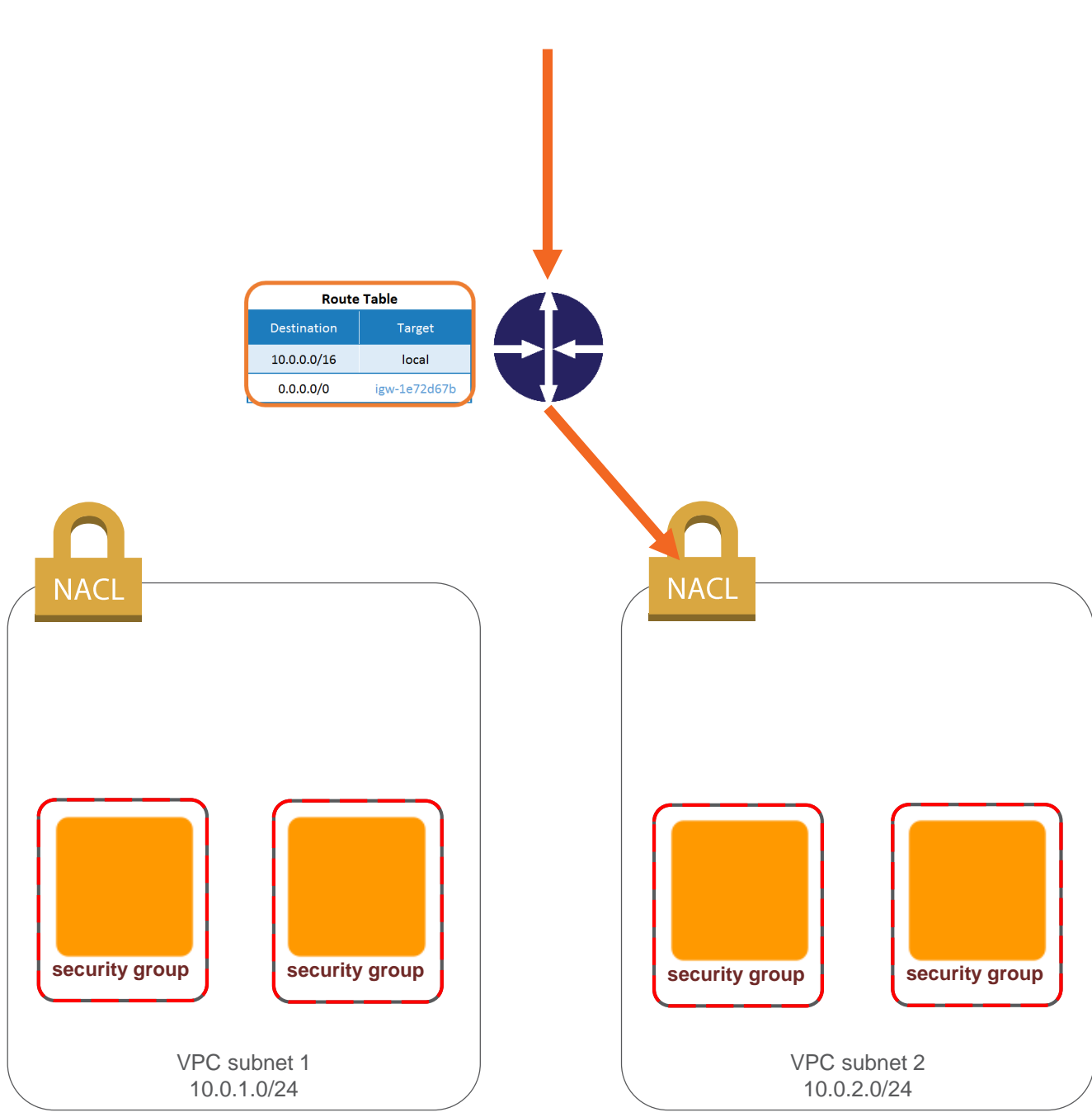
Outbound rules

Explicit ALLOW

Explicit DENY

Stateless





Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-1e72d67b



NACL



security group



security group

VPC subnet 1  
10.0.1.0/24



NACL



security group



security group

VPC subnet 2  
10.0.2.0/24

## Security Groups

Inbound rules

Outbound rules

Explicit ALLOW | Implicit DENY

Stateful

## Network ACLs

Inbound rules

Outbound rules

Explicit ALLOW

Explicit DENY

Stateless

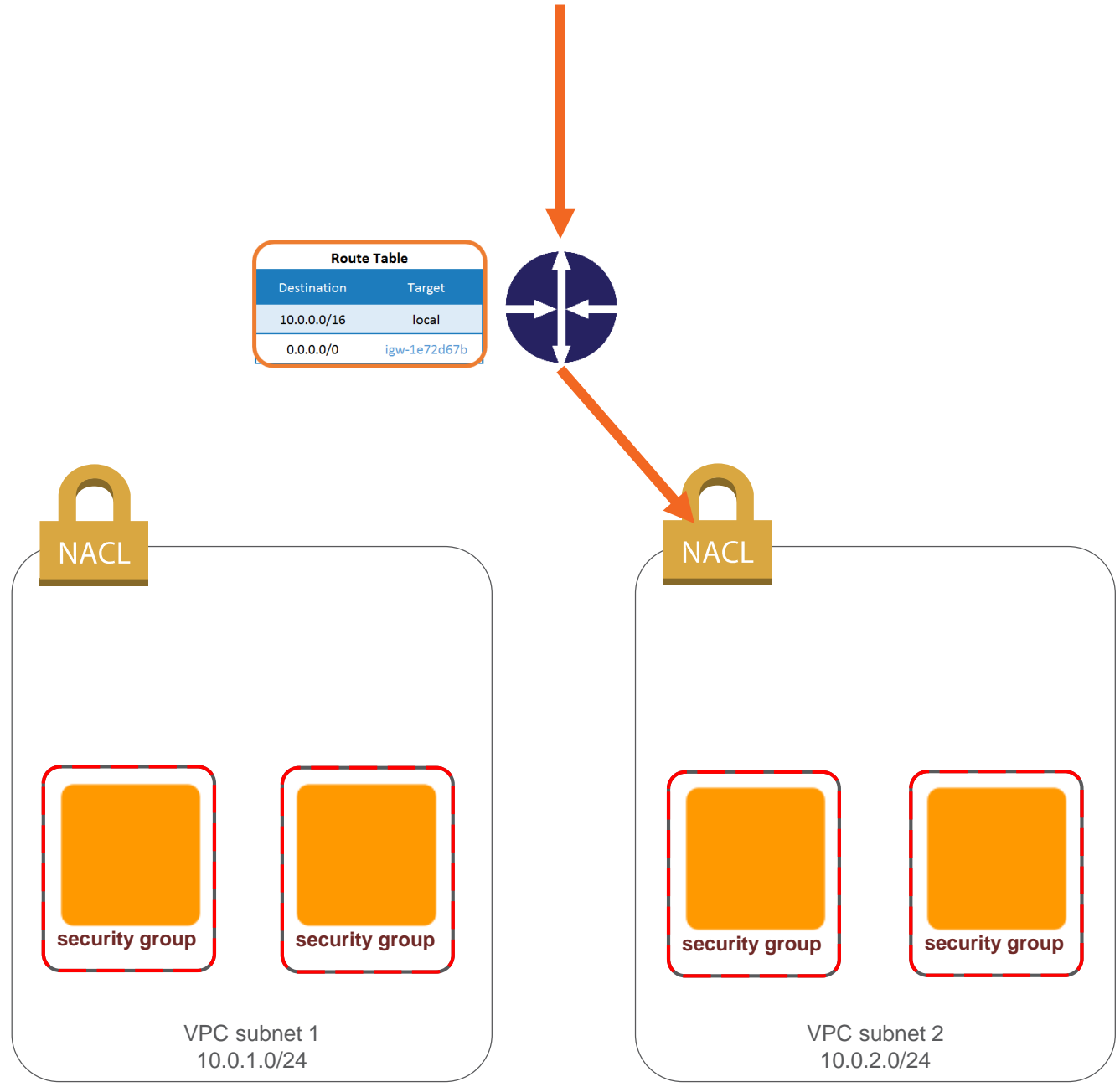
## acl-51d24c34 | Test-NACL

[Summary](#)[Inbound Rules](#)[Outbound Rules](#)[Subnet Associations](#)[Tags](#)

Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound rules.

[Edit](#)

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
200	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
300	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY



Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-1e72d67b



security group

security group

VPC subnet 1  
10.0.1.0/24



security group

security group

VPC subnet 2  
10.0.2.0/24

## Network ACLs

Inbound rules

Outbound rules

Explicit ALLOW

Explicit DENY

Stateless

Rules processed in # order

Rule processing stops upon match

Once NACL per Subnet

Summary

Inbound Rules

Outbound Rules

Subnet Associations

Allows inbound traffic. Because network ACLs are stateless, you must create inbound and outbound

Edit

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
200	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
300	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

## Network ACLs

Inbound rules

Outbound rules

Explicit ALLOW

Explicit DENY

Stateless

Rules processed in # order

Rule processing stops upon match

Once NACL per Subnet

200 NACLs per VPC

20 rules per NACL