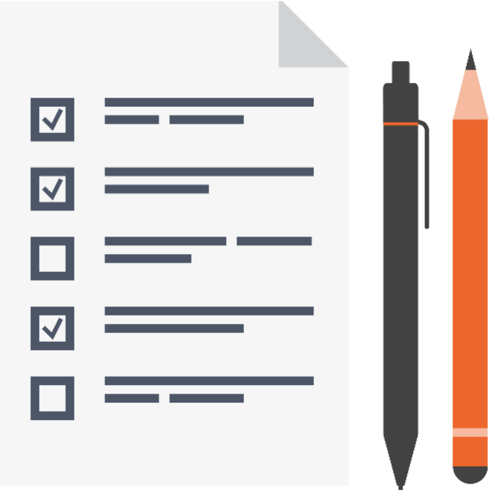
Securing Your VPC

Nigel Poulton

@nigelpoulton | www.nigelpoulton.com

Module Overview



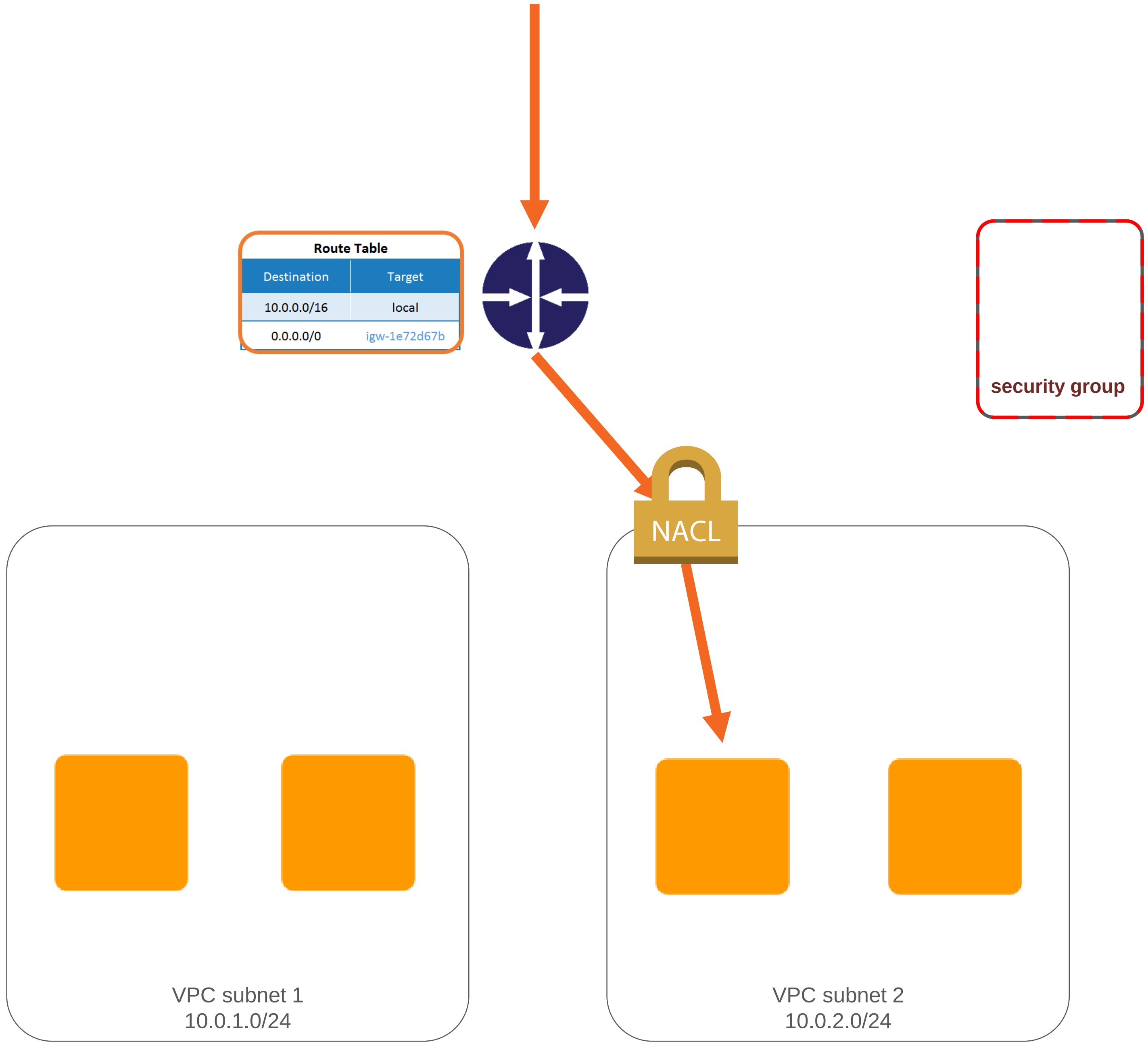
Security Groups (SG)

- Theory
- Practical

Network Access Control Lists (NACL)

- Theory
- Practical

The High Level Picture



Route Table

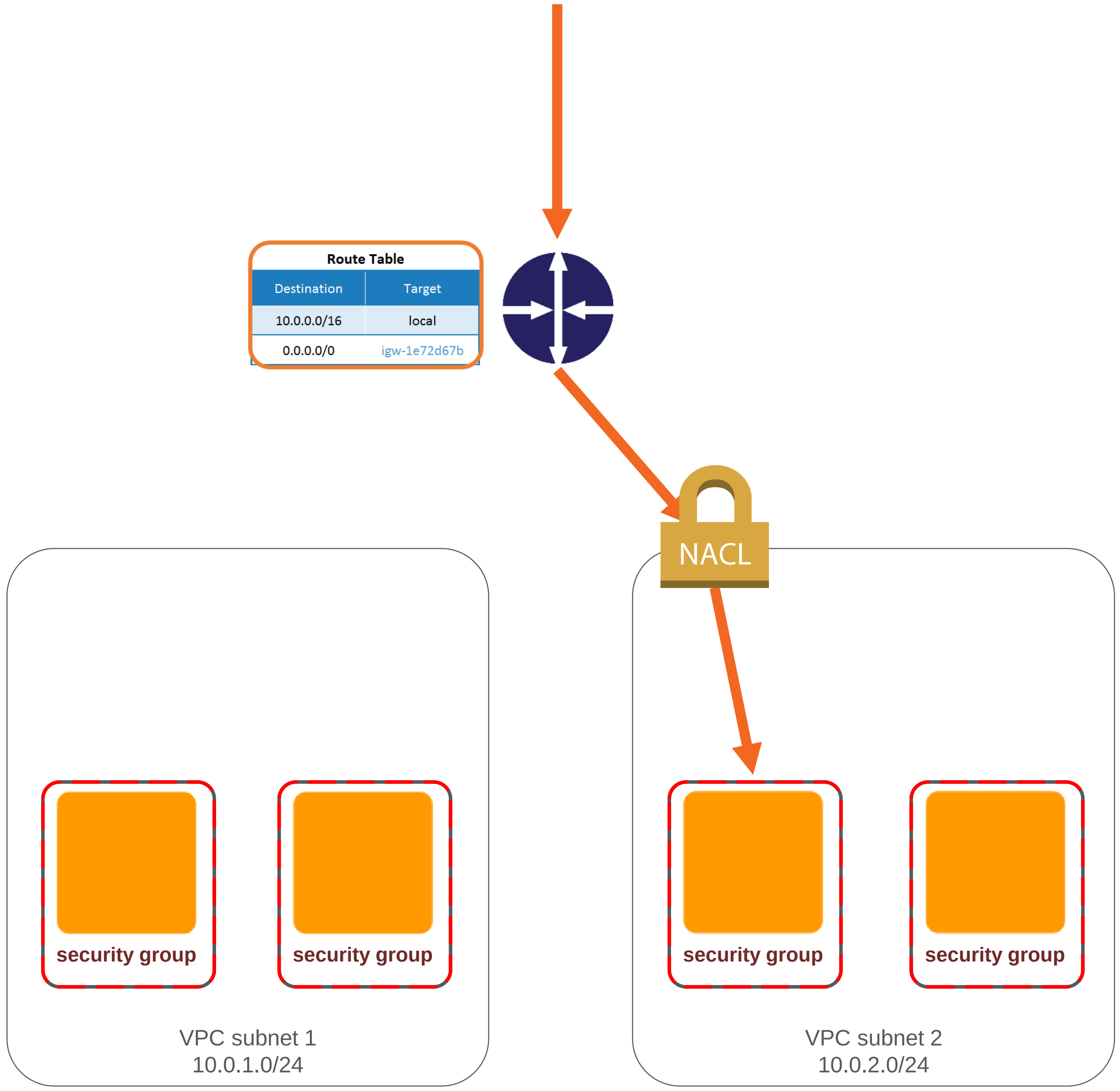
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-1e72d67b

security group

NACL

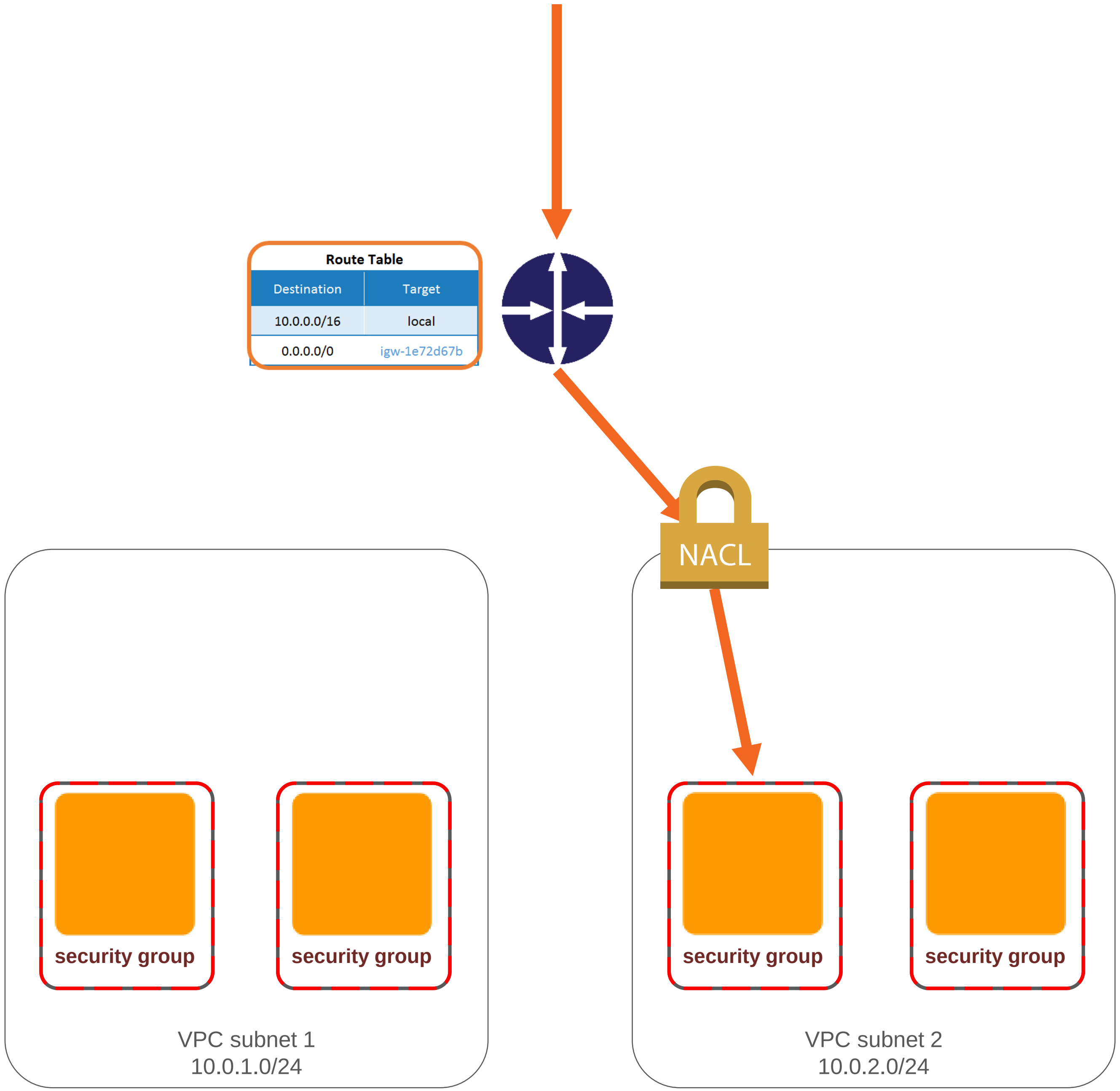
VPC subnet 1
10.0.1.0/24

VPC subnet 2
10.0.2.0/24



Route Table

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



Route Table

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

Security Groups

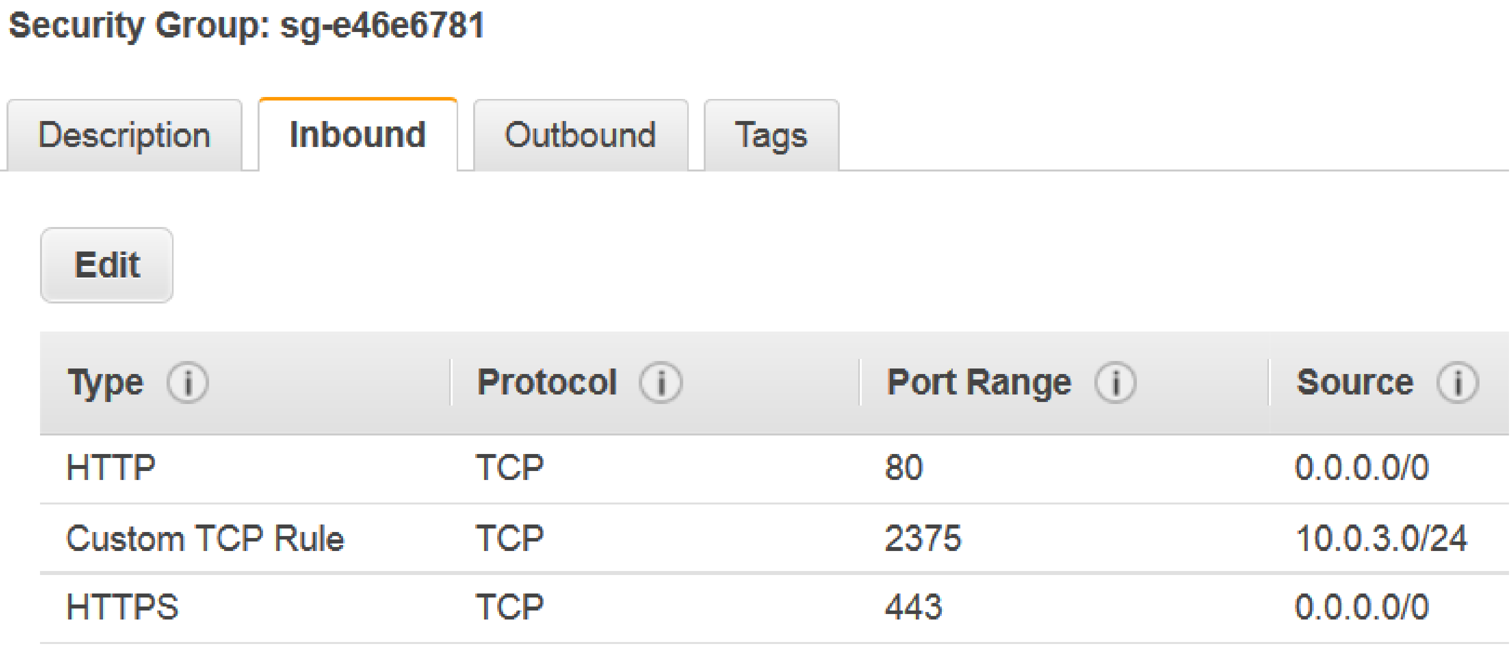
Every instance needs at least one

Up to 5

- per network interface

Manage traffic flow

- explicit ALLOW
- implicit DENY



Security Group: sg-e46e6781

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

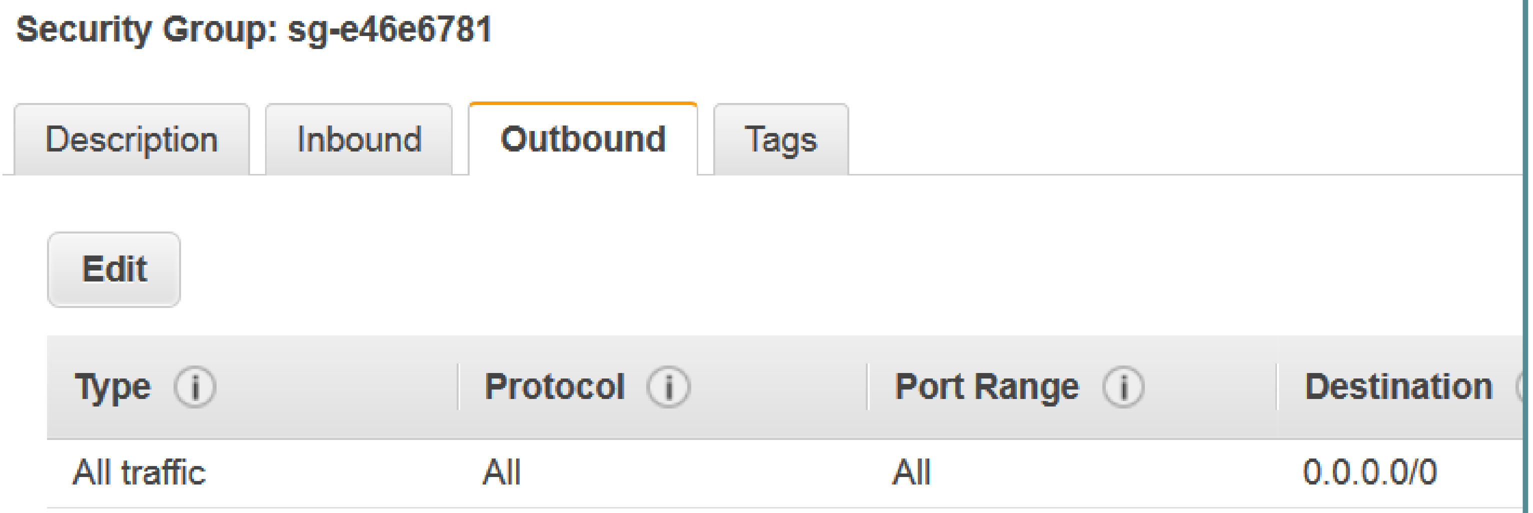
Manage traffic flow

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

Rules comprise

- protocol
- port
- source/dest

All rules get evaluated



Security Group: sg-e46e6781

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

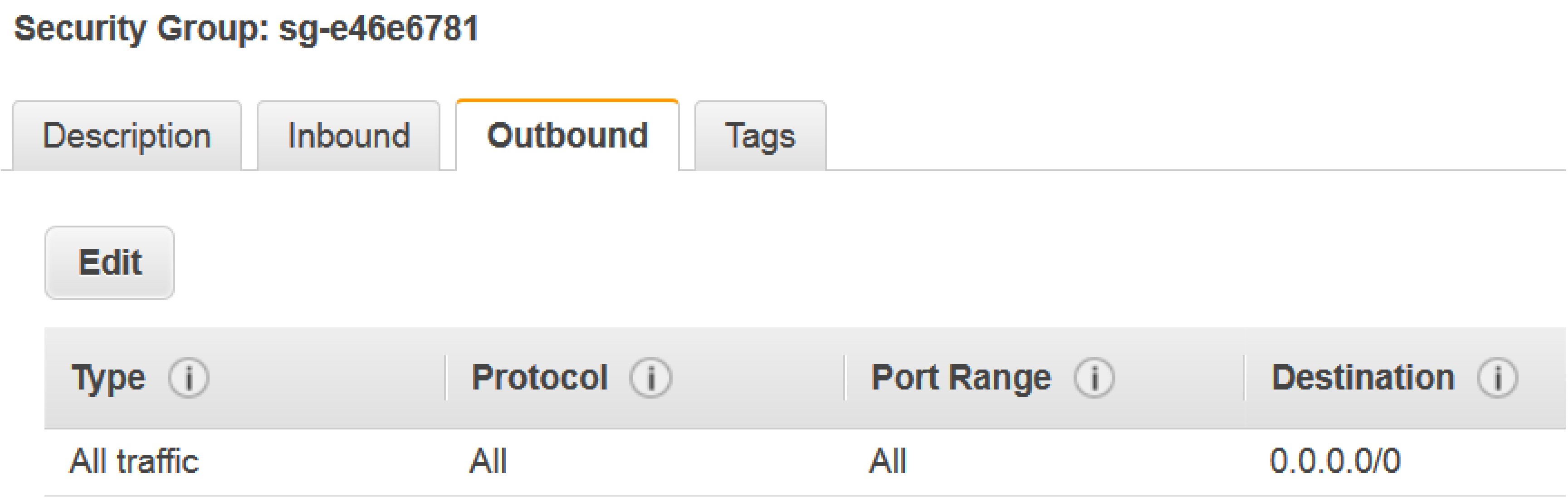
Rules comprise

- protocol
- port
- source/dest

All rules get evaluated

Stateful

Dynamic

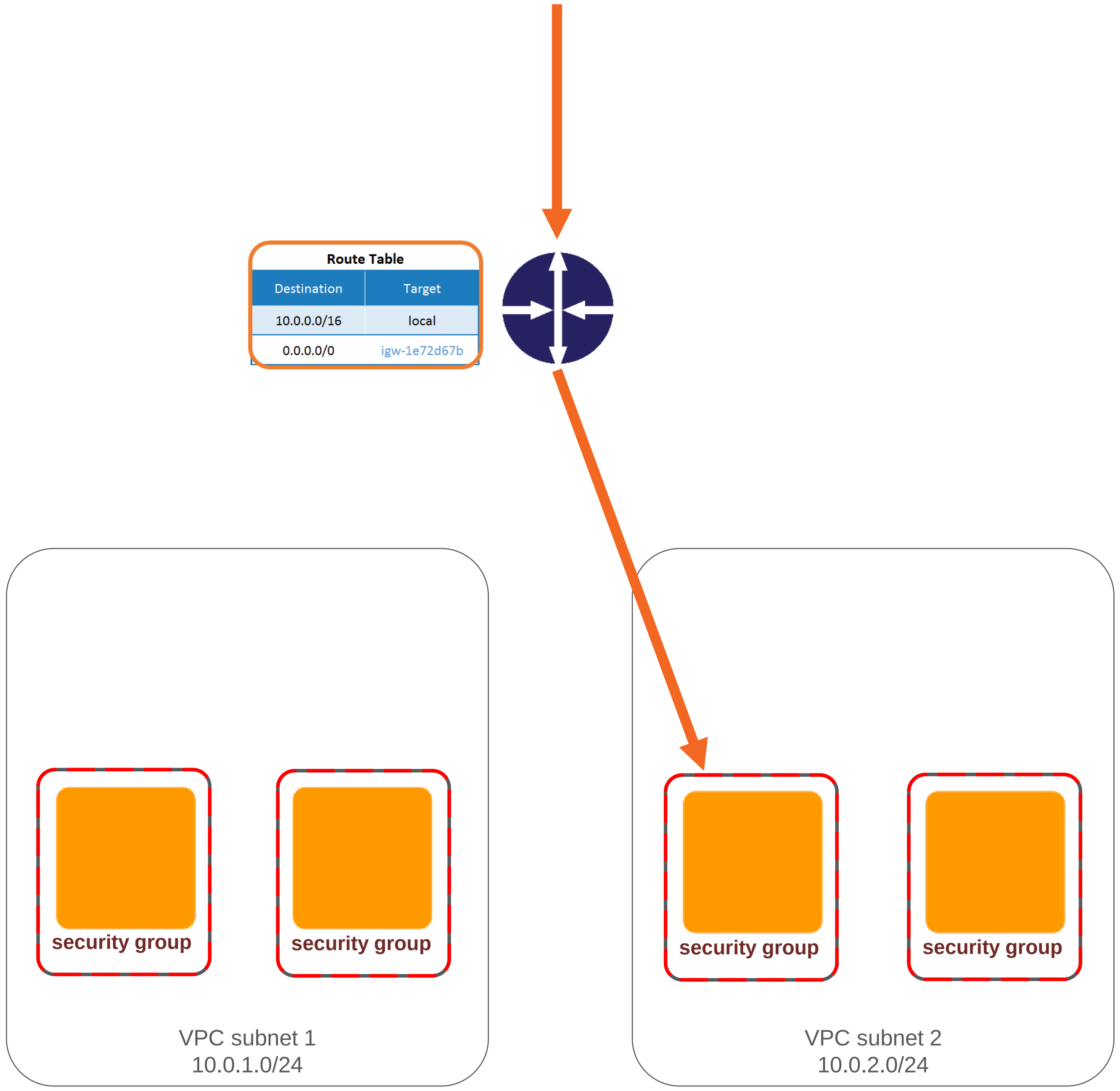


Security Group: sg-e46e6781

Type	Protocol	Port Range	Destination
All traffic	All	All	0.0.0.0/0

Network Access Control Lists

Security Groups for Subnets (kind of)



Route Table

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

security group

security group

security group

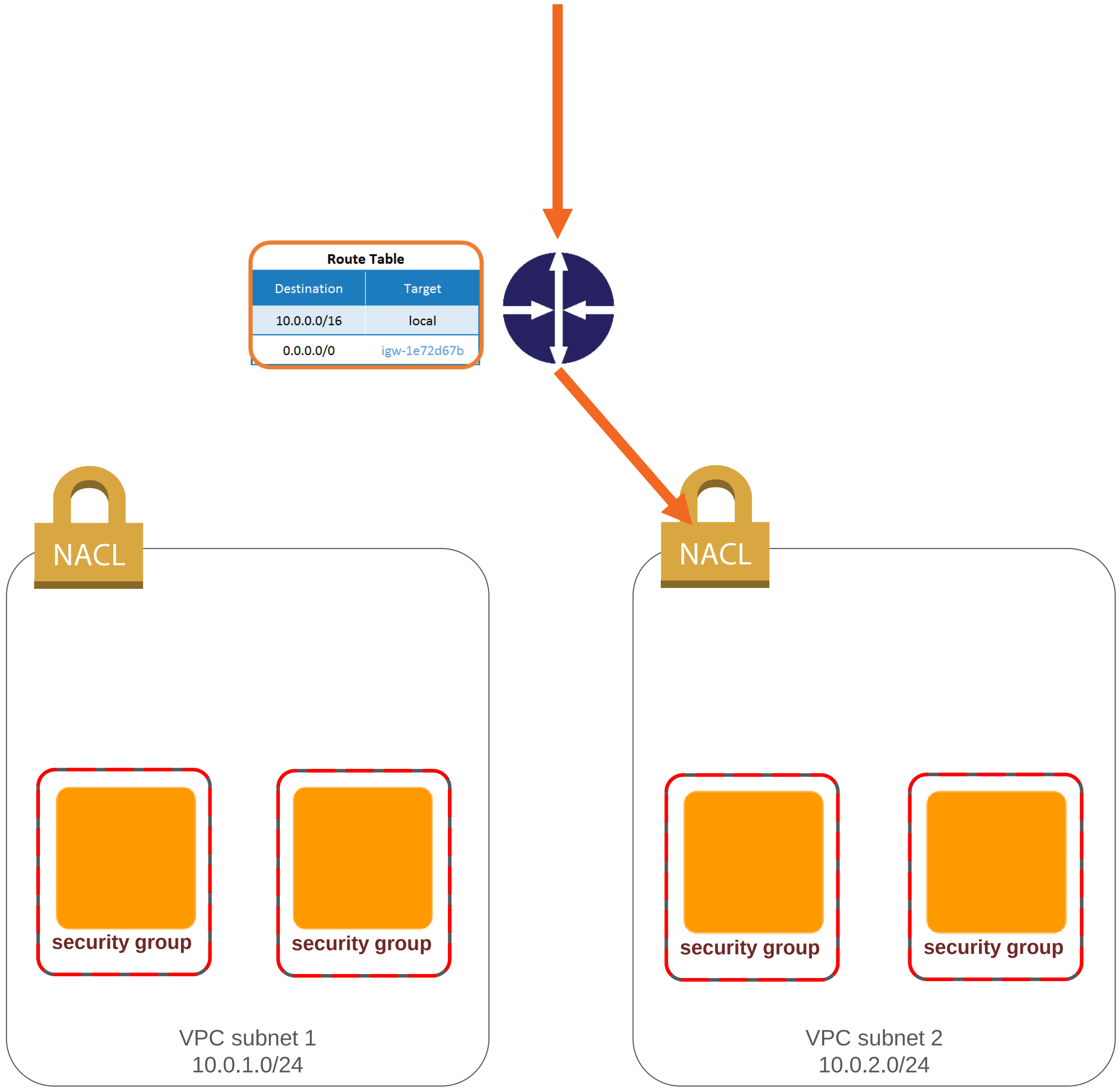
security group

VPC subnet 1
10.0.1.0/24

VPC subnet 2
10.0.2.0/24

Security Groups

- Inbound rules
- Outbound rules
- Explicit ALLOW | Implicit DENY
- Stateful



Route Table

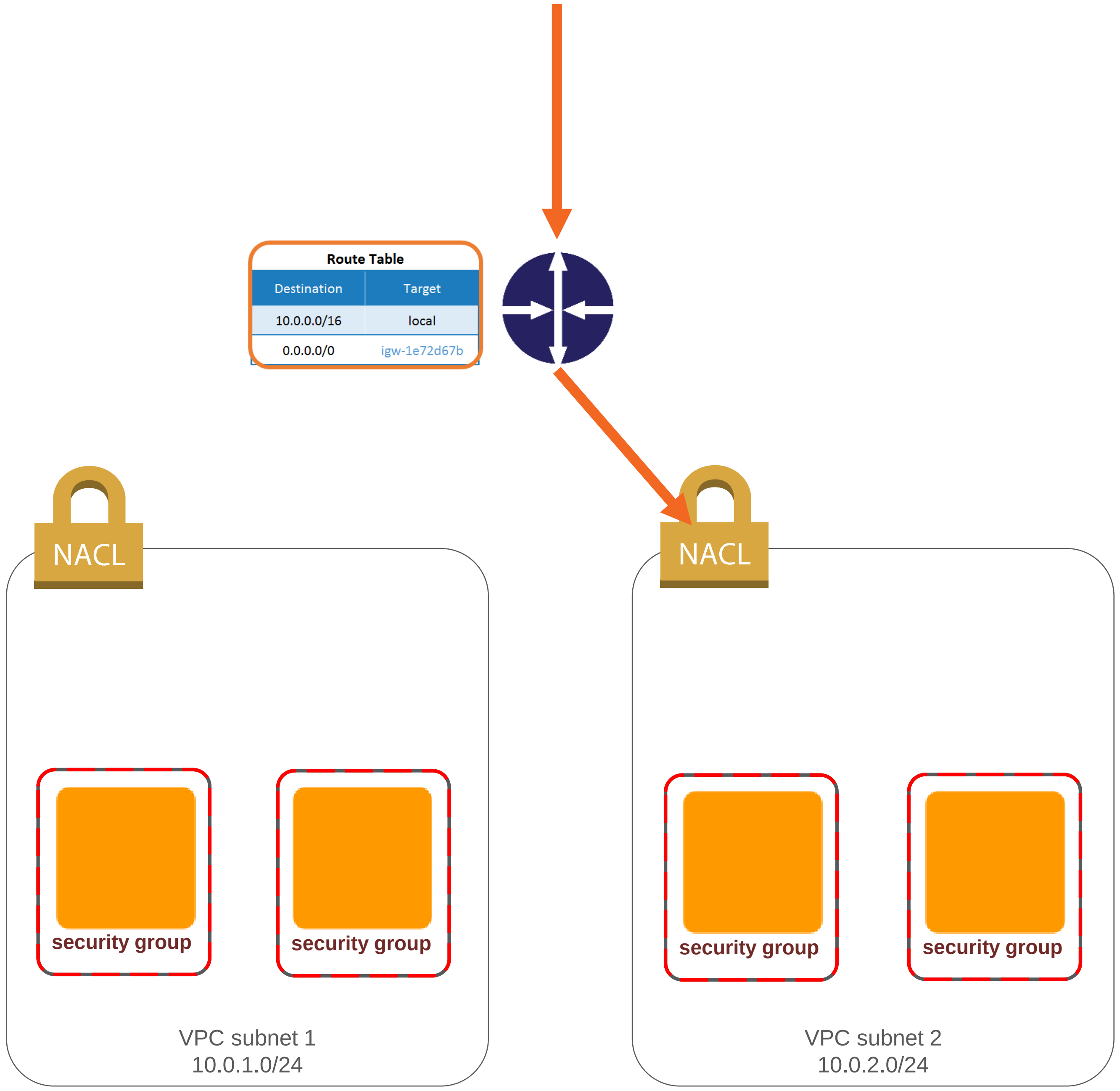
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-1e72d67b

Security Groups

- Inbound rules
- Outbound rules
- Explicit ALLOW | Implicit DENY
- Stateful

Network ACLs

- Inbound rules
- Outbound rules
- Explicit ALLOW
- Explicit DENY
- Stateless



Route Table

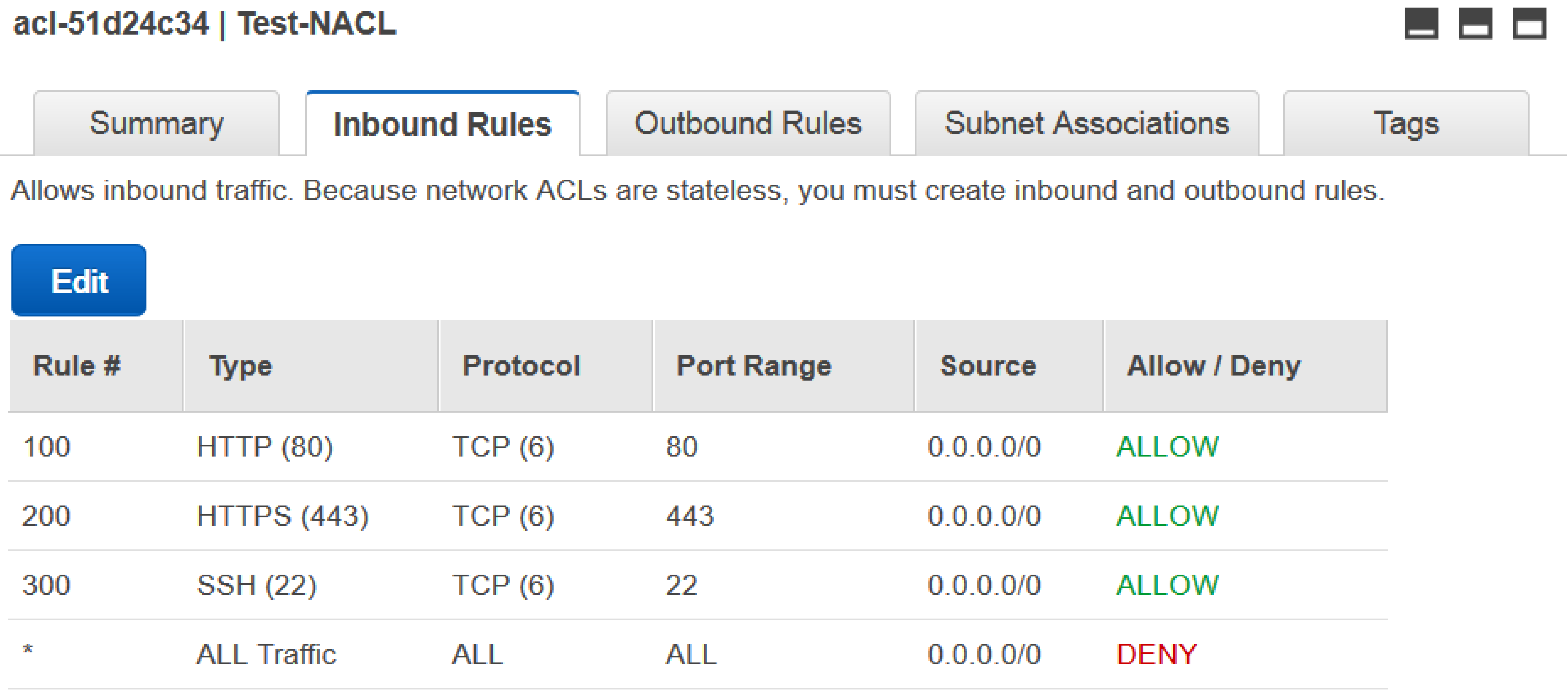
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-1e72d67b

Security Groups

- Inbound rules
- Outbound rules
- Explicit ALLOW | Implicit DENY
- Stateful

Network ACLs

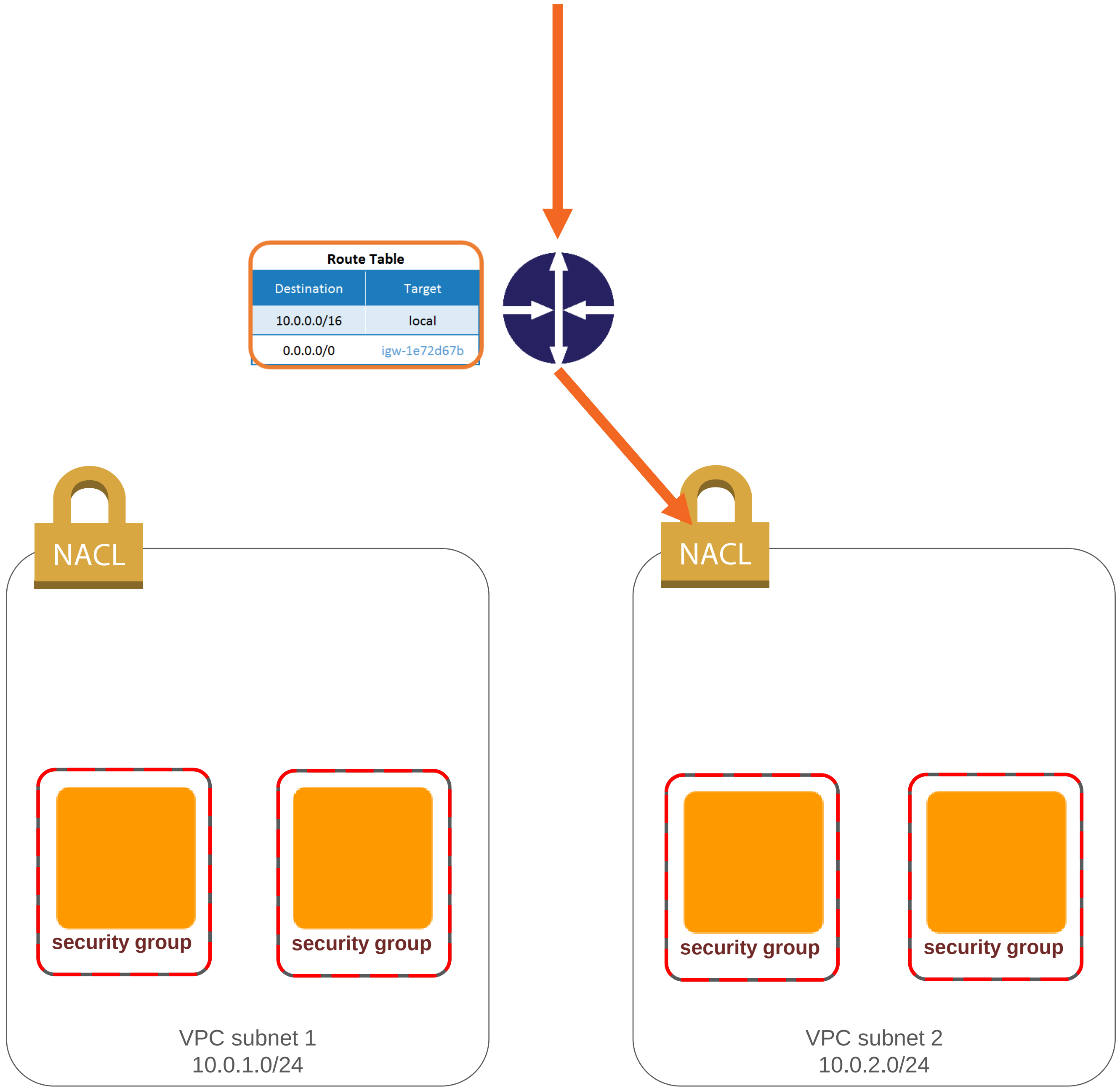
- Inbound rules
- Outbound rules
- Explicit ALLOW
- Explicit DENY
- Stateless



acl-51d24c34 | Test-NACL

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

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

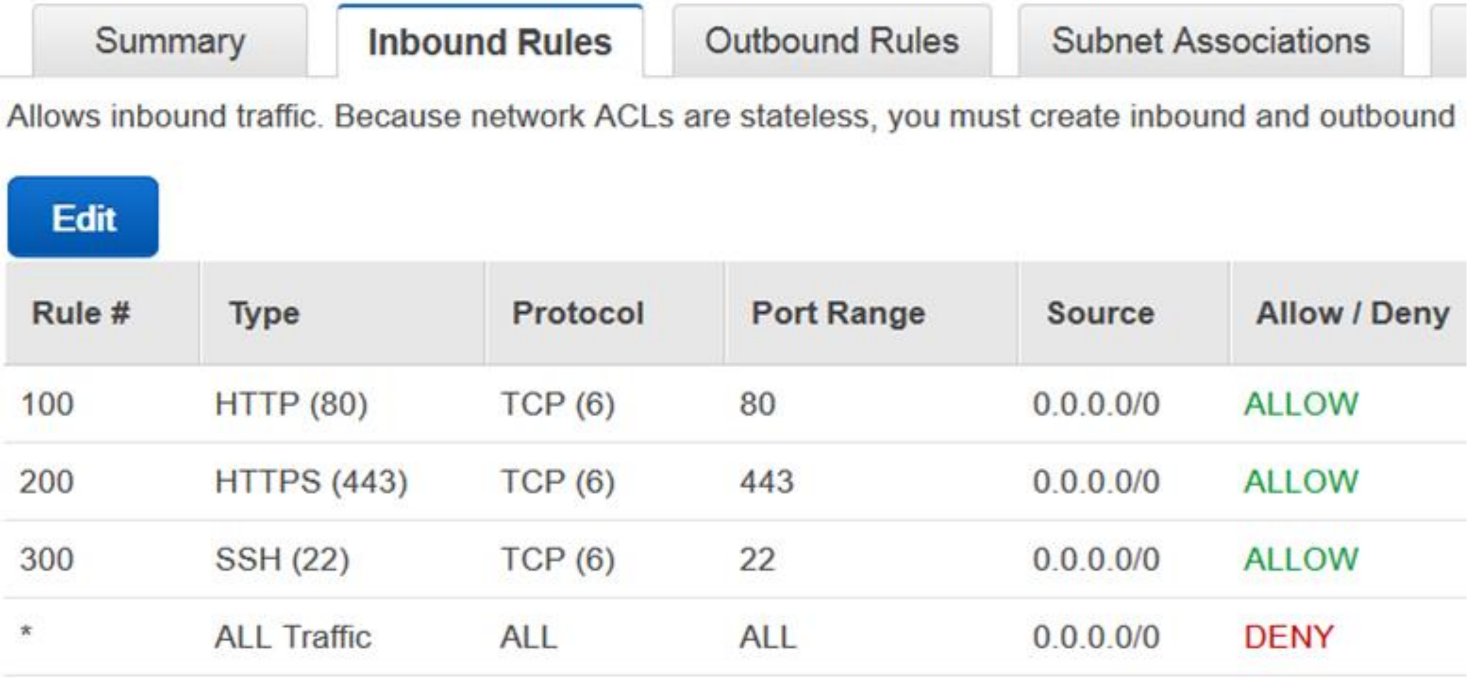


Route Table

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

Network ACLs

- Inbound rules
- Outbound rules
- Explicit ALLOW
- Explicit DENY
- Stateless
- Rules processed in # order
- Rule processing stops upon match
- Once NACL per Subnet



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

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

Summary

Multi-factor Authentication

HTTPS

Role-based Access Control

Anti-Virus

Encryption

AppArmor

Firewall

Minimized attack surface

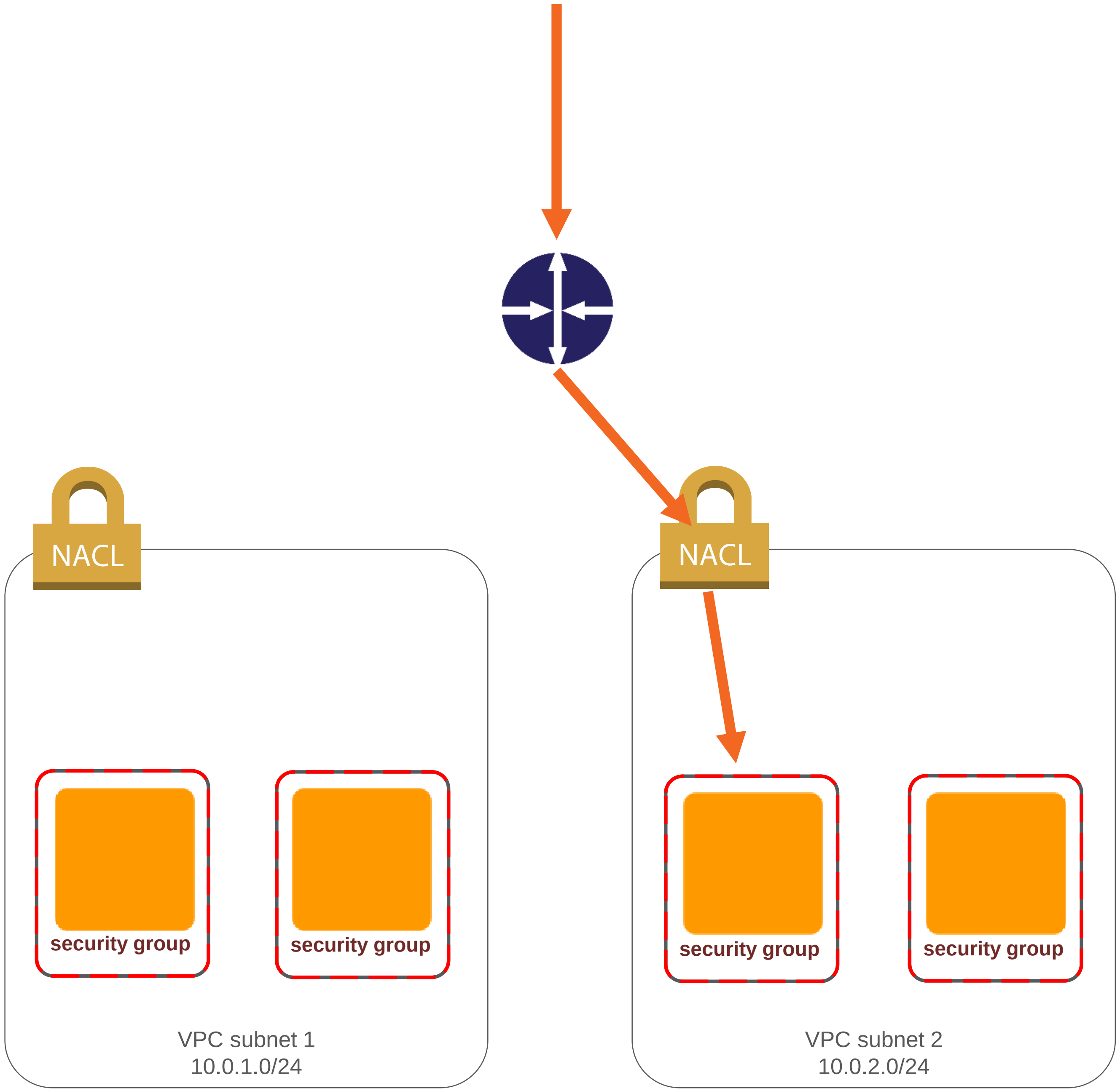
DMZ

SELinux

Sandboxes

Intrusion Detection Systems

IPsec



NACL
NACL
security group
security group
security group
security group
VPC subnet 1
10.0.1.0/24
VPC subnet 2
10.0.2.0/24

Coming Up Next…

Load Balancing