

# Traffic Control: Network Access Control Lists and Security Groups Part 2

---



**Brock Tubre**

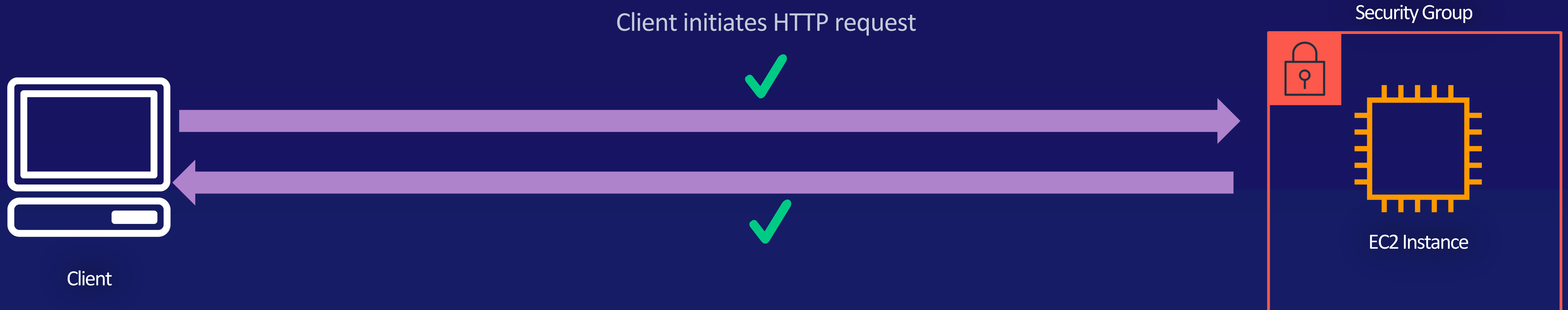
TECHNICAL INSTRUCTOR

Stateful

# Security Groups (Stateful)

Security Group - Inbound			
Type	Protocol	Port Range	Source
HTTP	TCP	80	0.0.0.0/0

Security Group - Outbound			
Type	Protocol	Port Range	Source
All Traffic	ALL	ALL	0.0.0.0/0

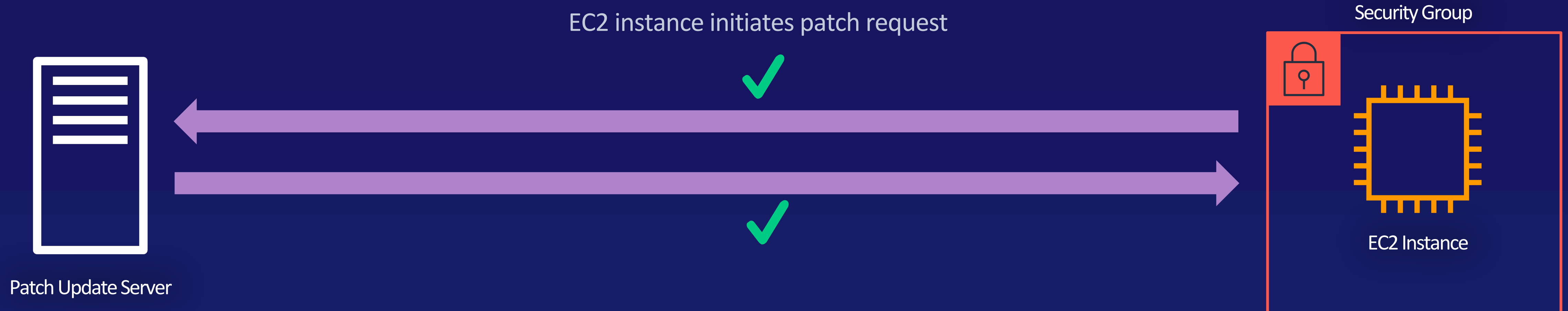


Stateful

# Security Groups (Stateful)

Security Group - Inbound			
Type	Protocol	Port Range	Source

Security Group - Outbound			
Type	Protocol	Port Range	Source
All Traffic	ALL	ALL	0.0.0.0/0

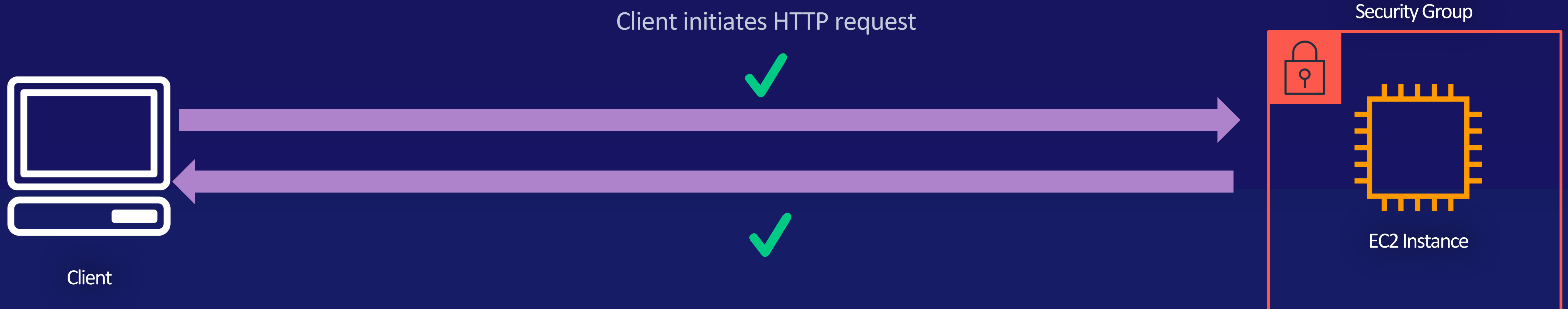


Stateful

# Security Groups (Stateful)

Security Group - Inbound			
Type	Protocol	Port Range	Source
HTTP	TCP	80	0.0.0.0/0

Security Group - Outbound			
Type	Protocol	Port Range	Source



Stateful

# Security Groups (Stateful)

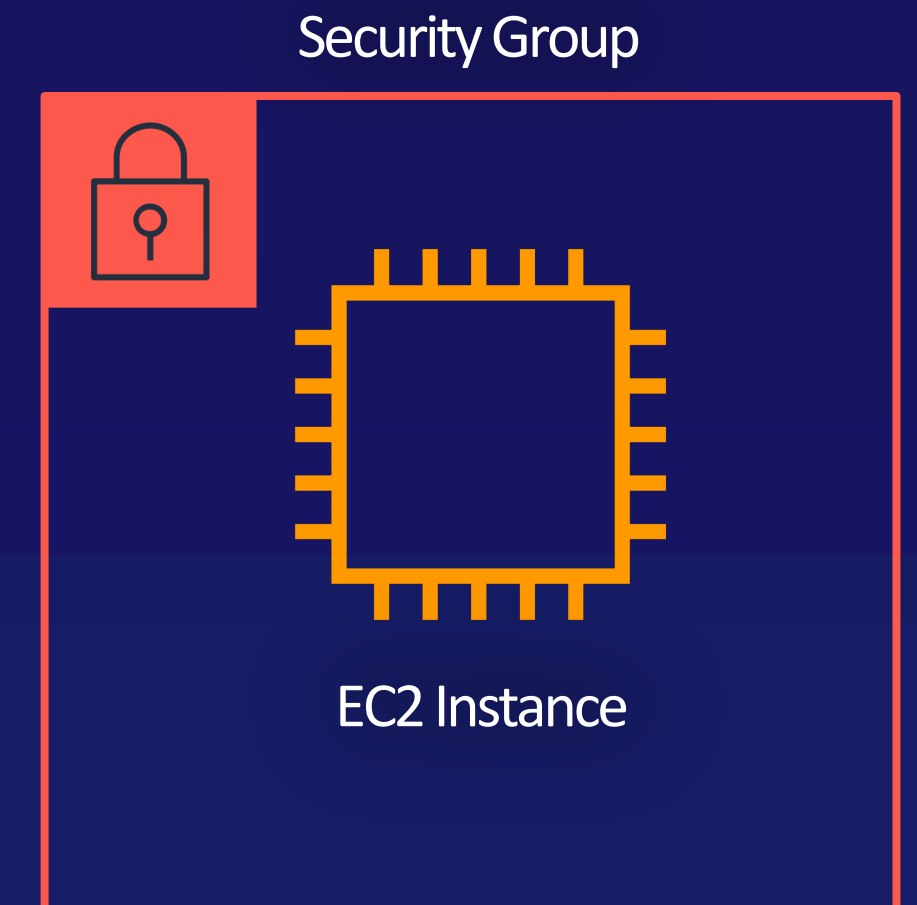
Security Group - Inbound			
Type	Protocol	Port Range	Source
HTTP	TCP	80	0.0.0.0/0

Security Group - Outbound			
Type	Protocol	Port Range	Source

EC2 instance initiates patch request

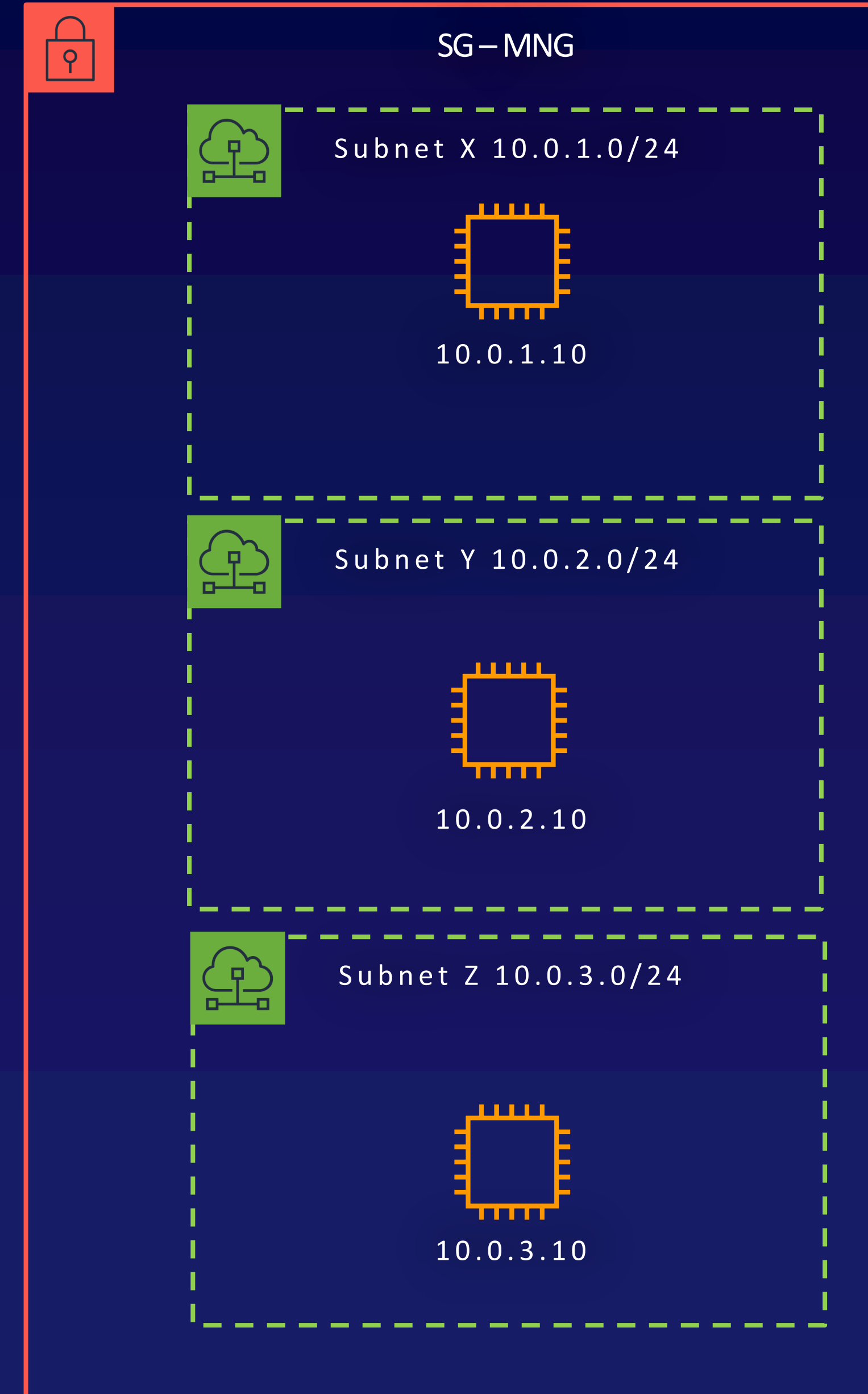
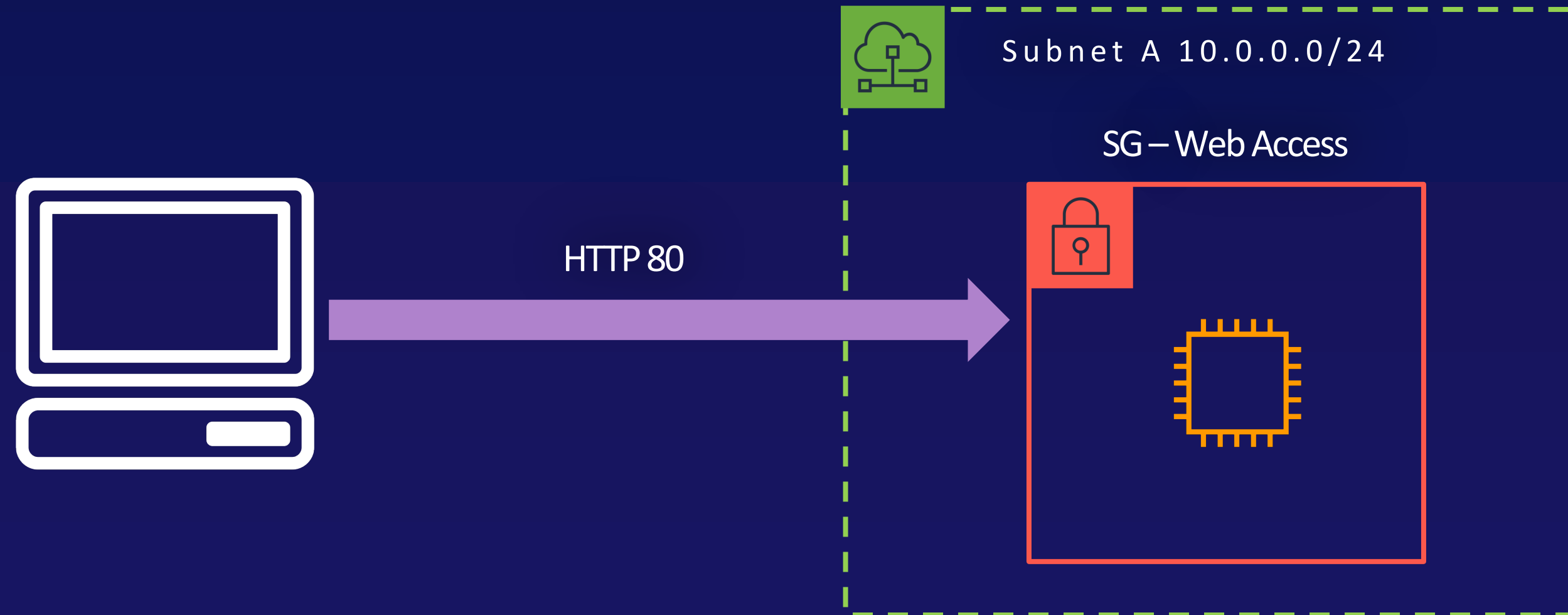


Patch Update Server



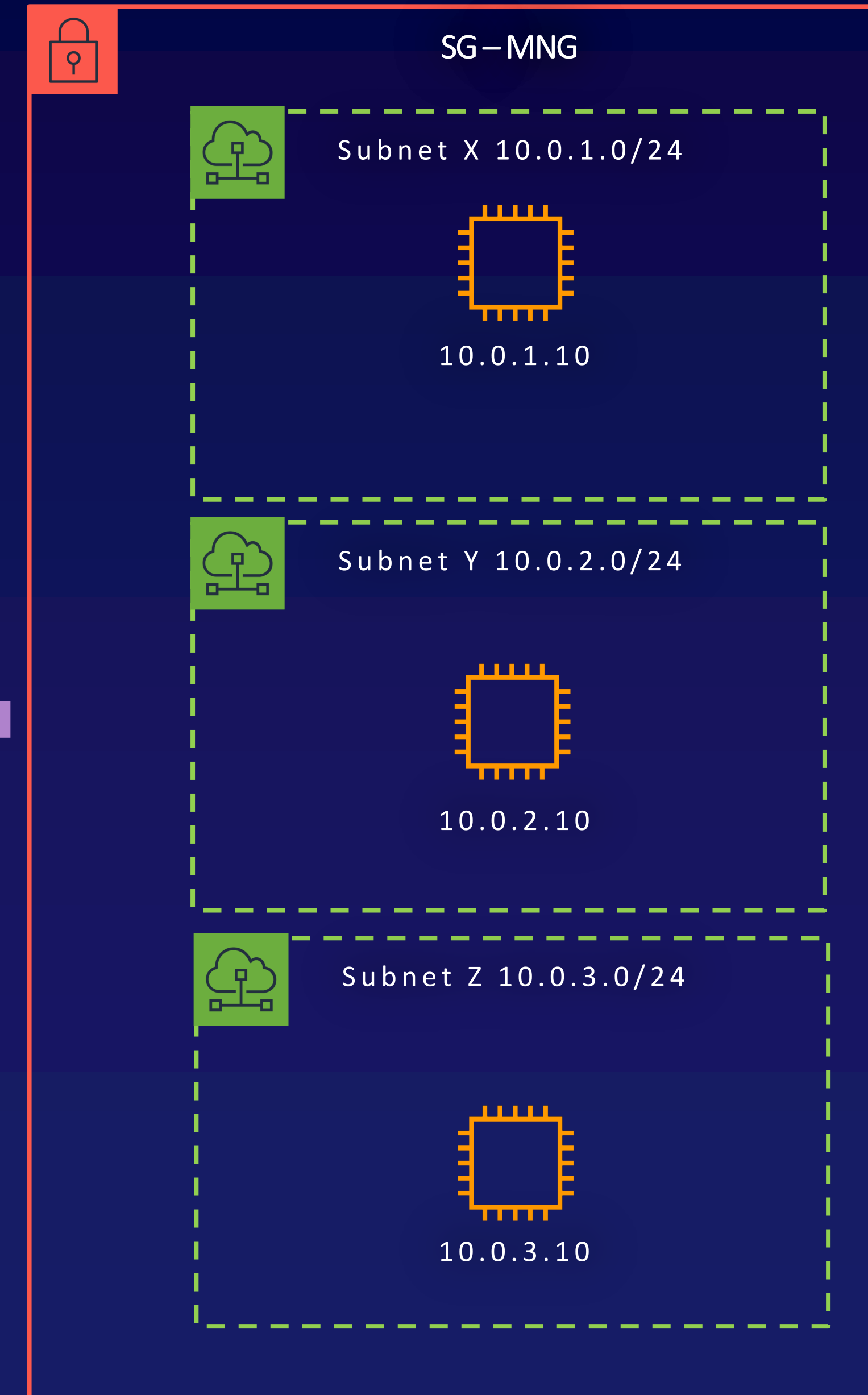
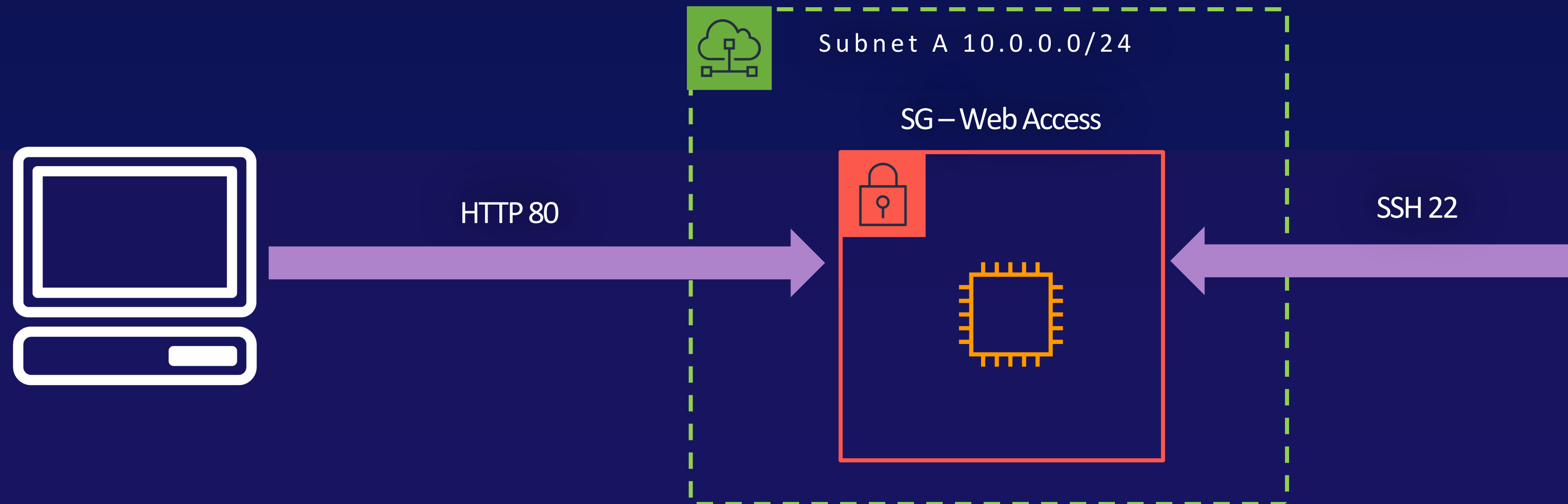
# Security Groups Self Referencing Feature

SG – Web Access (Inbound)			
Type	Protocol	Port Range	Source
HTTP	TCP	80	0.0.0.0/0

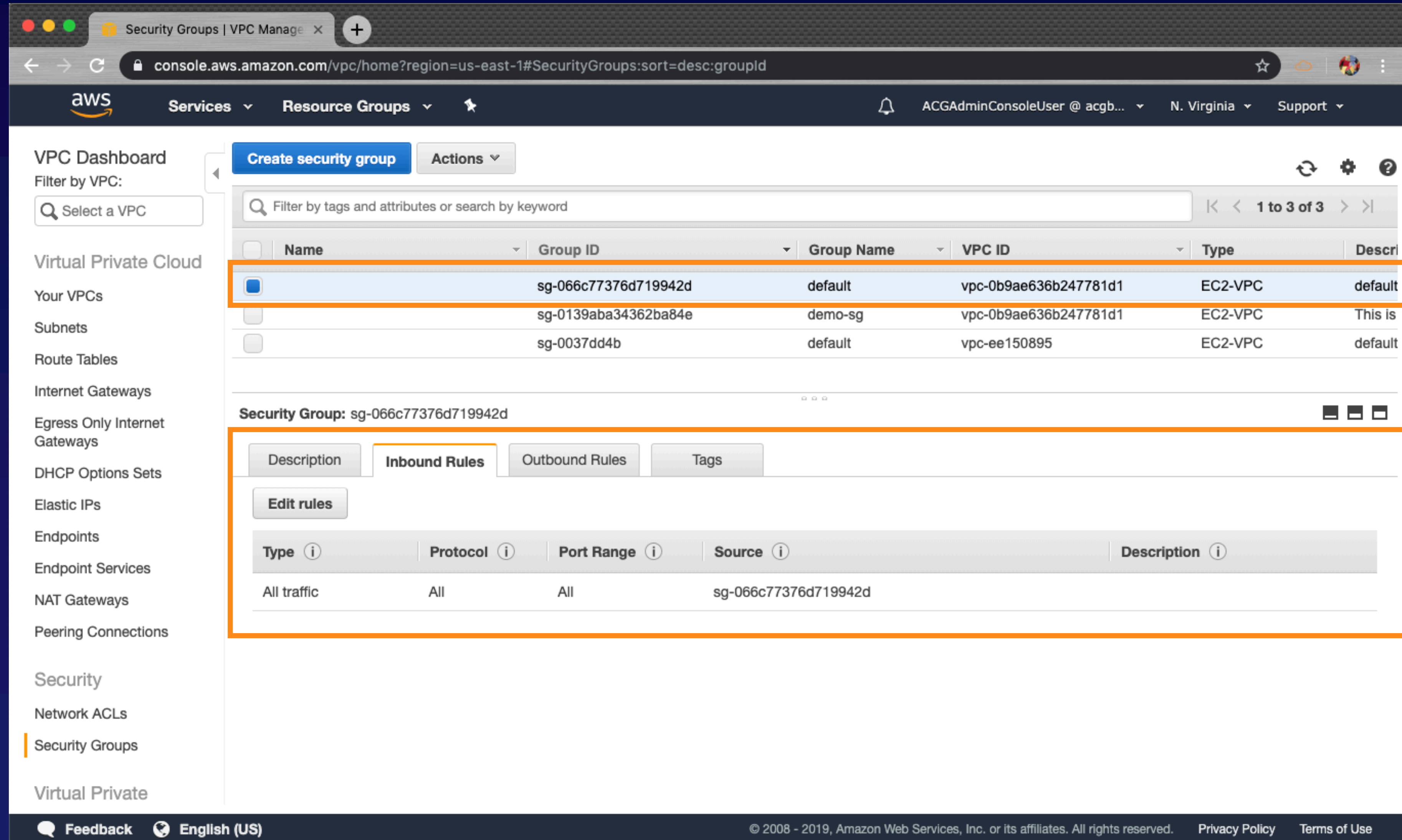


# Security Groups Self Referencing Feature

SG – Web Access (Inbound)			
Type	Protocol	Port Range	Source
HTTP	TCP	80	0.0.0.0/0
HTTP	TCP	22	SG - MNG



# Security Groups Self Referencing Feature



The screenshot shows the AWS Management Console interface for Security Groups. The first security group in the list is highlighted with an orange box. Below it, the 'Inbound Rules' tab for that security group is also highlighted with an orange box, showing a self-referencing rule.

Name	Group ID	Group Name	VPC ID	Type	Description
<input checked="" type="checkbox"/>	sg-066c77376d719942d	default	vpc-0b9ae636b247781d1	EC2-VPC	default
<input type="checkbox"/>	sg-0139aba34362ba84e	demo-sg	vpc-0b9ae636b247781d1	EC2-VPC	This is
<input type="checkbox"/>	sg-0037dd4b	default	vpc-ee150895	EC2-VPC	default

Type	Protocol	Port Range	Source	Description
All traffic	All	All	sg-066c77376d719942d	

# NACLs and Rule Ordering

NACL (Inbound)					
Rule #	Type	Protocol	Port Range	Source	Allow/Deny
100	SSH	TCP	22	0.0.0.0/0	ALLOW
200	HTTP	TCP	80	1.2.3.4/32	DENY
300	HTTP	TCP	80	0.0.0.0/0	ALLOW
400	HTTPS	TCP	443	0.0.0.0/0	ALLOW
500	Custom TCP	TCP	49152-65535	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY



Mandatory rule that cannot be edited or removed. It matches any request that has not matched any other rules. It always applies a DENY.

# NACLs and Rule Ordering

HTTP 3.3.3.3



HTTP 1.2.3.4



NACL (Inbound)					
Rule #	Type	Protocol	Port Range	Source	Allow/Deny
100	SSH	TCP	22	0.0.0.0/0	ALLOW
200	HTTP	TCP	80	1.2.3.4/32	DENY
300	HTTP	TCP	80	0.0.0.0/0	ALLOW
400	HTTPS	TCP	443	0.0.0.0/0	ALLOW
500	Custom TCP	TCP	49152-65535	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

# NACLs and Rule Ordering

HTTP 3.3.3.3



HTTP 1.2.3.4



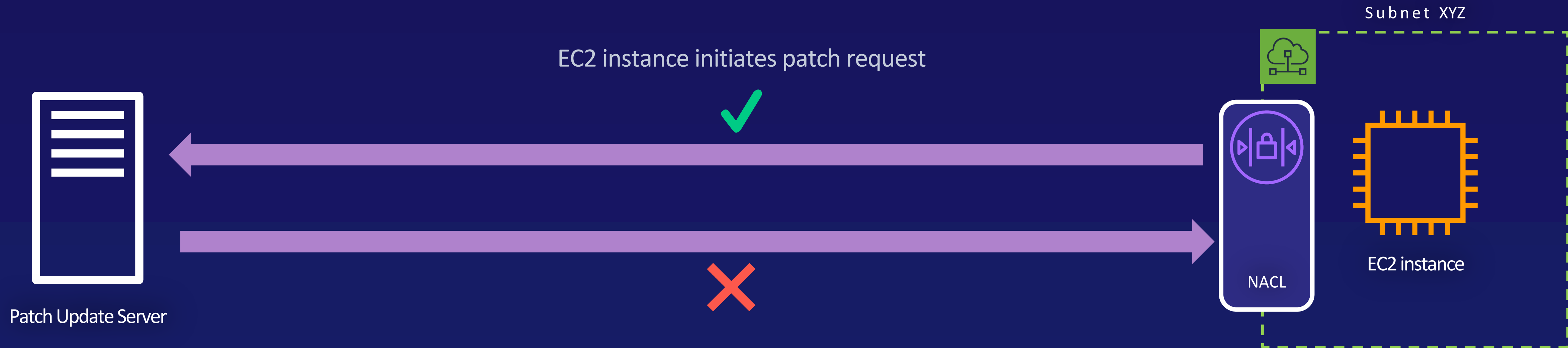
NACL (Inbound)					
Rule #	Type	Protocol	Port Range	Source	Allow/Deny
100	SSH	TCP	22	0.0.0.0/0	ALLOW
200	HTTP	TCP	80	1.2.3.4/32	DENY
300	HTTP	TCP	80	0.0.0.0/0	ALLOW
400	HTTPS	TCP	443	0.0.0.0/0	ALLOW
500	Custom TCP	TCP	49152-65535	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

Stateless

# Network ACLs (Stateless)

NACL - Inbound					
Rule #	Type	Protocol	Port Range	Source	Allow/Deny
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

NACL - Outbound					
Rule #	Type	Protocol	Port Range	Destination	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY



# NACLs and Rule Ordering

HTTP 3.3.3.3



NACL (Inbound)					
Rule #	Type	Protocol	Port Range	Source	Allow/Deny
100	SSH	TCP	22	0.0.0.0/0	ALLOW
200	HTTP	TCP	80	1.2.3.4/32	DENY
300	HTTP	TCP	80	0.0.0.0/0	ALLOW
400	HTTPS	TCP	443	0.0.0.0/0	ALLOW
500	Custom TCP	TCP	49152-65535	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

# NACLs and Rule Ordering

NACL (Inbound)					
Rule #	Type	Protocol	Port Range	Source	Allow/Deny
100	SSH	TCP	22	0.0.0.0/0	ALLOW
200	HTTP	TCP	80	1.2.3.4/32	DENY
300	HTTP	TCP	80	0.0.0.0/0	ALLOW
400	HTTPS	TCP	443	0.0.0.0/0	ALLOW
500	Custom TCP	TCP	49152-65535	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY



Mandatory rule that cannot be edited or removed. It matches any request that has not matched any other rules. It always applies a DENY.

## Implicit and Explicit

---

*Implicit deny = default wildcard rule*

*Explicit allow = specific allow rule*

*Explicit deny = specific deny rule*

Stateless

# Network ACLs (Stateless)

NACL - Inbound					
Rule #	Type	Protocol	Port Range	Source	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

NACL - Outbound					
Rule #	Type	Protocol	Port Range	Destination	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY



Stateless

# Network ACLs (Stateless)

NACL - Inbound					
Rule #	Type	Protocol	Port Range	Source	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

NACL - Outbound					
Rule #	Type	Protocol	Port Range	Destination	Allow/Deny
<del> </del>	<del> </del>	<del> </del>	<del> </del>	<del> </del>	<del> </del>
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY



Stateless

# Network ACLs (Stateless)

NACL - Inbound					
Rule #	Type	Protocol	Port Range	Source	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

NACL - Outbound					
Rule #	Type	Protocol	Port Range	Destination	Allow/Deny
<del>100</del>	<del>All IPv4 traffic</del>	<del>All</del>	<del>All</del>	<del>0.0.0.0/0</del>	<del>ALLOW</del>
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

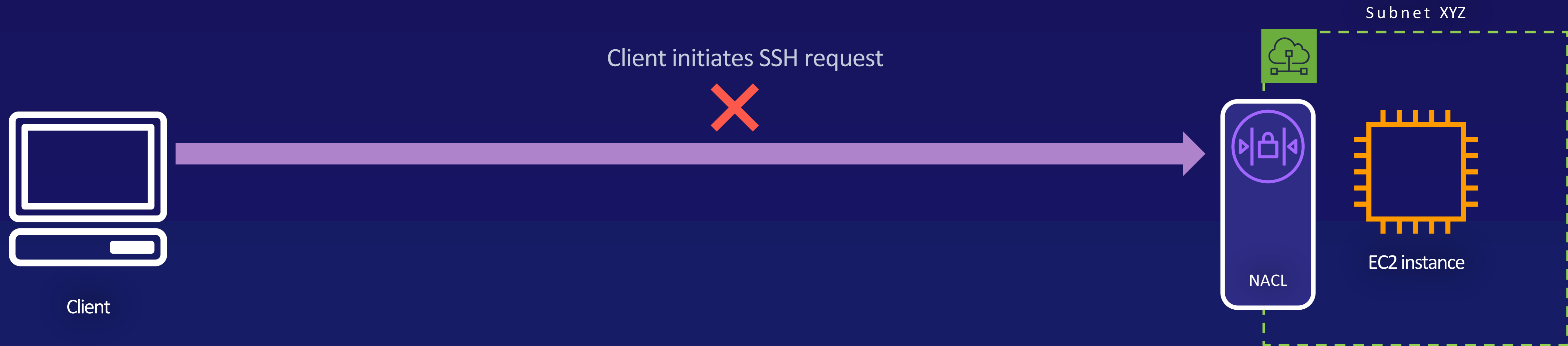


Stateless

# Network ACLs (Stateless)

NACL - Inbound					
Rule #	Type	Protocol	Port Range	Source	Allow/Deny
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY

NACL - Outbound					
Rule #	Type	Protocol	Port Range	Destination	Allow/Deny
100	All IPv4 traffic	All	All	0.0.0.0/0	ALLOW
*	All IPv4 traffic	All	All	0.0.0.0/0	DENY



# Default and Custom NACLs

The screenshot shows the AWS Management Console interface for Network ACLs. The left sidebar contains navigation options like 'VPC Dashboard', 'Virtual Private Cloud', and 'Security'. The main content area shows a list of Network ACLs, with the first one selected. Below, the 'Inbound Rules' tab is active, displaying a table of rules for the selected ACL.

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

# Ephemeral

LASTING  
FOR A VERY  
SHORT TIME



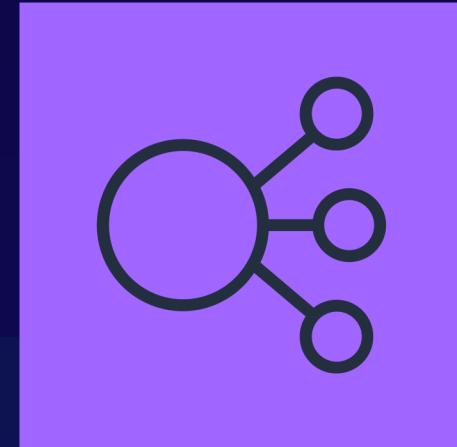
# ACG Dominates Deepracer



# Ephemeral Ports



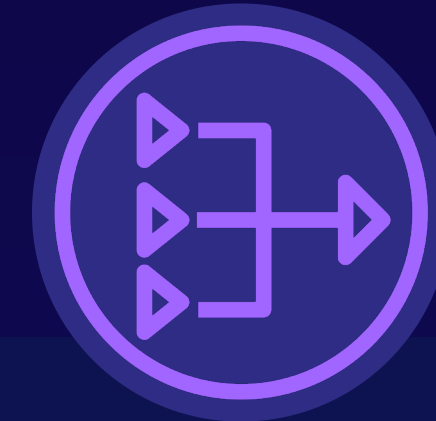
Linux  
32768-61000



Elastic Load Balancer  
32768-61000

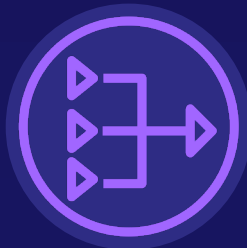
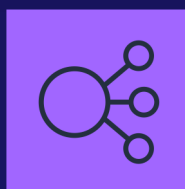


Windows Server 2003  
1025-5000

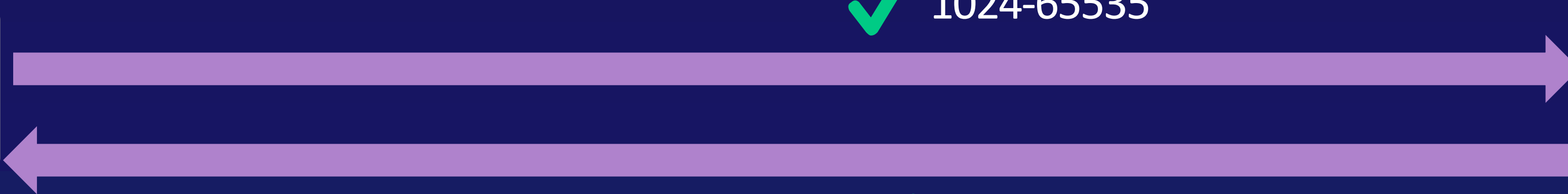


NAT Gateway  
1024-65535

Windows Server 2008+  
49152-65535



Client



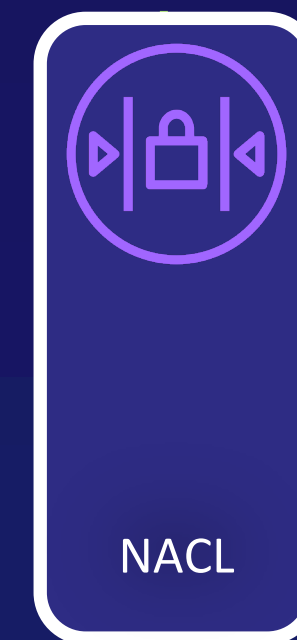
✓ 1024-65535



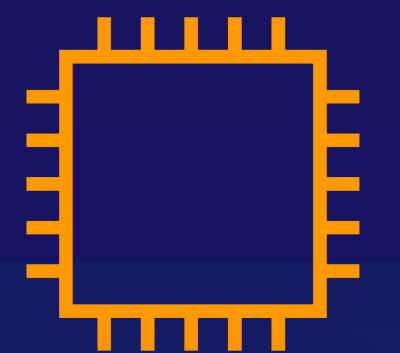
1024-65535 ✓



Subnet XYZ



NACL



EC2 instance

## Fast Takeaways

---

You can assign multiple security groups to a single ENI

---

Security groups have allow rules but no deny rules

---

Security groups are stateful

## Fast Takeaways

---

Every subnet must be associated with a NACL and operate at the subnet level

---

NACLs have both allow and deny rules

---

NACLs are stateless

## Fast Takeaways

---

Use a deny all approach

---

Only allow access where access needs to be granted

---

Be able to diagnose network issues that could be caused by SGs and NACLs