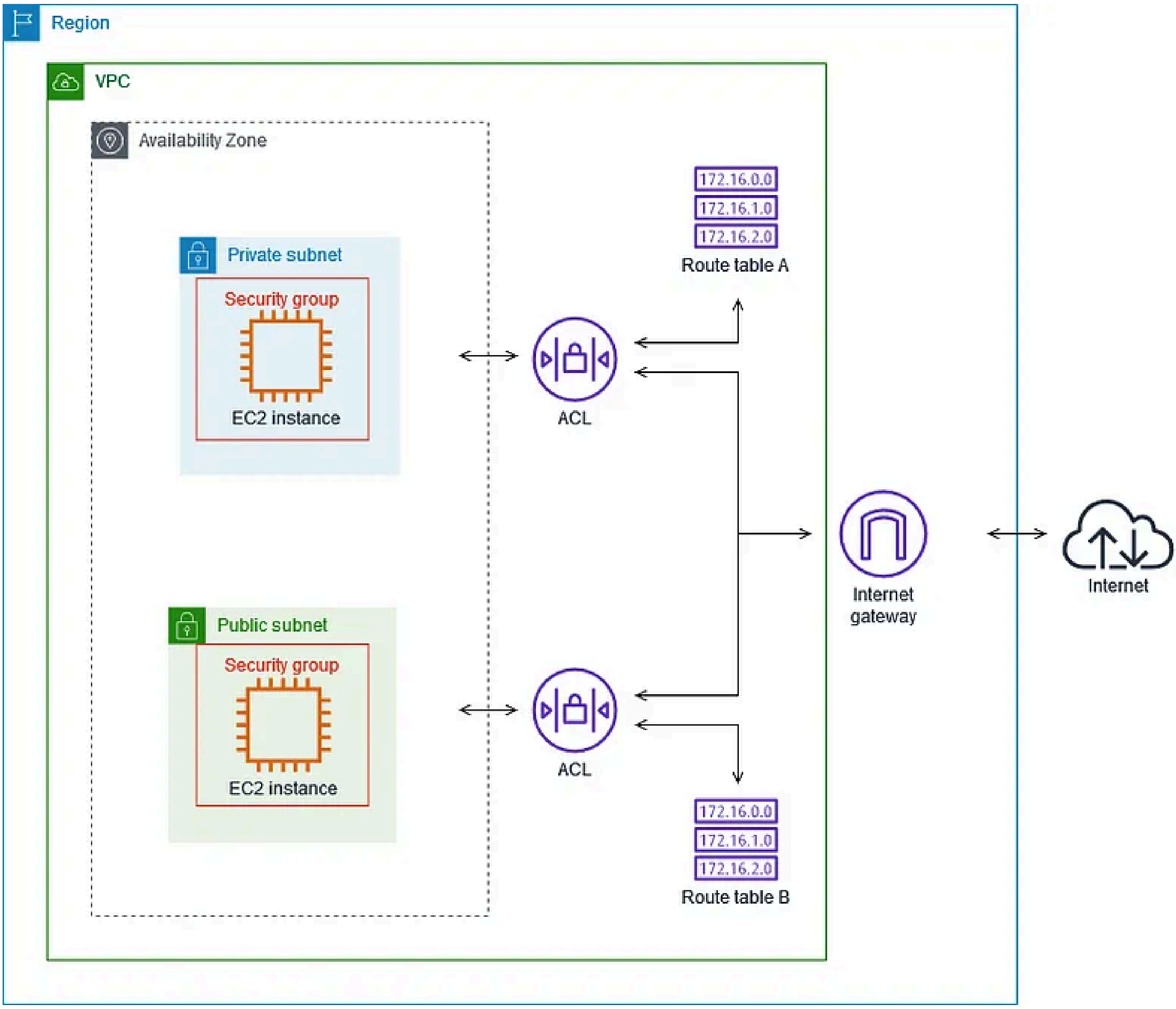
AWS — Difference between Security Groups and Network Access Control List (NACL)

Ashish Patel · Follow

Published in Awesome Cloud

2 min read · Apr 14, 2019

Comparison: VPC Security Group vs NACL in AWS.



Awesome Cloud — Security Groups and Network ACLs

TL;DR:

Security group is the firewall of EC2 **Instances**.
Network ACL is the firewall of the VPC **Subnets**.

Key Differences: Security group vs NACL

Scope: Subnet or Instance (where to apply)

Security Groups operate at Instance (Network Interface) level. Security Group has to be assigned explicitly to the instance.

Network ACLs at the subnet level. Applies automatically to all instances deployed in the associated subnet.

State: Stateful or Stateless

Security groups are stateful. Return traffic is allowed, regardless of the rules.
e.g. If you allow an incoming traffic on port 80, the outgoing traffic on port 80 will be automatically allowed.

Network ACLs are stateless. Return traffic must be explicitly allowed by the rules. Meaning any changes applied to an incoming rule will not be applied to outgoing rule.
e.g. If you allow an incoming port 80, you would also need to apply the rule for outgoing traffic.

Rule Type: Allow or Deny

Security group supports allow rules only (everything else is denied implicitly). You can specify allow rules, but not deny rules.
e.g. You cannot deny a certain IP address from establishing a connection.

Network ACL supports allow and deny rules.
e.g. By deny rules, you could explicitly deny a certain IP address to establish a connection to an EC2 Instance.

Rule Process order

Security group evaluates all rules before deciding whether to allow traffic.
(When you associate multiple security groups with a resource, the rules from each

security group are aggregated to form a single set of rules that are used to determine whether to allow access.)

Network ACL evaluates rules in order, starting with the lowest numbered rule, when deciding whether to allow traffic.
If matching rule found during evaluation, remaining rules won't be evaluated.

Occurrence

Instance can have multiple Security groups.

Subnet can have only one NACL.

Rule Destination

Security group rule allows CIDR, IP, and Security Group as destinations.

Network ACL rule only allows CIDR as a destination.

Defense order

Security group first layer of defense, whereas Network ACL is the second layer of defense for outbound/egress traffic.

Network ACL first layer of defense, whereas the Security group is the second layer of defense for inbound/ingress traffic.

> *Consider creating Network ACLs with rules similar to your security groups, to add an additional layer of security to your VPC.*

View more from *Awesome Cloud*

- Difference between SQS and SNS
- Difference between Application load balancer and Network load balancer
- Difference between Amazon Aurora and Amazon RDS
- Difference between Internet Gateway and NAT Gateway

- Difference between Secrets Manager and Parameter Store
- Difference between EKS and ECS

Happy Clouding!!!

AWS Vpc Security Nacl Securitygroup

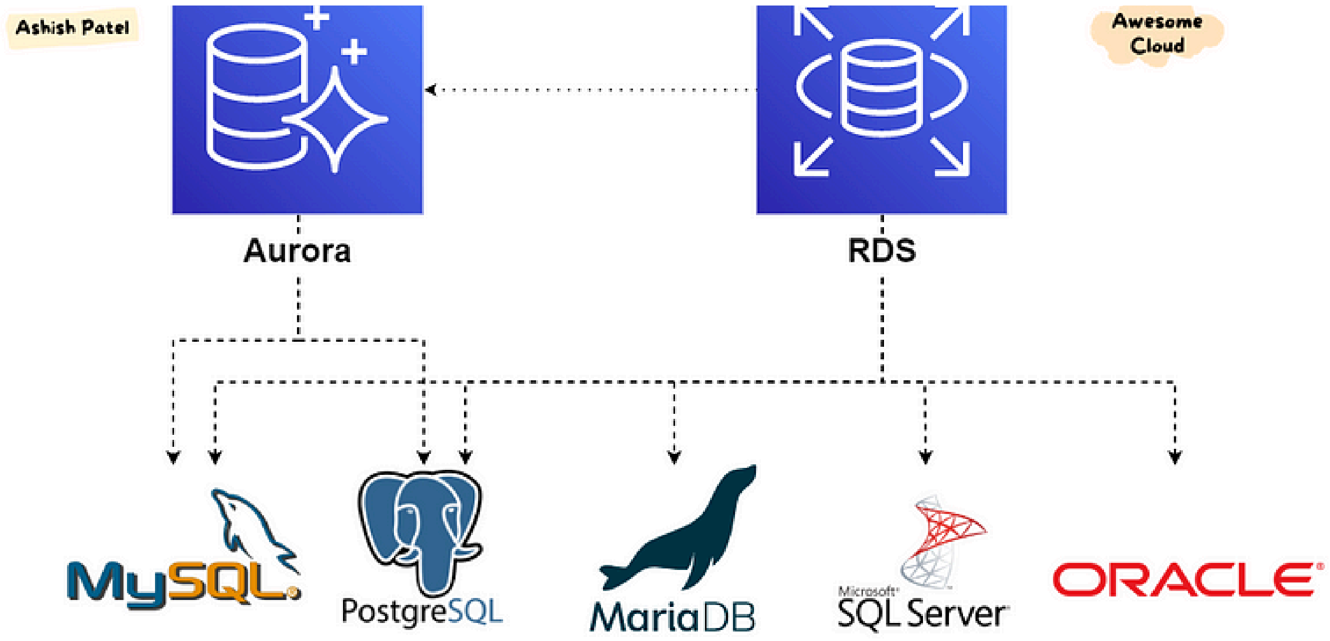
Follow

Written by Ashish Patel

18.9K Followers · Editor for Awesome Cloud

Cloud Architect • 4x AWS Certified • 6x Azure Certified • 1x Kubernetes Certified • MCP • .NET • Terraform • DevOps • Blogger [https://bit.ly/iamashishpatel]

More from Ashish Patel and Awesome Cloud



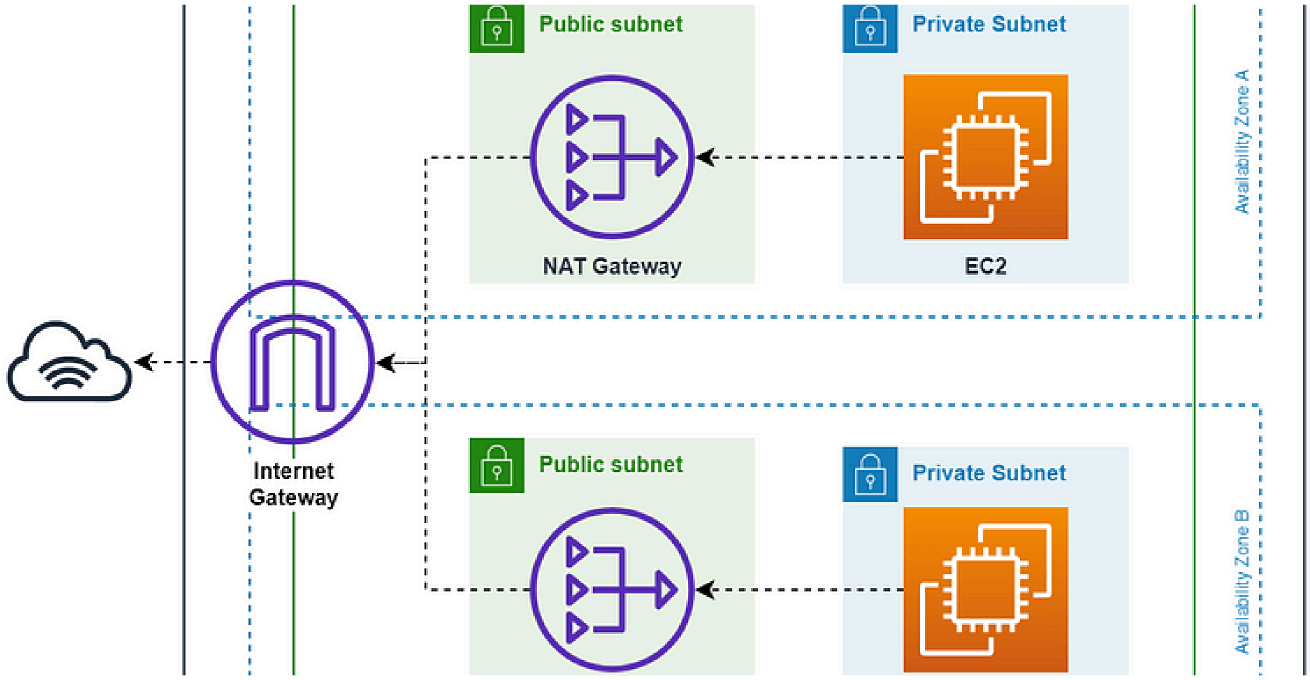
Ashish Patel in Awesome Cloud

AWS—Difference between Amazon Aurora and Amazon RDS

Comparison: Amazon Aurora vs Amazon RDS.

7 min read · Feb 7, 2022

1K 4



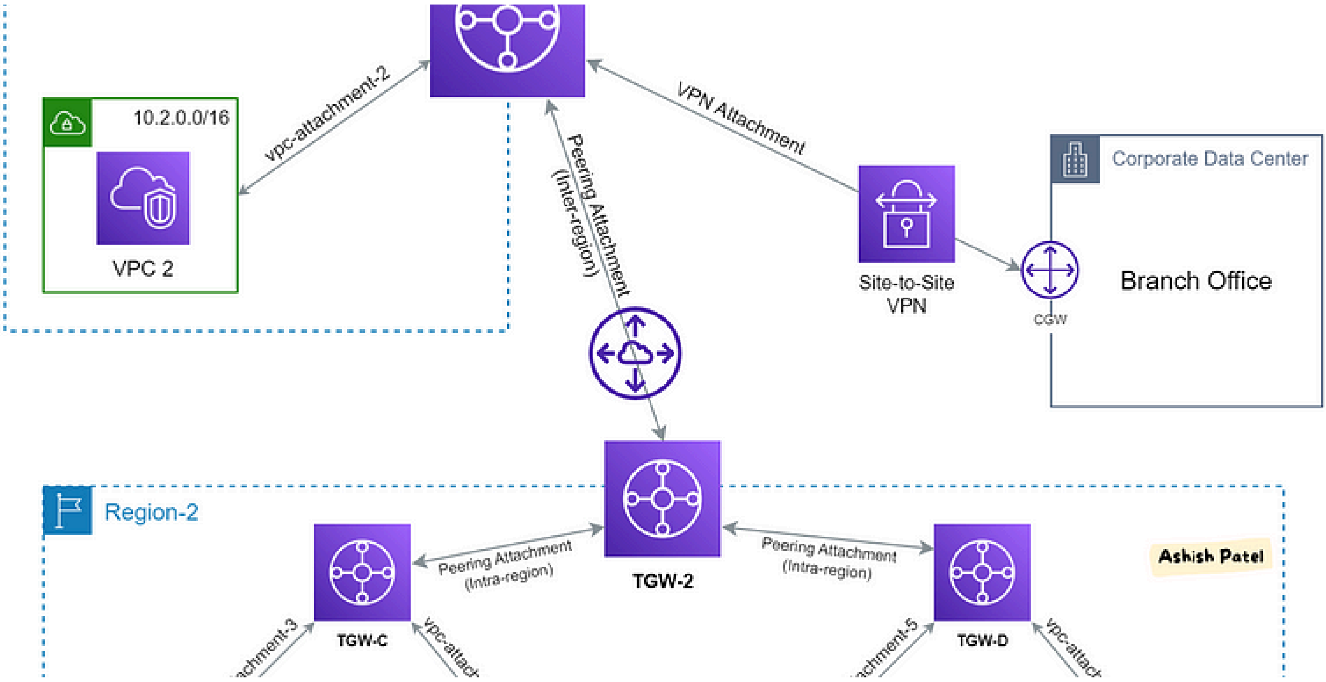
Ashish Patel in Awesome Cloud

AWS—Difference between Internet gateway and NAT gateway

Internet gateway vs NAT gateway in AWS

2 min read · May 25, 2019

1.2K 12



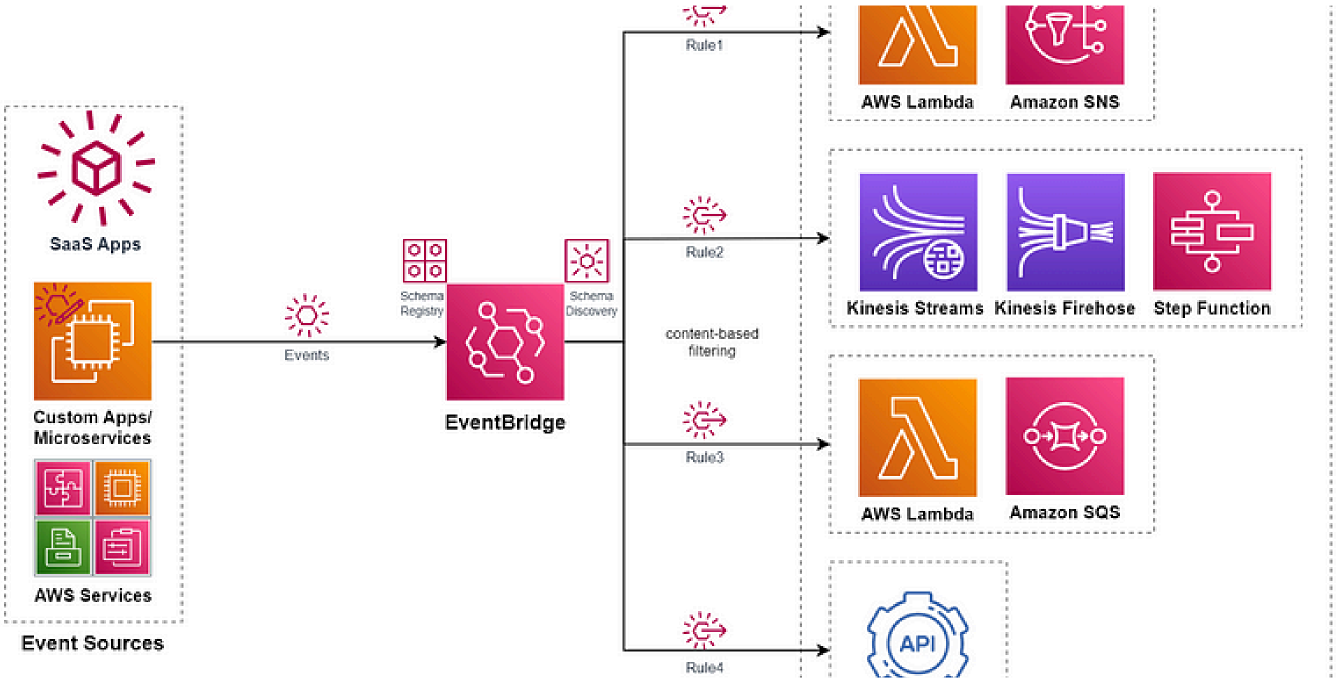
Ashish Patel in Awesome Cloud

AWS—Difference between VPC Peering and Transit Gateway

Comparisons: AWS VPC Peering vs AWS Transit Gateway in AWS

4 min read · Jan 8, 2023

270 3



Ashish Patel in Awesome Cloud

AWS—Amazon EventBridge Overview

What is Amazon EventBridge?—Introduction to AWS EventBridge.

6 min read · Mar 7, 2022

301 3

See all from Ashish Patel

See all from Awesome Cloud

Recommended from Medium

Faisal Kuzhan

DAY_25/90 => INTERVIEW QUESTIONS ON AWS

Below are some basic AWS interview questions along with the answers. ✍️

17 min read · Feb 12, 2024

91 3

Abdullah Muhammad

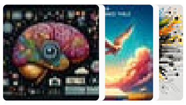
Deep Dive into AWS VPC and its Network and Security Components

This article assumes the reader has a basic understanding of cloud service providers such as AWS. Development experience is helpful, but...

13 min read · Jan 17, 2024

6

Lists



Natural Language Processing

1489 stories · 1001 saves

Georgi_V

How I passed the AWS Certified Security—Specialty exam SCS-C02 in 4 weeks!

Hi there, I am back with another certification success story and study tips. This time it's for the new AWS Certified Security—Specialty...

3 min read · Dec 17, 2023

194 2

Saloni Singh

AWS Solutions Architect Associate Certification — CheatSheet

This is a short guide which covers all those topics you need to cover to clear this exam. I have made this cheat-sheet while I was...

4 min read · Mar 16, 2024

105 6

Neal Davis

Top 20 AWS Solutions Architect Interview Questions

Being well-prepared is crucial for any tech interview, especially when aiming for a specialized position in cloud computing. For those…

9 min read · Dec 11, 2023

312 6

Meriem Terki in AWS Tip

Blocking web traffic with WAF in AWS

Looking to learn about AWS WAF and its usecases ?

11 min read · Jan 7, 2024

108 4

See more recommendations