



DAY 12: SECURITY GROUPS, NACLs, AND VPC PEERING

A Deep Dive into AWS VPC Security and Networking Features

Mohd Shahid

26-Apr-2025



INTRODUCTION TO VPC SECURITY IN AWS

- AWS VPC enables you to launch AWS resources in a virtual network that you define.
- Security is crucial to ensure that only authorized entities access your resources.
- AWS provides Security Groups, NACLs, and VPC Peering to manage access, traffic, and connectivity within your VPC.

SECURITY GROUPS – OVERVIEW

- What is a Security Group?
- A virtual firewall to control inbound and outbound traffic for EC2 instances.
- Features:
 - Stateful
 - Can associate with multiple instances
 - Supports IPv4 and IPv6
- Use Cases:
 - Allowing HTTP (port 80) for web servers
 - Allowing SSH (port 22) for remote administration



HOW SECURITY GROUPS WORK

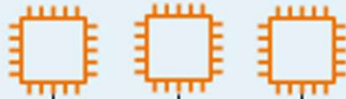
- Inbound Rules:
 - - Define which incoming traffic is allowed to reach instances.
- Outbound Rules:
 - - Define which outbound traffic is allowed from instances.
- Security groups are stateful, meaning response traffic is automatically allowed.



VPC



Subnet A



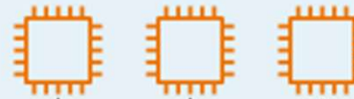
Source	Protocol	Port
198.51.100.0/24	TCP	22
Subnet A CIDR	All	All

Destination	Protocol	Port
0.0.0.0/0	All	All

Security group 1



Subnet B



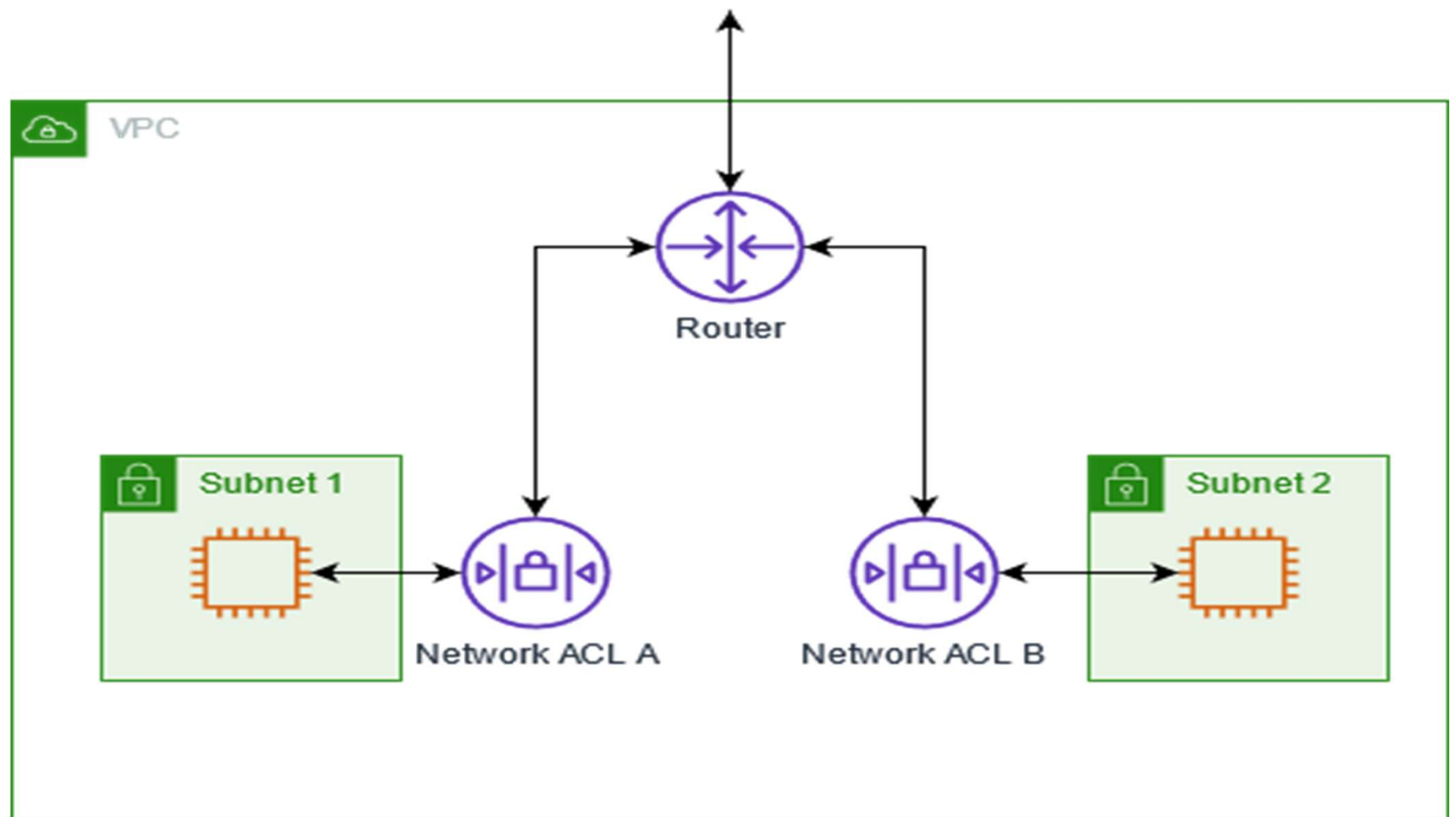
Source	Protocol	Port
Subnet B CIDR	All	All
Subnet A CIDR	TCP	22

Destination	Protocol	Port
0.0.0.0/0	All	All

Security group 2

NACLs VS SECURITY GROUPS

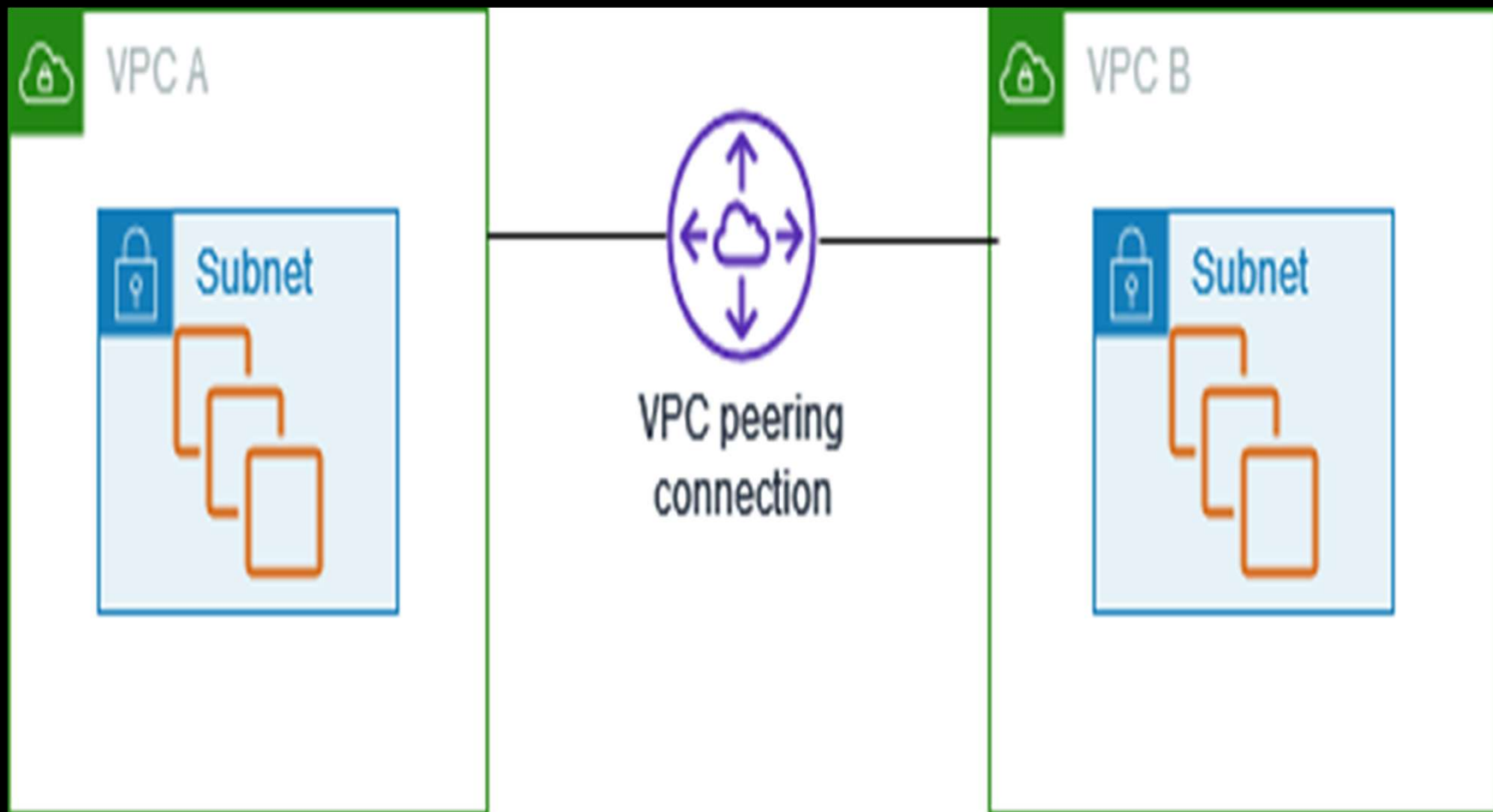
- What is a NACL?
- A network-level firewall that controls inbound and outbound traffic for subnets.
- Stateless: Each request must be explicitly allowed or denied in both directions.
- Differences from Security Groups:
 - NACLs are applied to subnets; Security Groups to instances.
 - NACLs are stateless, Security Groups are stateful.





VPC PEERING – OVERVIEW

- What is VPC Peering?
- Allows communication between two VPCs in the same or different AWS accounts.
- Enables private IP traffic between VPCs.
- Use Cases:
 - Cross-region peering for disaster recovery
 - Inter-VPC communication in multi-region architectures

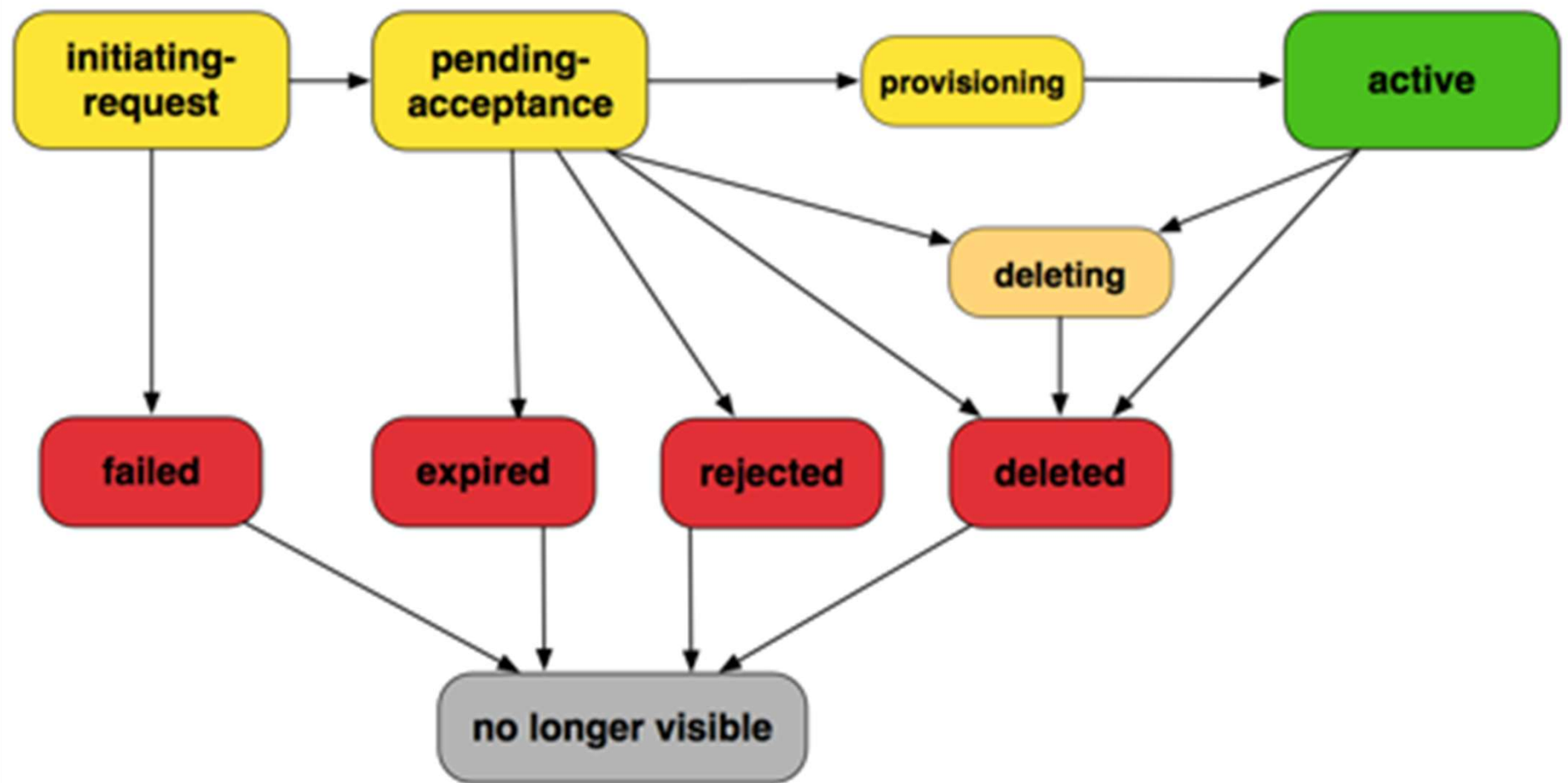






VPC PEERING LIMITATIONS

- Non-Transitive Peering:
 - - VPC A cannot route traffic to VPC C via VPC B.
- CIDR Block Overlap:
 - - Peering cannot be established if CIDR blocks overlap.
- No Support for Edge-to-Edge Routing:
 - - VPC Peering only allows communication between VPCs.

VPC PEERING CONNECTION LIFECYCLE



- 
- A VPC Peering Connection goes through several well-defined states. Each state determines what actions can be taken and how long the connection remains visible.
 1. Initiating-request
 2. Failed
 3. Pending-acceptance
 4. Expired
 5. Rejected
 6. Provisioning
 7. Active



State	Action Required	Expires In	Visibility
Initiating-request	Wait for system to process	N/A	Requester
Failed	No action possible	2 hours	Requester
Pending-acceptance	Accept / Reject / Delete	7 days	Both
Expired	No further action allowed	2 days	Both
Rejected	No further action allowed	2 days / 2 hours	Depends on account relationship
Provisioning	No action required	N/A	Both
Active	Functional, can delete	N/A	Both

USE CASES FOR VPC PEERING

- Multi-Region Applications:
 - - Connecting different regions for high availability and disaster recovery.
- Multiple Account Setups:
 - - Connecting VPCs across different AWS accounts.
- Private Connectivity:
 - - Ensures secure data flow over private network.

VPC PEERING CONNECTION QUOTAS – AWS

Name	Default Limit	Adjustable
Active VPC peering connections per VPC	50	Yes (up to 125)
Outstanding (pending) VPC peering requests per VPC	25	Yes
Expiry time for unaccepted peering request	1 week (168 hours)	✗ No



EXAMPLE: CONFIGURATION

- Step 1: Create VPCs (A, B, and C) with appropriate CIDR ranges.
- Step 2: Set up Security Groups for each VPC and define inbound/outbound rules.
- Step 3: Create NACLs to restrict specific traffic between VPCs.
- Step 4: Establish VPC Peering between VPCs and update route tables.



ROUTE TABLE CONFIGURATION OVERVIEW

1. Update each VPC's route table
2. Include peering connection CIDRs
3. Ensure no overlapping CIDR ranges
4. Test connectivity between VPCs after peering and route table updates



UPDATING ROUTE TABLES FOR PEERING

Each VPC must have its route table updated to include:

- The CIDR range of other VPCs (e.g., VPC B, VPC C)
- The peering connection as the target for routing traffic

This allows VPCs to communicate securely and efficiently.

VPC A - ROUTE TABLE

Destination CIDR	Target
10.0.0.0/16	default route
10.1.0.0/16	peering-A-B
10.2.0.0/16	peering-A-C



ADDITIONAL CONSIDERATIONS

1. Ensure CIDR blocks of peered VPCs do not overlap
2. Update route tables for each VPC involved in peering
3. No transitive peering between VPCs
4. Use proper security controls like Security Groups and NACLs



BEST PRACTICES

- Security Groups:
 - - Apply least privilege to inbound/outbound rules.
- NACLs:
 - - Use for broader subnet-level security.
 - - Allow return traffic for stateless NACLs.
- VPC Peering:
 - - Avoid overlapping CIDR blocks.
 - - Keep in mind limitations and design accordingly.