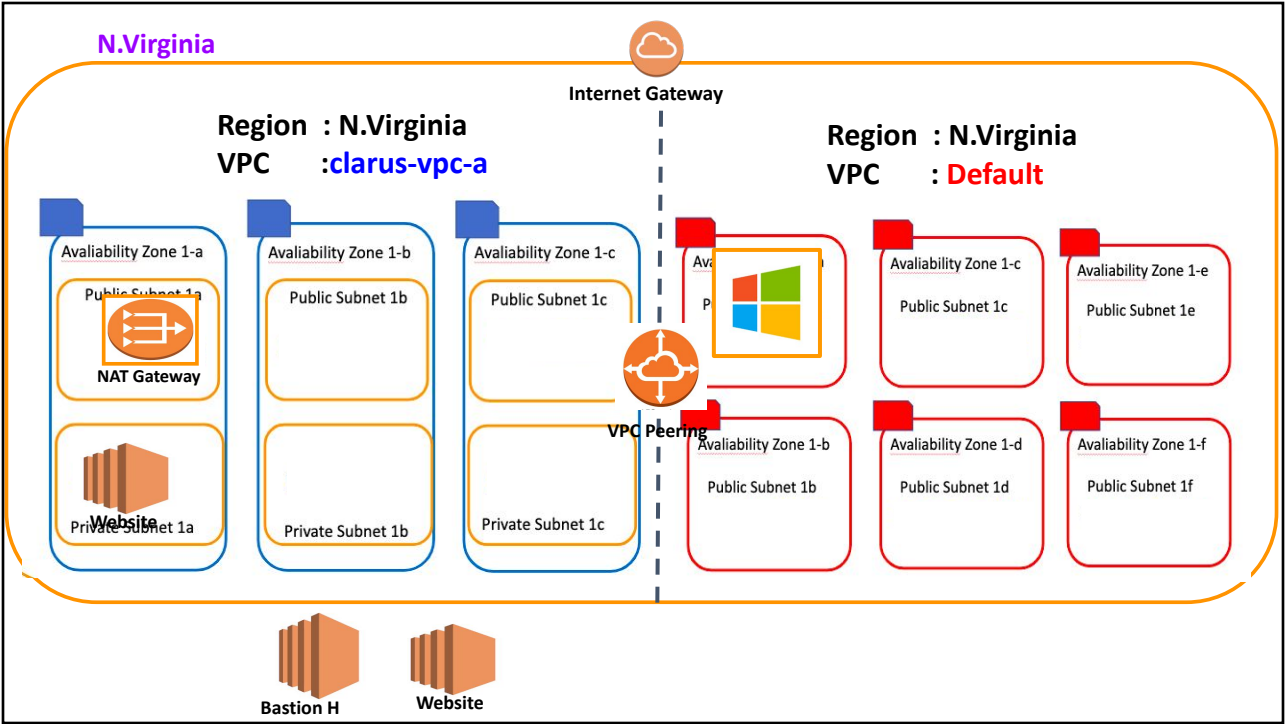
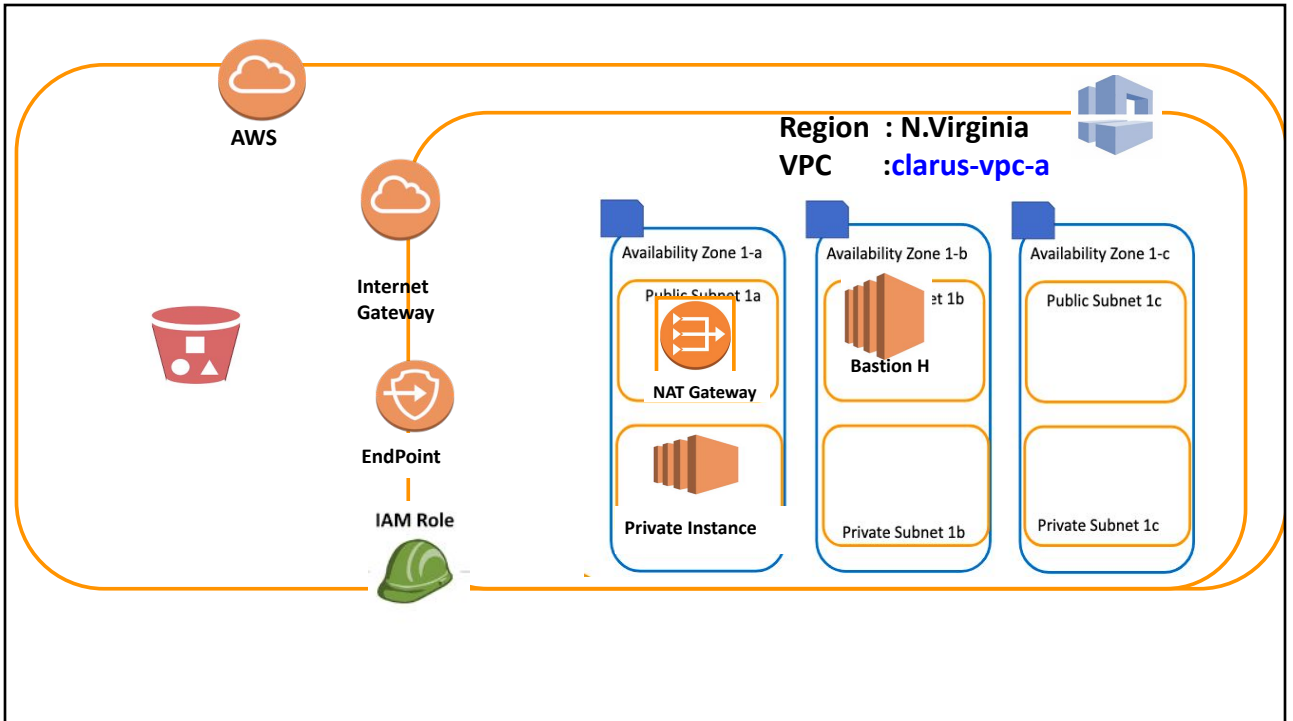
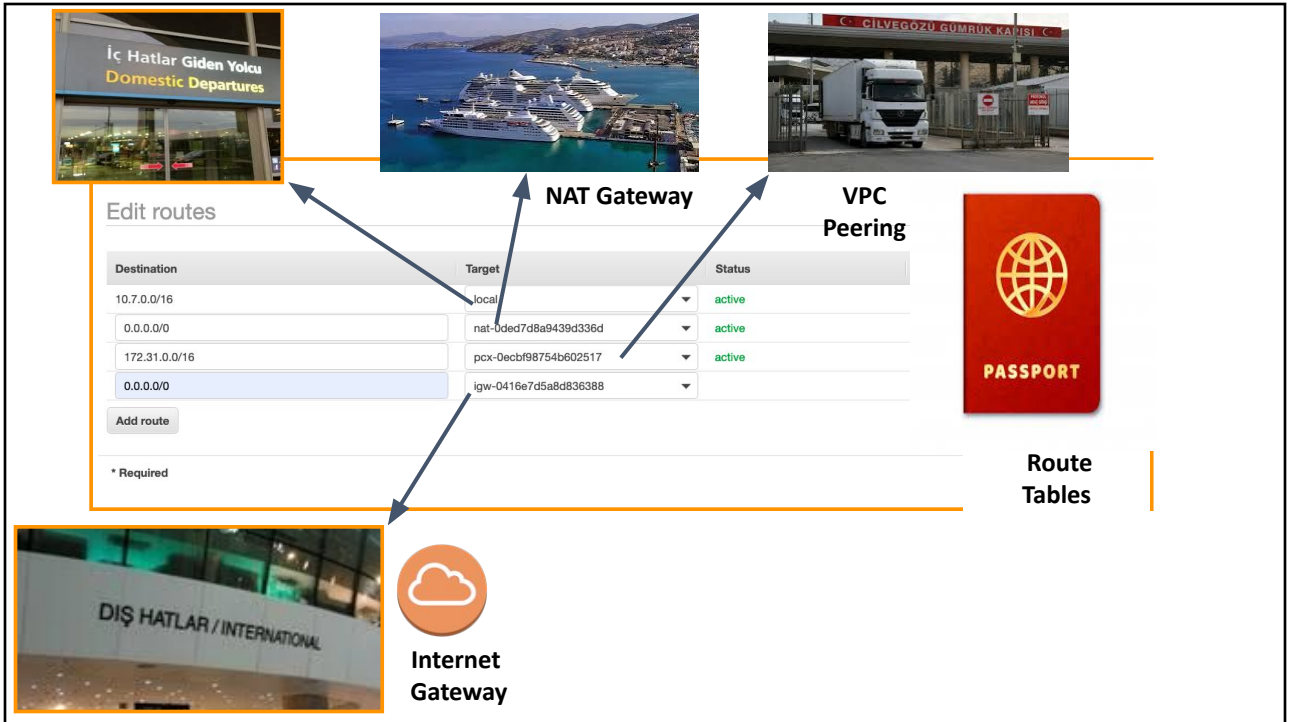
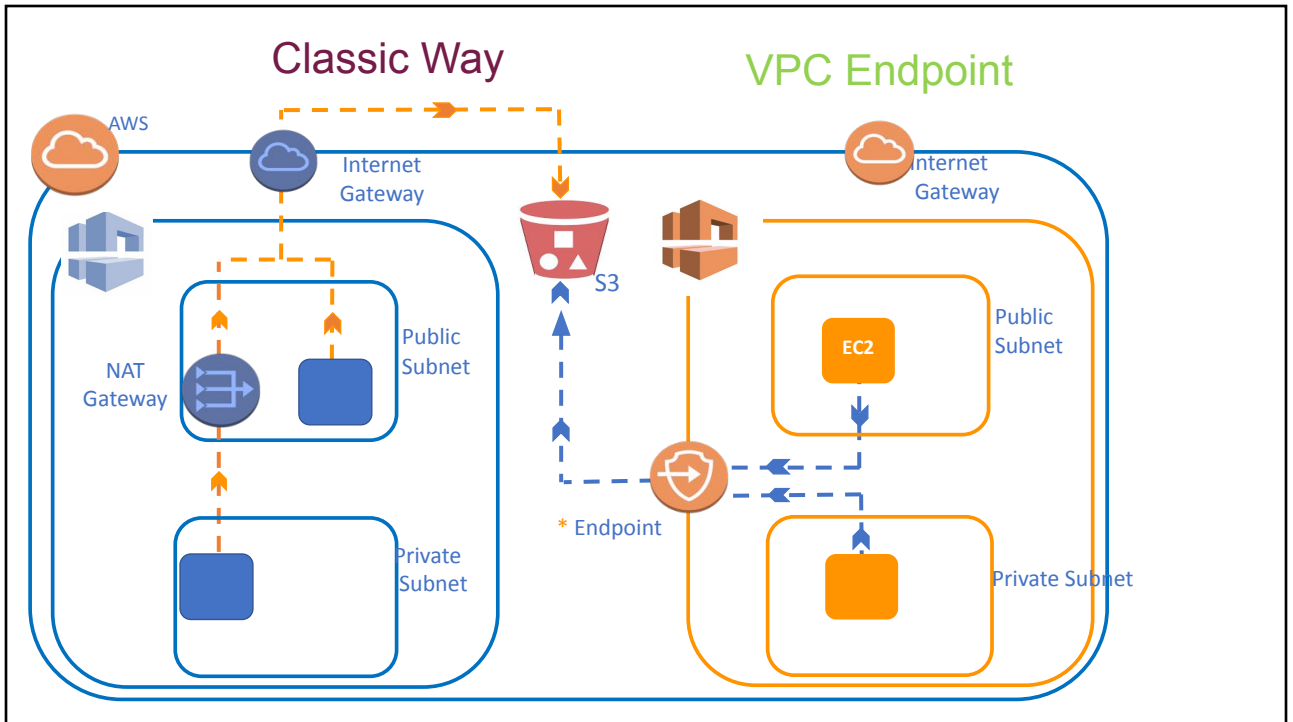


# AWS VPC (VPC ENDPOINT, VPC PEERING)







	Interface Endpoint	Gateway Endpoint
What	<u>Elastic Network Interface with a Private IP</u>	A gateway that is a target for a specific <u>route</u>
How	Uses DNS entries to redirect traffic	Uses prefix lists in the route table to redirect traffic
Which services	API Gateway, CloudFormation, CloudWatch etc.	<u>Amazon S3, DynamoDB</u>
Security	Security Groups	VPC Endpoint Policies

**VPC endpoint** enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS **PrivateLink** without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection

**PrivateLink** is a technology that enables you to **privately access services by using private IP addresses**.

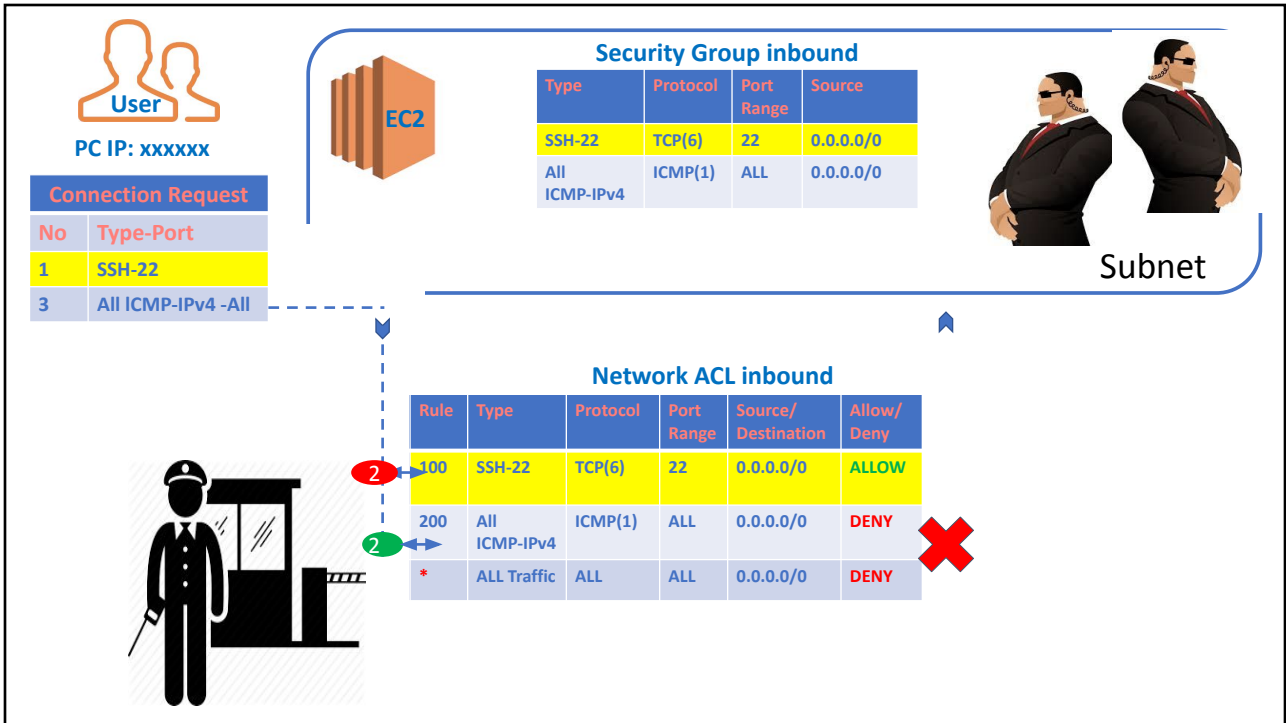
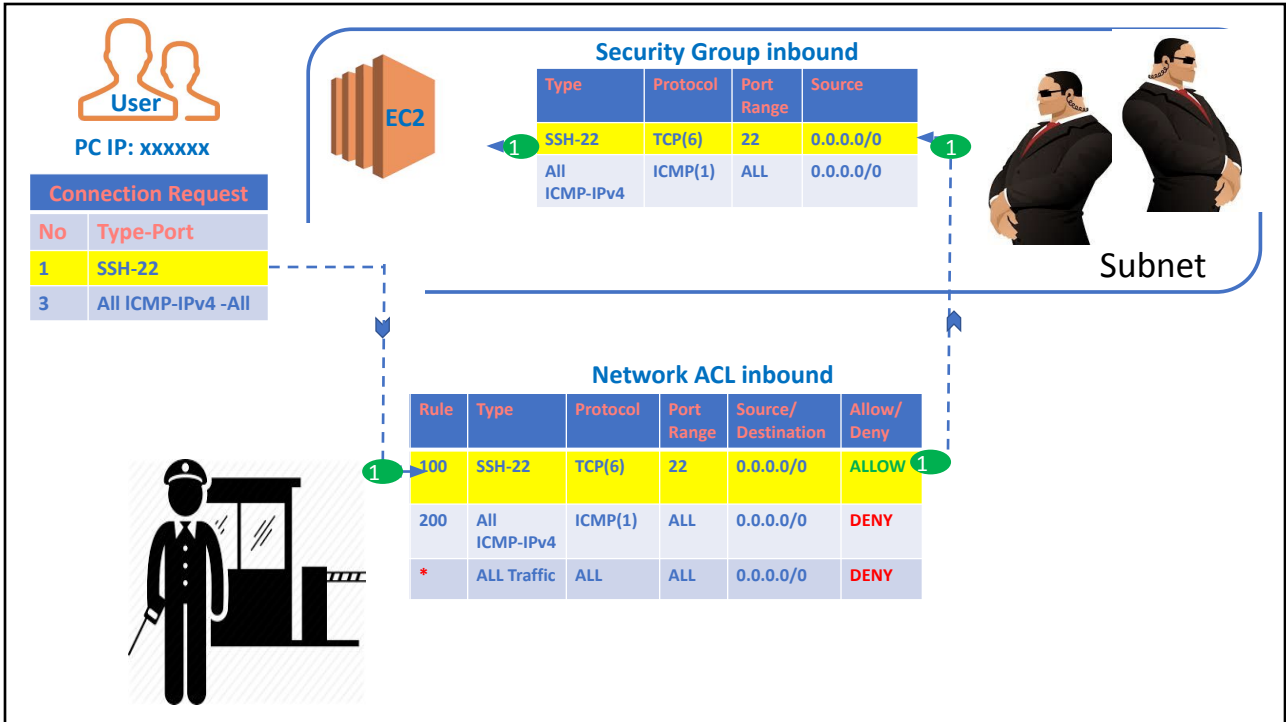
There are two different types of VPC endpoint:

An **interface endpoint** is an elastic network interface with a private IP address from the IP address range of your subnet. It serves as an entry point for traffic destined to a supported AWS service or a VPC endpoint service. Interface endpoints are powered by **AWS PrivateLink**

Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

With a **gateway endpoint** you configure your route table to point to the endpoint. Amazon S3 and DynamoDB use gateway endpoints.



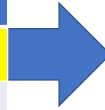


(Statefull) **Security Group inbound**

Type	Protocol	Port Range	Source	
SSH-22	TCP(6)	22	0.0.0.0/0	ALLOW Only
All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	

**Network ACL inbound** (Stateless)

Rule	Type	Protocol	Port Range	Source/Destination	Allow/Deny
100	SSH-22	TCP(6)	22	0.0.0.0/0	ALLOW
200	All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY



(Stateless) **Network ACL outbound**

Rule	Type	Protocol	Port Range	Destination	Allow/Deny
100	*Custom TCP	TCP(6)	*32768 - 65535	0.0.0.0/0	ALLOW
200	All ICMP-IPv4	ICMP(1)	ALL	0.0.0.0/0	*ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY