Cloud Networking

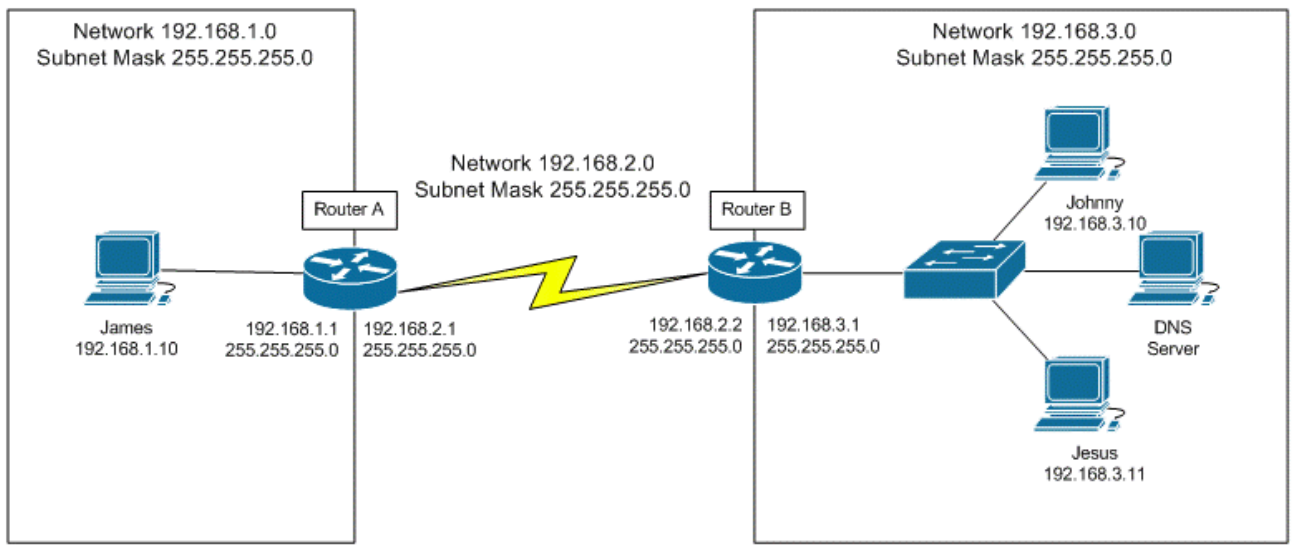
IT4090 – Cloud Computing

Lecture Outline

- Networking Recap
- Software Defined Networking
- Network Function Virtualization
- Virtual Networks and Subnets
- Access Controlling
- Network Gateway Services
- Network Peering
- Hybrid Connectivity
- Private Access to Cloud Services
- Flow Logs

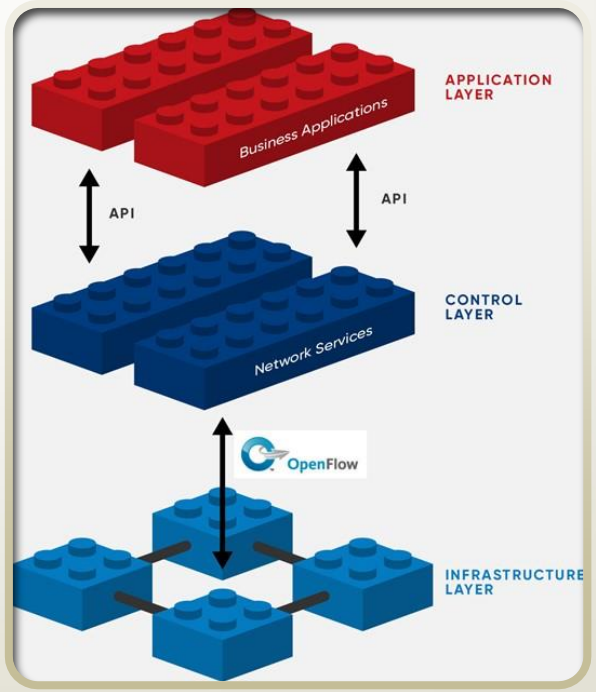
Networking Recap

- IP addresses
- Subnets / VLSM
- Basic Routing
- Default Gateways



Software Defined Networking (SDN)

- SDN is a network management architecture that enables, dynamic, programmable network configuration in order to improve network performance and monitoring.
- This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services



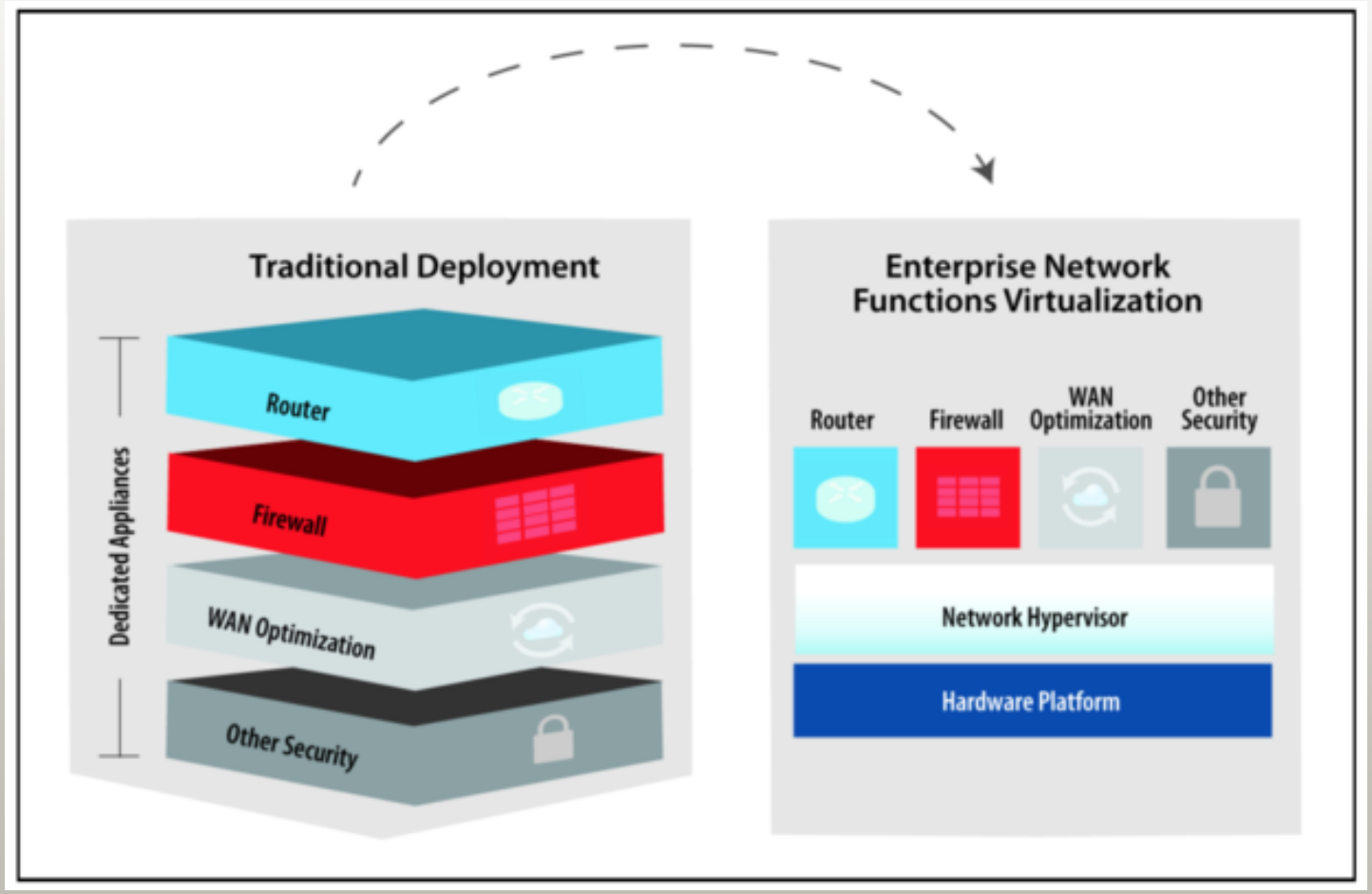
Network Function Virtualization (NFV)

NFV is a network architecture which decouples Physical Network Functions (PNF) from proprietary hardware appliances and run them as software in virtual machines (virtual network functions).

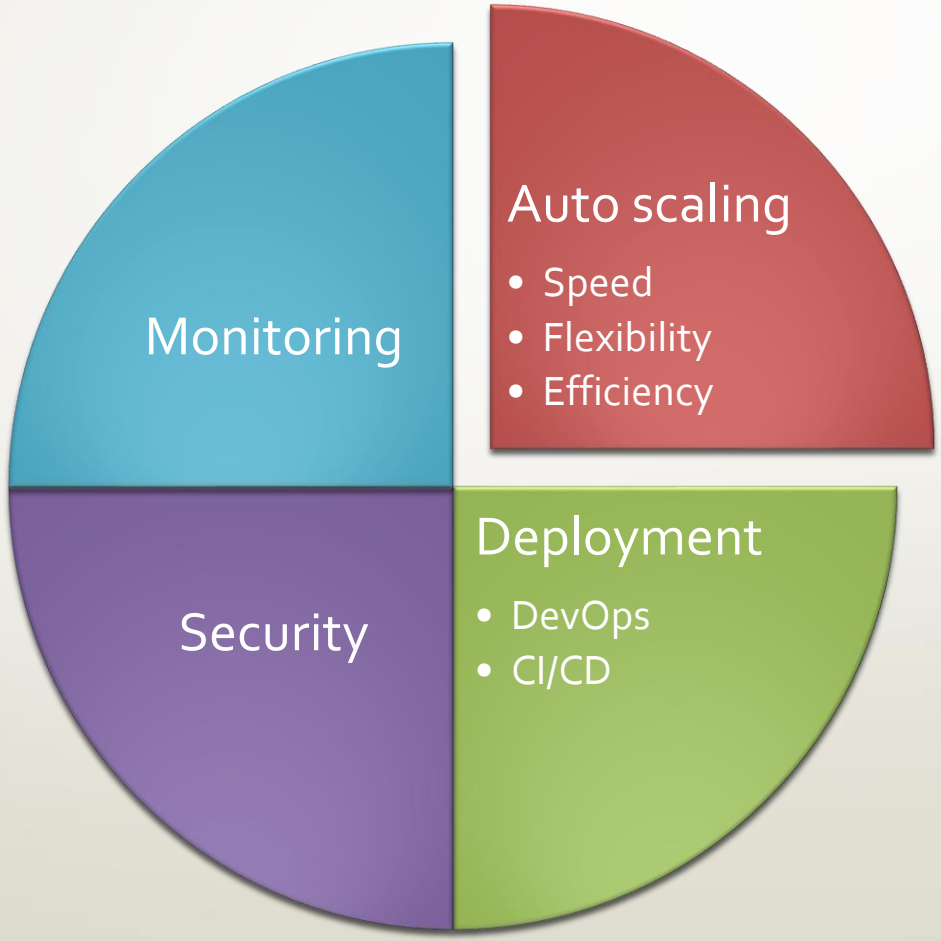
These Virtual Network Functions (VNFs) include network functions such as firewalls, traffic control, virtual routing etc.

Cloud-native Network Functions (CNF) is the successor of VNFs, which is a software implementation of a PNF which runs inside a Linux container.

Network Function Virtualization (NFV)



Advantages of CNF



SDN vs. NFV

Similarities

- Both use network abstraction
- Both depend heavily on virtualization

Differences

- SDN separates Network Control Functions from Forwarding Functions, while NFV abstracts all Network Functions from underlying hardware.
- SDN defines the big picture aspect of the infrastructure, while NFV deliver a wide range of specific functionalities.

Virtual Networks

Cloud networking service which provides networking functions to cloud resources.

Logically isolated from other virtual networks.

Has one or more IP ranges.

Has one or more subnets.

Can peer with other virtual networks if IP ranges do not overlap.

Implementations

- AWS VPC (Virtual Private Cloud)
- Azure Virtual Network

Subnets

Segments virtual network IP range even further

Subnet CIDR blocks cannot overlap within a virtual network

Traffic can be restricted using Access Control Lists

AWS offers private and public subnets

- Instances in public subnets can send outbound traffic directly to internet.
- Instances in private subnets cannot send outbound traffic directly to internet.

Azure does not have the public/private subnet concept.

- All subnets can be considered as public subnets
- Can implement private subnet functionality through route tables

Virtual Networks & Subnet Sizing

Allowed IP ranges – RFC 1918 Private IP Ranges

- 10.0.0.0/8 – (10.0.0.0 – 10.255.255.255)
- 172.16.0.0/12 – (172.16.0.0 – 172.31.255.255)
- 192.168.0.0/16 – (192.168.0.0 – 192.168.255.255)

IPv4 Allowed Block Sizes

- Azure – between /2 netmask to /29 netmask
- AWS – between /16 netmask to /28 netmask

Five IPs from each subnet IP block is reserved

- 1st IP – Network Address
- 2nd IP – Reserved for the Router
- 3rd IP – Reserved for DNS
- 4th IP – Reserved for DNS/future use
- Last IP – Network Broadcast Address

Subnet IP Reservation

10.0.0.0/24	1st IP	10.0.0.0 – Network Address
	2nd IP	10.0.0.1 – Reserved
	3rd IP	10.0.0.2 – Reserved
	4th IP	10.0.0.3 – Reserved
	Last IP	10.0.0.255 – Broadcast Address
	First usable IP	10.0.0.4
	Last usable IP	10.0.0.254
	Number of usable IPs	$2^8 - 5 = 251$

Subnet IP Reservation

172.16.10.128/25	1st IP	172.16.10.128 – Network Address
	2nd IP	172.16.10.129 – Reserved
	3rd IP	172.16.10.130 – Reserved
	4th IP	172.16.10.131 – Reserved
	Last IP	172.16.10.255 – Broadcast Address
	First usable IP	172.16.10.132
	Last usable IP	172.16.10.254
	Number of usable Ips	$2^7 - 5 = 123$

Subnet IP Reservation

192.168.0.64/27	1st IP	192.168.0.64 – Network Address
	2nd IP	192.168.0.65 – Reserved
	3rd IP	192.168.0.66 – Reserved
	4th IP	192.168.0.67 – Reserved
	Last IP	192.168.0.95 – Broadcast Address
	First usable IP	192.168.0.68
	Last usable IP	192.168.0.94
	Number of usable Ips	$2^5 - 5 = 27$

Virtual Network Interfaces

A logical networking component which represents the network interface card (NIC).

Enables a compute instance to communicate with other compute instances and/or internet.

Attaches to a compute instance.

Can attach more than one virtual network interfaces to the same compute instance.

Can have one public IP and one or more private Ips

Implementations

- AWS – Elastic Network Interface (ENI)
- Azure – Network Interface Card (NIC)

Access Controlling

Implements a simple firewall functionality to control inbound and outbound traffic to a subnet / virtual network interface.

Need to add ACL rules which contains

- Rule number
- Protocol
- Source / Destination Port Ranges
- Source / Destination IP Ranges
- Allow / Deny Action

Usage varies in CSPs

- AWS Security Groups – Assigned to an EC2 instance
- AWS Network Access Control List (NACL) – Assigned to a subnet
- Azure Network Security Groups (NSG) – Can be assigned to both subnets and NICs

Stateful / Stateless Rules

Stateful Rules

- Only need to specify the security rule for the request, no need to specify a security rule for the response.

Stateless Rules

- Need to specify security rules for the request as well as the response.

Implementations

- AWS SG – Stateful
- AWS NACL – Stateless
- Azure NSG - Stateful

Network Gateway Services

Virtual Network Functions associated with providing connectivity between cloud resources and outside networks / internet.

- Internet Gateway
- NAT Gateway
- VPN Gateway
- Network Transit Gateway

Internet Gateway

Provides connectivity between internet and virtual network

Scales horizontally

No bandwidth constraints

Implementations

- AWS Internet Gateway

Azure does not have the internet gateway concept

- Internet connectivity is provided by default through the default gateway

NAT Gateway

Provides Network Address Translation (NAT) to compute instances in private subnets

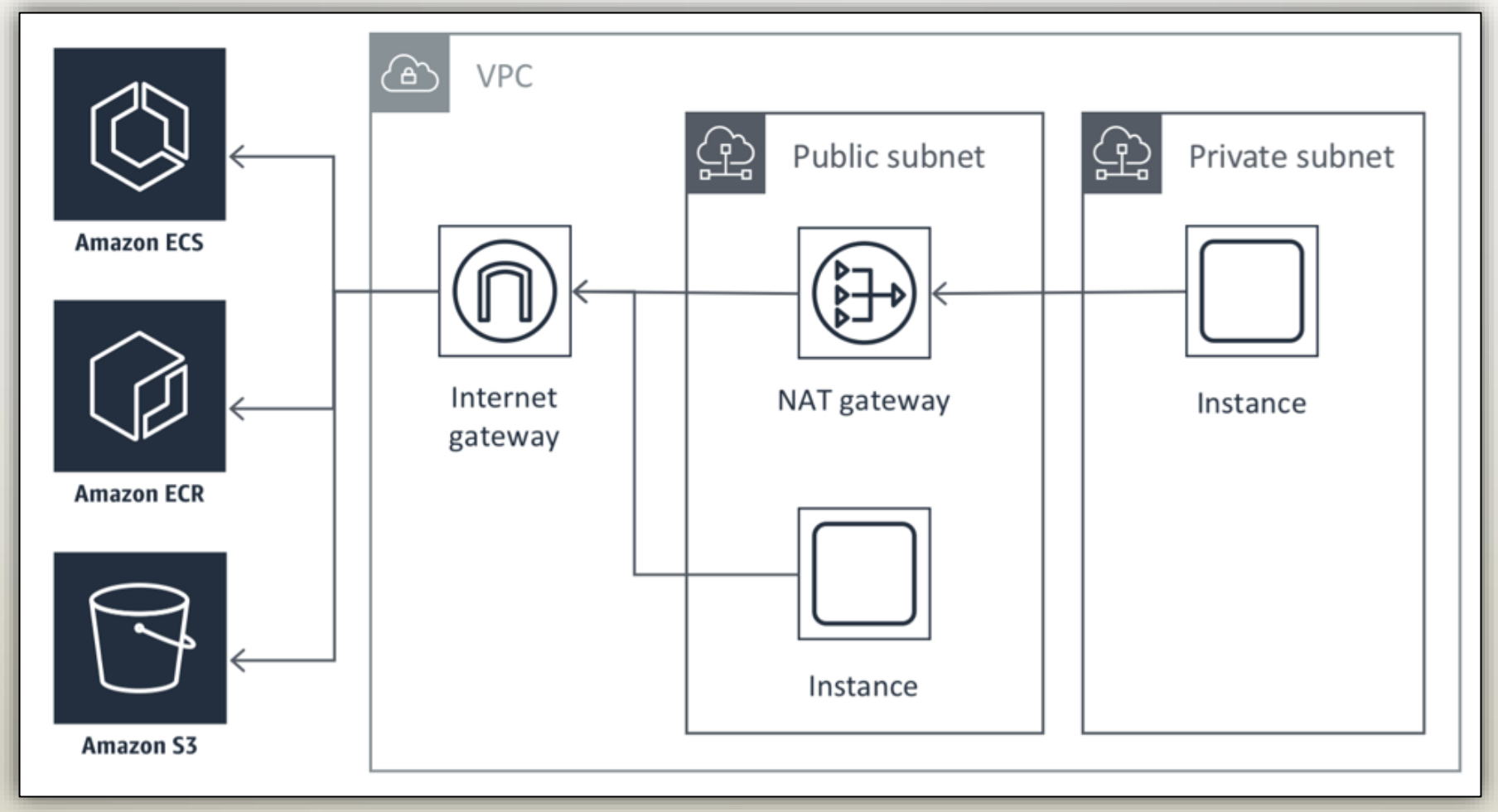
Prevents connections to subnets getting initiated from the internet.

NAT Gateway should be deployed in a public subnet.

Implementations

- AWS NAT Instance
- AWS NAT Gateway
- Azure Virtual Network NAT

AWS Internet Gateway & NAT Gateway



VPN Gateway

VPN Gateways are used to create encrypted tunnels over the public internet to send encrypted traffic between virtual networks and on-premises networks.

Implementations

- Azure VPN Gateway
- AWS Virtual Private Gateway

VPN Services

Two types of VPN services are provided by CSPs

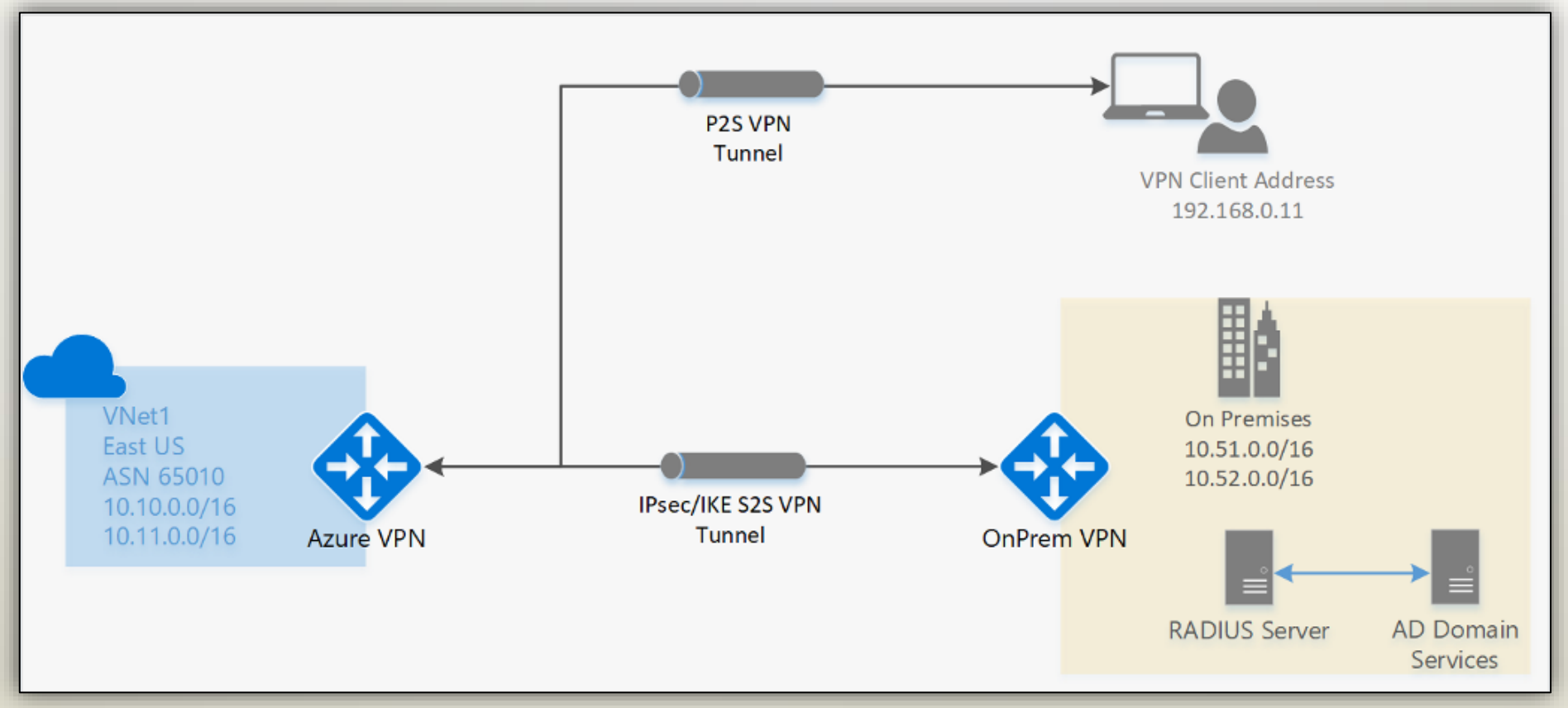
- Site-to-site VPN – VPN connectivity between virtual network and on-premises network, or between two virtual networks
- Point-to-site VPN – VPN connectivity between virtual network and a client PC with a special client VPN software

Azure VPN Gateway provides both site-to-site and point-to-site VPN connectivity

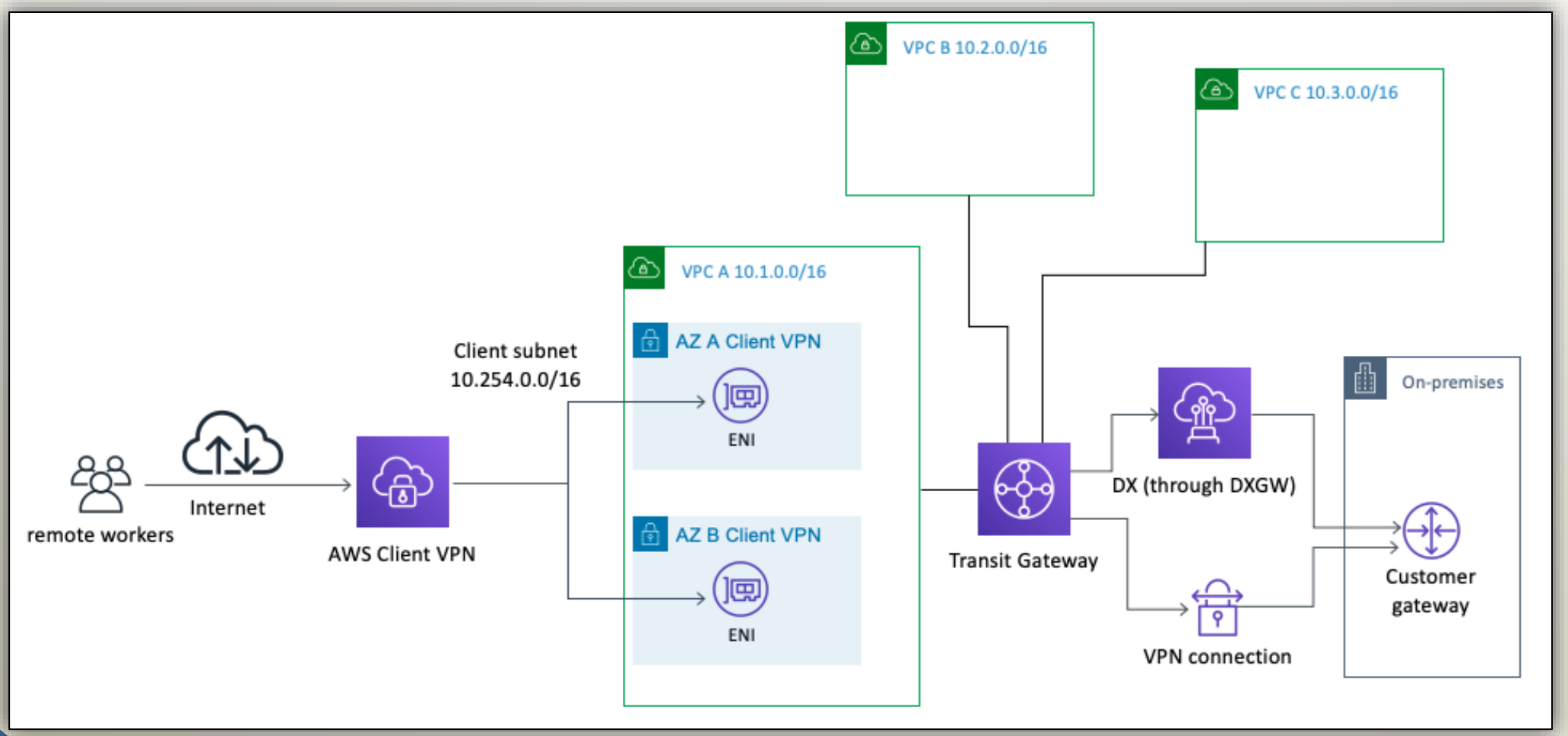
AWS Virtual Private Gateway provides only site-to-site connectivity.

AWS provides point-to-site connectivity through a separate service called AWS Client VPN

Azure VPN Services



AWS VPN Services



Network Transit Gateway

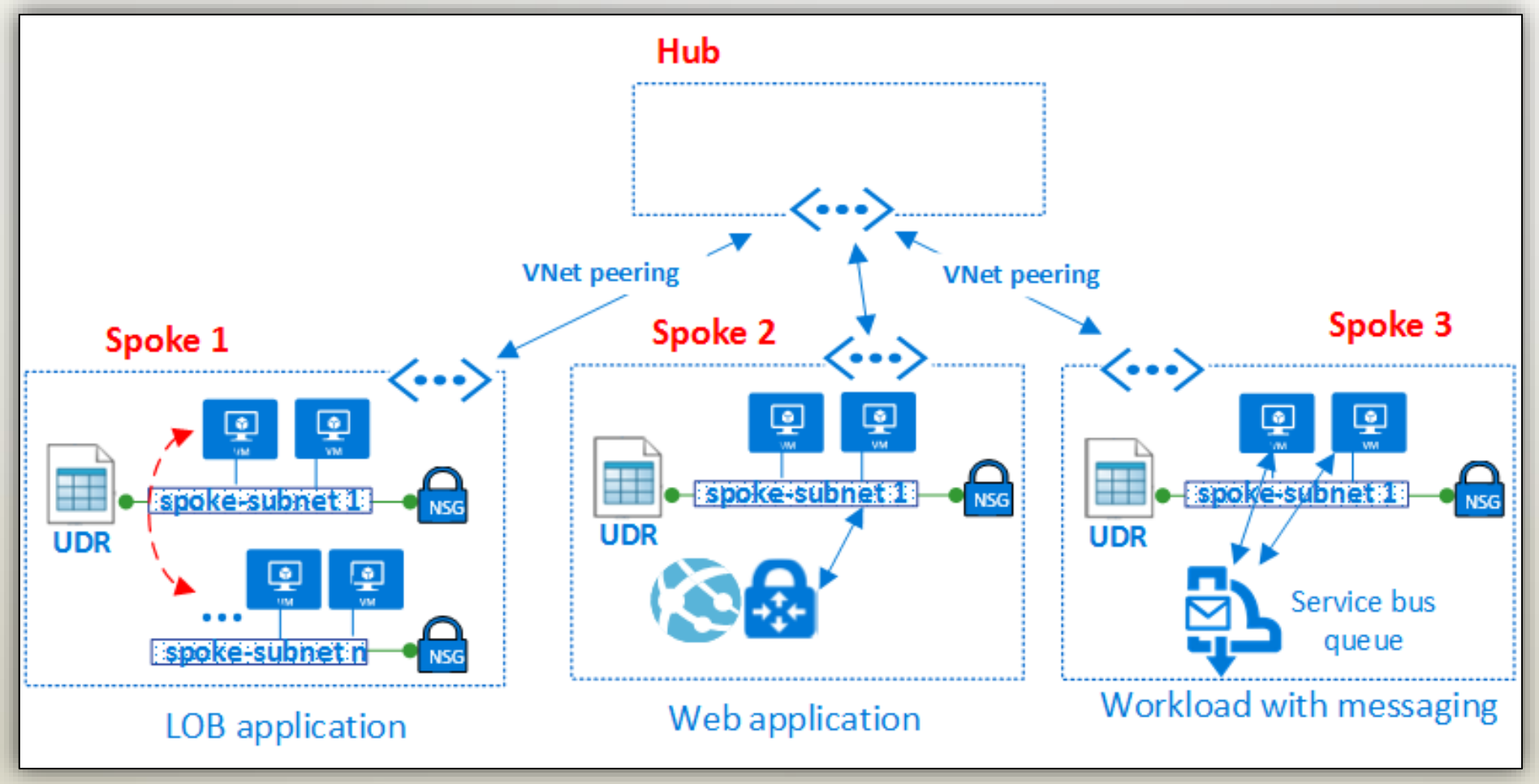
A service which connects multiple virtual networks and on-premises networks through a central hub.

This architecture used to be implemented through the hub-spoke model.

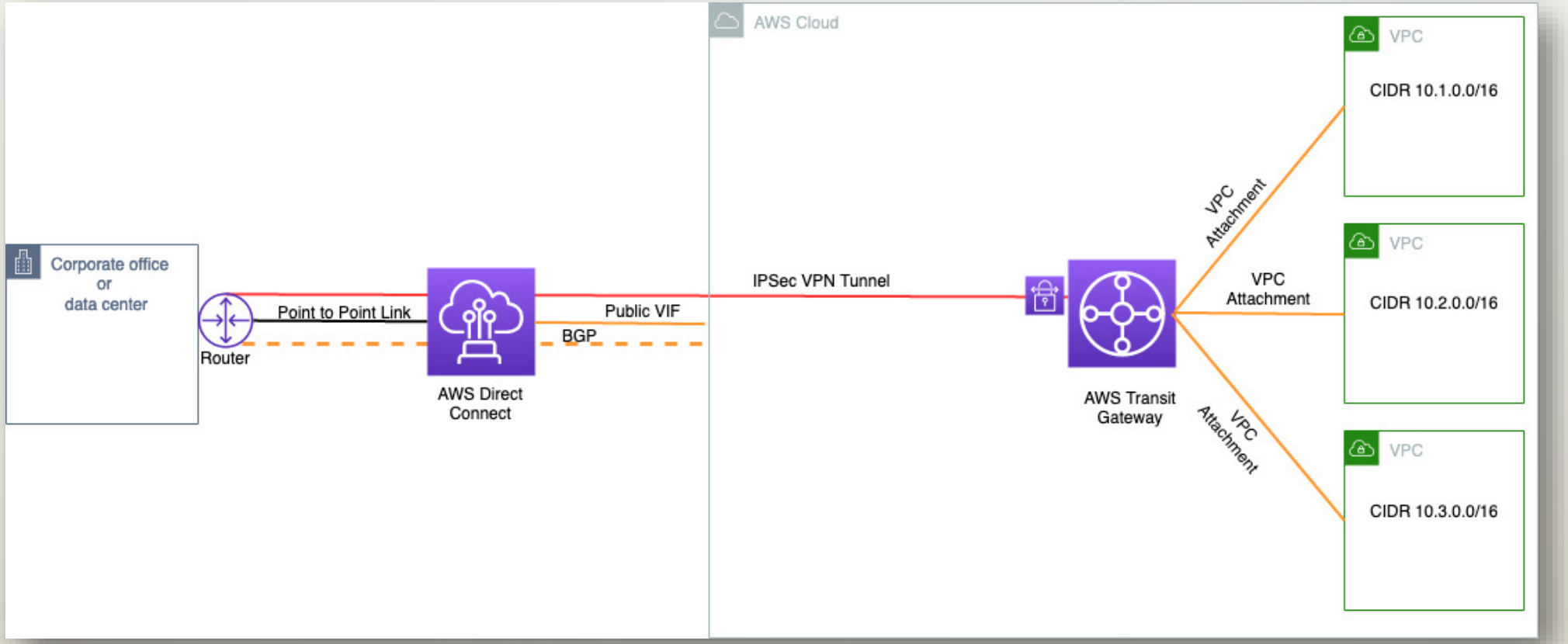
Implementations

- AWS Transit Gateway
- Azure Virtual WAN

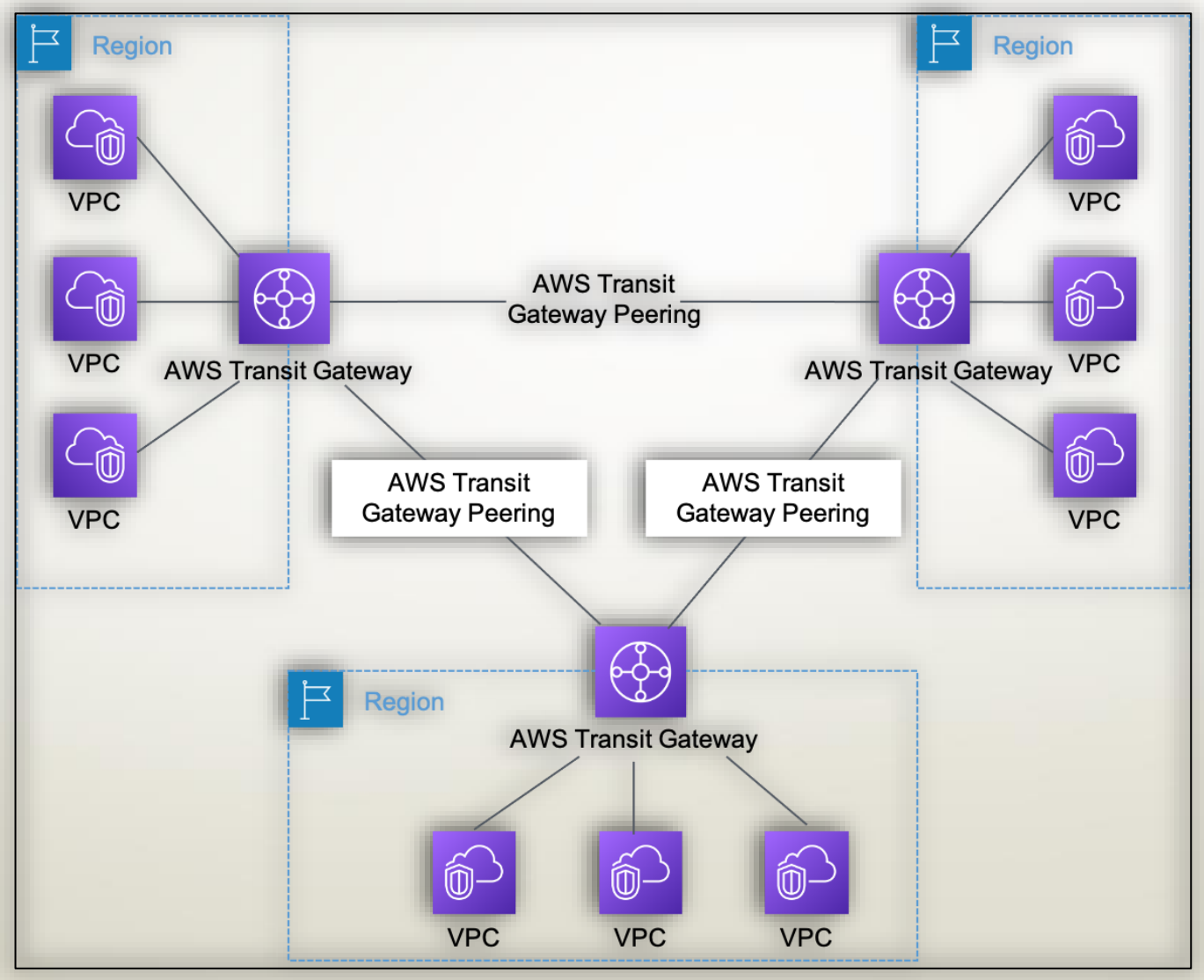
Hub and Spoke Architecture



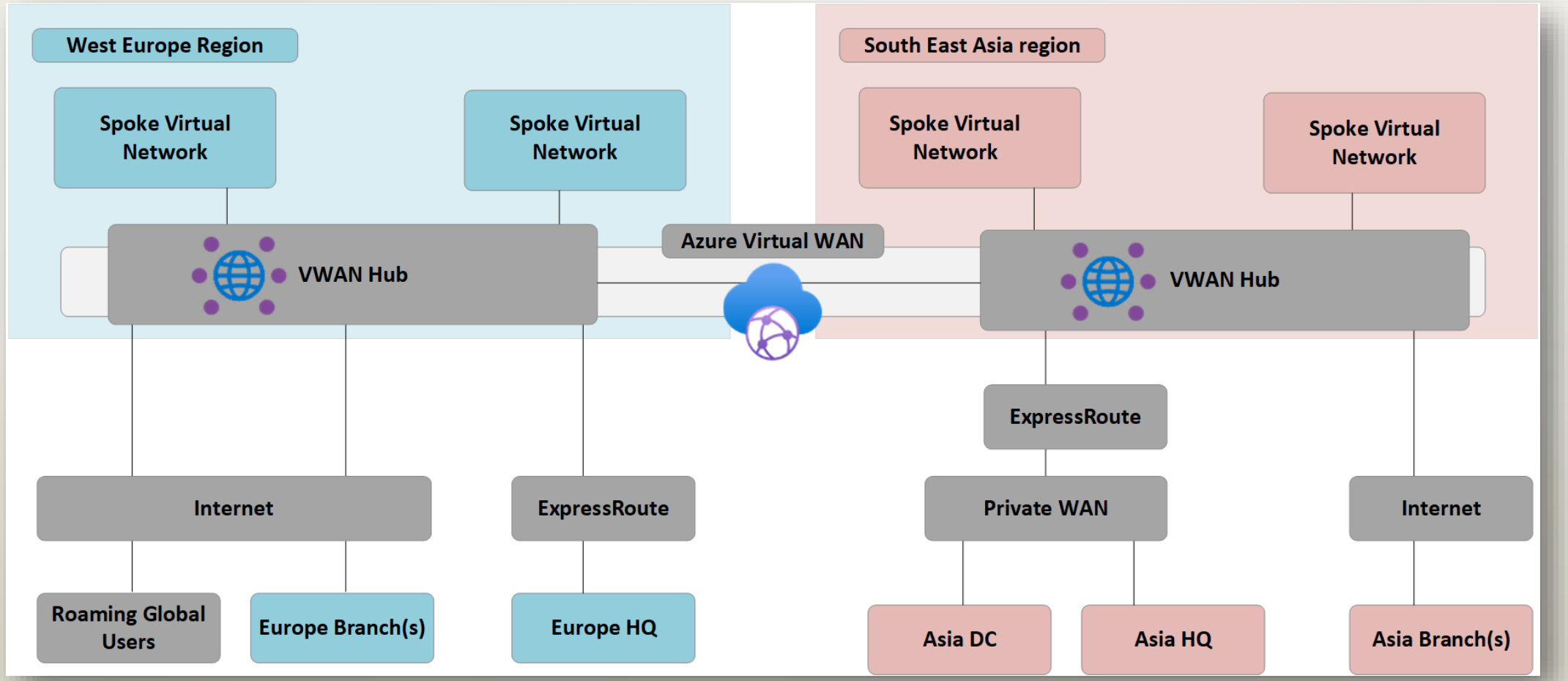
AWS Transit Gateway



AWS Transit Gateway



Azure Virtual WAN



Network Peering

Allows to connect and communicate between two virtual networks.

Used to be implemented through VPN Gateways.

Each virtual network can be peered to more than one virtual networks.

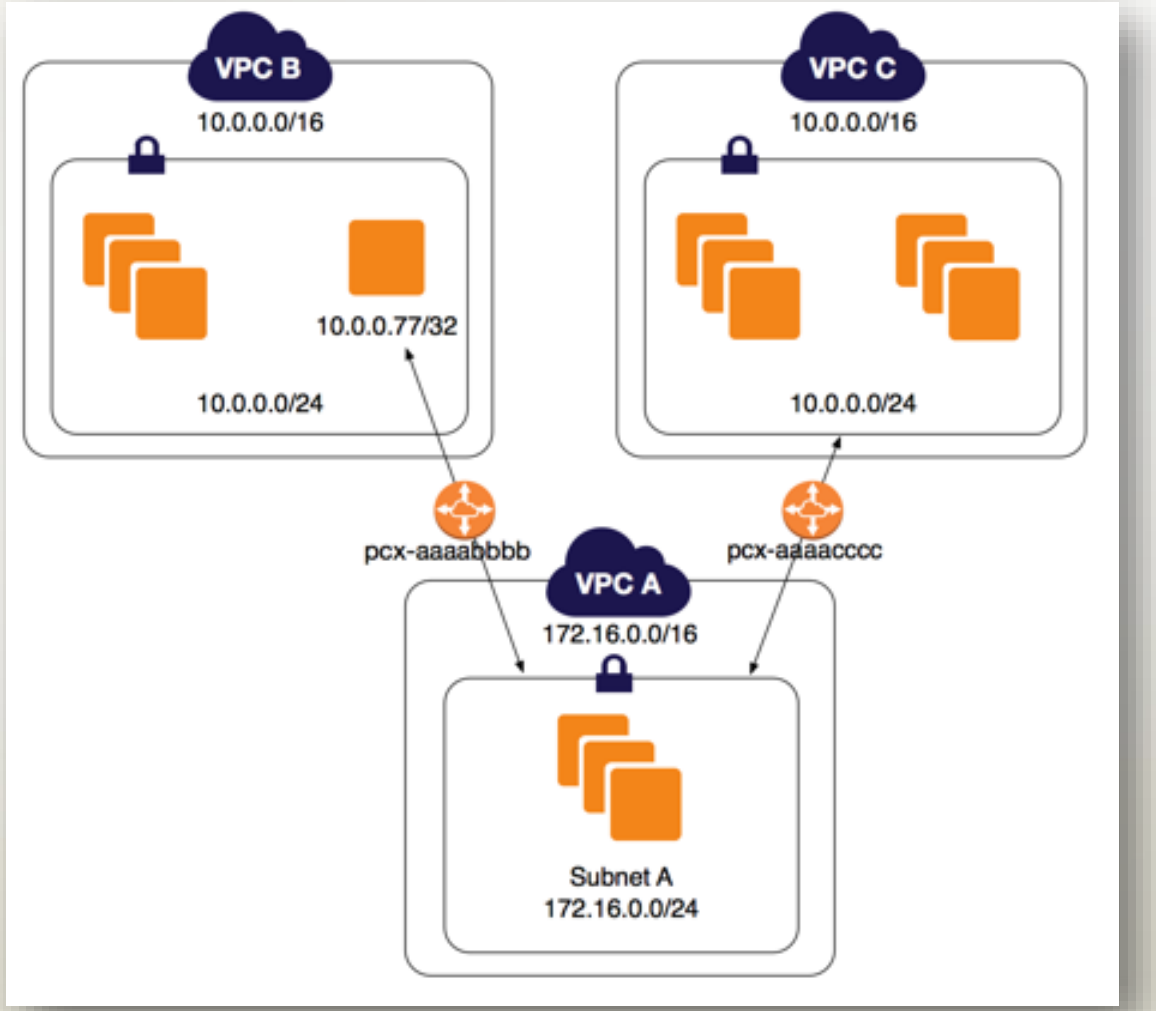
Can peer virtual networks across accounts / subscriptions.

Does not support transitive peering.

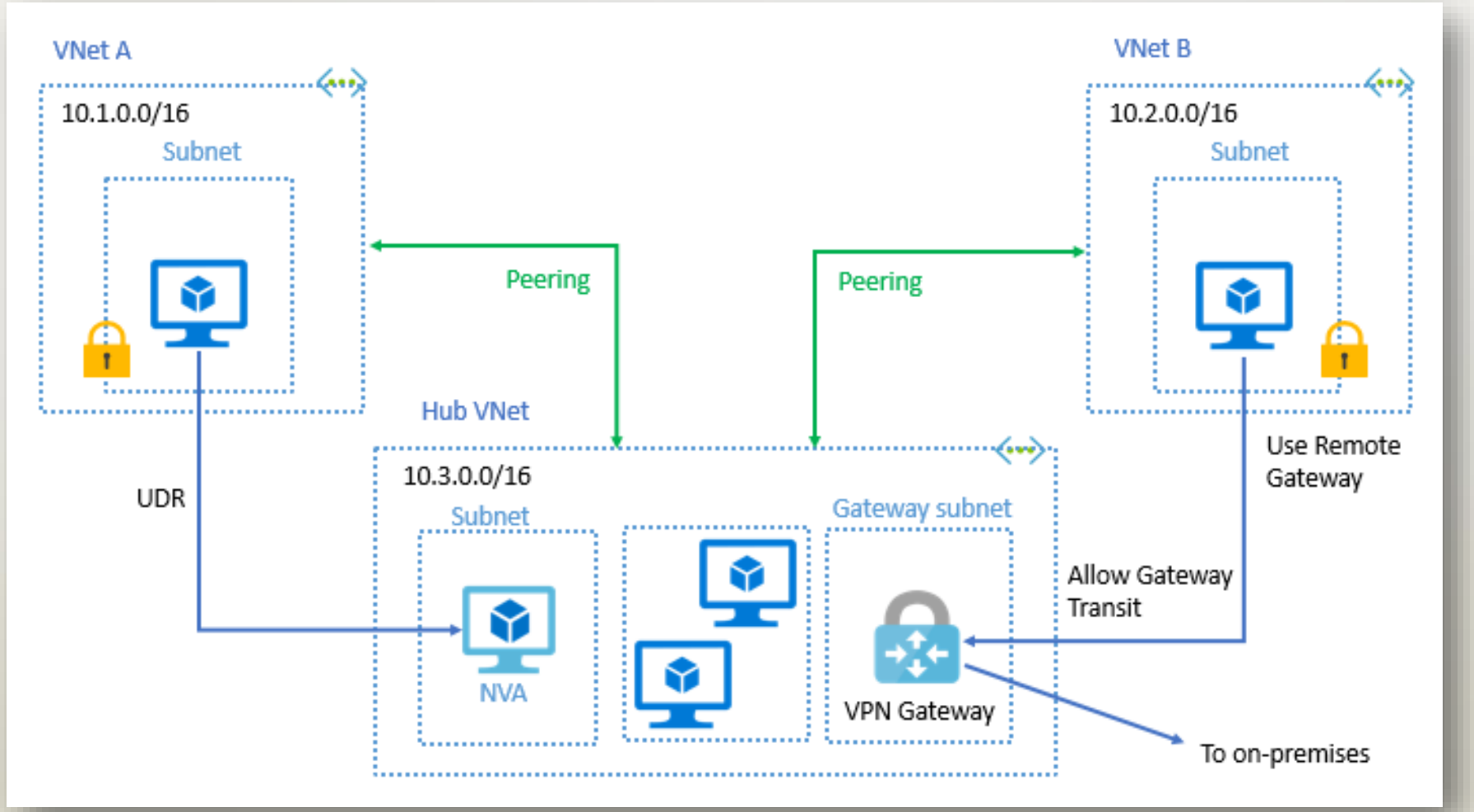
- If VNet A is peered with VNet B and VNet B is peered with VNet C, VNet A cannot communicate with VNet C and vice-versa

Both AWS and Azure have implemented this feature

AWS VPC Peering



Azure VNet Peering



Bastion Hosts

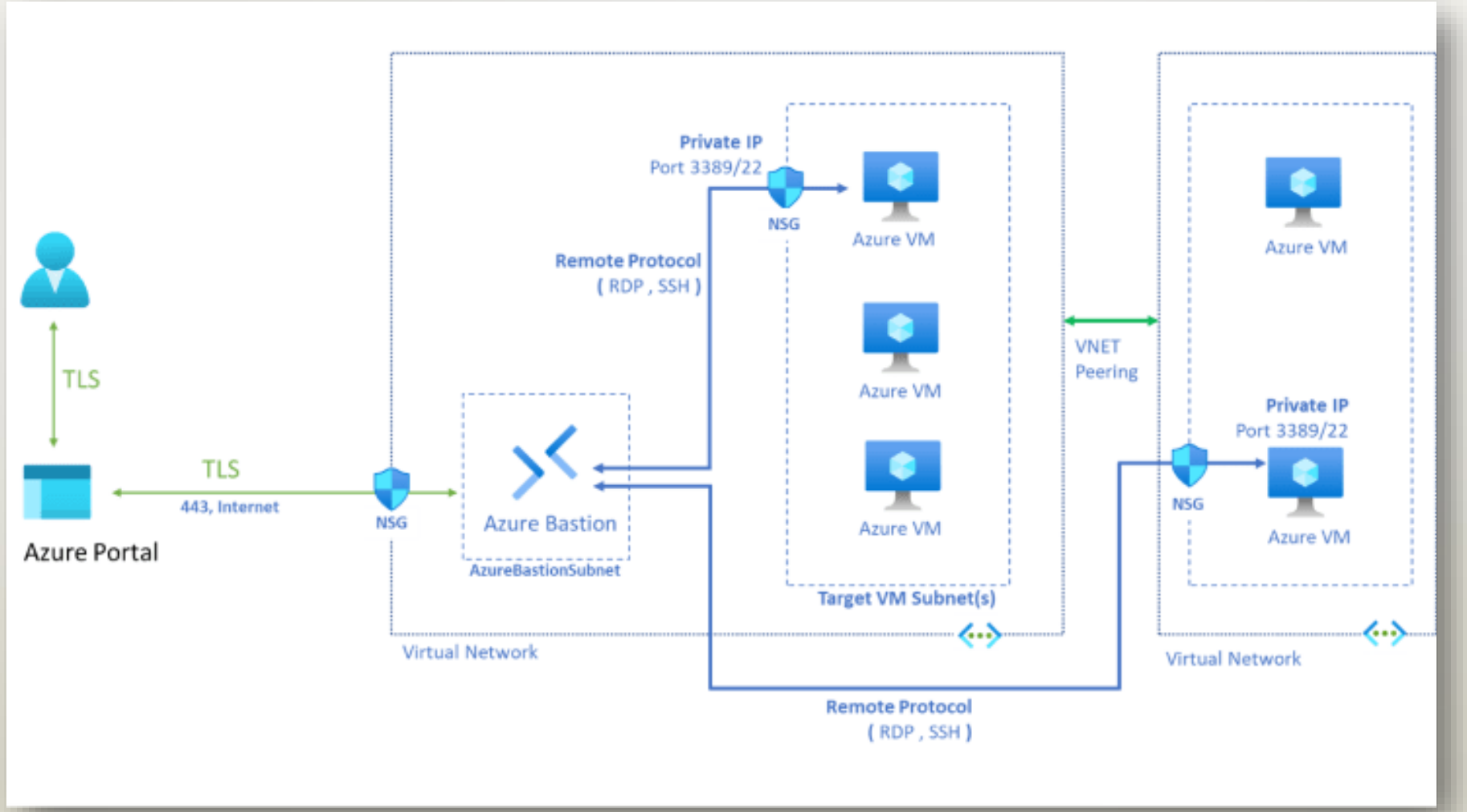
Also called as a Jump Host

A special compute instance deployed to provide secure management access to other compute instances in private subnets.

Can connect to private instances without exposing them to internet.

The bastion host must be placed in a public subnet and provided with a public IP.

Azure Bastion Host



Hybrid Connectivity

There are few ways we can use to get connected to a virtual network in CSP

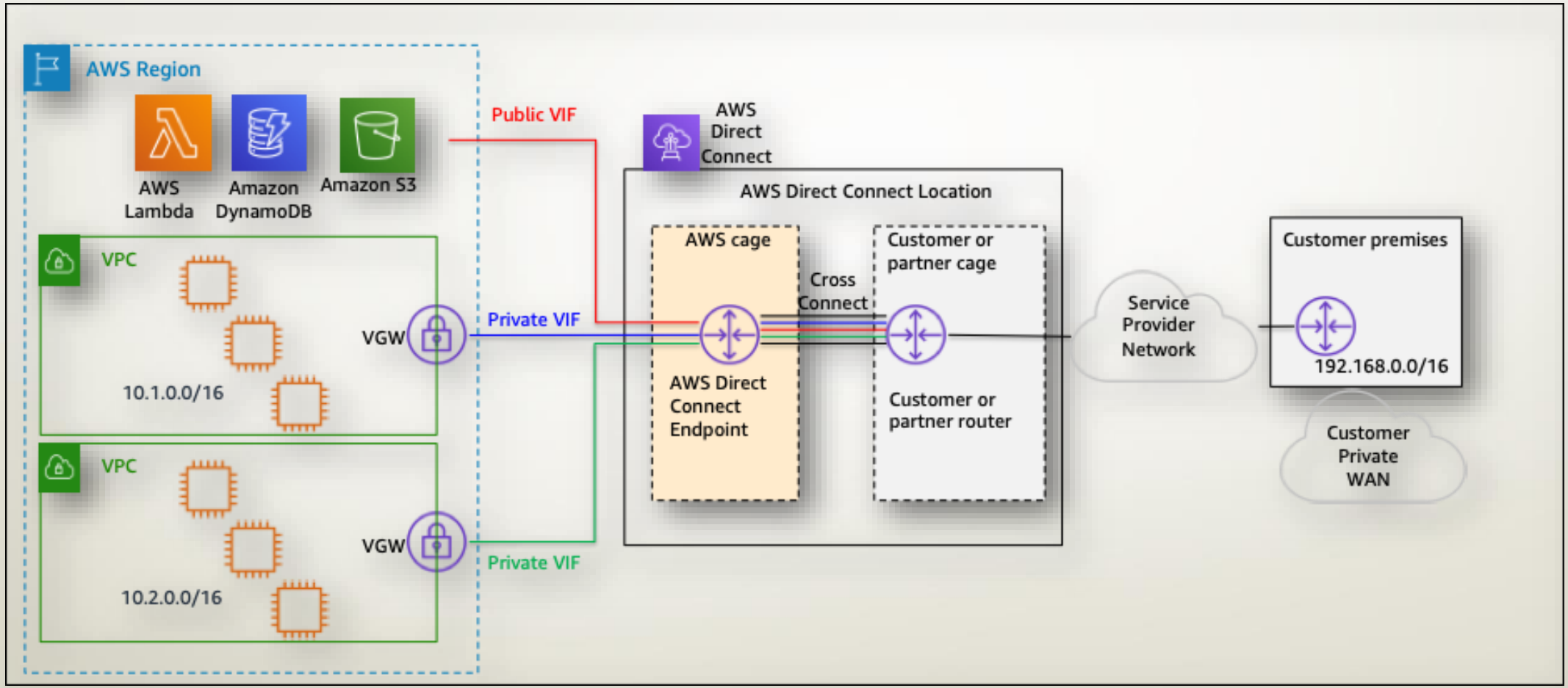
Connect Remote Users

- Direct internet connectivity
- Through VPN
  - Azure Point-to-Site VPN
  - AWS Client VPN

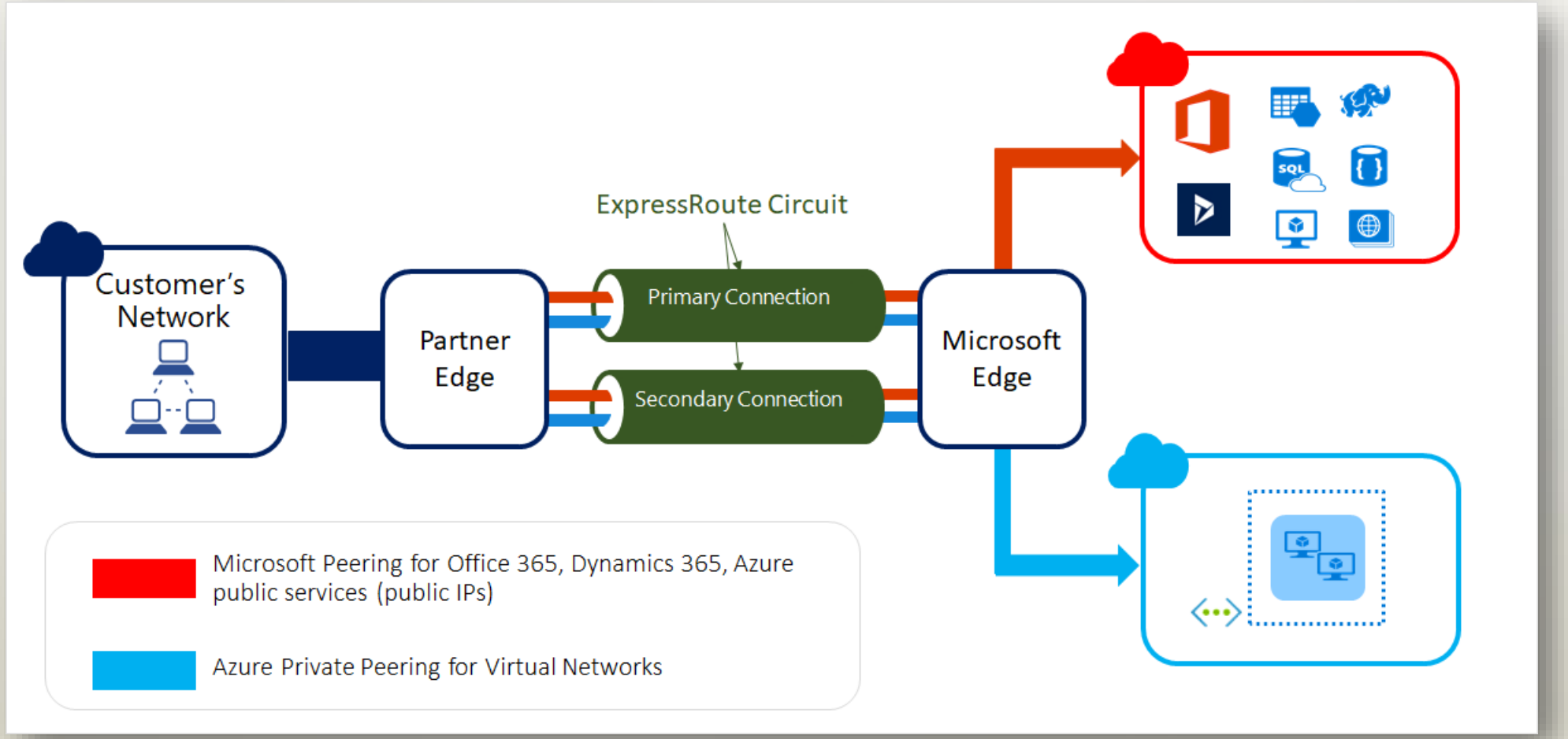
Connect Remote Networks

- Site-to-Site VPN
- Direct Connectivity
  - Azure Express Route
  - AWS Direct Connect

AWS Direct Connect



Azure Express Route



Private Access to Cloud Services

Private Links

- Provide access to PaaS services of the CSP from the virtual network without going through the public internet.

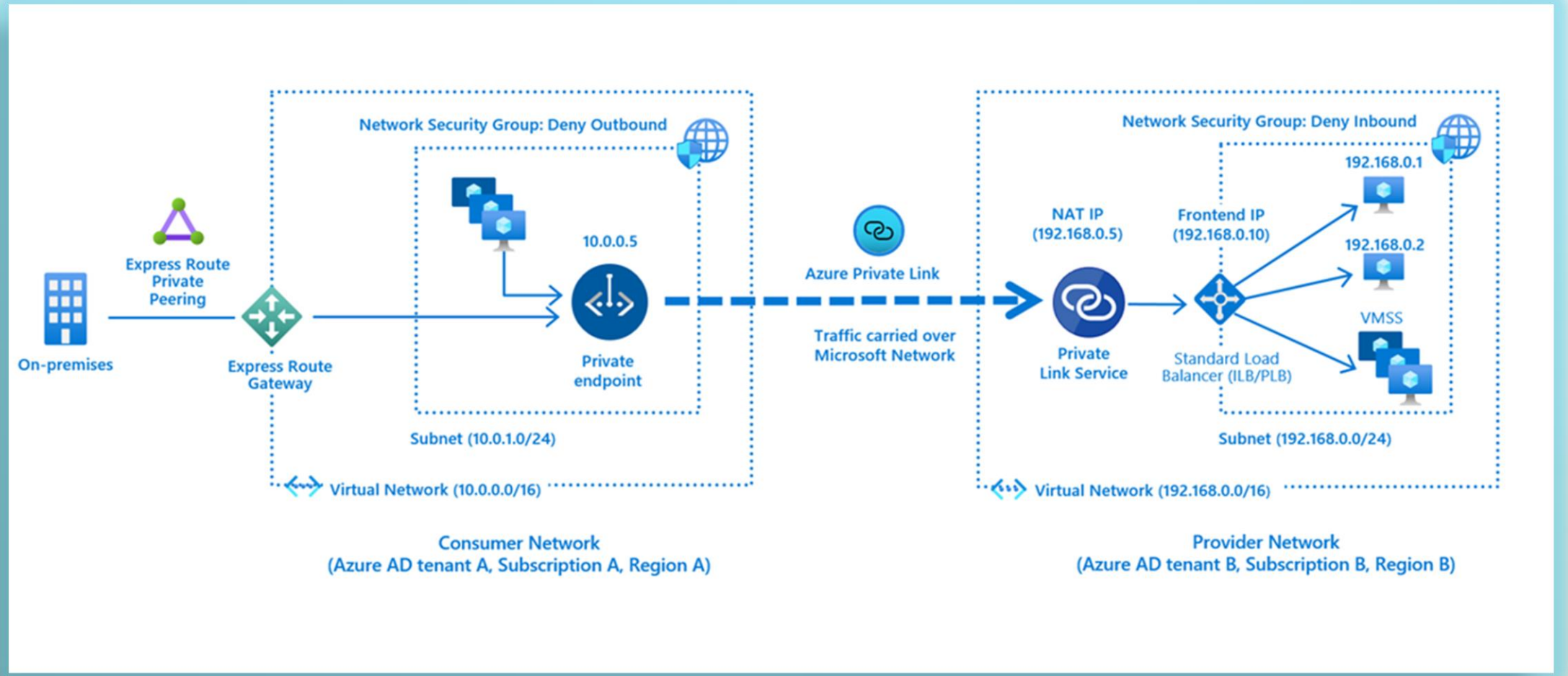
Private Endpoints

- Can be connected to a virtual network with an IP
- Provides access between other resources in the virtual network and PaaS services through Private Links.

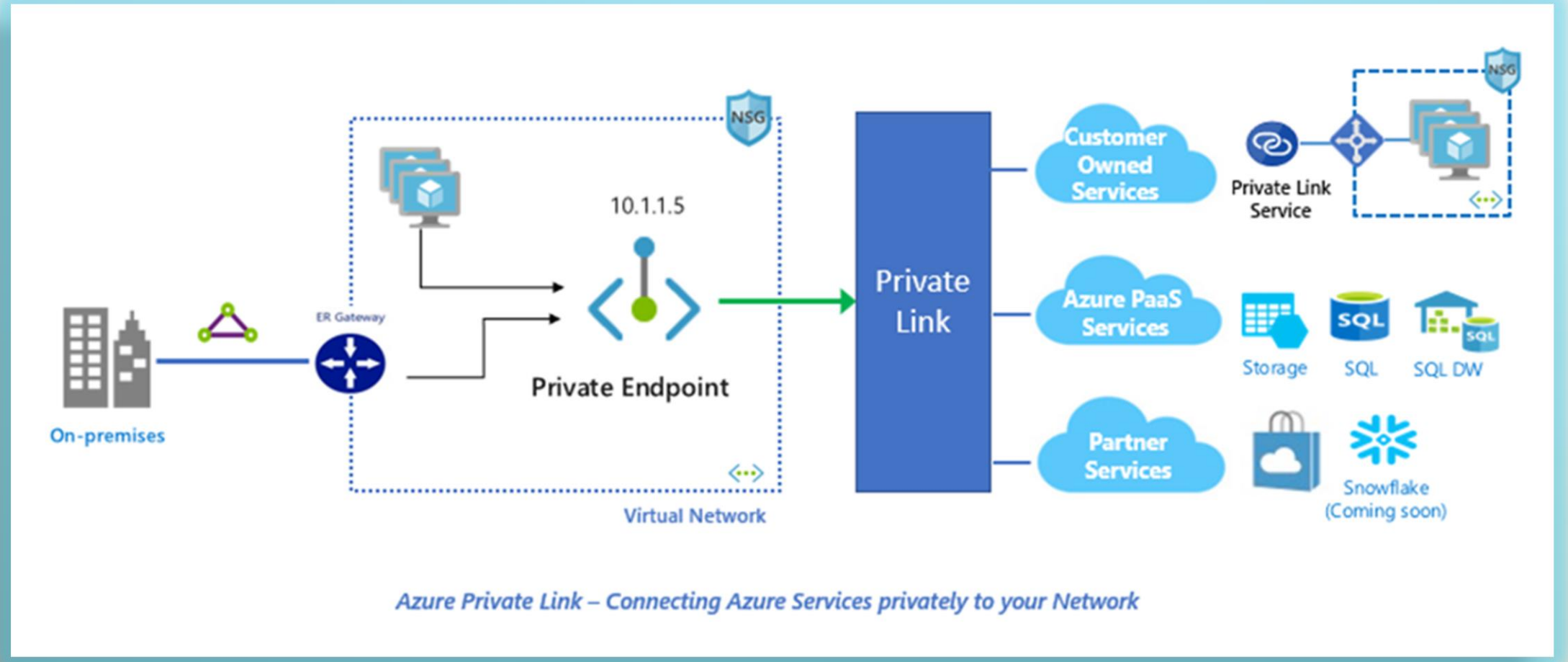
Azure Service Endpoints

- Provide secure and direct connectivity to Azure PaaS services over an optimized route over the Azure backbone network.
- Traffic from the virtual network will still hit the public endpoint of the PaaS service.

Azure Private Link

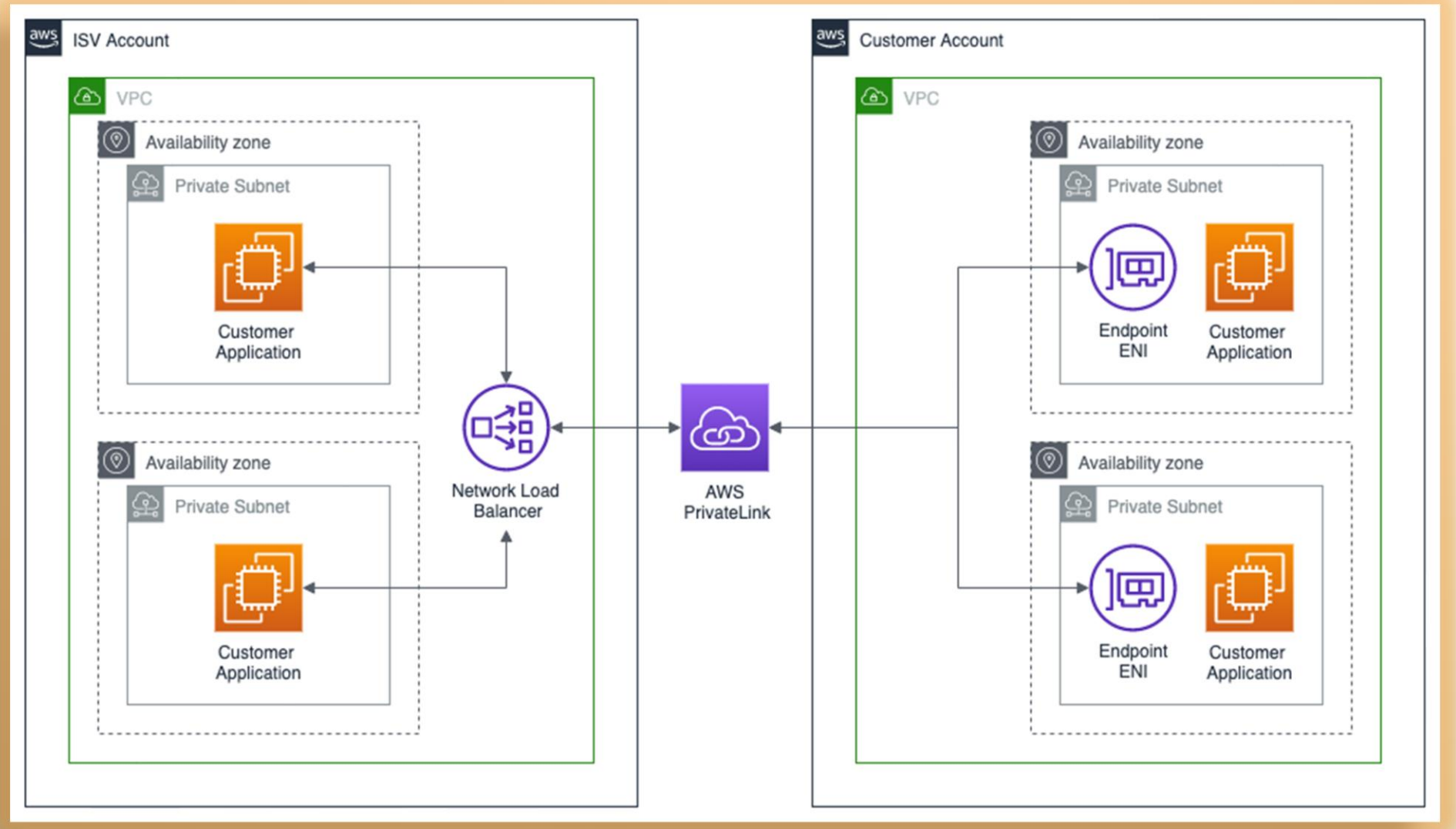


Azure Private Link

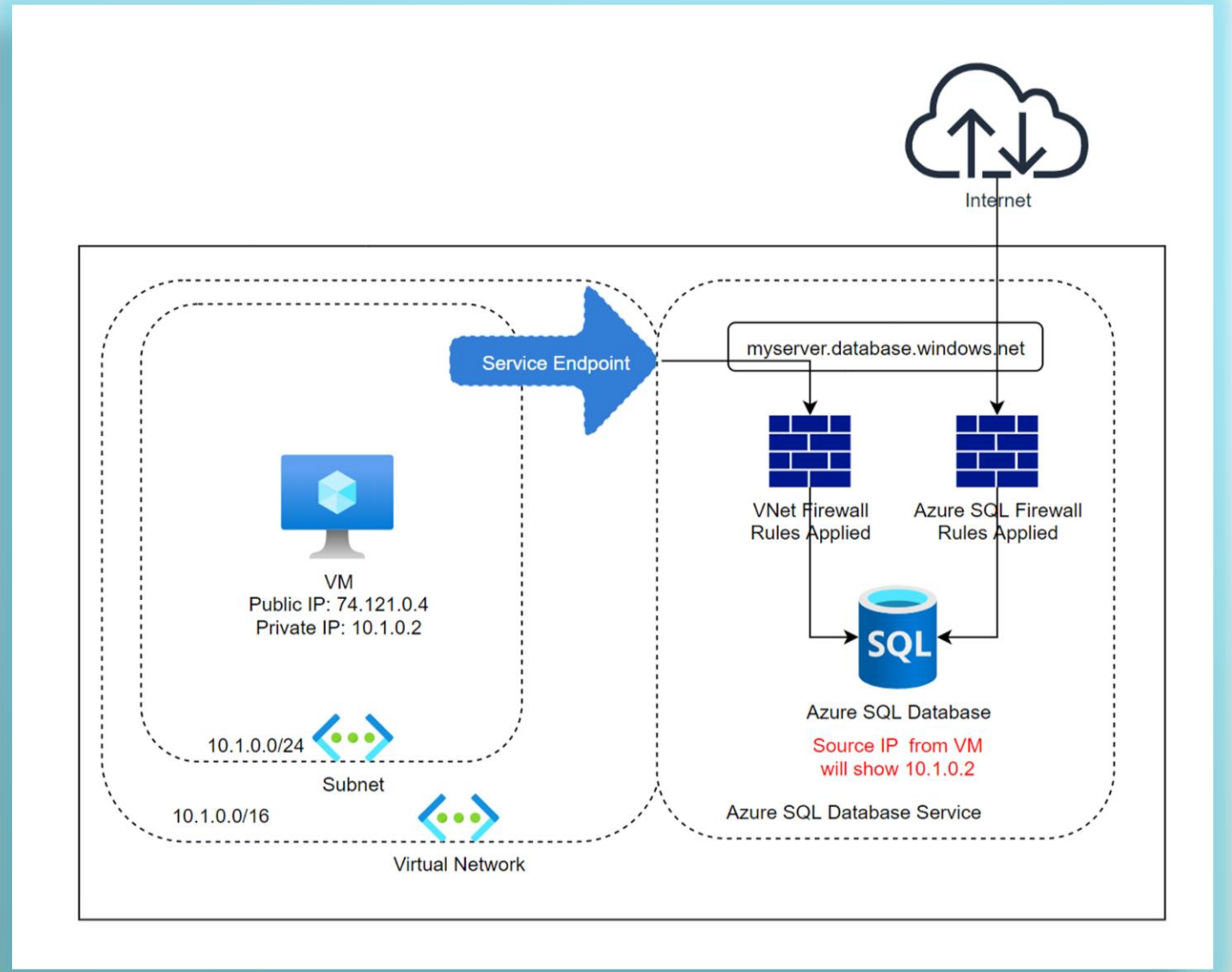


Azure Private Link – Connecting Azure Services privately to your Network

AWS Private Link



Azure Service Endpoint



Network Flow Logs

Capture information about IP traffic going in and out of your network interfaces in the virtual network.

Log data is collected outside of the network traffic path

Does not affect network throughput or latency

Flow log data can be stored in a separate object storage (AWS S3 / Azure Blobs)

Azure Flow Logs are captured from NSGs, AWS Flow Logs can be created for VPCs, subnets and/or ENIs.

Use cases

- Troubleshooting connectivity issues
- Intrusion/anomaly detection
- Archival for compliance/regulatory/legal purposes