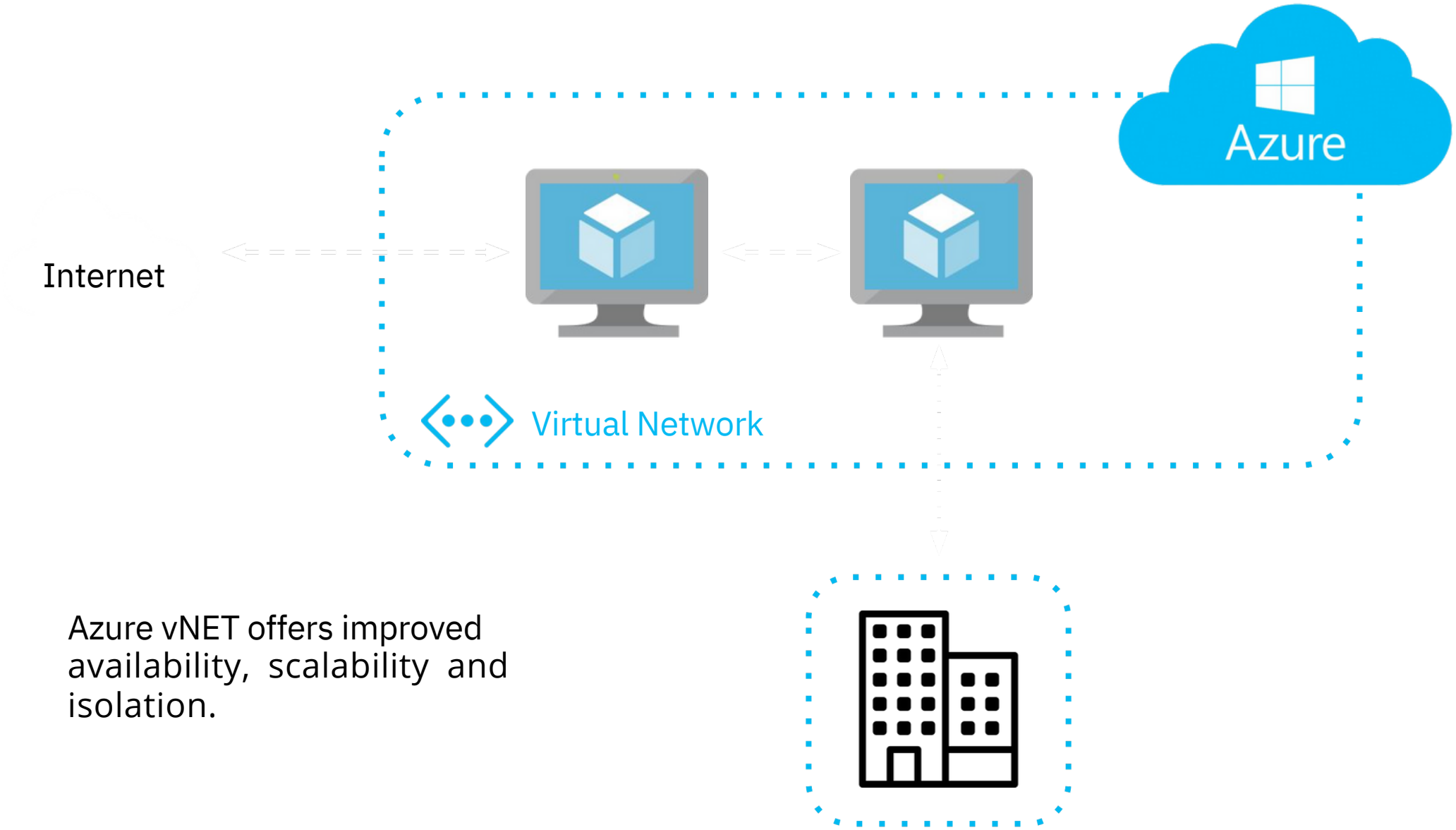
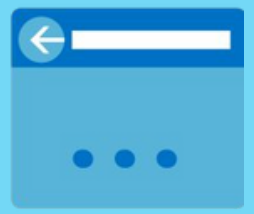
Getting Started with Azure Virtual Networks

Concepts and Best Practices

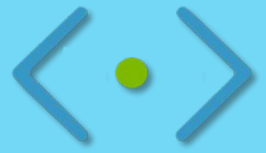


Azure vNET offers improved availability, scalability and isolation.

Concepts and Best Practices



Address space



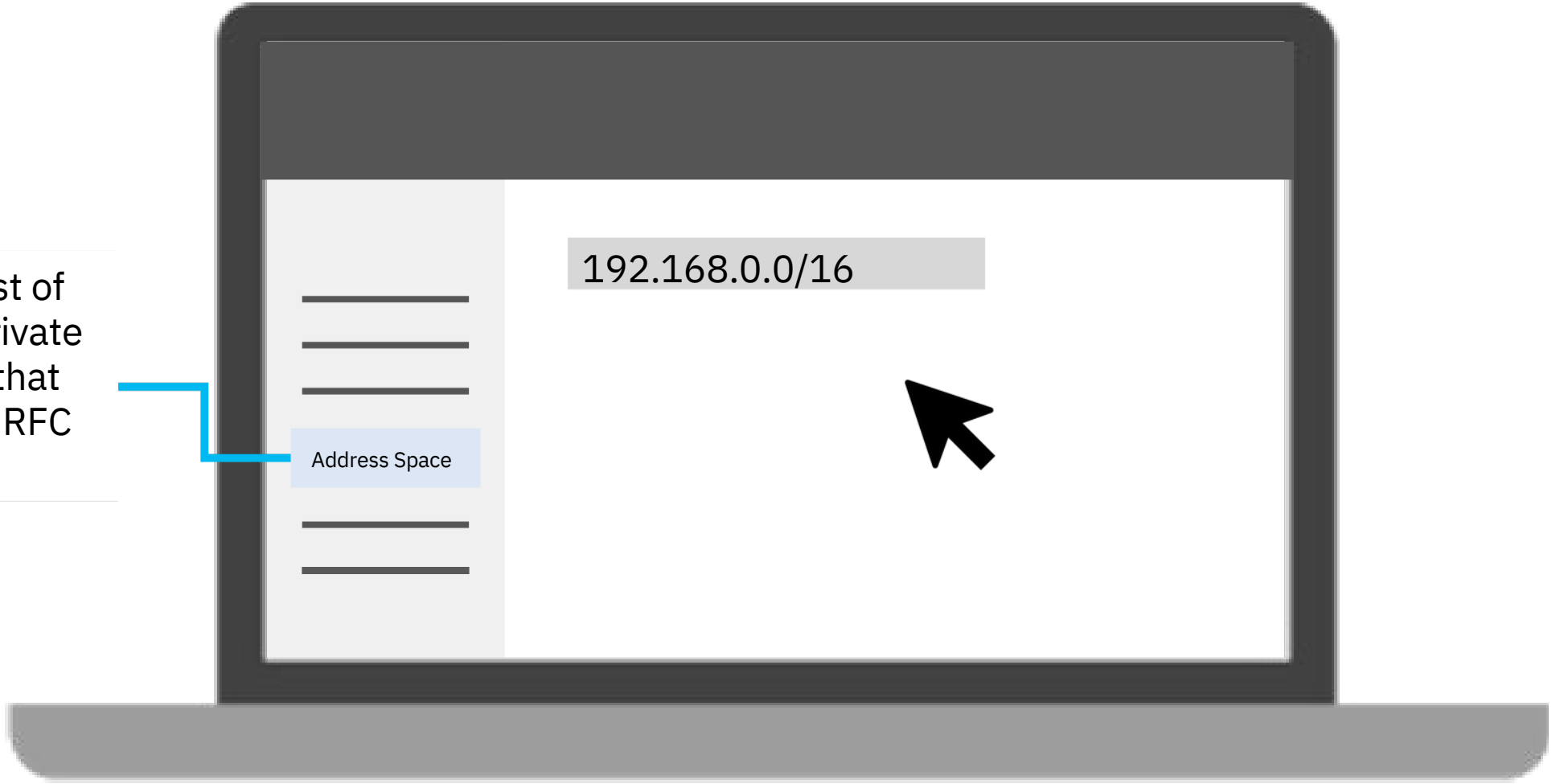
Subnets

Regions

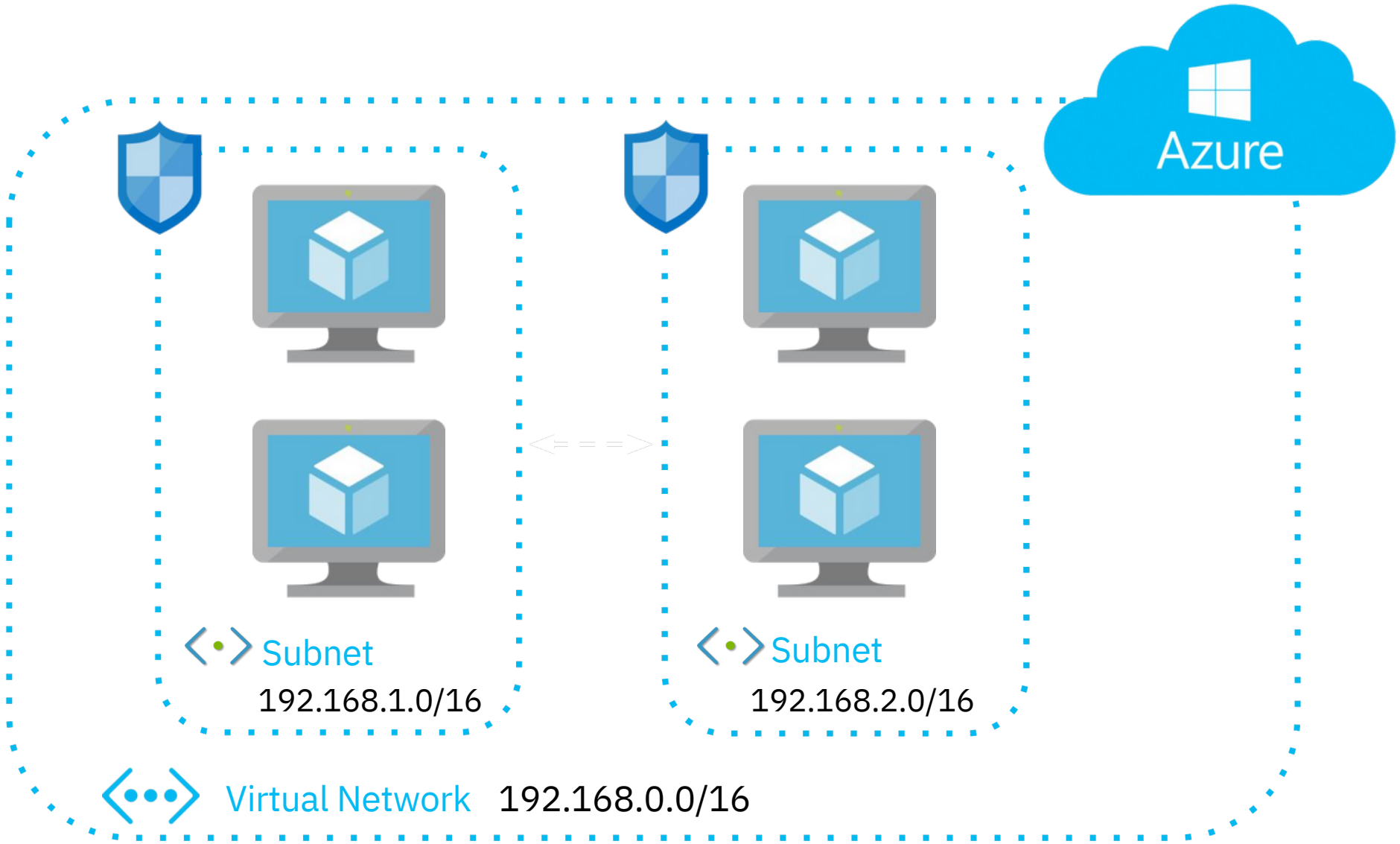
Subscriptions

Concepts and Best Practices

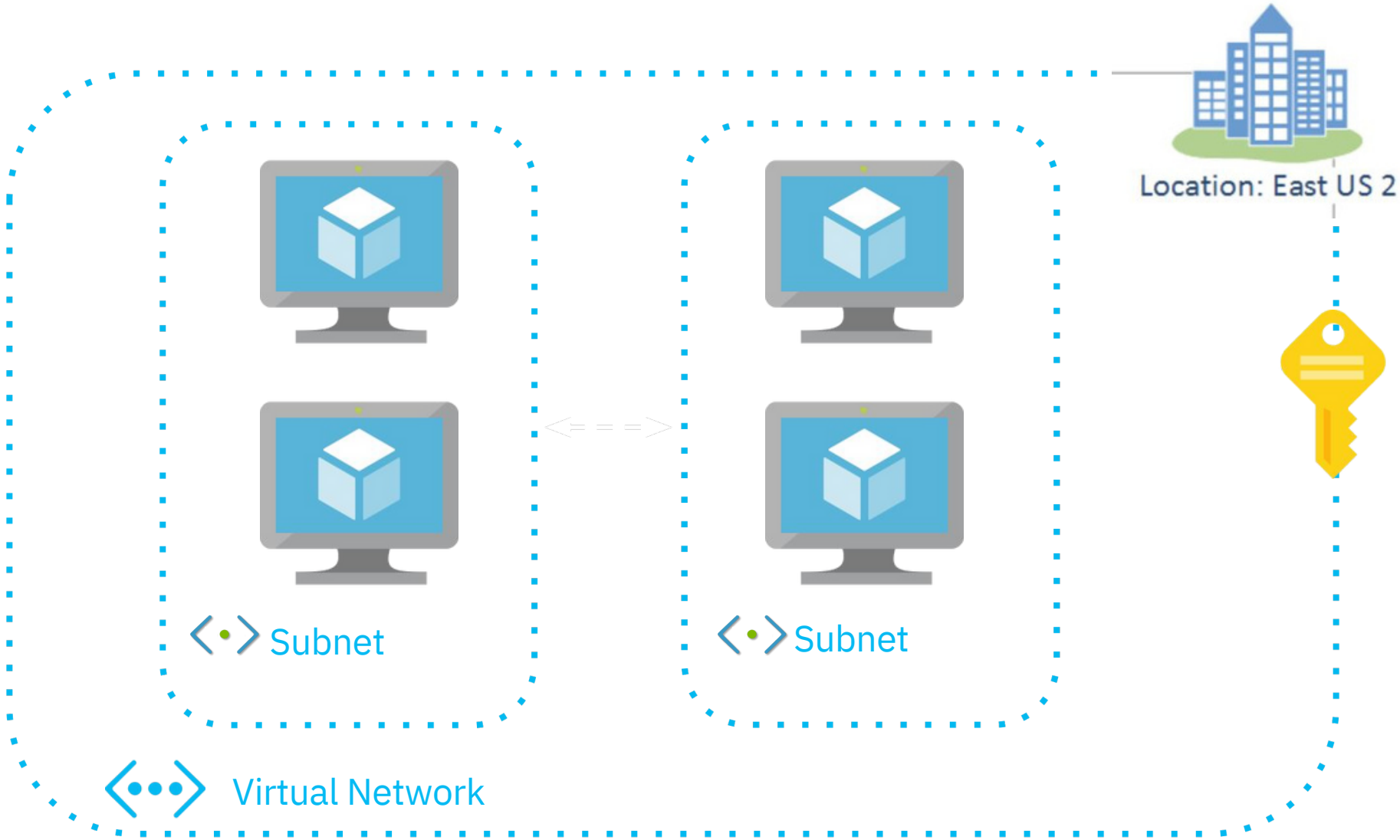
Must consist of public or private addresses that conform to RFC 1918.



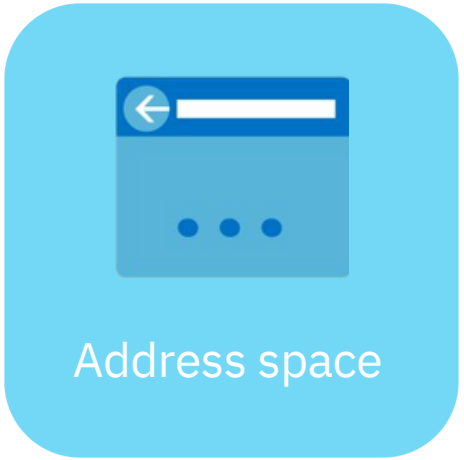
Concepts and Best Practices



Concepts and Best Practices

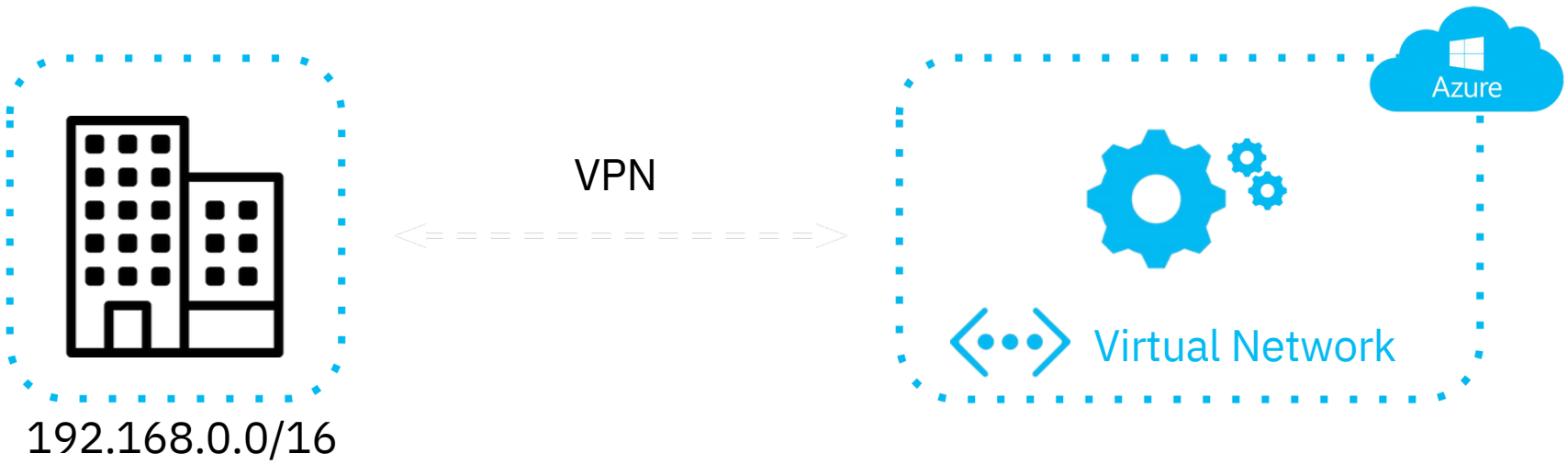


Concepts and Best Practices

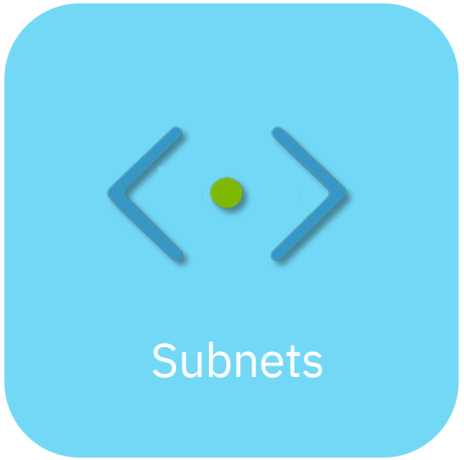


When deploying a virtual network, ensure that the address space does not overlap with any other network ranges that your organization uses.

Concepts and Best Practices

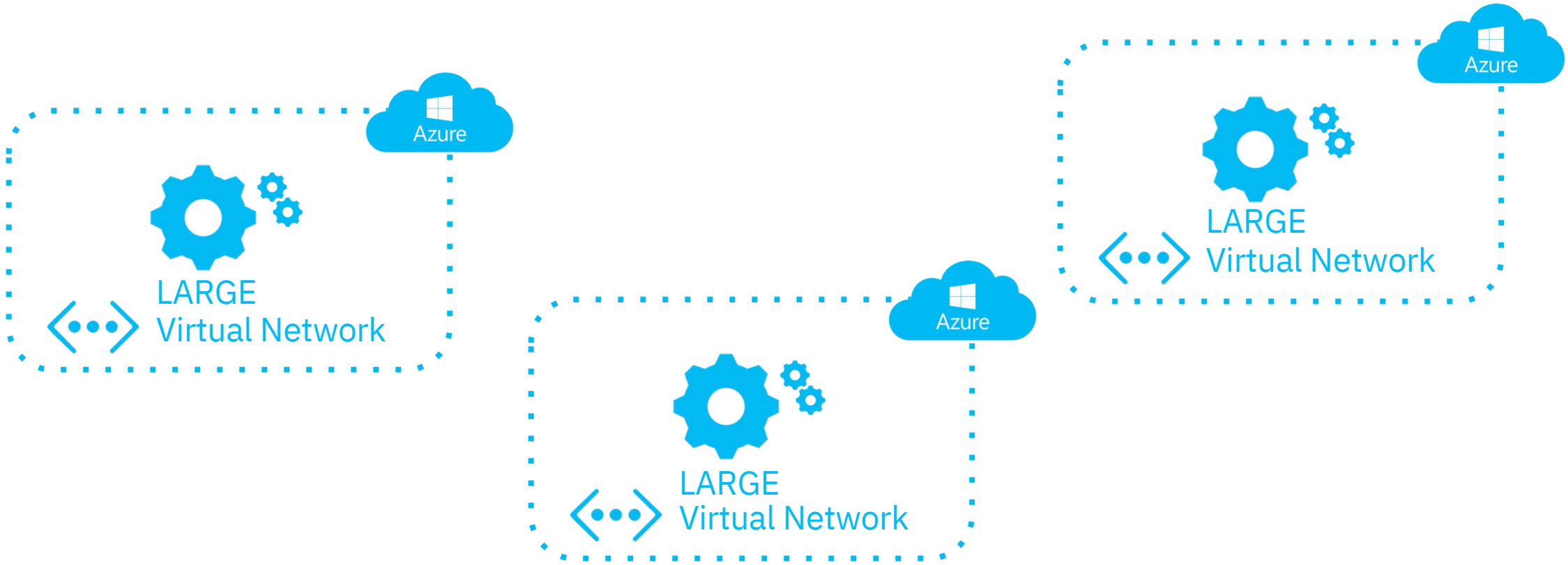


Concepts and Best Practices



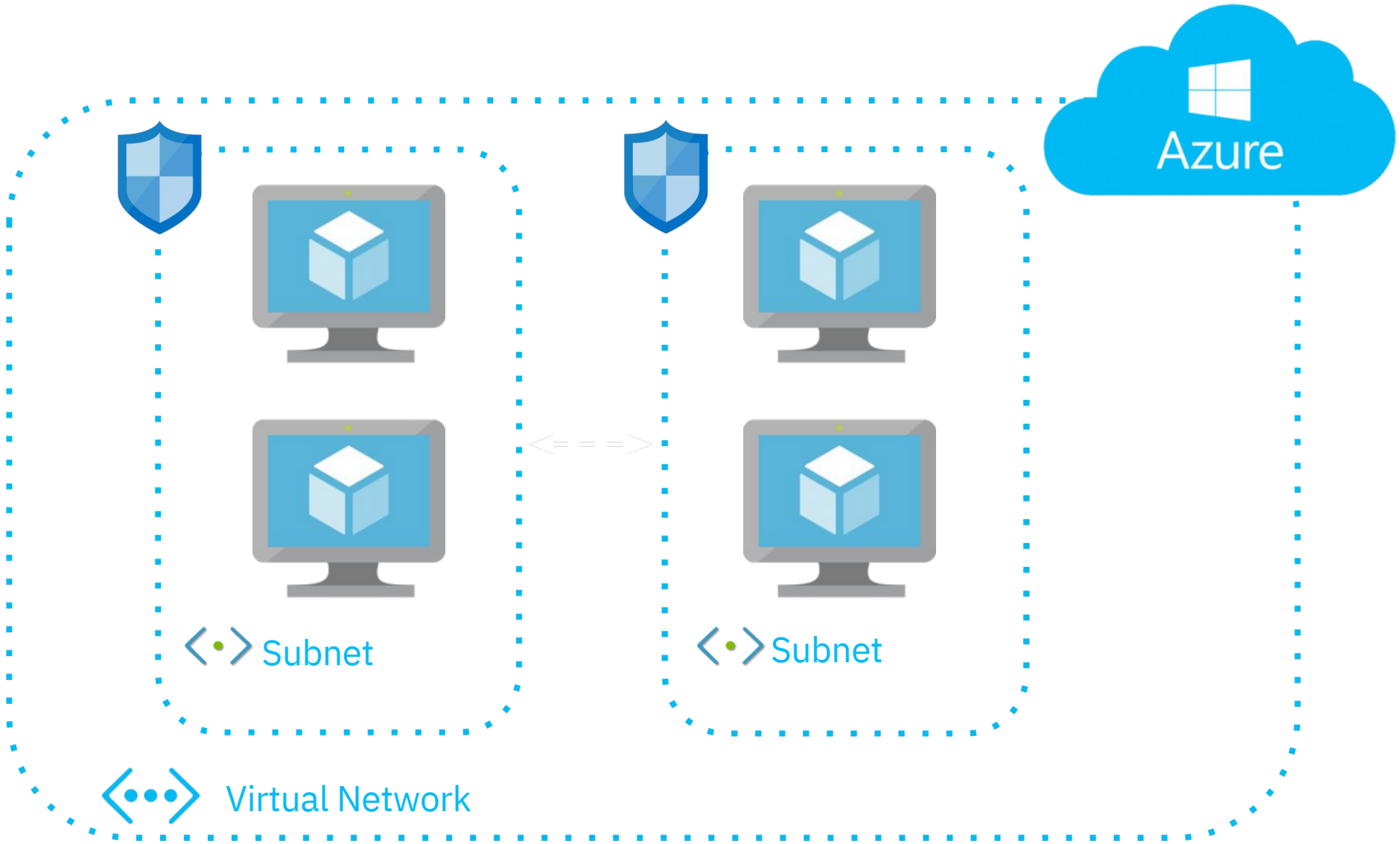
Never create a subnet that encompasses the entire address space of the virtual network.

Concepts and Best Practices



Define fewer large vNETs rather than numerous small vNETs.

Concepts and Best Practices



Concepts and Best Practices

Network Security Group:

- used to filter network traffic to and from Azure resources that are attached to a virtual network

- contains rules that allow or deny inbound and outbound network traffic to and from subnets

Communications

Communications – Recap

Virtual networks are used to facilitate communication:

With the internet

- Outbound communication to the internet is available by default
- Inbound communications from the internet are achieved via a public load balancer or public IP address.

Between Azure resources

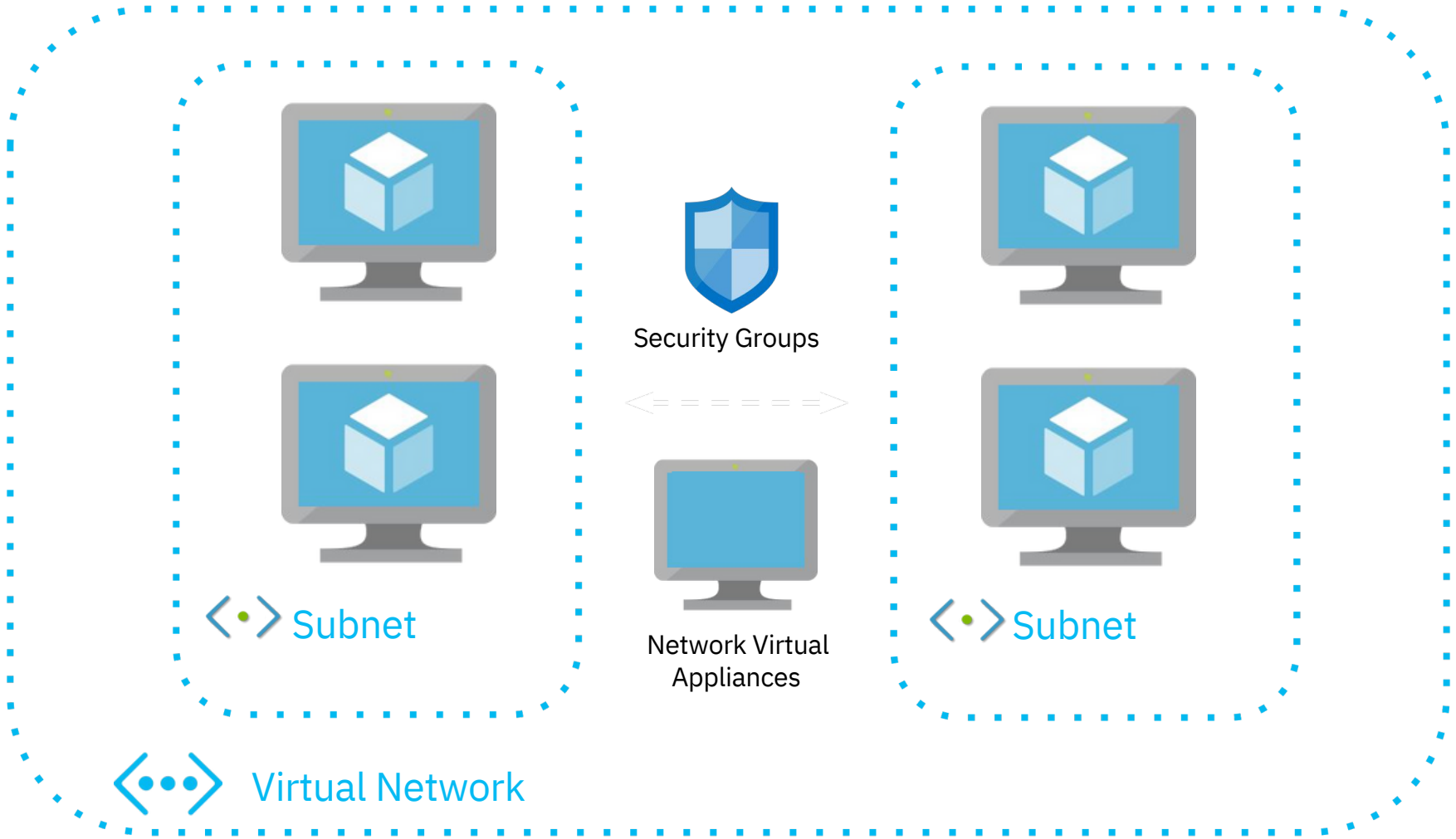
- Communications between azure resources is achieved through a virtual network, a virtual network service endpoint, or through vNet peering.

With an on-prem environment

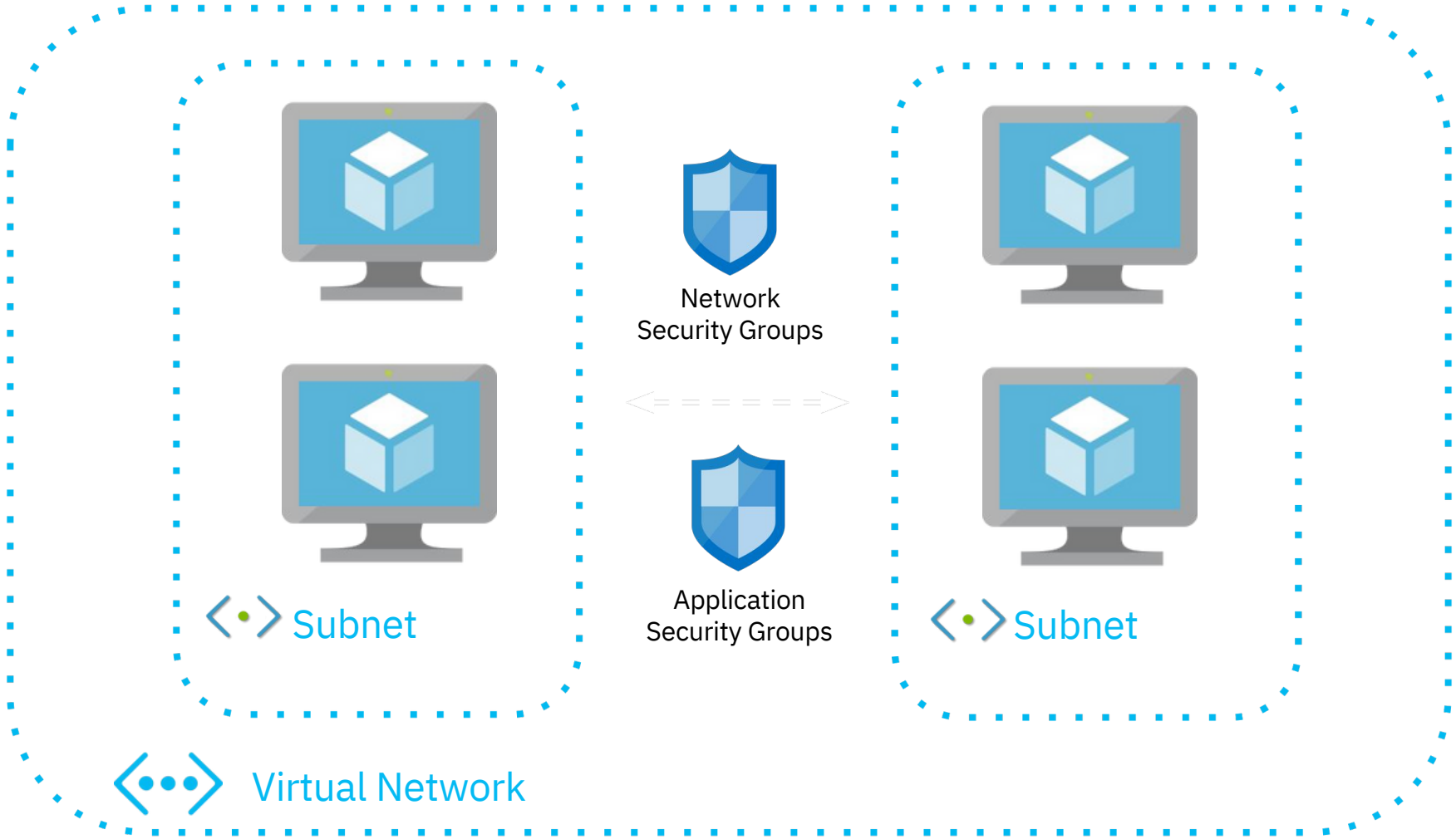
- To establish communications between an Azure environment and an on-prem environment, you can deploy a point-to-site VPN, and site-to-site VPN, or an Azure ExpressRoute connection.

Filtering, Routing and Integration

Filtering, Routing and Integration – Filtering Network Traffic



Filtering, Routing and Integration – Filtering Network Traffic



Filtering, Routing and Integration – Filtering Network Traffic

Network
Security Groups

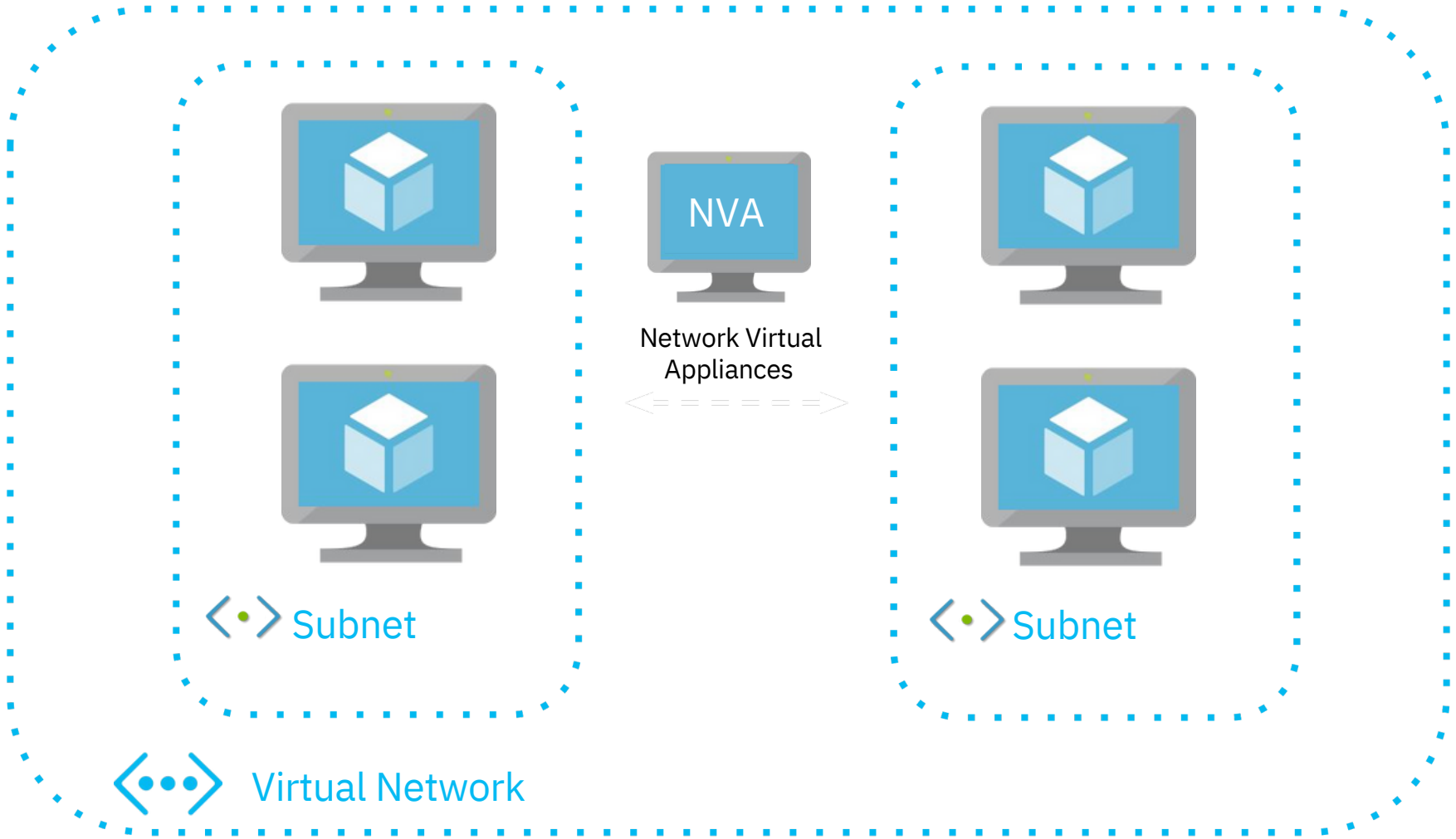
- can be assigned to a specific NIC or to an entire subnet
- rules defined within the network security group are then applied to that NIC or to all NICs and virtual machines on the subnet
- this works for most scenarios

Filtering, Routing and Integration – Filtering Network Traffic

Application Security Groups

- you can logically group the NICs of several different virtual machines on the same virtual network
- then apply a network security group rule to only those grouped NICs
- this allows you to create different traffic rules for different groups of NICs on the same network
- You can have a group of SQL VMs connected to the same vNet as your group of application VMs
- using a separate application security group for each group of VMs allows you to manage the network security rules for each different group of VMs

Filtering, Routing and Integration – Filtering Network Traffic



Filtering, Routing and Integration – Filtering Network Traffic

Network Virtual Appliances

A virtual machine used to perform a specific network task, eg:

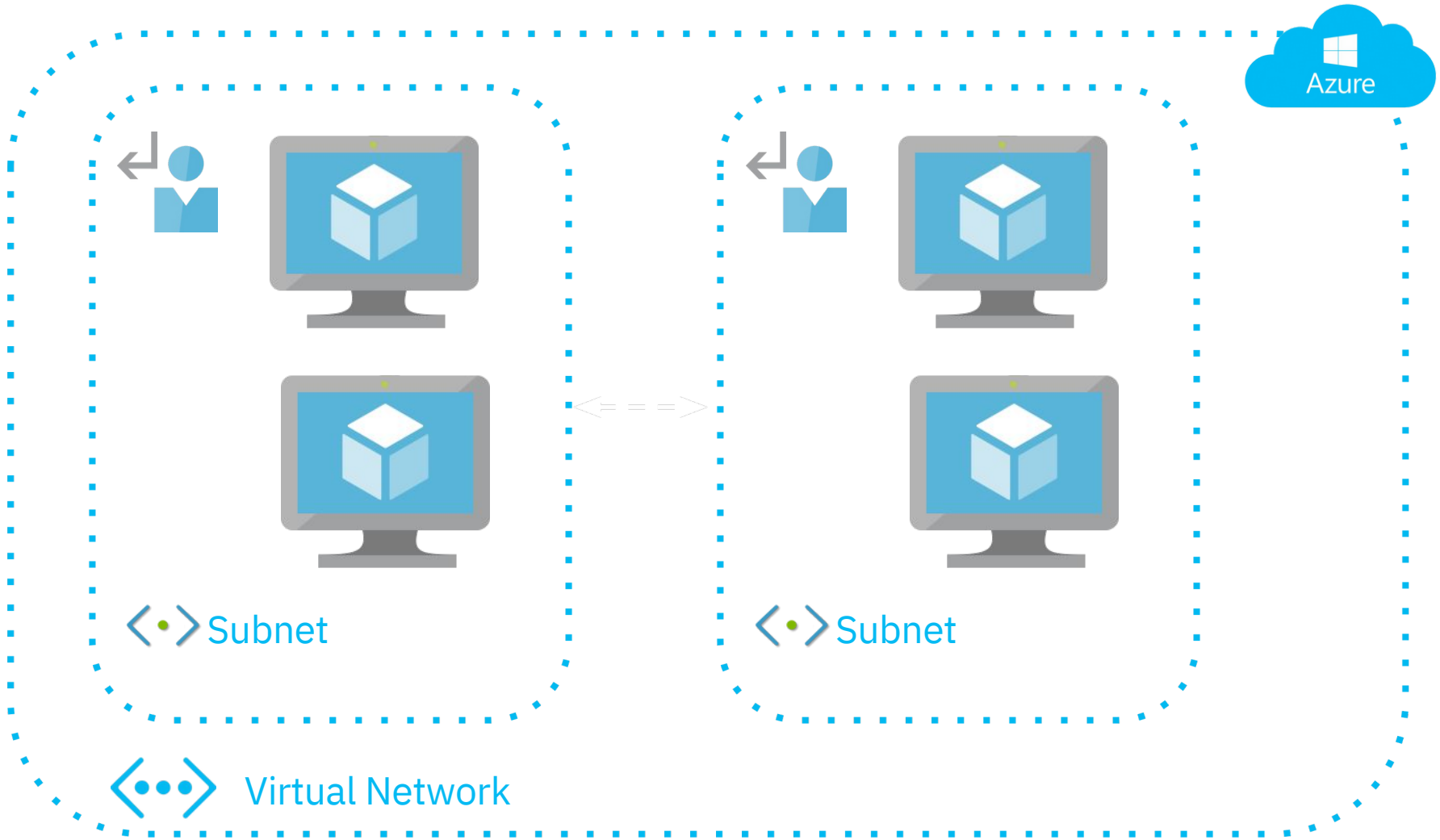
- to act as a firewall
- to provide WAN optimization

Available NVAs include:

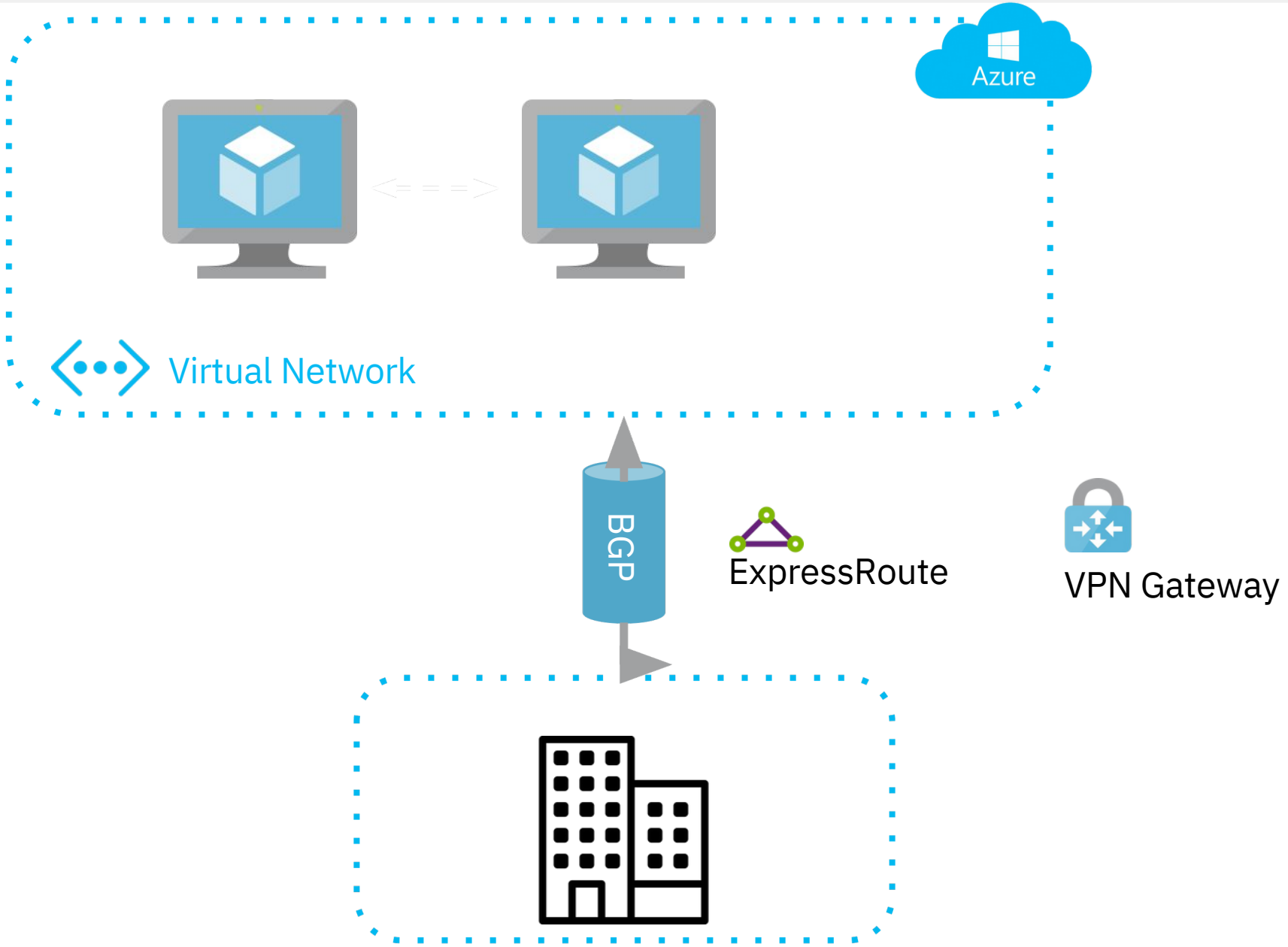
- Barracuda CloudGen WAF for Azure
- Citrix SD-WAN Center

Filtering, Routing and Integration – Routing Network Traffic

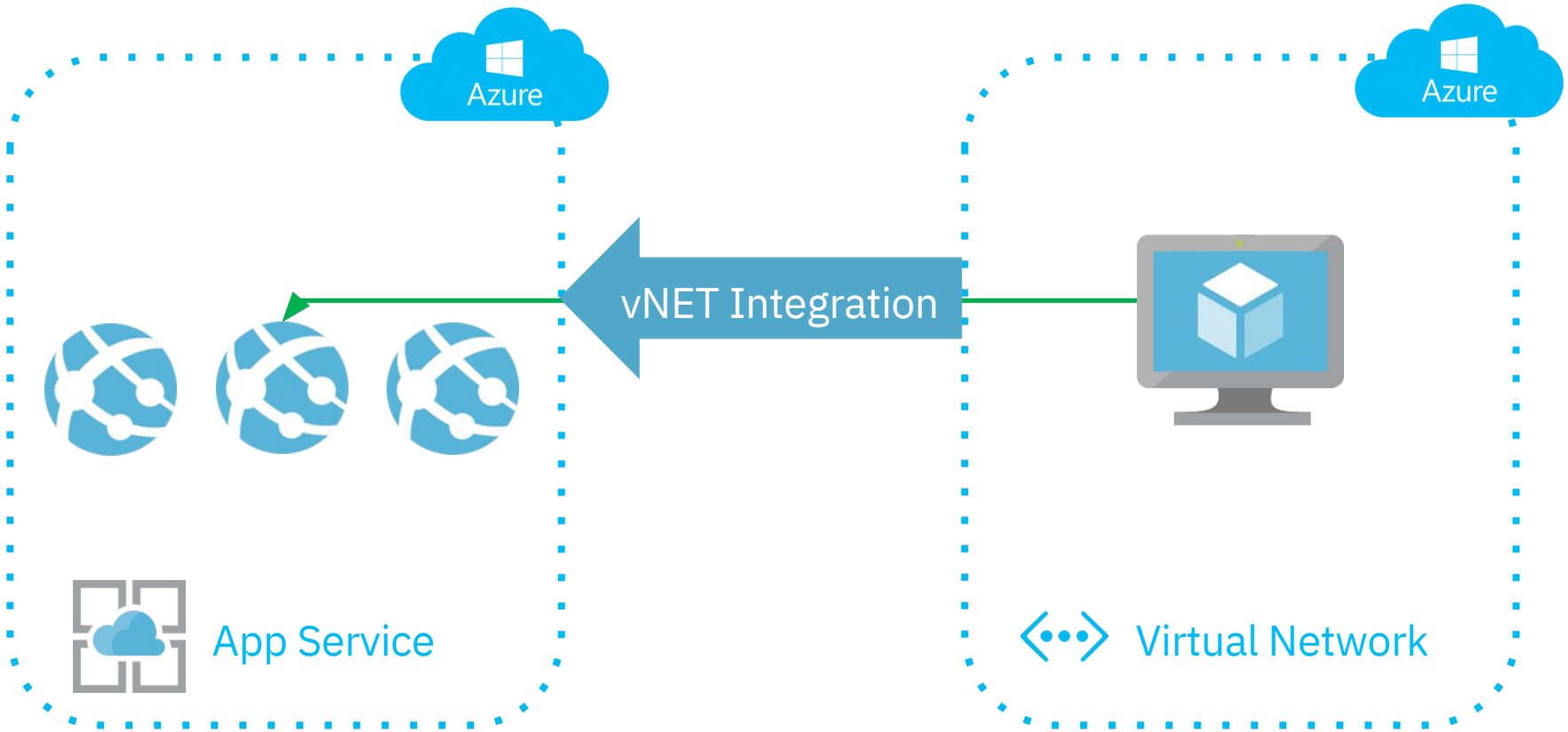
Filtering, Routing and Integration – Routing Network Traffic



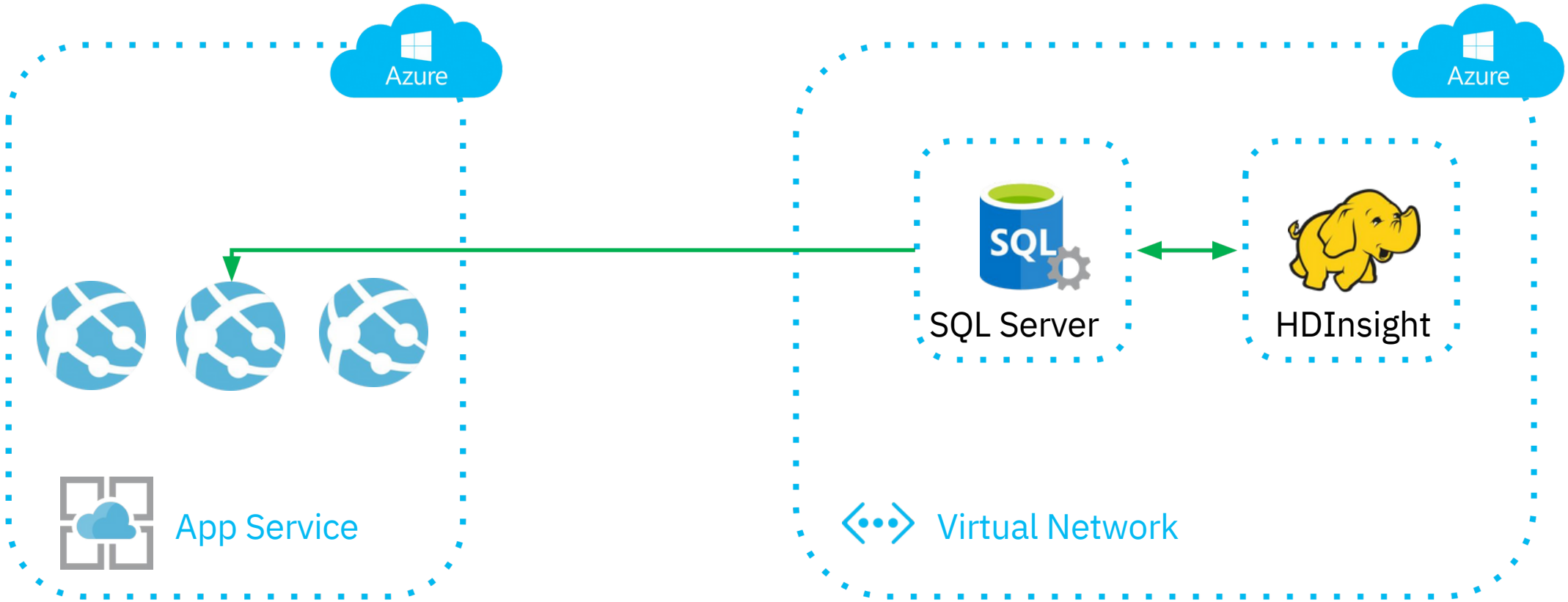
Filtering, Routing and Integration – Routing Network Traffic



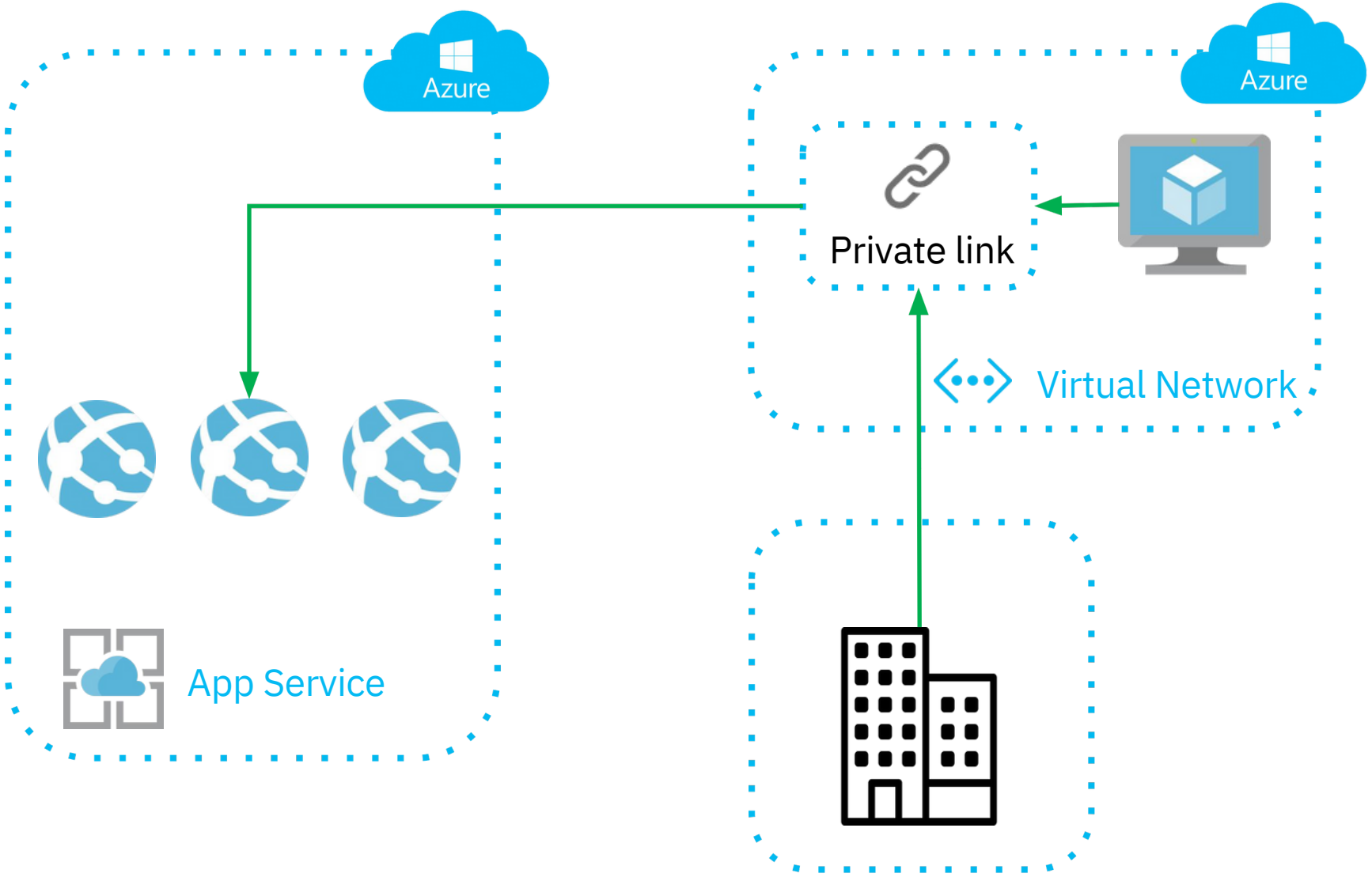
Filtering, Routing and Integration – vNET Integration



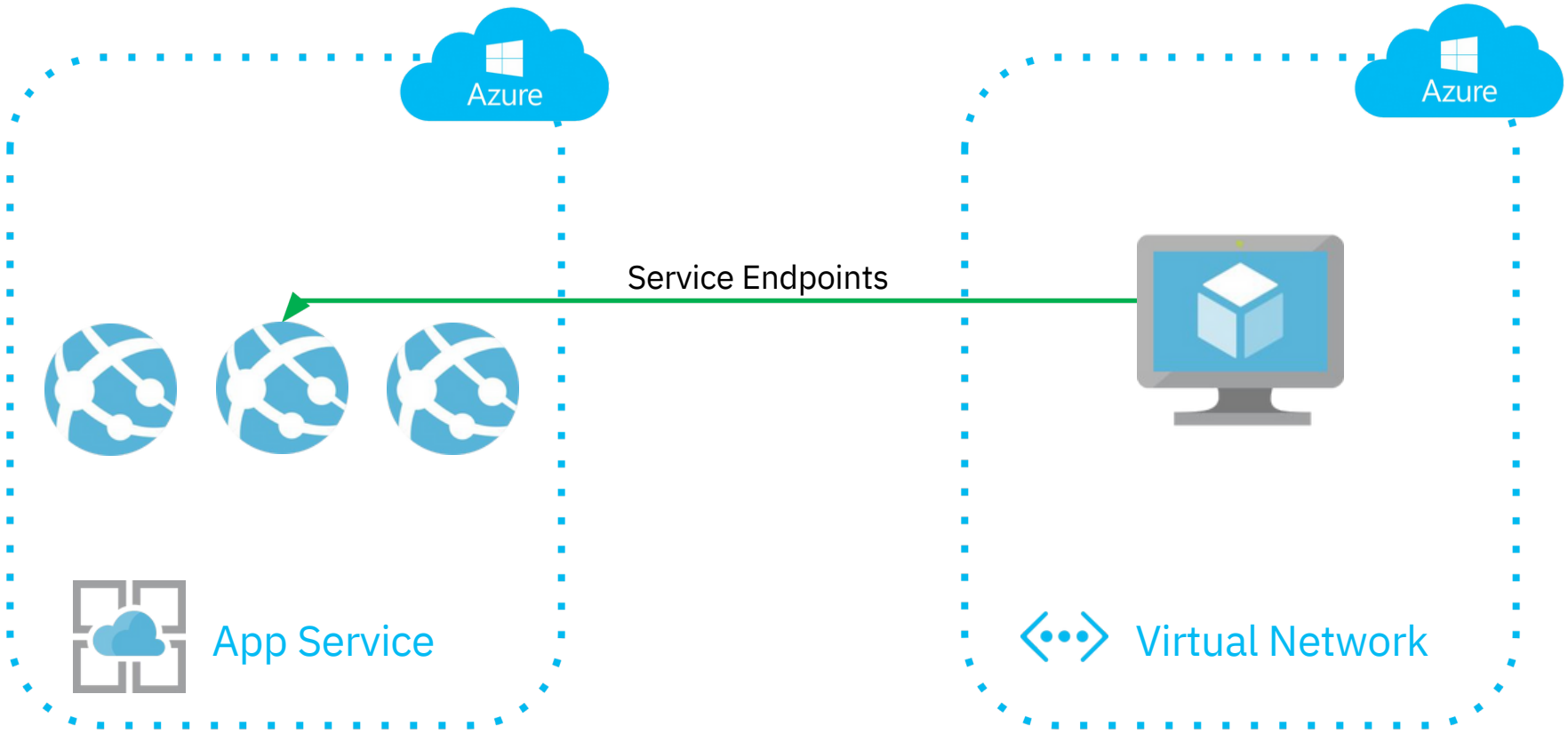
Filtering, Routing and Integration – vNET Integration



Filtering, Routing and Integration – vNET Integration



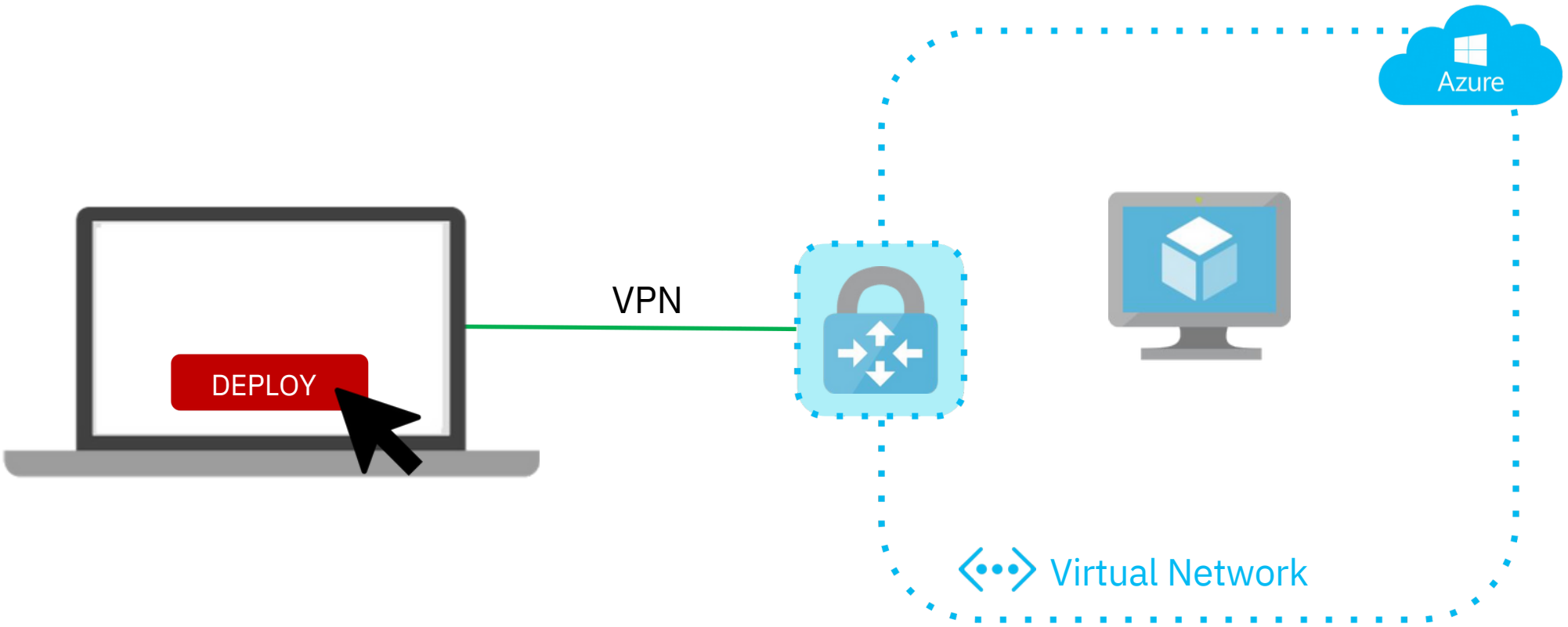
Filtering, Routing and Integration – vNET Integration



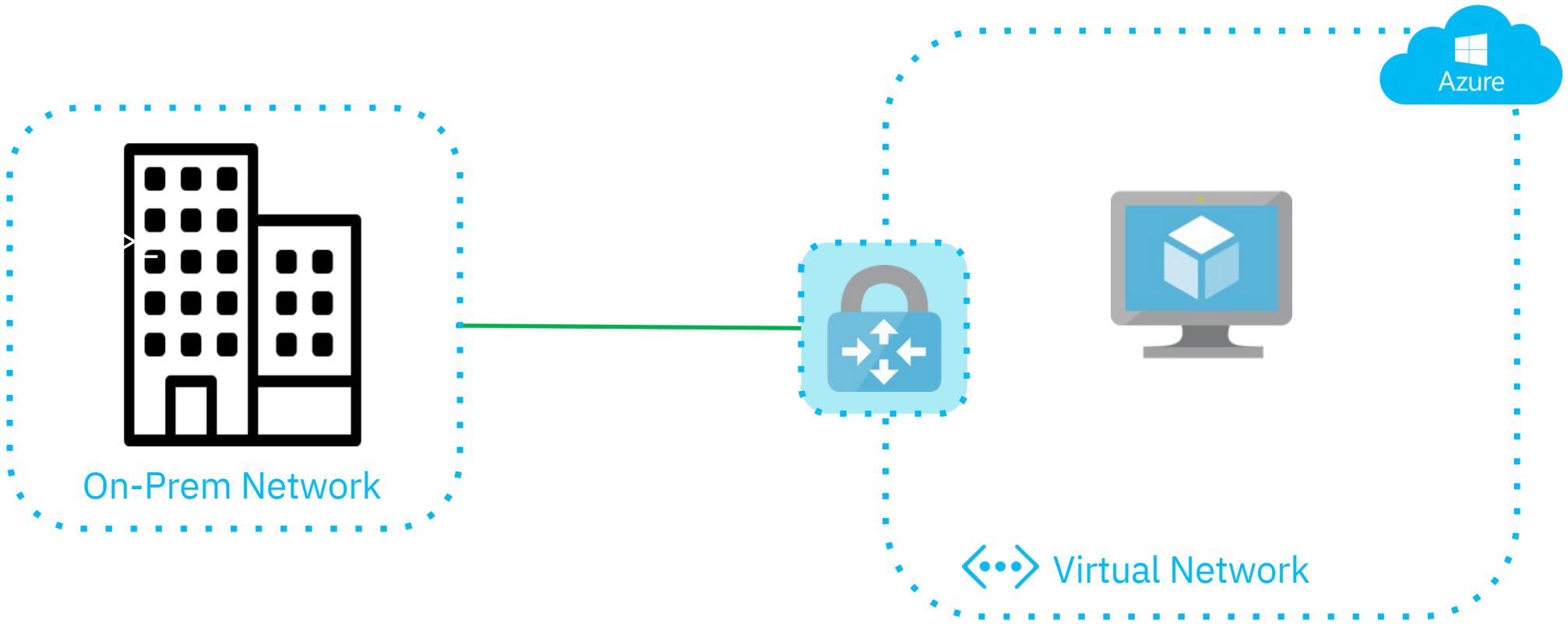
You can use service endpoints to create secure and direct connectivity to Azure resources over an optimized route across the Azure backbone network.

VPN Gateways

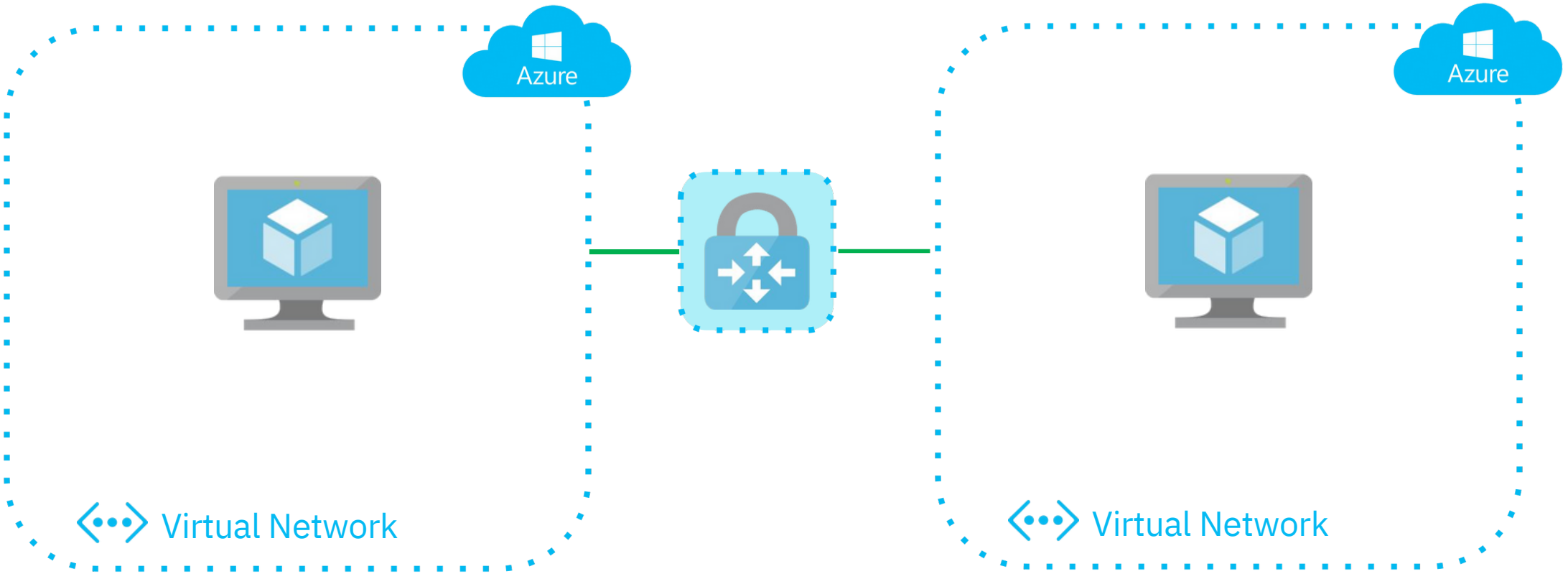
VPN Gateways



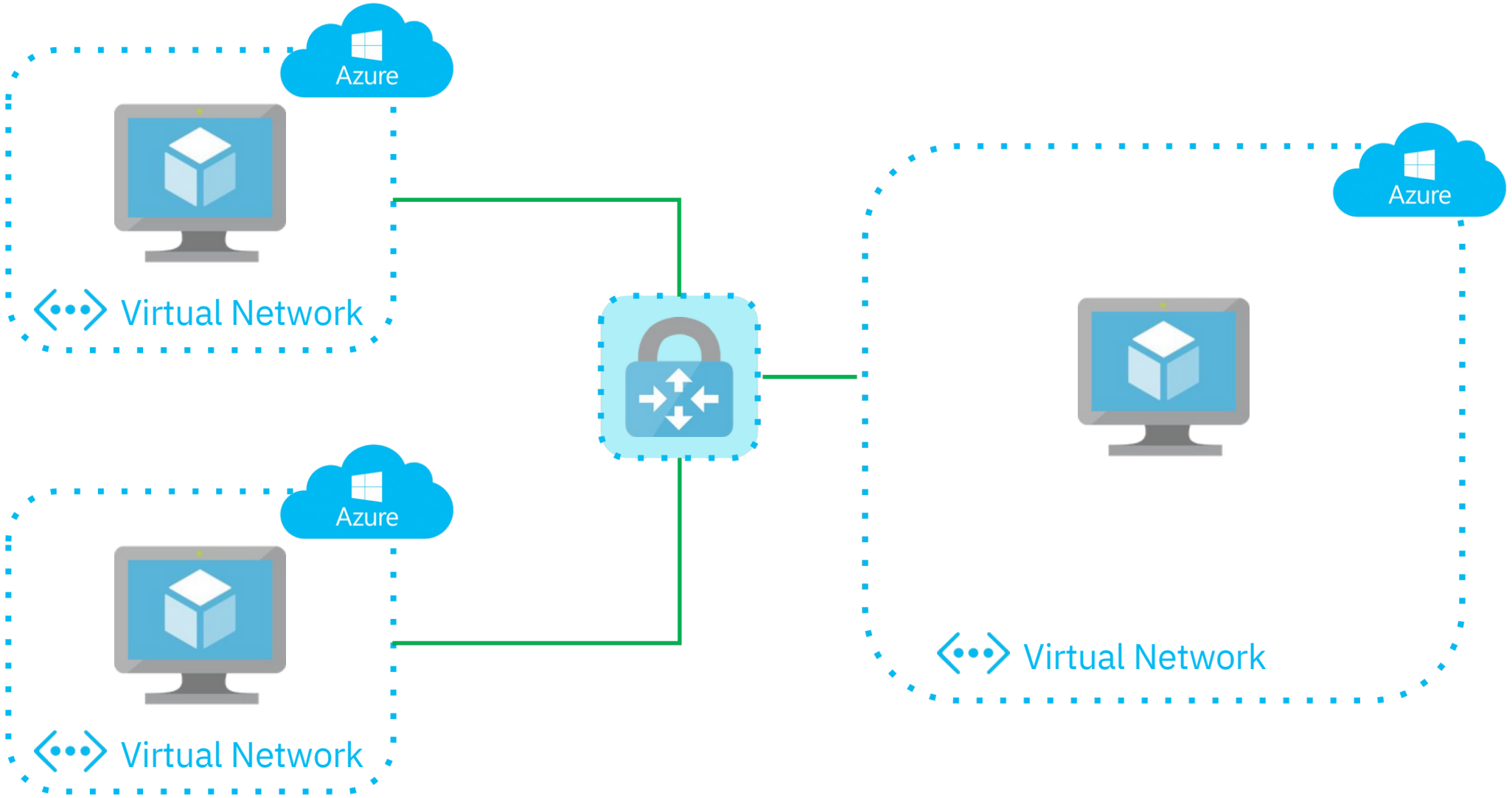
VPN Gateways



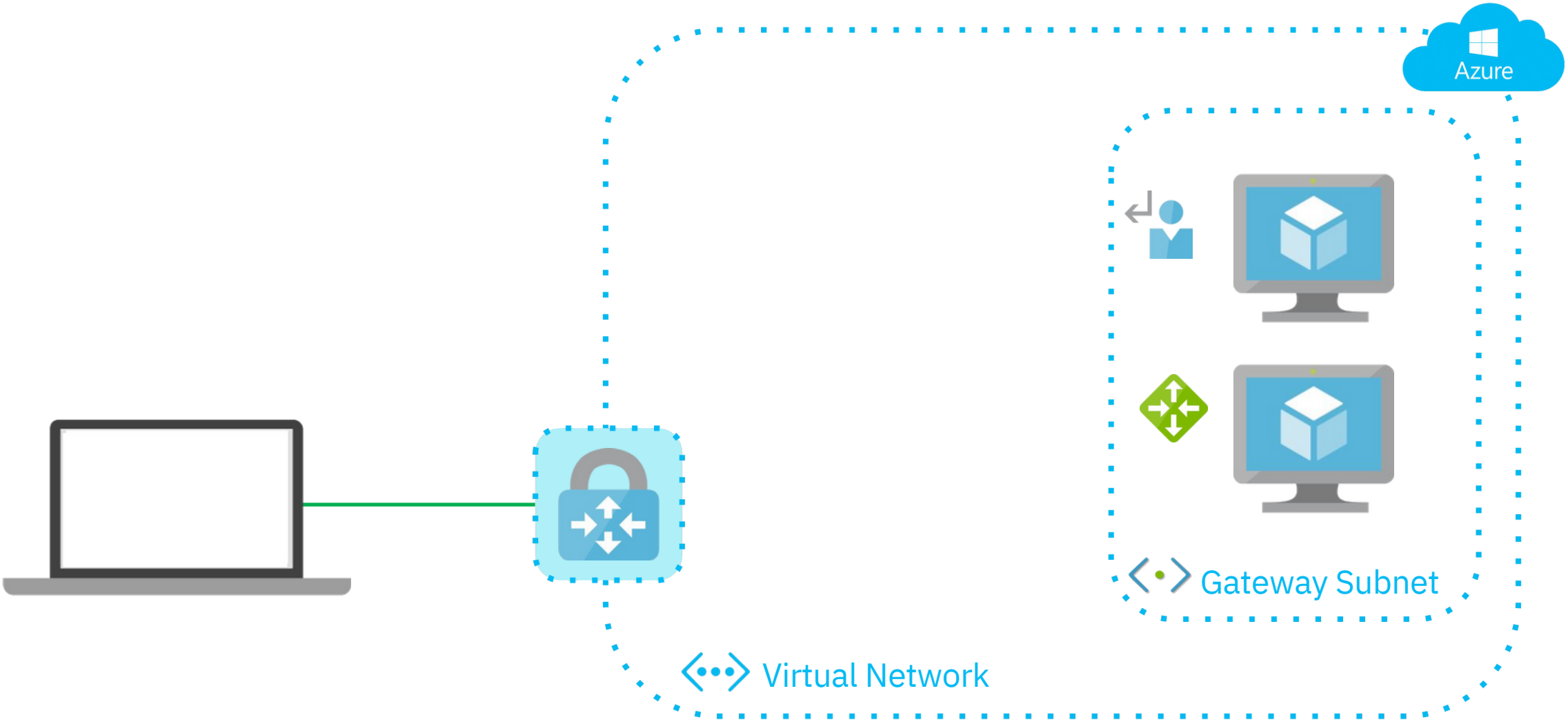
VPN Gateways



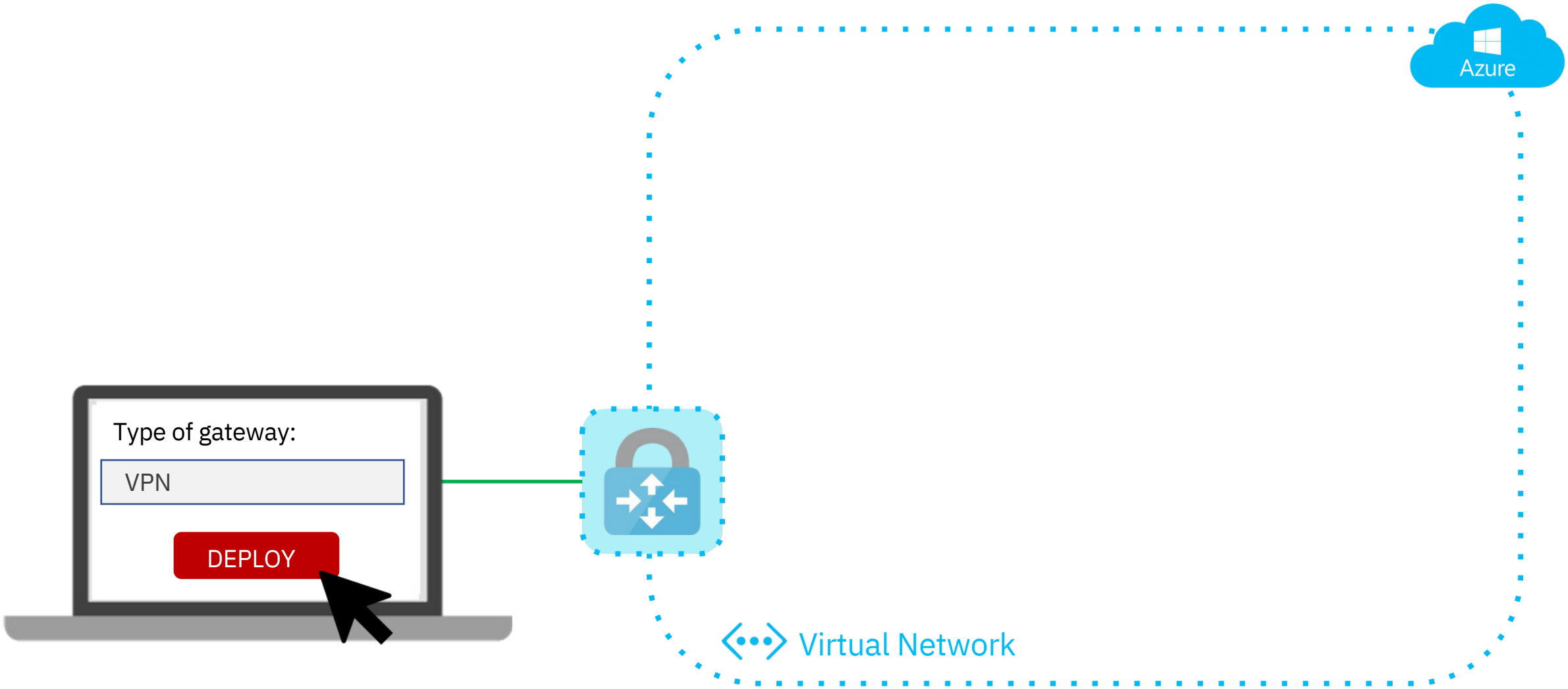
VPN Gateways



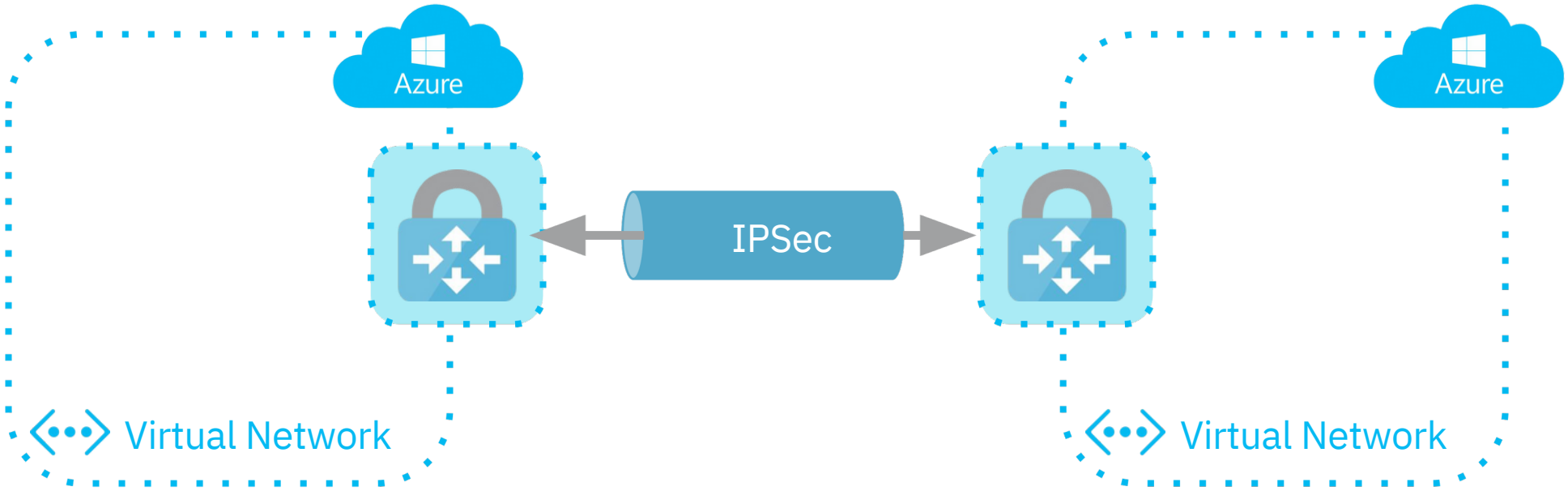
VPN Gateways



VPN Gateways

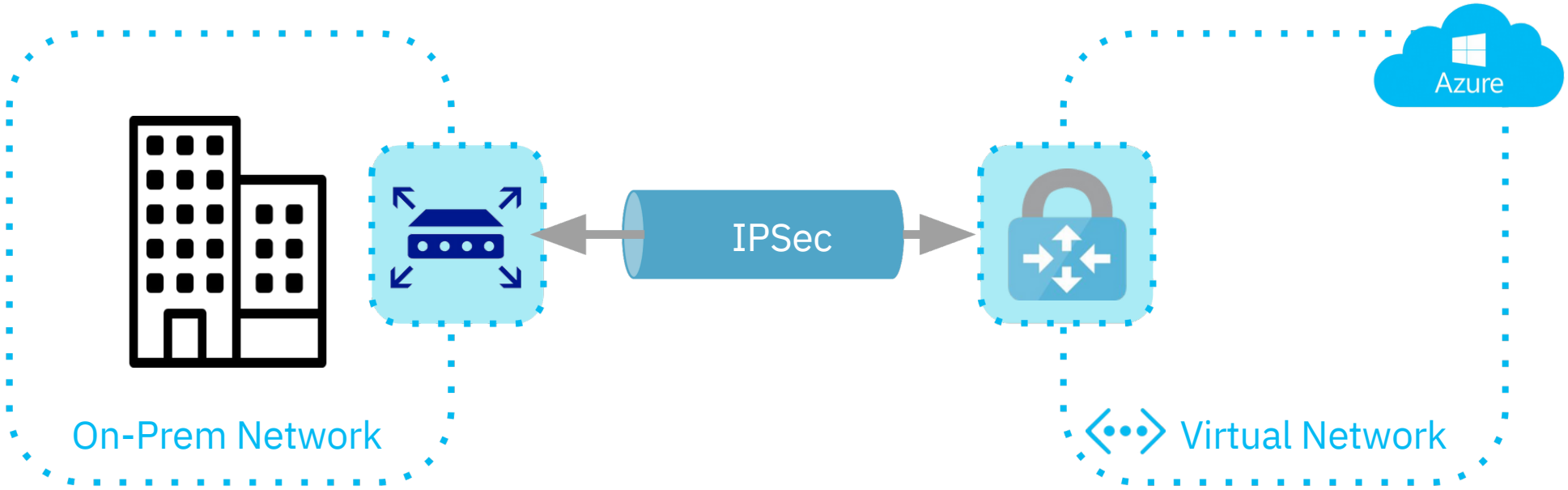


VPN Gateways



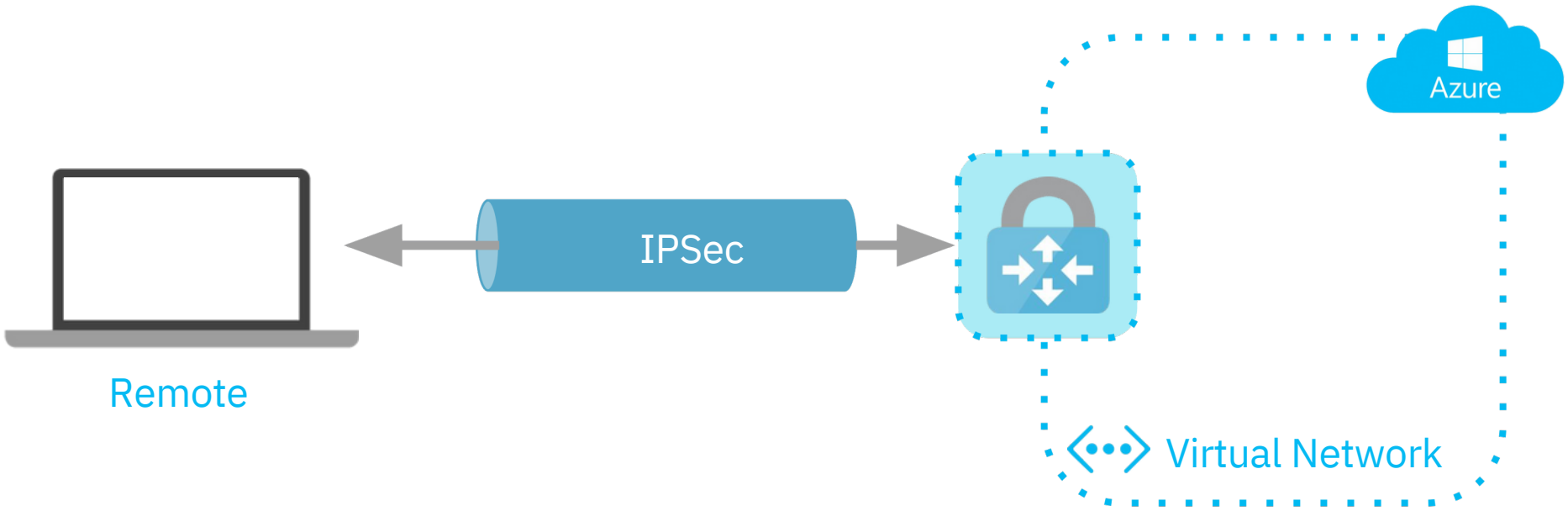
vNet-to-vNet

VPN Gateways



Site-to-Site

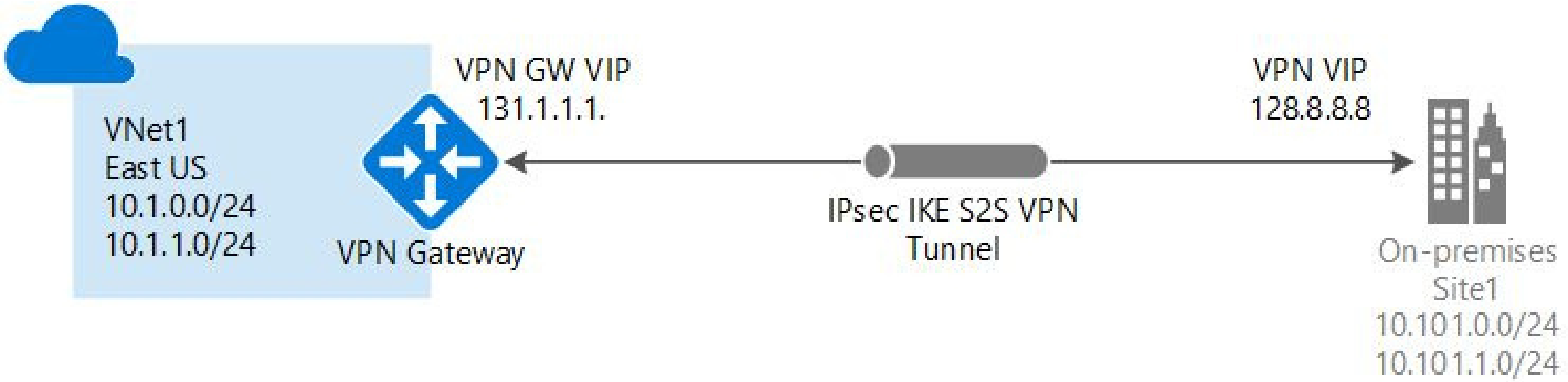
VPN Gateways



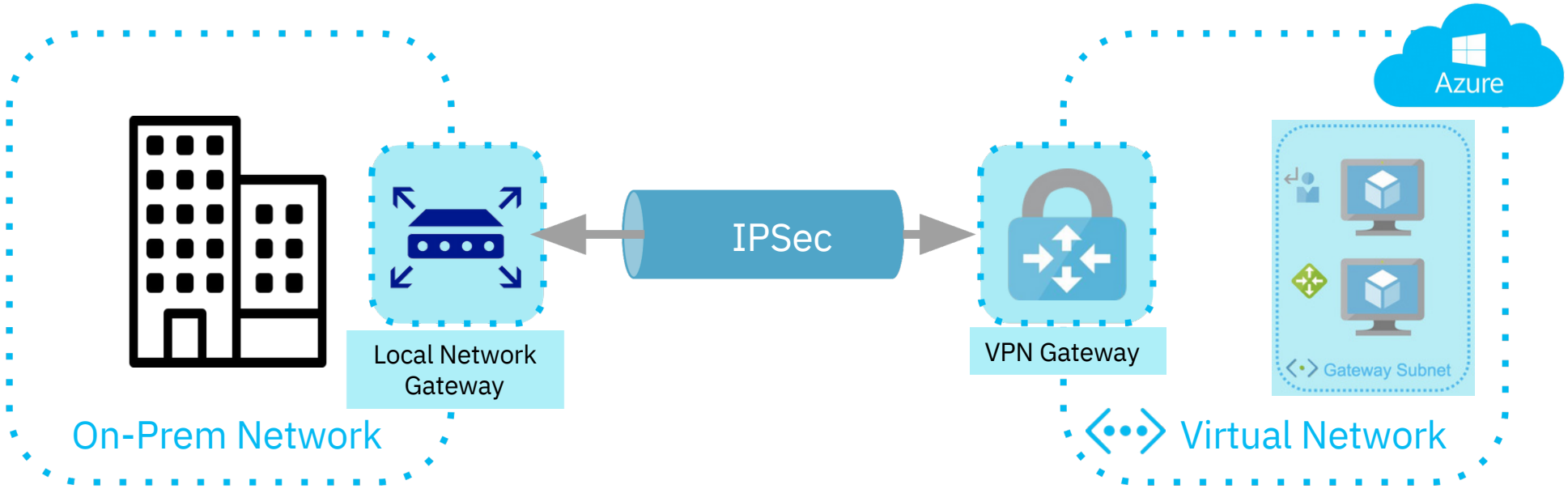
Point-to-Site

Site-to-Site VPNs

Site-to-Site VPNs

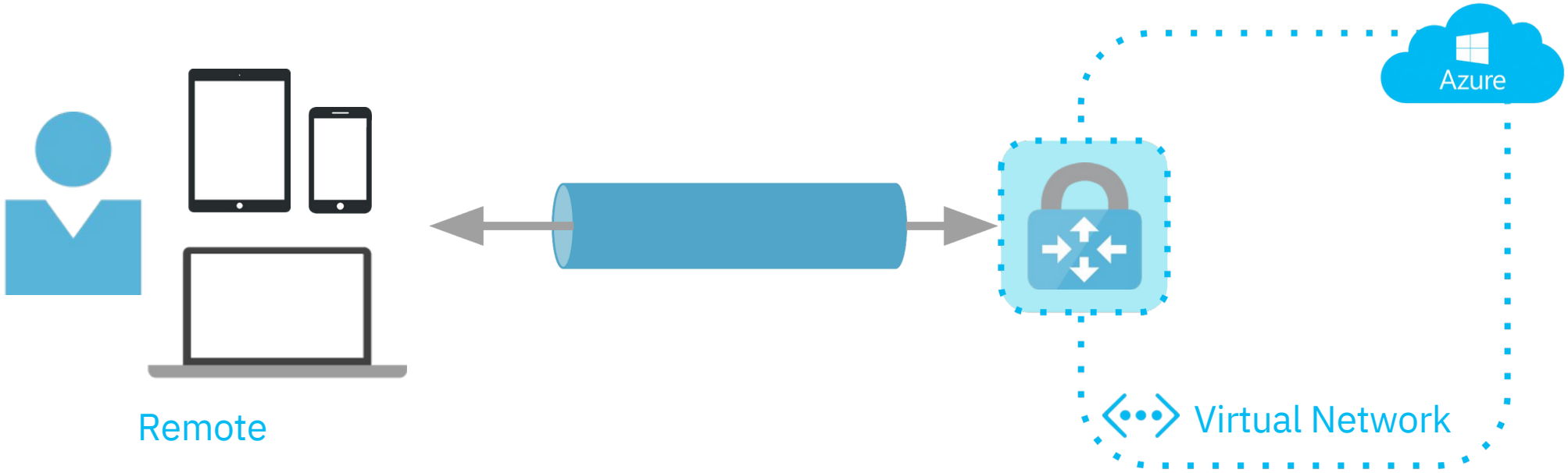


Site-to-Site VPNs



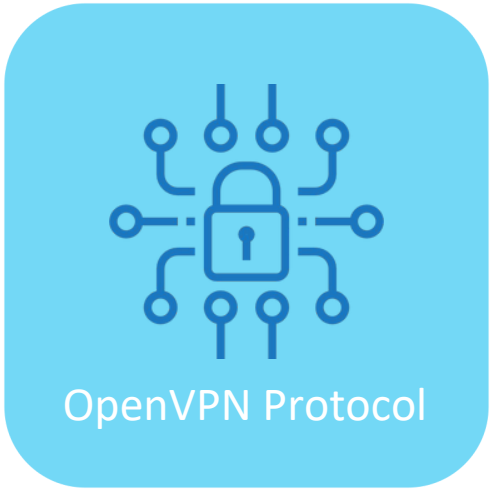
Point-to-Site VPNs

Point-to-Site VPNs

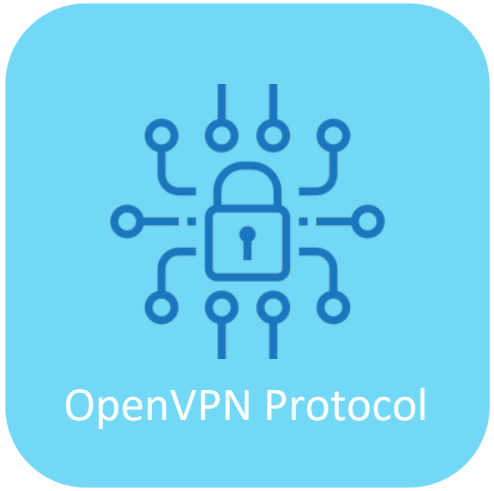


Point-to-Site VPNs

When you create a point-to-site VPN, you have a choice of protocols:



Point-to-Site VPNs



- SSL/TLS-based VPN protocol that can be used through a firewall

- Can be used to connect from a variety of client machines, including those running Android, Windows, Linux, and Mac OSX

Point-to-Site VPNs

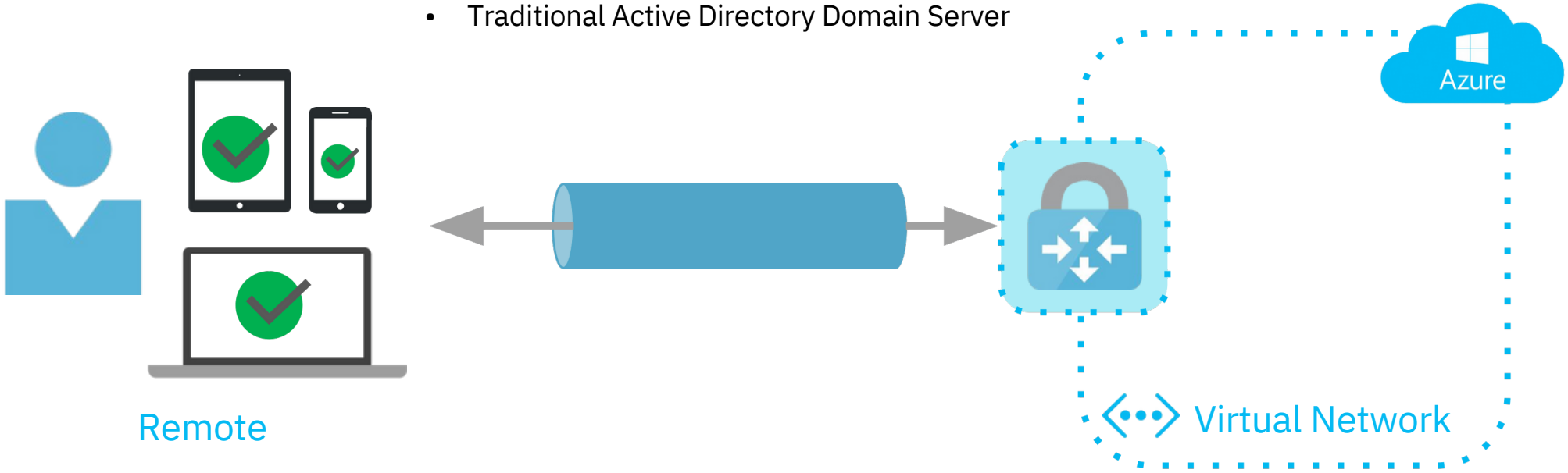
- A proprietary VPN protocol that leverages TLS
- Can be used through firewalls
- Only supports Windows devices

Point-to-Site VPNs

- A standards-based IPSec VPN solution
- Can be used to connect from Mac OSX devices

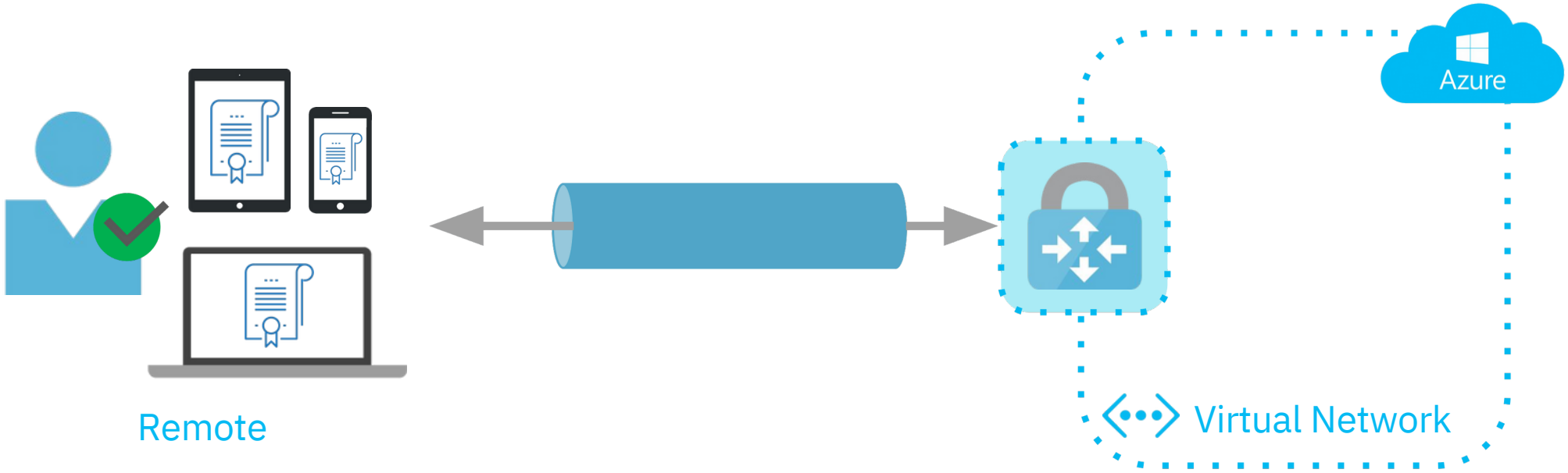
Point-to-Site VPNs

- Native Azure certificate authentication
- Native Azure AD authentication
- Traditional Active Directory Domain Server



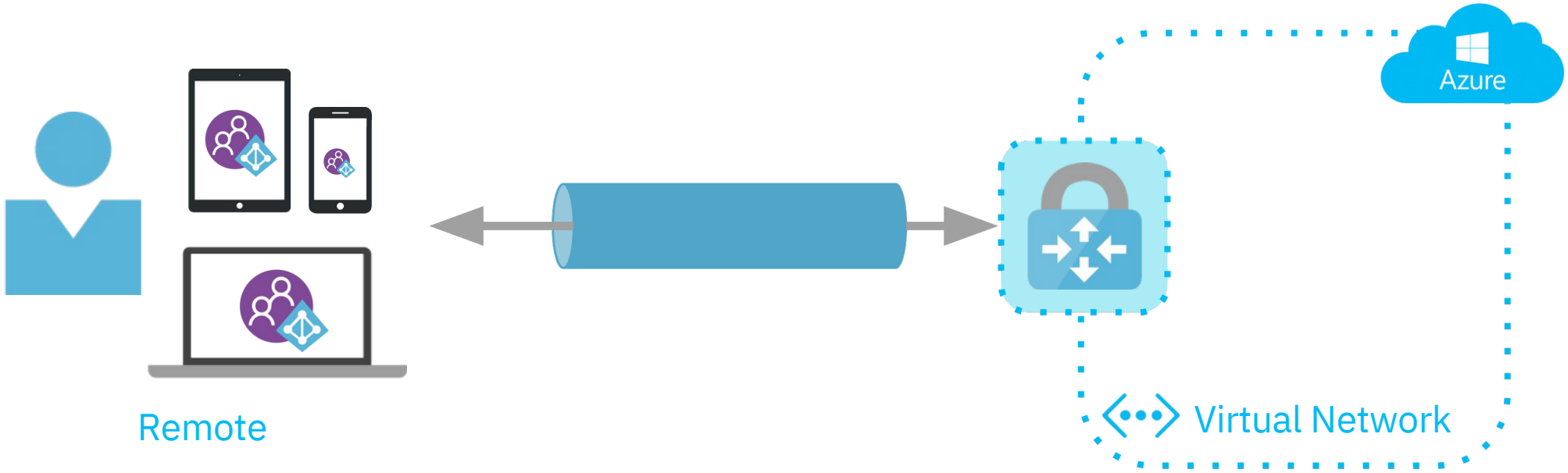
Point-to-Site VPNs

Azure certificate authentication



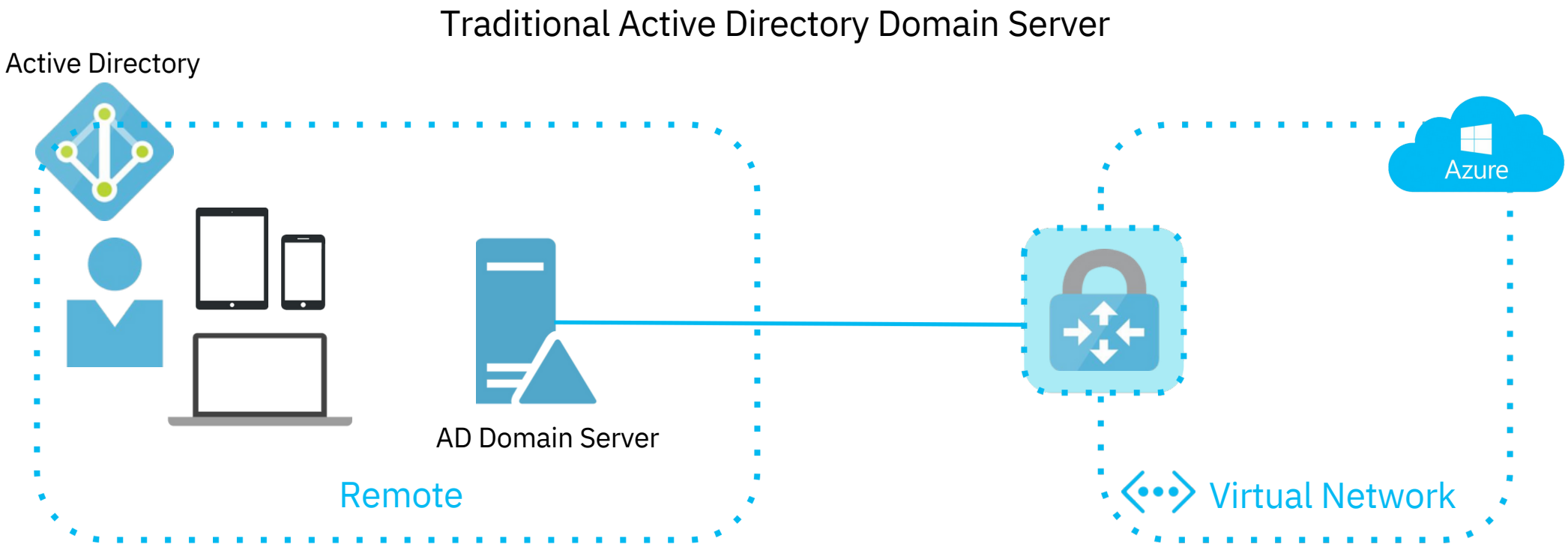
Point-to-Site VPNs

Azure AD authentication



This option is only supported for OpenVPN protocol.
Windows 10 will also require the use of the Azure VPN Client to make this work.

Point-to-Site VPNs

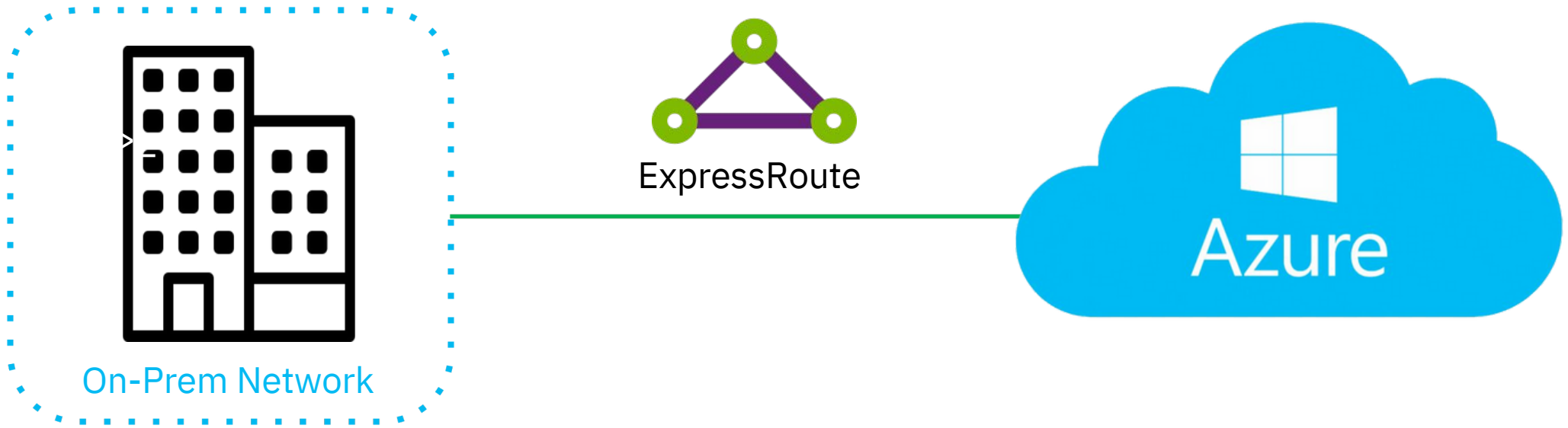


Point-to-Site VPNs

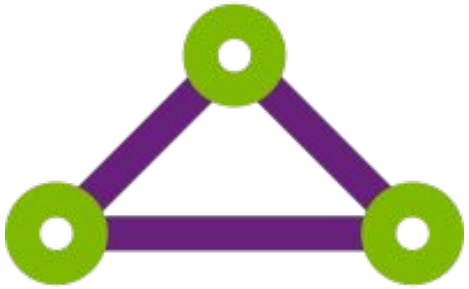
VPN Gateway Generation	SKU	S2S/VNet-to-VNet Tunnels	P2S SSTP Connections	P2S IKEv2/OpenVPN Connections	Aggregate Throughput Benchmark	BGP	Zone-redundant
Generation1	Basic	Max. 10	Max. 128	Not Supported	100 Mbps	Not Supported	No
Generation1	VpnGw1	Max. 30*	Max. 128	Max. 250	650 Mbps	Supported	No
Generation1	VpnGw2	Max. 30*	Max. 128	Max. 500	1 Gbps	Supported	No
Generation1	VpnGw3	Max. 30*	Max. 128	Max. 1000	1.25 Gbps	Supported	No
Generation1	VpnGw1AZ	Max. 30*	Max. 128	Max. 250	650 Mbps	Supported	Yes
Generation1	VpnGw2AZ	Max. 30*	Max. 128	Max. 500	1 Gbps	Supported	Yes
Generation1	VpnGw3AZ	Max. 30*	Max. 128	Max. 1000	1.25 Gbps	Supported	Yes
Generation2	VpnGw2	Max. 30*	Max. 128	Max. 500	1.25 Gbps	Supported	No
Generation2	VpnGw3	Max. 30*	Max. 128	Max. 1000	2.5 Gbps	Supported	No
Generation2	VpnGw4	Max. 30*	Max. 128	Max. 5000	5 Gbps	Supported	No
Generation2	VpnGw5	Max. 30*	Max. 128	Max. 10000	10 Gbps	Supported	No
Generation2	VpnGw2AZ	Max. 30*	Max. 128	Max. 500	1.25 Gbps	Supported	Yes
Generation2	VpnGw3AZ	Max. 30*	Max. 128	Max. 1000	2.5 Gbps	Supported	Yes
Generation2	VpnGw4AZ	Max. 30*	Max. 128	Max. 5000	5 Gbps	Supported	Yes
Generation2	VpnGw5AZ	Max. 30*	Max. 128	Max. 10000	10 Gbps	Supported	Yes

ExpressRoute

ExpressRoute



ExpressRoute



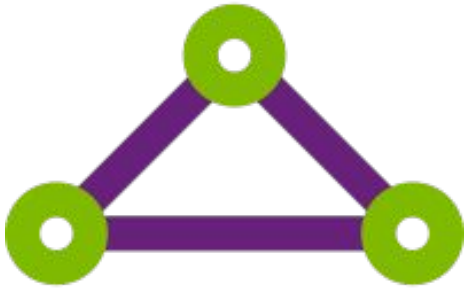
ExpressRoute

You can use ExpressRoute to establish connectivity from

- an any-to-any network
- a point-to-point Ethernet network
- a virtual cross-connection through a connectivity provider at a co-location facility

Connections made with ExpressRoute do NOT traverse the public internet.

ExpressRoute



ExpressRoute

Benefits:

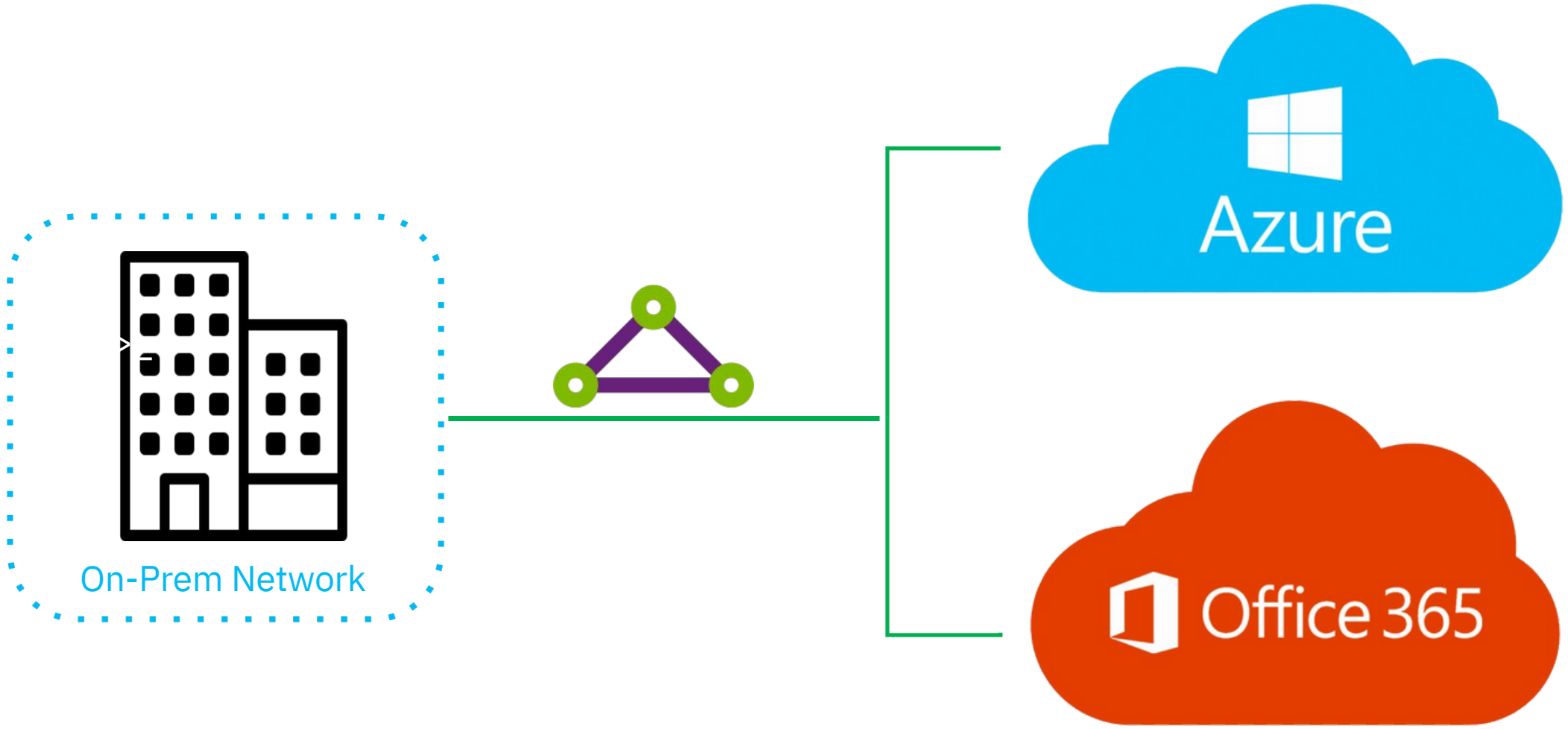
- connectivity to Microsoft cloud services across all regions within a geopolitical region

- Global connectivity achieved through using the ExpressRoute premium add-on

- dynamic routing between your on-prem networks and Microsoft via BGP
  high reliability
-

- connection uptime SLA of 99.95% for ExpressRoute dedicated circuit availability

ExpressRoute

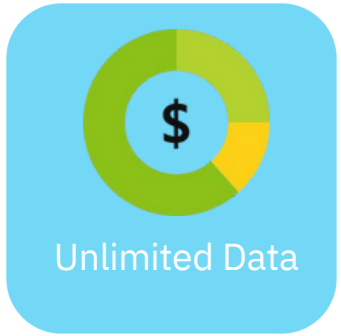


ExpressRoute

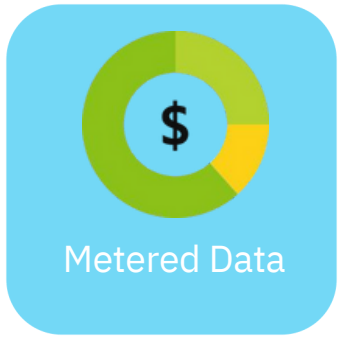
BANDWIDTH
50 Mbps
100 Mbps
200 Mbps
500 Mbps
1 Gbps
2 Gbps
5 Gbps
10 Gbps

You can increase the bandwidth of your ExpressRoute circuit without having to tear down existing connections.

ExpressRoute – Billing Models



- based on a monthly fee
- offers unlimited inbound and outbound transfer

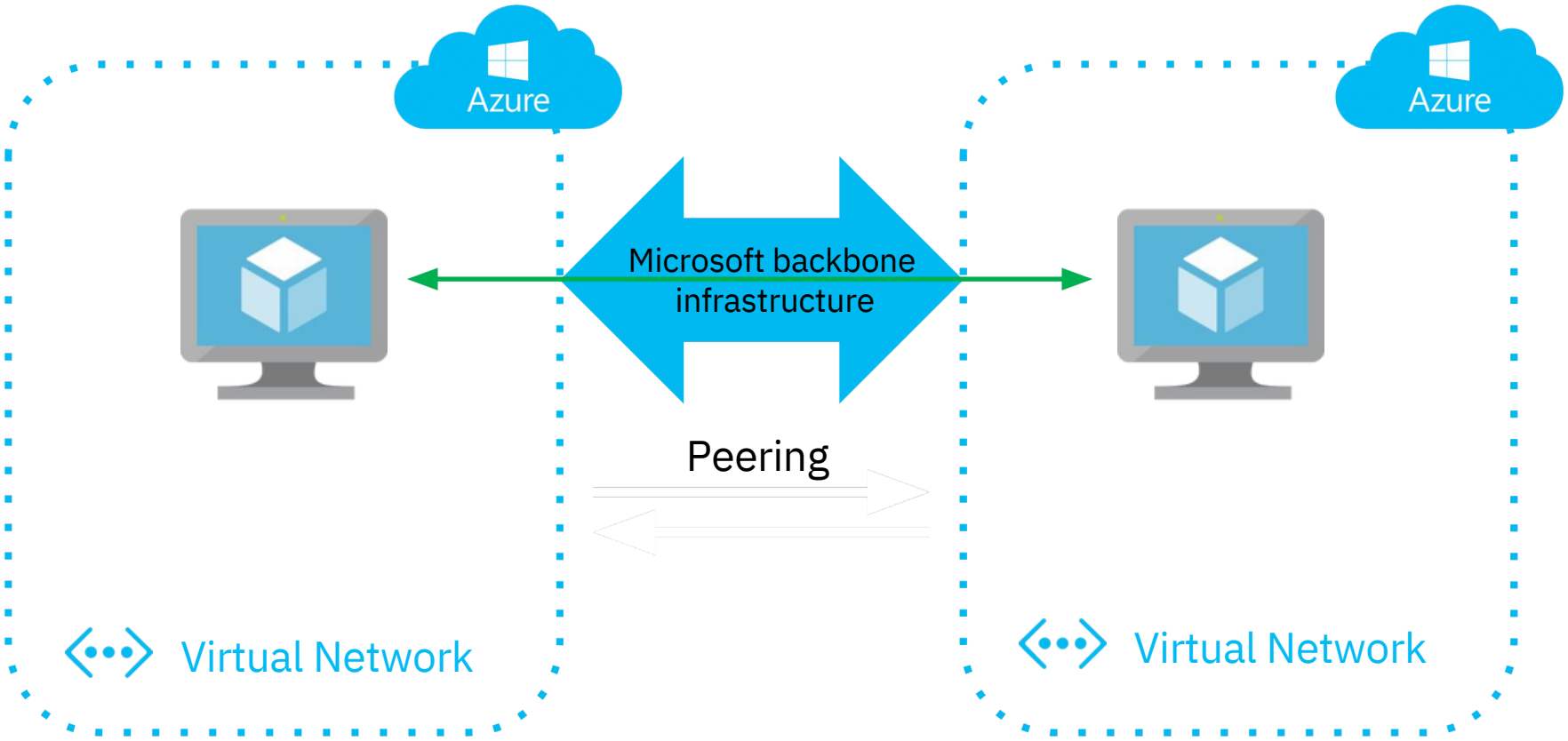


- based on a monthly fee
- all inbound data transfer is included free of charge
- outbound data transfers are charged on a “per-GB” basis

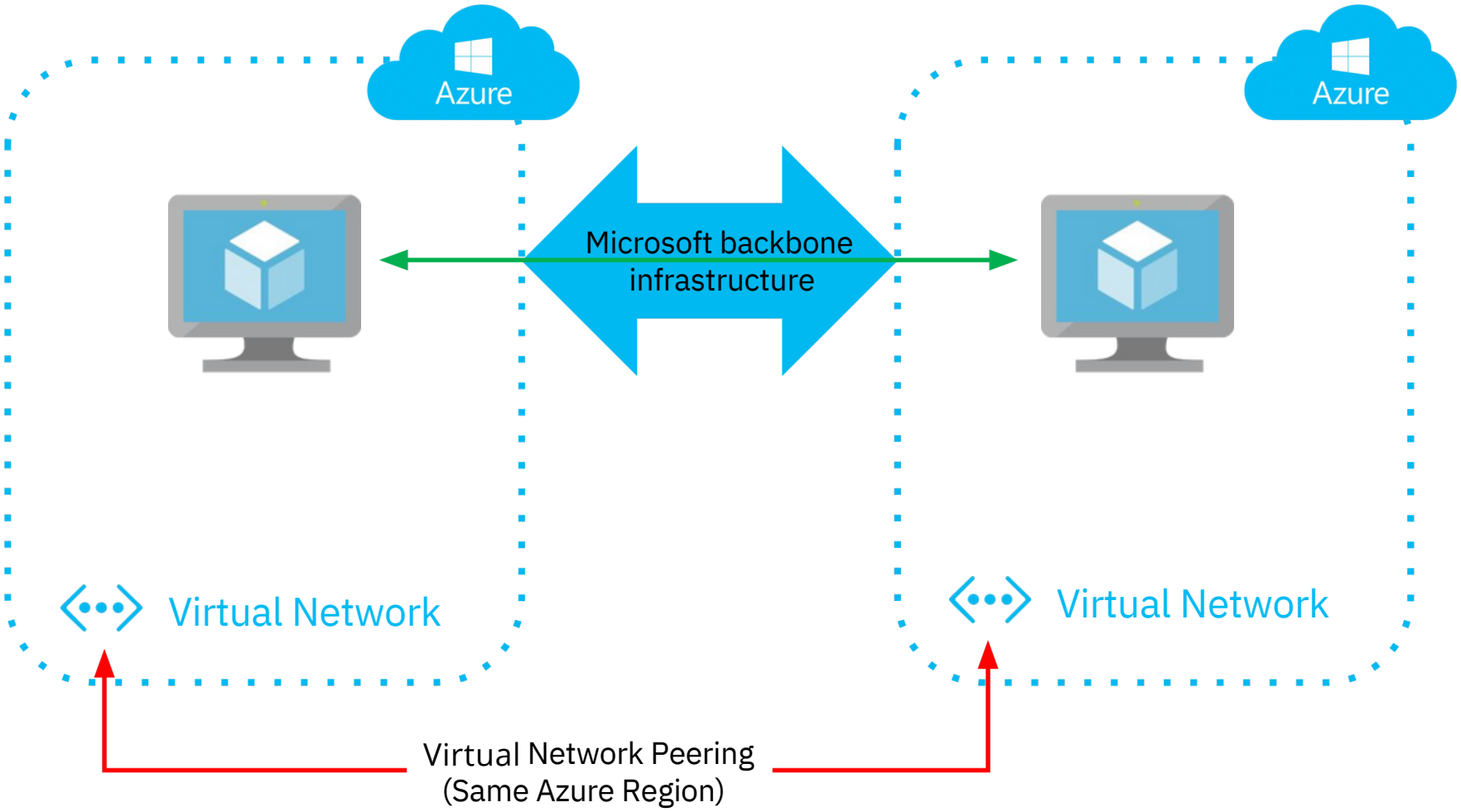
- a paid add-on
- number of route limits for Azure public and private peering increased to
- 10,000 routes
- global connectivity across any region except for the national clouds number of vNet links per circuit increased from 10 to a larger limit determined by the bandwidth of the circuit that you purchase

vNet Peering

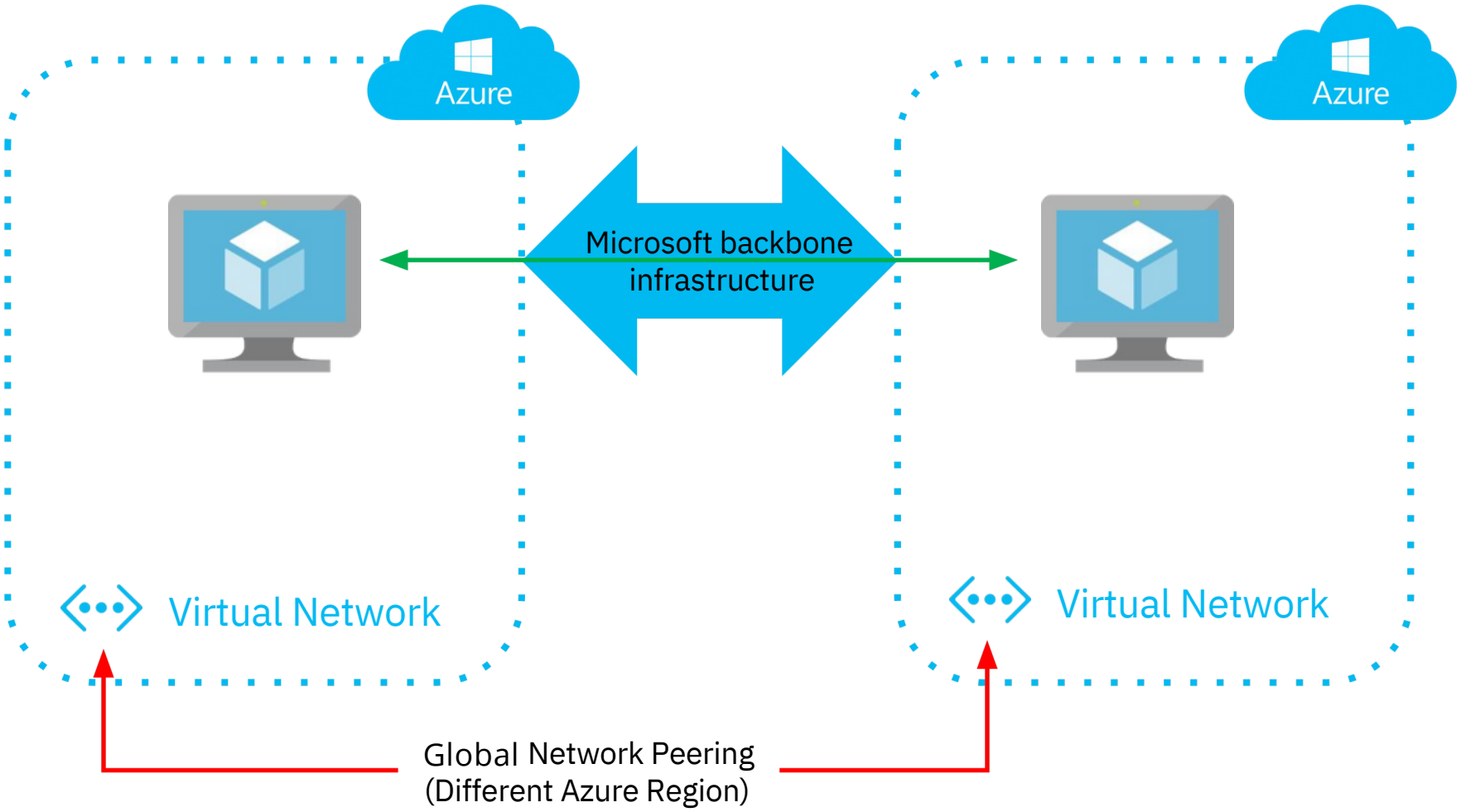
vNet Peering



vNet Peering



vNet Peering



vNet Peering

- low-latency, high-bandwidth connectivity between Azure resources that are connected to different virtual networks

- facilitates data transfer across different virtual networks, even when they are in different Azure subscriptions, Azure Active Directory tenants, and Azure regions

- enables you to connect virtual networks that were created through the Azure Resource Manager

Any Questions?

- Your feedback is important to us.