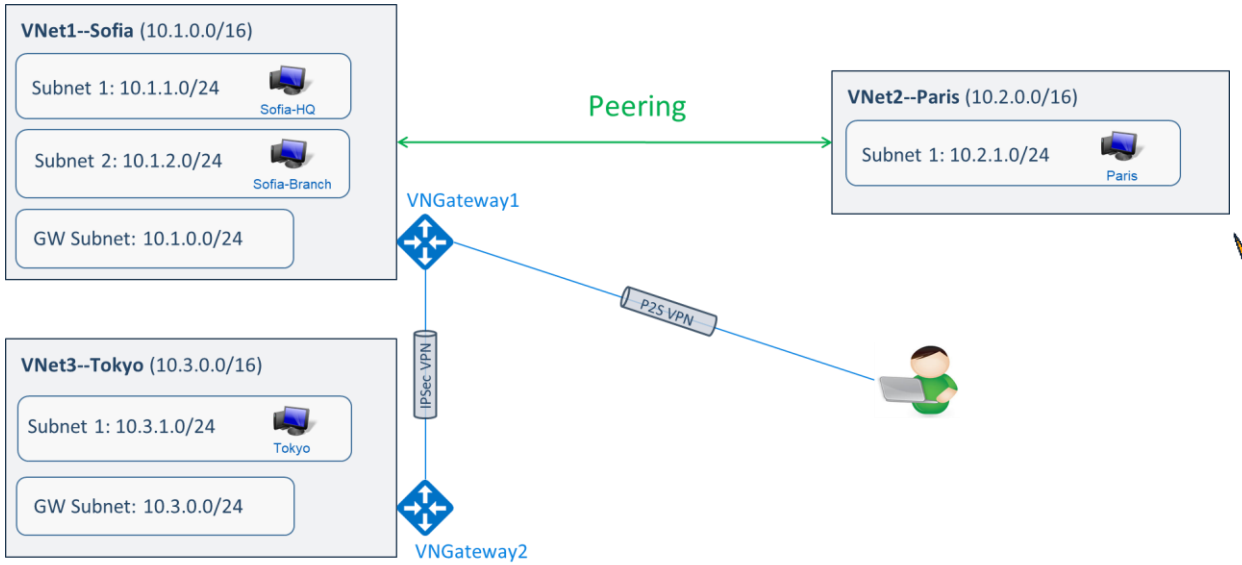
Cloud Networking with Microsoft Azure

Lecture 12



SoftUni Team

Technical Trainers

Software University

SoftUni

Software University

https://softuni.bg

Table of Contents

Have a Question?

Software University

sli.do

#CNA

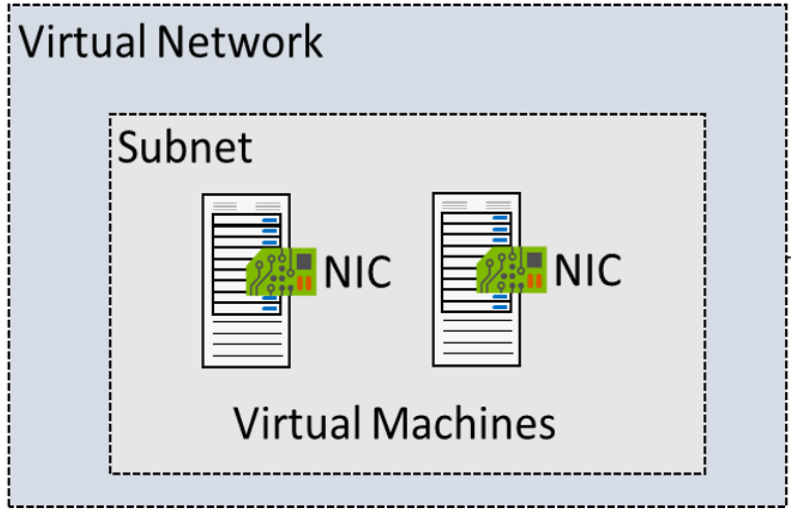
Introduction to Azure Networking

Azure Networking Components

- Virtual networks ★
- Front Door and CDN profiles
- Network interfaces
- Route tables
- Service endpoint policies
- Private Link
- DNS zones
- NAT gateways
- Firewall Policies
- Local network gateways
- Network security groups (classic)
- Azure Synapse Analytics (private link hubs)
- Network Watcher
- Public IP addresses
- Application security groups
- Private DNS zones ★
- Virtual WANs
- Traffic Manager profiles
- IP Groups
- Firewalls
- Virtual network gateways ★
- Virtual networks (classic)
- Load balancers
- Network security groups
- Public IP Prefixes
- DDoS protection plans
- Web Application Firewall policies (WAF)
- Bastions
- Application gateways
- Firewall Manager
- Connections
- Route Servers
- Reserved IP addresses (classic)

Virtual Networks in Azure (VNets)

- VNets are logical representation of your own network, they let you create your own private space in Azure
- The traffic between virtual machines in a VNet uses the Microsoft backbone infrastructure

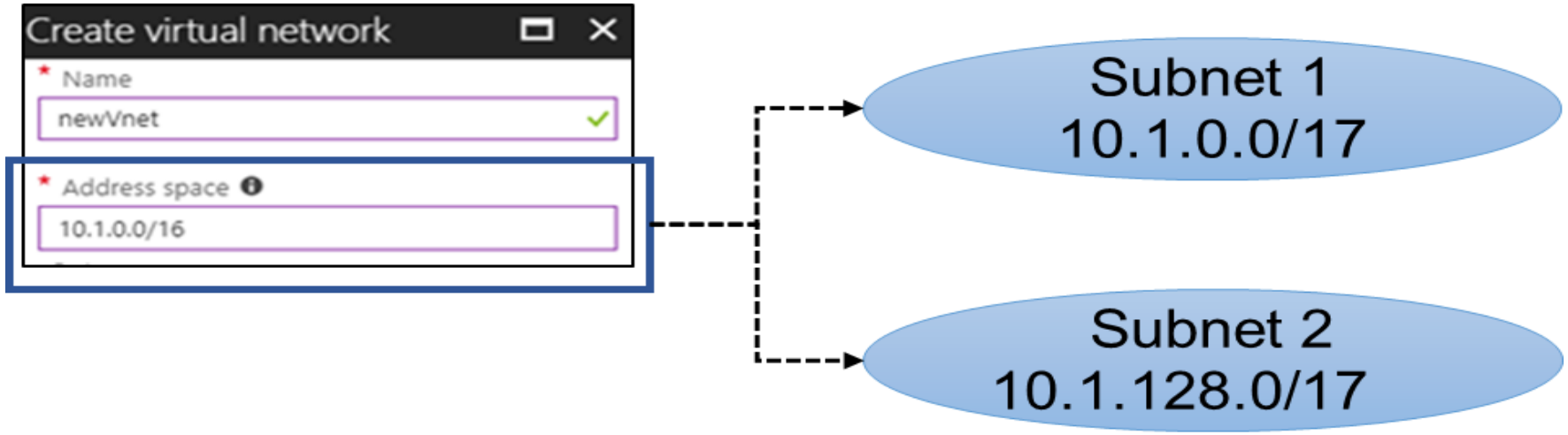


Creating a Virtual Network

Setting	Value
Name	Enter *myVirtualNetwork*.
Address space	Enter *10.1.0.0/16*.
Subscription	Select your subscription.
Resource group	Select **Create new**, enter *myResourceGroup*, then select **OK**.
Location	Select **East US**.
Subnet - Name	Enter *myVirtualSubnet*.
Subnet - Address range	Enter *10.1.0.0/24*.

Subnets

- A virtual network can be segmented into one or more subnets
- Subnets provide logical divisions within your network
- Benefits of subnetting a virtual network include security and performance
- Each subnet must have a unique address range - cannot overlap with other subnets in the virtual network in the subscription



IP Addressing

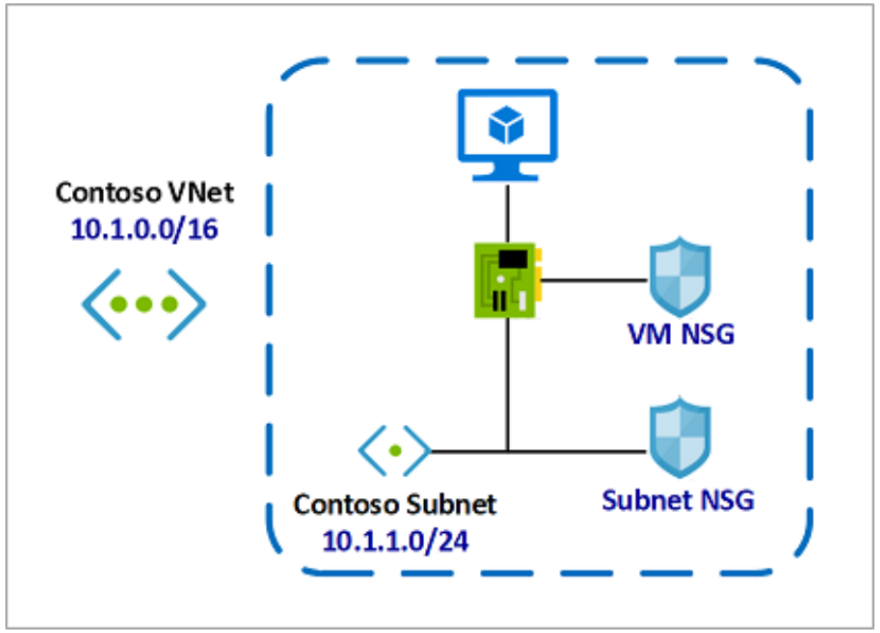
- There are two types of IP addresses you can use in Azure:
  - **Public IP addresses**: Used for communication with the Internet, including Azure public-facing services
  - **Private IP addresses**: Used for communication within an Azure virtual network (VNet), and your on-premises network (if you use VPN gateway or ExpressRoute)
- Remember the private IP address ranges?

IP Addressing

- For the private addresses, Azure reserves the first four in each subnet address range
- Allocation methods (for both public and private IP addresses)
  - **Dynamic**
  - **Static**
- Even the selected allocation method is "static", you should avoid assigning IP addresses within the virtual machine's operating system

Network Security Groups (NSG)

- You can limit network traffic to resources in a virtual network
- An NSG contains a list of security rules that allow or deny inbound or outbound network traffic
- An NSG can be associated to a subnet or a network interface
- Similar to Access Control Lists discussed before



NSG Rules

- Security groups have default inbound and outbound rules and you can add custom ones
- Rules are processed in priority order. The lower the number, the higher the priority
- To match a traffic, specify port, protocol, source and destination
- After the traffic is matched, an action is applied (allow or deny) and then processing stops

Inbound security rules

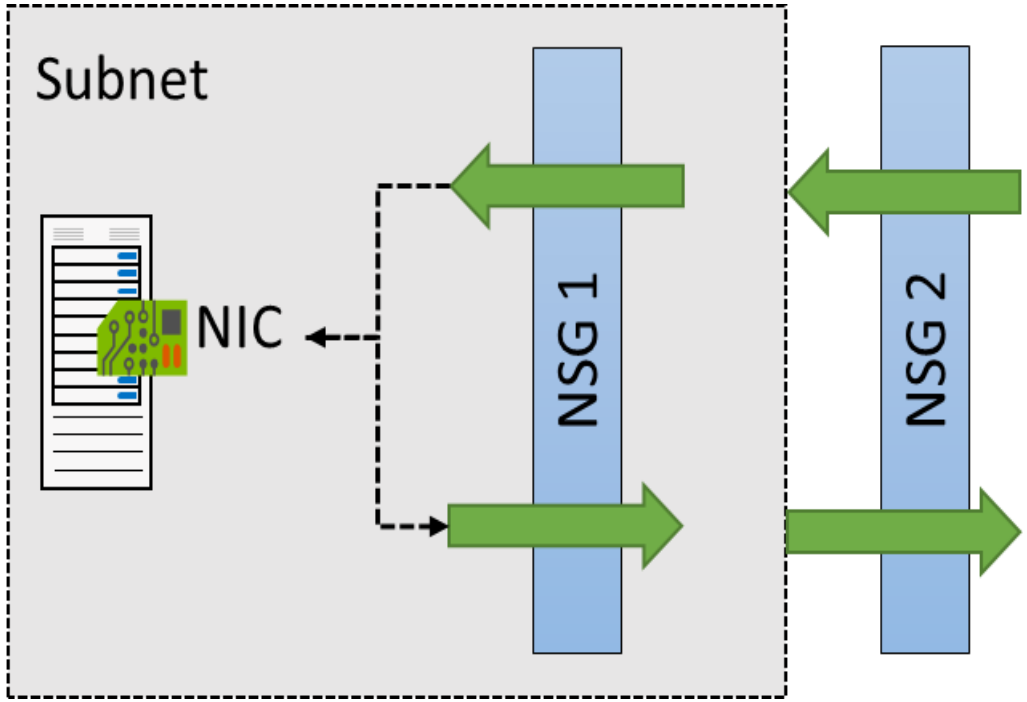
Priority	Name	Port	Protocol	Source	Destination	Action
300	RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

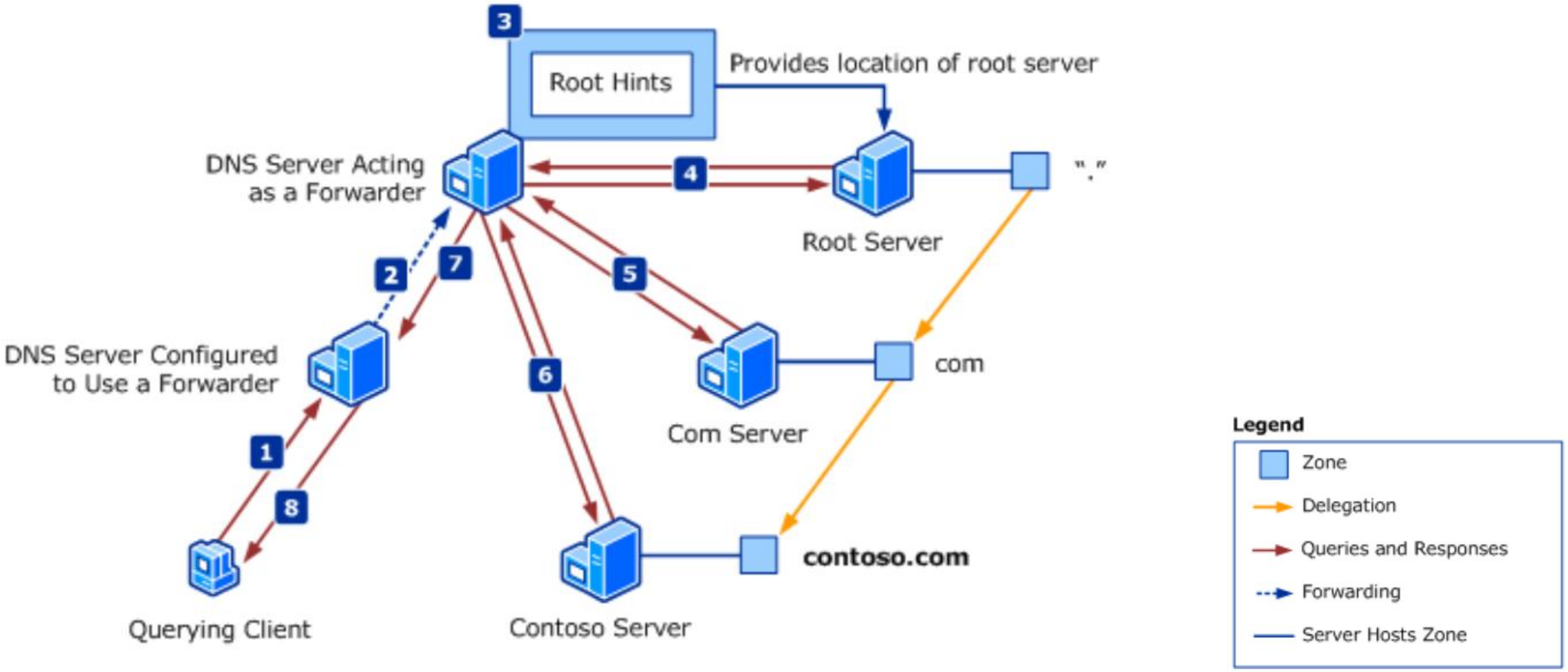
NSG Effective Rules

- NSGs are evaluated independently for the subnet and NIC
- Use the Effective Rules link if you are not sure which security rules are being applied



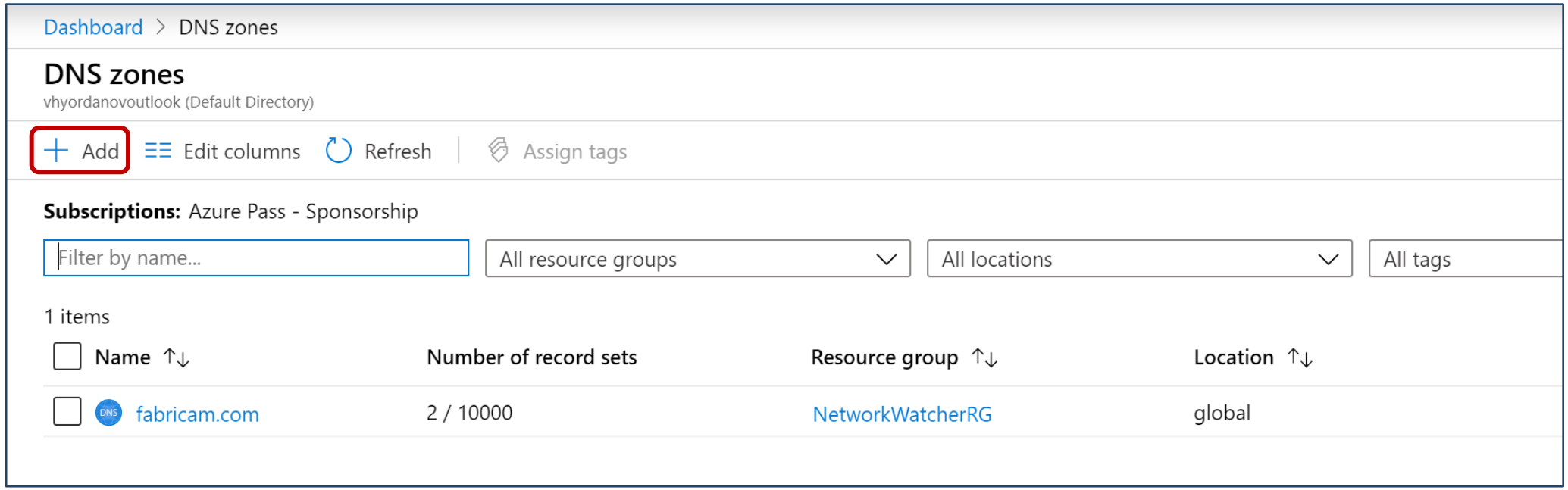
DNS Hosting in Azure

Remembering How DNS Works



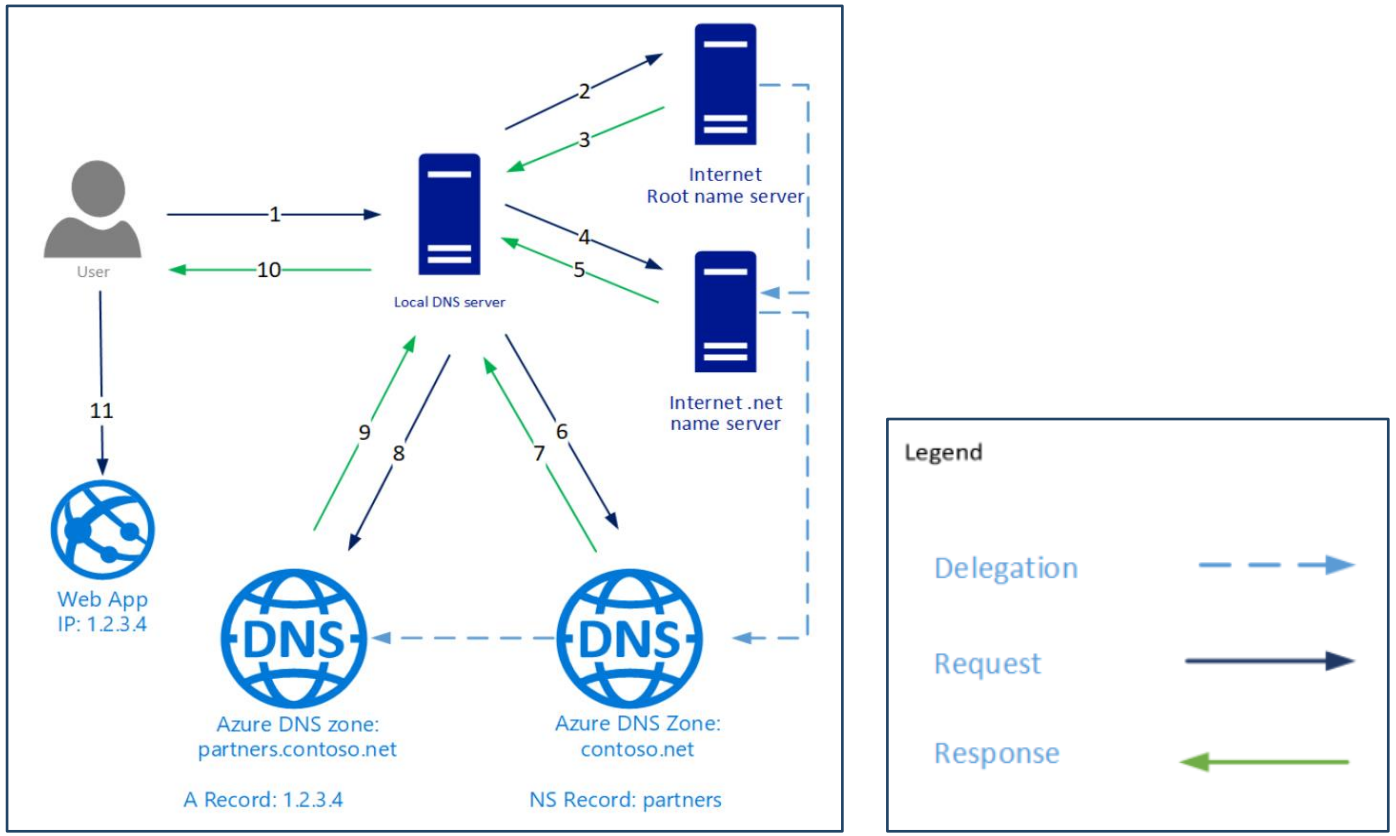
Azure DNS Zones

- Azure offers a DNS service where you can host your DNS zones
- You do not have to own the domain to create a DNS zone with that domain name in Azure
- But…if you want the records in your domain to be resolved by everyone in Internet, then:
  - You must own the domain
  - You must change the name servers in your domain register to point to your Azure DNS zone



DNS Delegation

- For DNS queries to a domain to reach Azure DNS, the domain must be delegated to Azure DNS from the parent (point the name servers to the "child", hosting the zone)



DNS Record Sets

- Inside a DNS zone, you create DNS records
- Some examples of common DNS records:

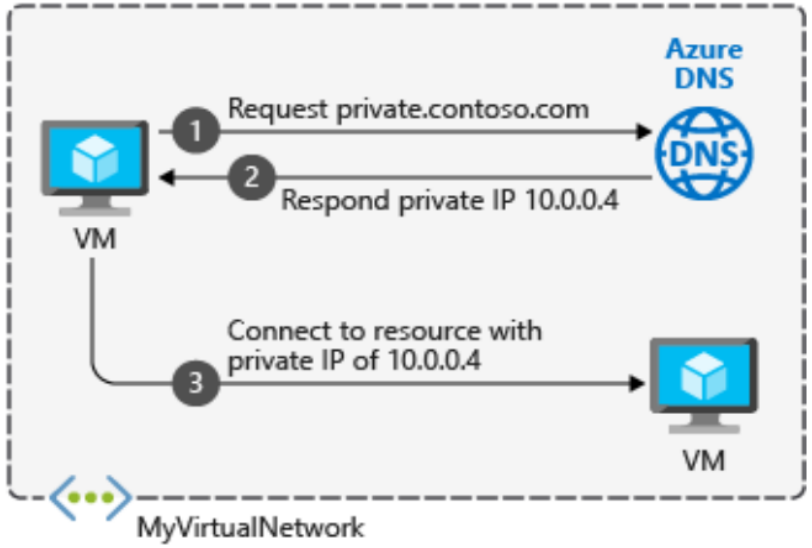
A: a name which points to an IPv4 address	**SRV**: used for service discovery
CNAME (alias): a name which points to another name	**NS**: shows which are the name servers for the zone
MX: shows who is the mail server for that domain	**SOA**: contains administrative information about the zone

- In Azure, DNS records are created in record sets (inside a zone)
- A record set is collection of DNS records which have the same name and are of the same type: (although most record sets contain a single record)

```
www.contoso.com.        3600    IN    A    134.170.185.46
www.contoso.com.        3600    IN    A    134.170.188.221
```

Private DNS Zones

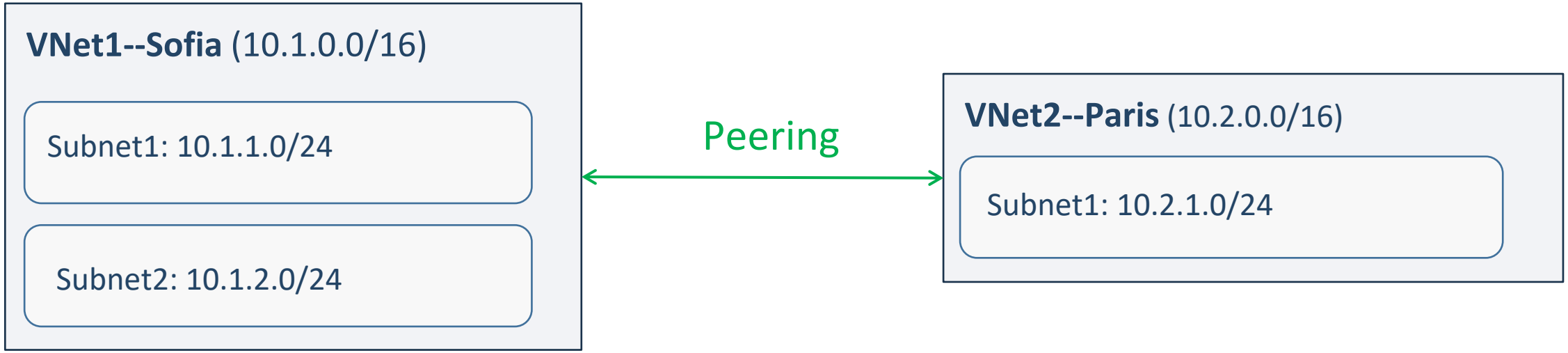
- Private DNS zones provide name resolution in virtual networks without the need to add a custom DNS solution
- Not accessible over the Internet
- Capabilities and benefits:
  - All common DNS records types are supported
  - Hostname resolution between virtual networks
  - Automatic hostname record management
  - Available in all Azure regions
- When you create a Private DNS zone, you have to link it with one or more virtual networks



Inter-site Connectivity Options

Virtual Network Peering

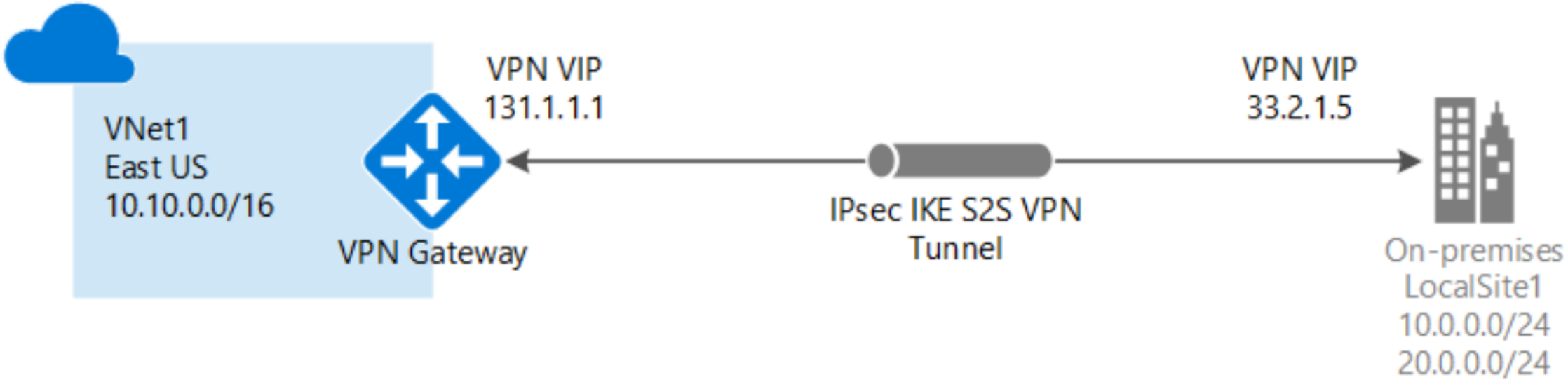
- VNet peering connects two Azure virtual networks
- Peered networks use the Azure backbone for privacy and isolation
- Easy to setup, seamless data transfer and great performance



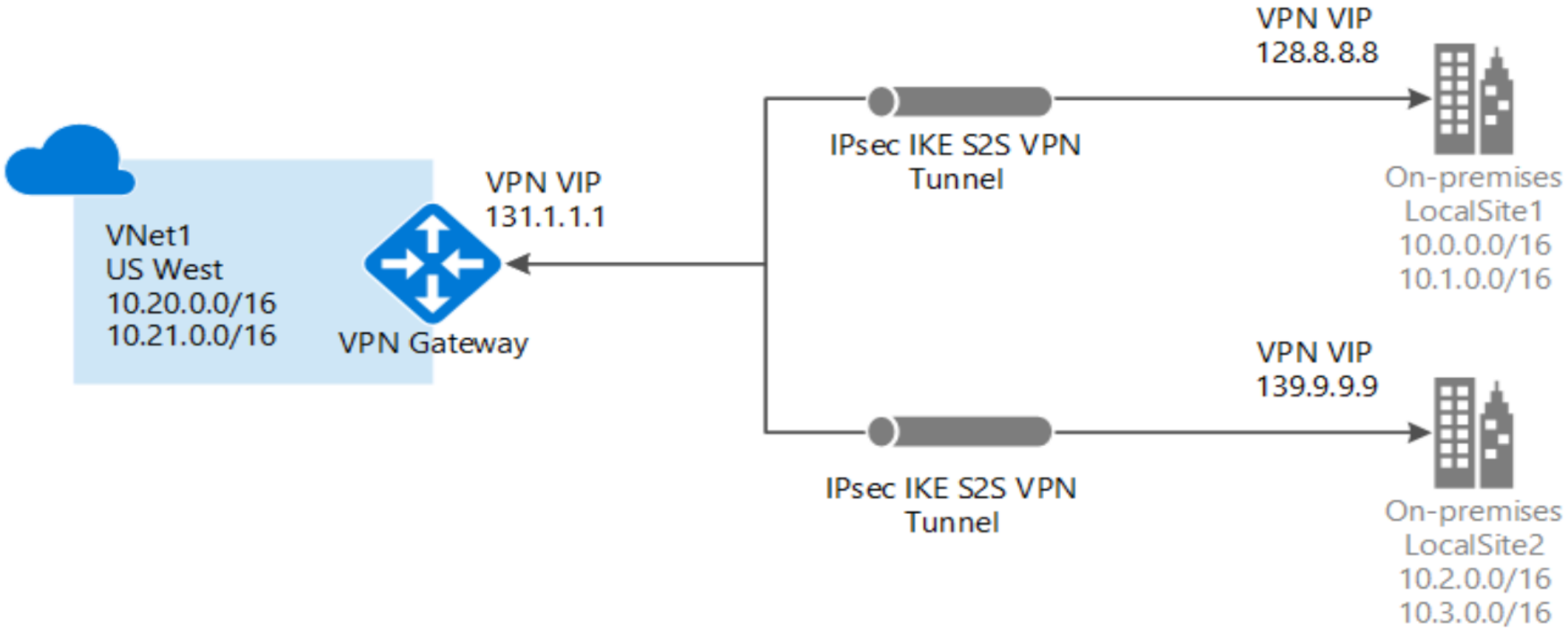
VPN Gateway

- Used to send encrypted traffic between Azure and on-premise
- Can also create tunnels between Azure virtual networks
- Can accept multiple connections
- Each VNet can have only one VPN gateway
- Special VNet subnet is required before creating the VPN gateway
- Different connection topology diagrams are supported (next slides)

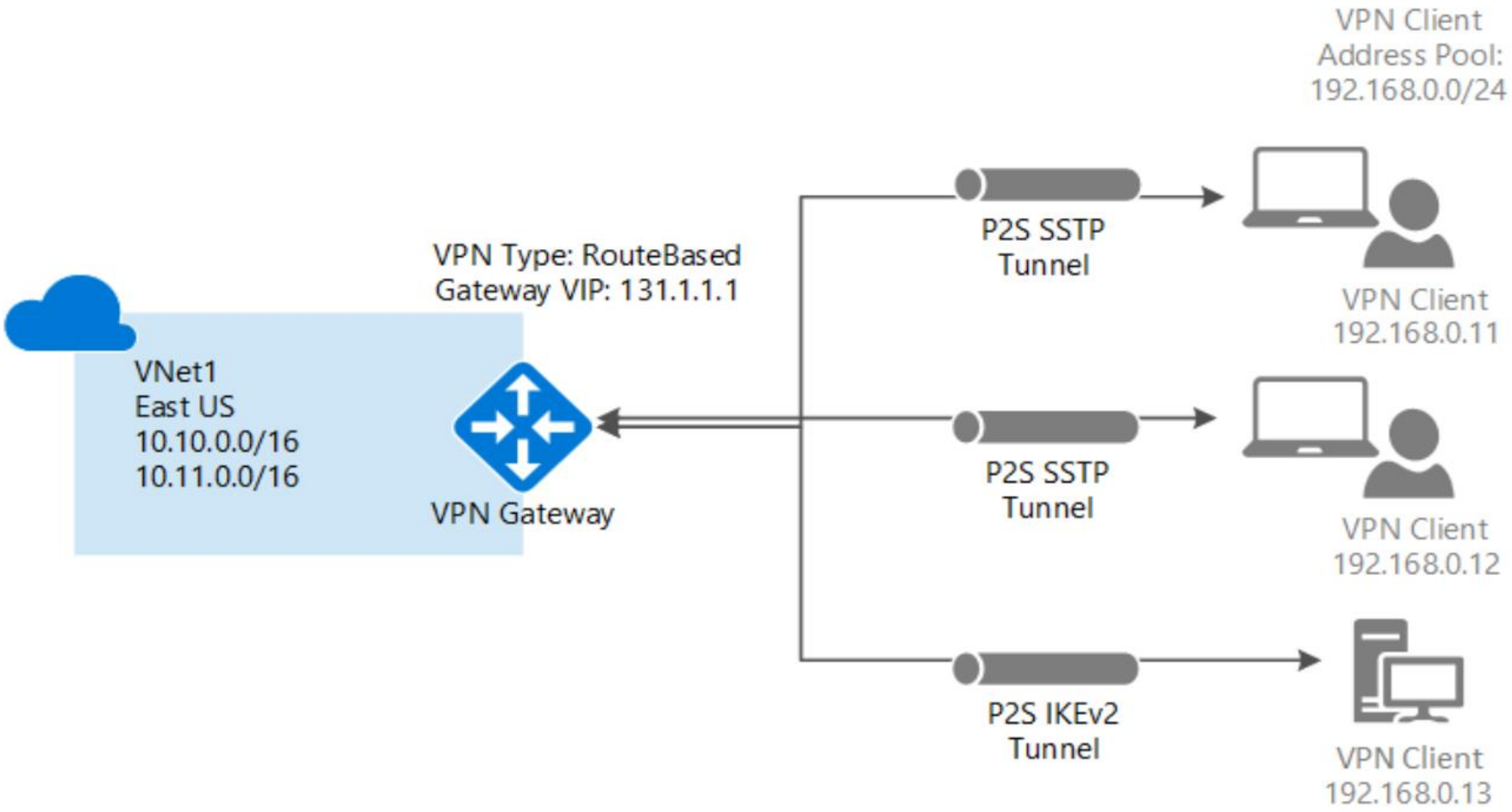
Site-to-Site (IPsec/IKE VPN Tunnel)



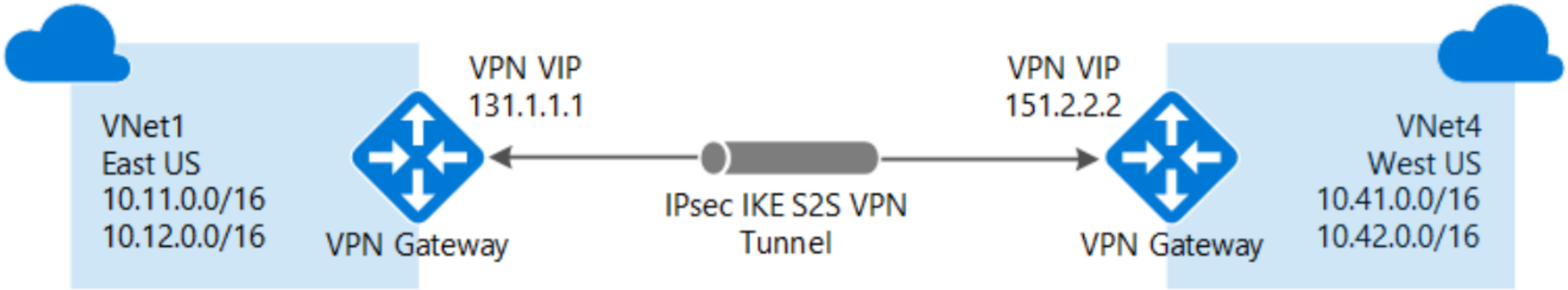
Multi-Site (IPsec/IKE VPN Tunnel)



Point-to-Site (VPN Over IKEv2 or SSTP)

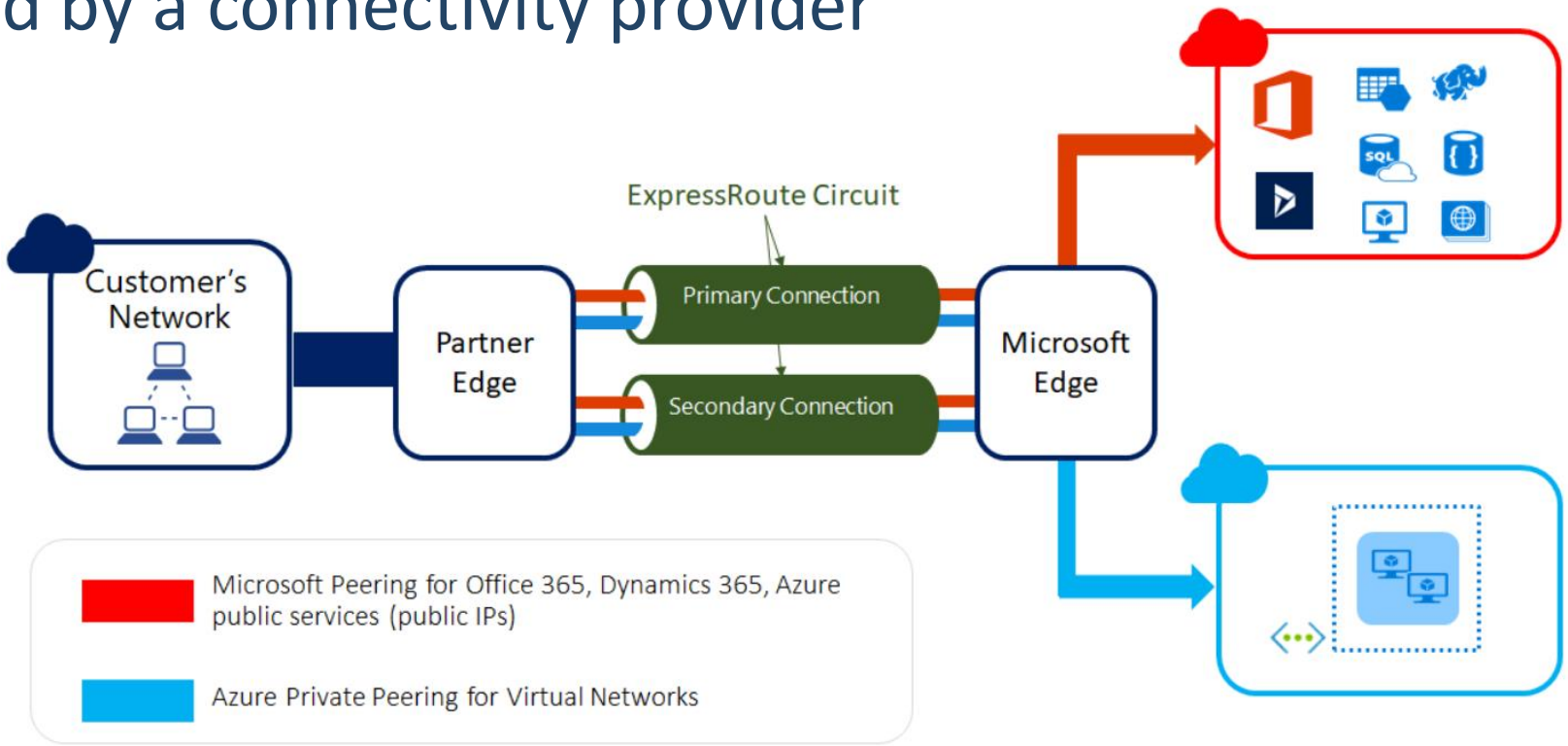


VNet-to-VNet Connections (IPsec/IKE VPN Tunnel)



ExpressRoute

- Let's you extend your on-premises networks into the Microsoft cloud over a private connection
- Facilitated by a connectivity provider



Virtual Network Traffic Routing

System Routes

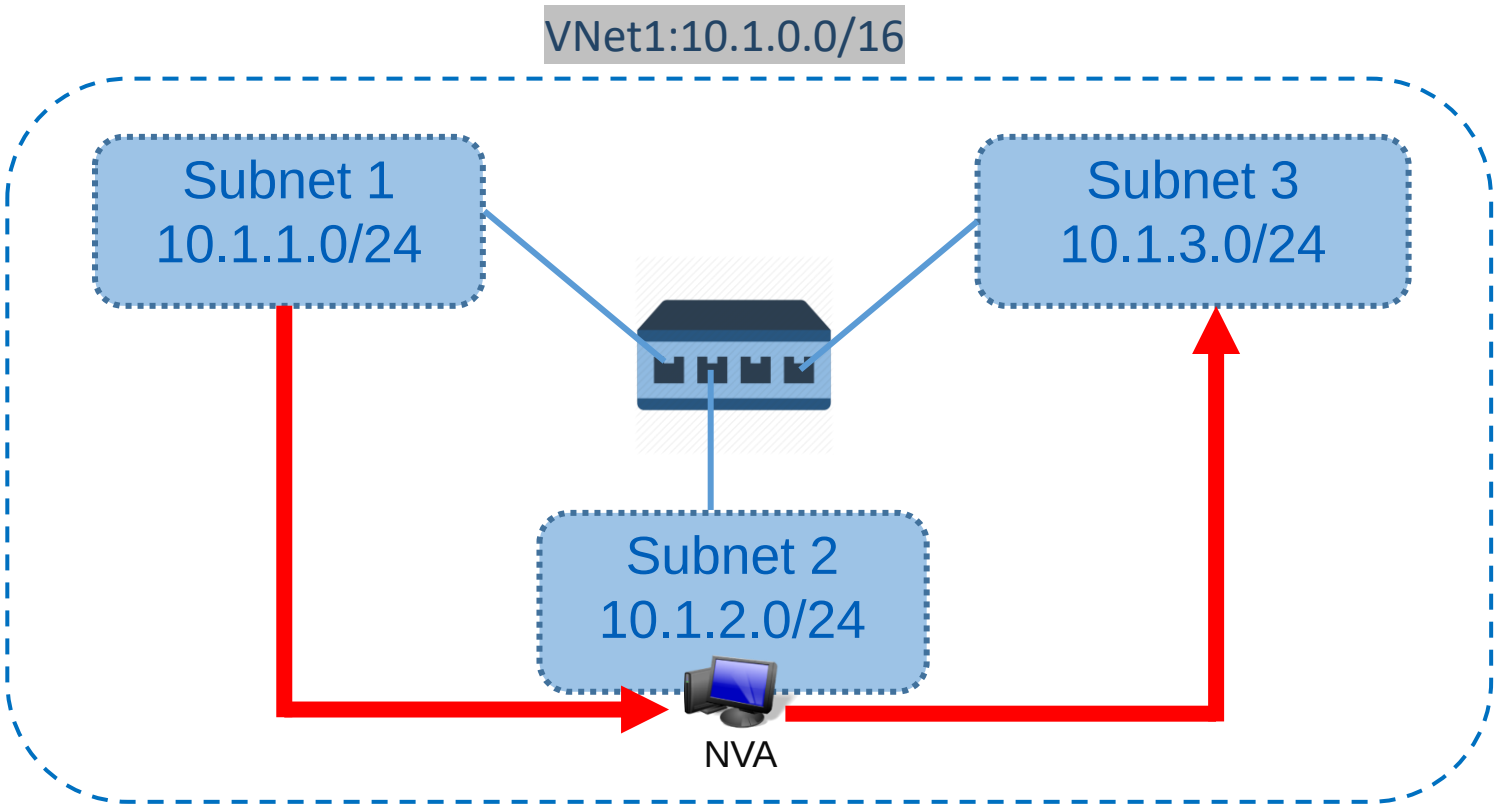
- System routes direct network traffic between virtual machines, on-premises networks and the Internet:
  - Traffic between VMs in the same subnet
  - Between VMs in different subnets in the same virtual network
  - Data flow from VMs to the Internet
  - Communication between VMs using a VNet-to-VNet Peering
  - Communication between VMs using a VNet-to-VNet VPN
  - Site-to-Site and ExpressRoute communication through the VPN gateway

User-defined Routes (UDR)

- You can create custom (user-defined) routes in Azure to override Azure's default system routes, or to add additional routes to a subnet's route table
- User-defined routes control network traffic by defining routes that specify the next hop of the traffic flow
- A route table contains a set of rules, called routes, that specifies how packets should be routed in a virtual network
- The next hop can be:
  - Virtual appliance
  - Virtual Network Gateway
  - Virtual Network
  - Internet
  - None

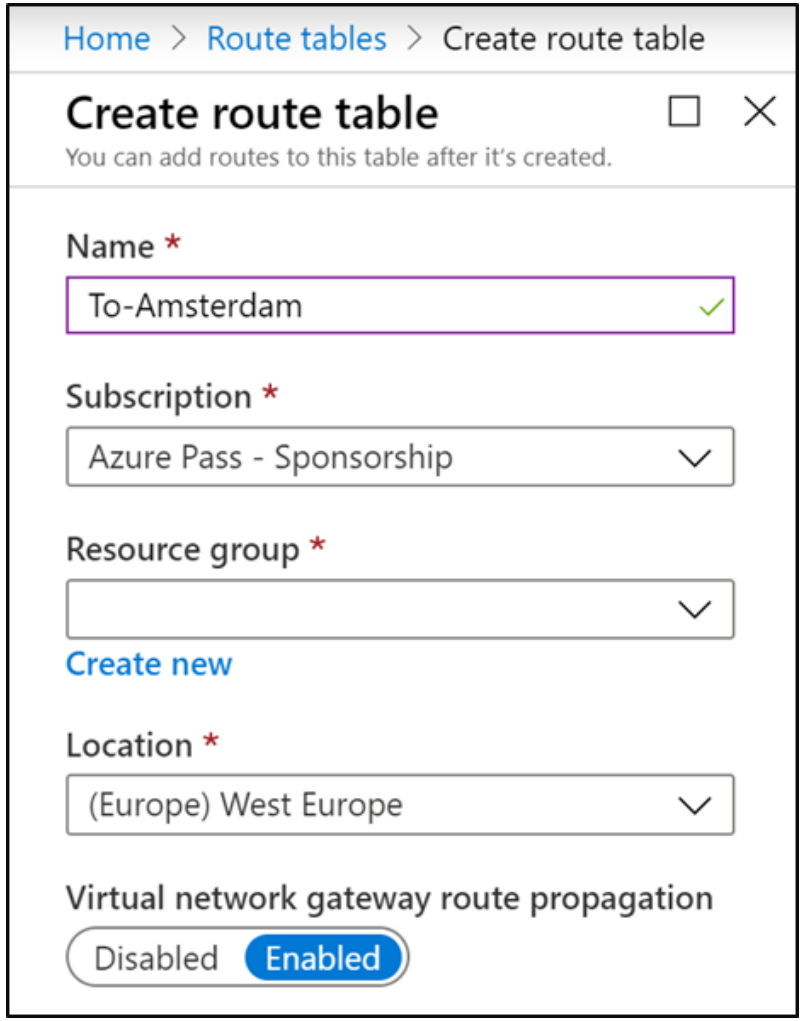
Routing Example

- Before the UDR, system routes connects VMs from each subnet directly
- After a UDR is created, the routing table for Subnet 1 is updated so the traffic goes via the Virtual appliance in Subnet 2



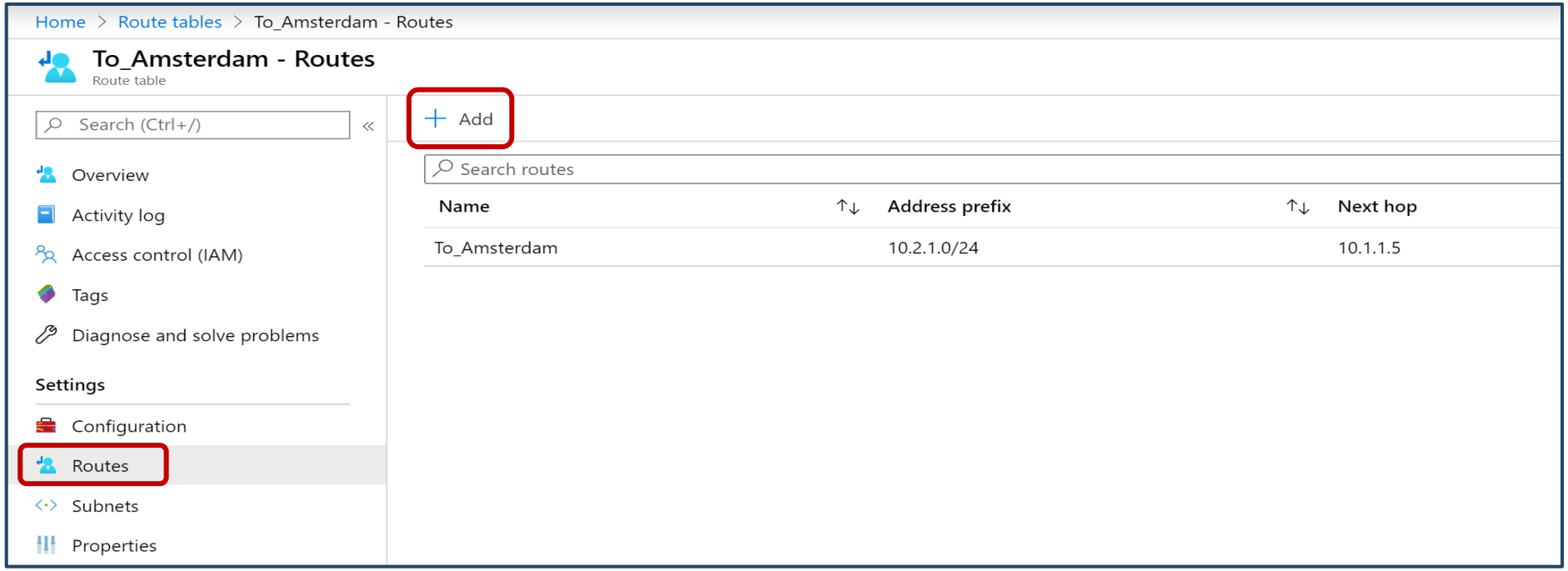
Creating a Route Table

- The first thing for a UDR is to create a route table
- Create a name and select subscription, resource group and location
- "Virtual network gateway route propagation" should be enabled if you want your on-premises routes to be propagated to the subnet



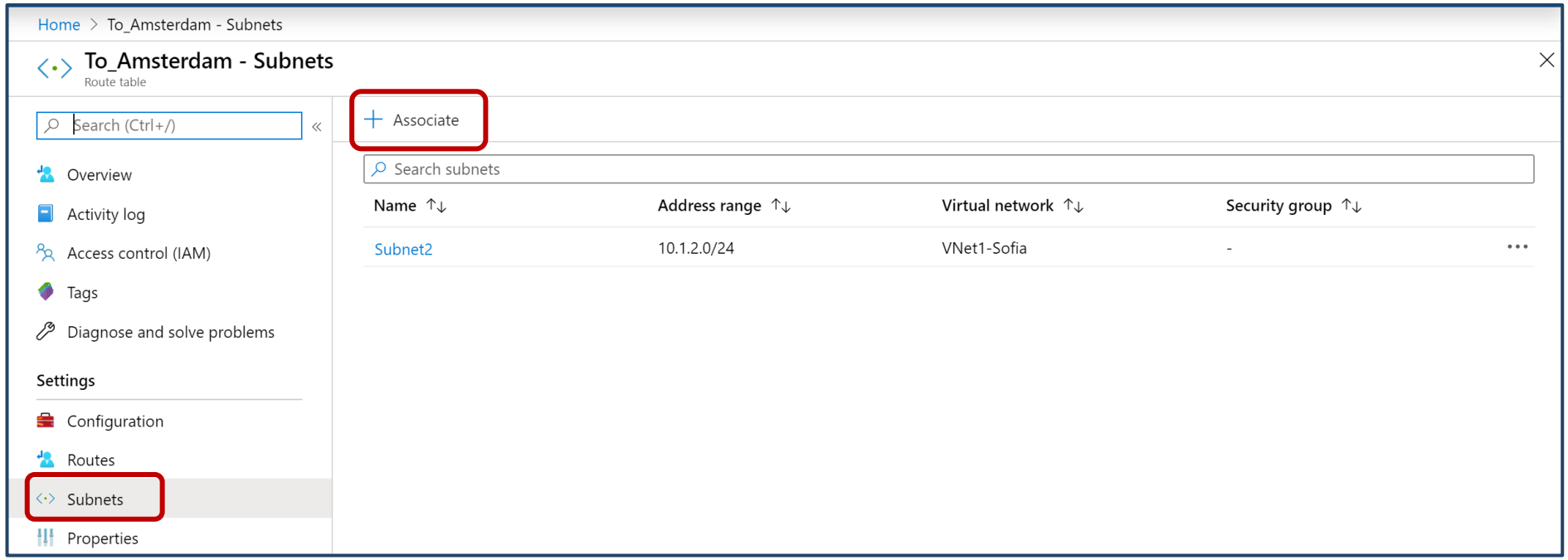
Creating a Custom Route

- The second thing is to create a route in your routing table
- The custom route specifies:
  - Where do you want to route your traffic to? (the "Address prefix" section in CIDR format)
  - How to go there? (the "Next hop type")



Associate the Route Table

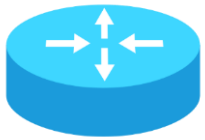
- Finally, associate the route table with a subnet(s)
- Each route table can be associated with multiple subnets, but one subnet can be associated with a maximum one route table



How Azure Selects a Route

When there are overlapping subnets, Azure uses the rule of the longest match

My routing table:
192.168.0.0/16 via 10.1.1.1
192.168.5.0/24 via 10.15.15.1
0.0.0.0/0 via 10.32.32.1



How do I reach 192.168.5.18?

Answer: via 10.15.15.1

How do I reach 192.168.12.6?

Answer: via 10.1.1.1

How do I reach 4.3.2.1?

Answer: via 10.32.32.1

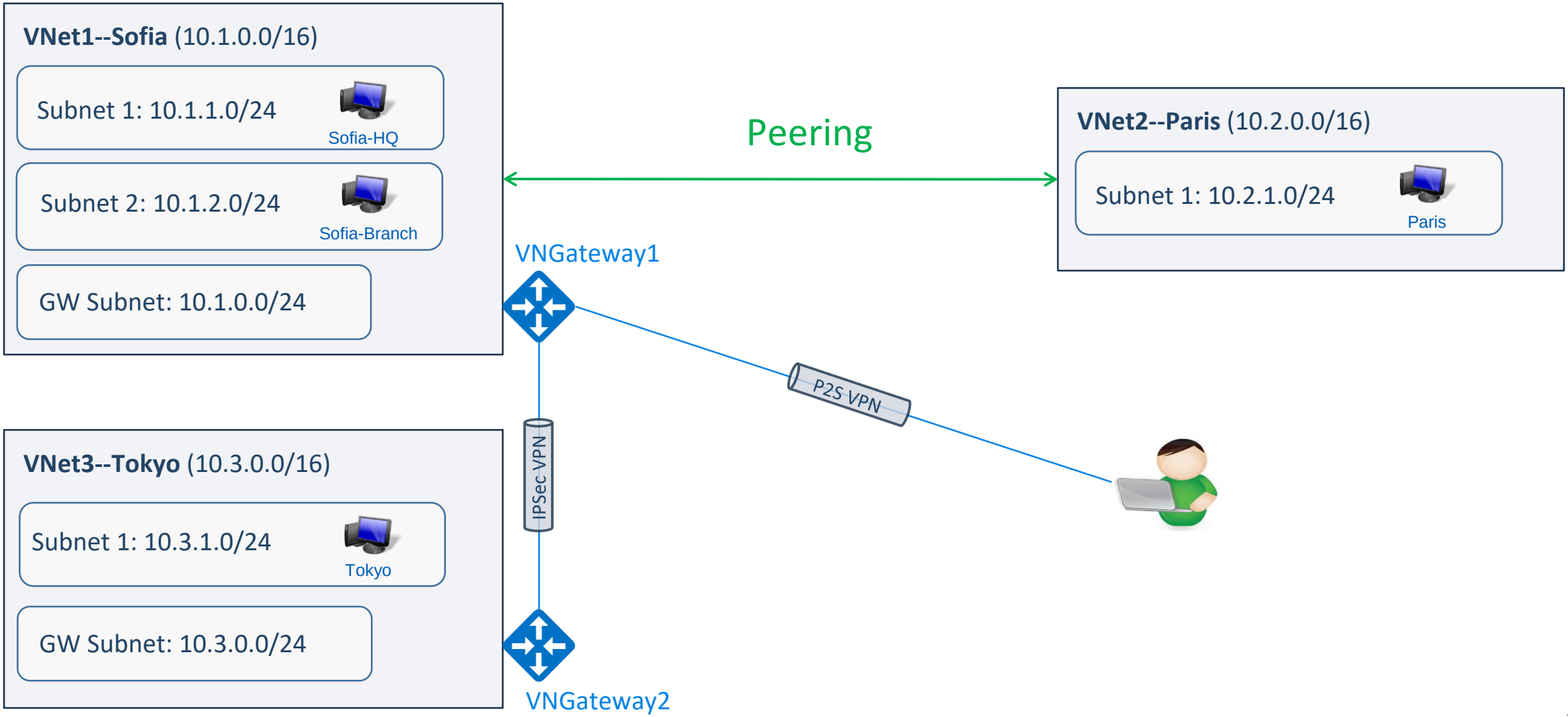
How Azure Selects a Route (2)

- If multiple routes contain the same address prefix, Azure selects the route type based on the following priority:
  1. User-defined route
  2. System route
- Example:

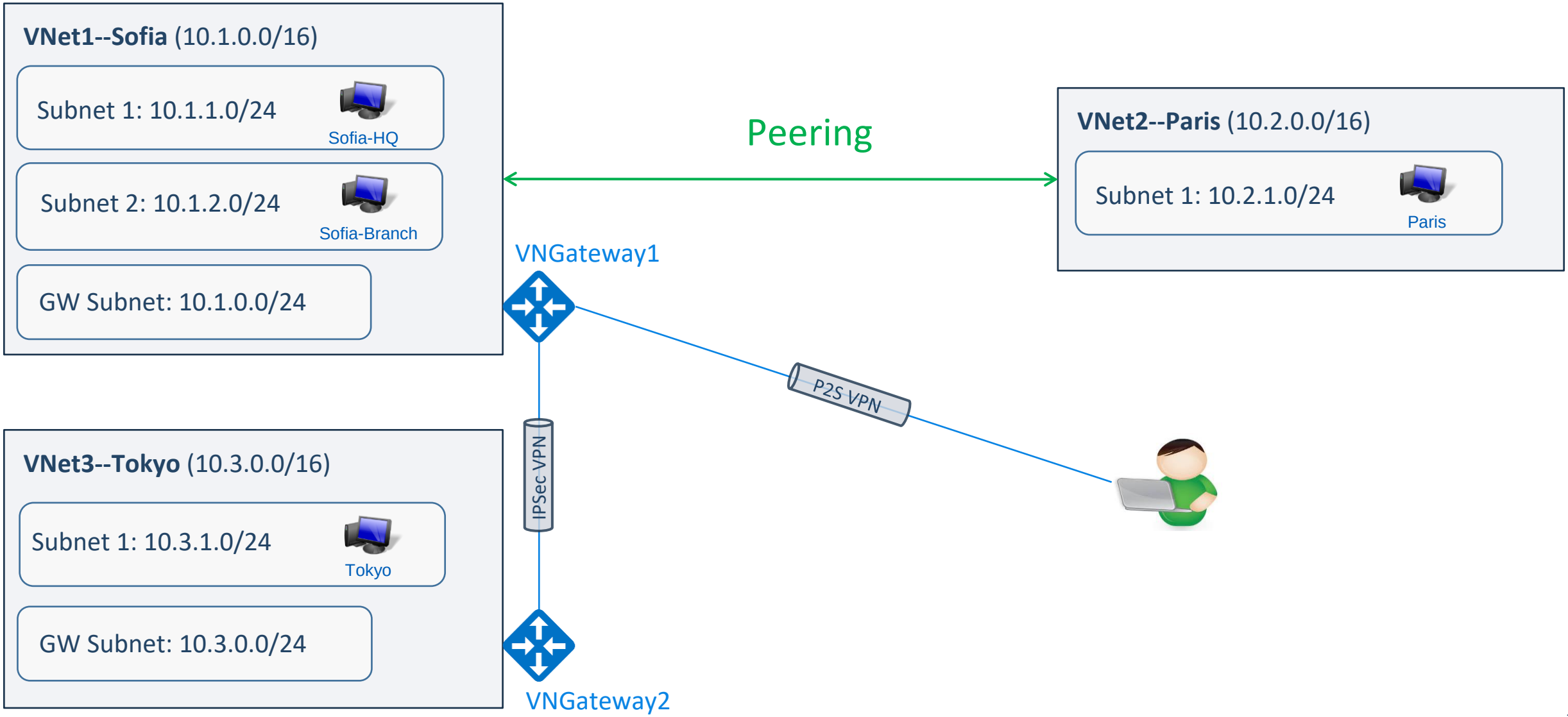
Source	Address prefixes	Next hop type
Default	0.0.0.0/0	Internet
User	0.0.0.0/0	Virtual network gateway

Demonstration

Demonstration Topology



Demonstration Topology (no animations)



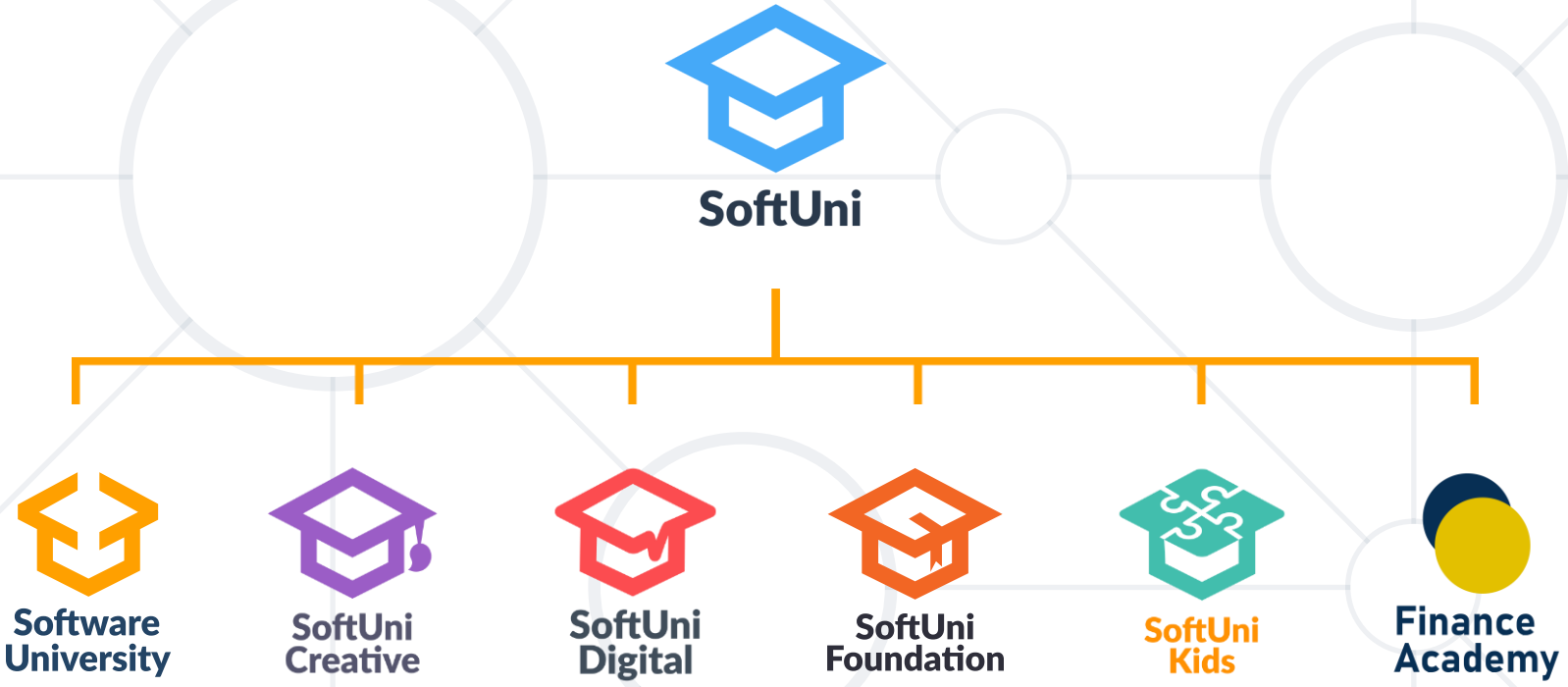
Demonstration Details

1. Create the VNets, subnets and gateways and attach the respective VMs
2. Create a private DNS zone and link it with all VNets
3. Create a peering between **VNet1--Sofia** and **VNet2--Paris**
4. Create NSG for **VNet2-Paris** to deny incoming ICMP (ping). After the test, update it with "allow" statement for incoming ICMP with higher priority
5. Create the VNet-to-VNet VPN between **VNet1--Sofia** and **VNet3--Tokyo**
6. Allow **VNGateway1** to make the connection between **VNet2--Paris** and **VNet3--Tokyo**
7. Create a point-to-site VPN from a local machine to **VNet1--Sofia**
8. Change the default routing path between **Sofia-Branch** and **Paris**. Now all the traffic should go via **Sofia-HQ**

Summary

1. Introduction to Azure networking
2. DNS hosting in Azure
3. Inter-site connectivity options
4. Virtual network traffic routing
5. Demonstration

Questions?



SoftUni Diamond Partners

Software University

SmartIT

Coca-Cola HBC Bulgaria

SOFTWARE GROUP

DXC TECHNOLOGY

createX

Postbank
Решения за твоето утре

SUPER HOSTING .BG

DRAFT KINGS

VIVACOM

INDEAVR
Serving the high achievers

AMBITIONED

PHAR VISION

Trainings @ Software University (SoftUni)

- Software University – High-Quality Education, Profession and Job for Software Developers
  - softuni.bg, about.softuni.bg
- Software University Foundation
  - softuni.foundation
- Software University @ Facebook
  - facebook.com/SoftwareUniversity
- Software University Forums
  - forum.softuni.bg