

# Core Services of Azure IaaS



## Compute

Virtual machines  
Availability sets  
VM scale sets



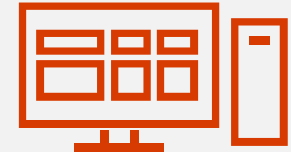
## Storage

Disks  
Blob storage  
Files



## Networking

Virtual networks  
VPN, ExpressRoute  
Load Balancer  
DNS, Traffic Manager

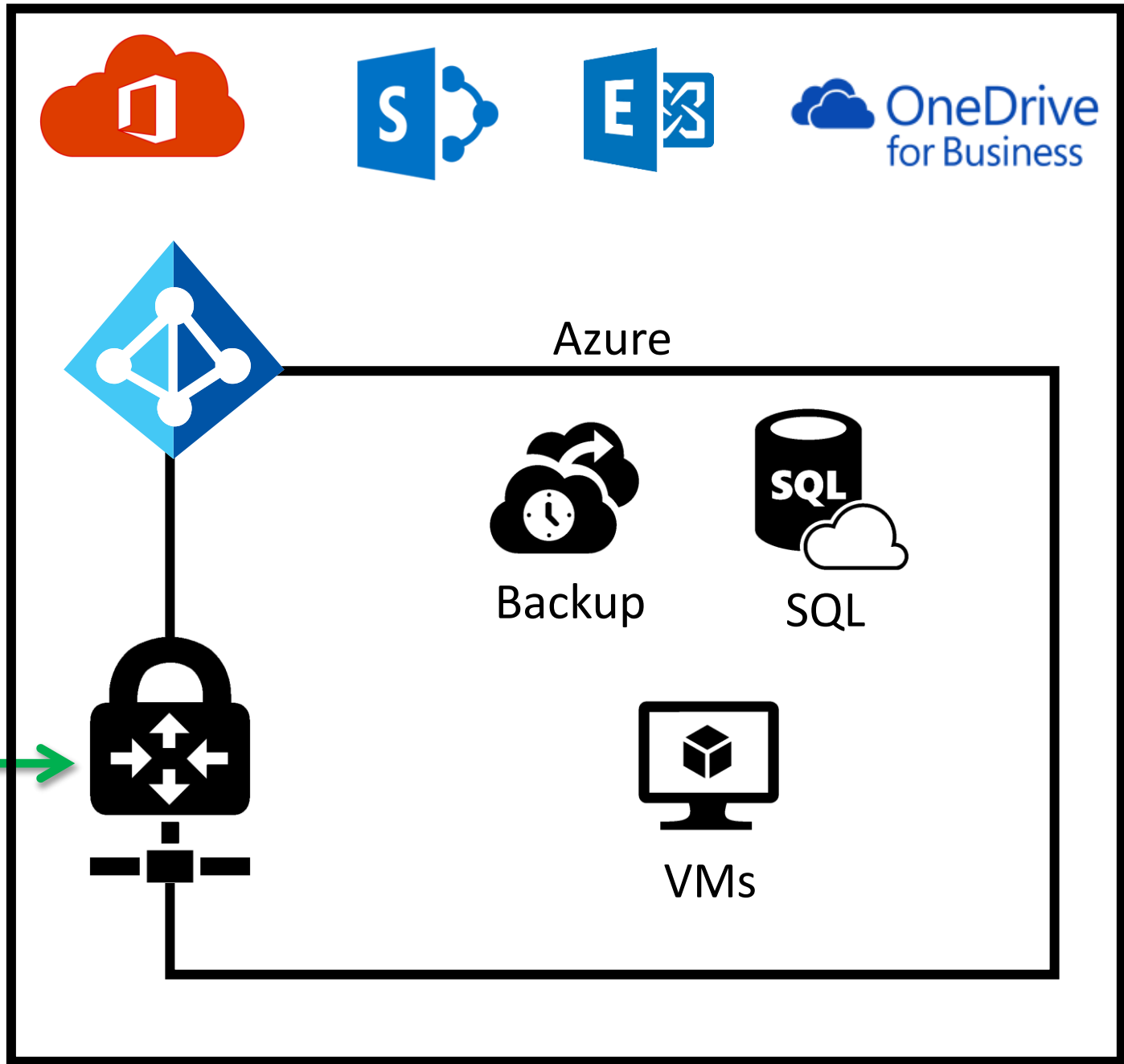
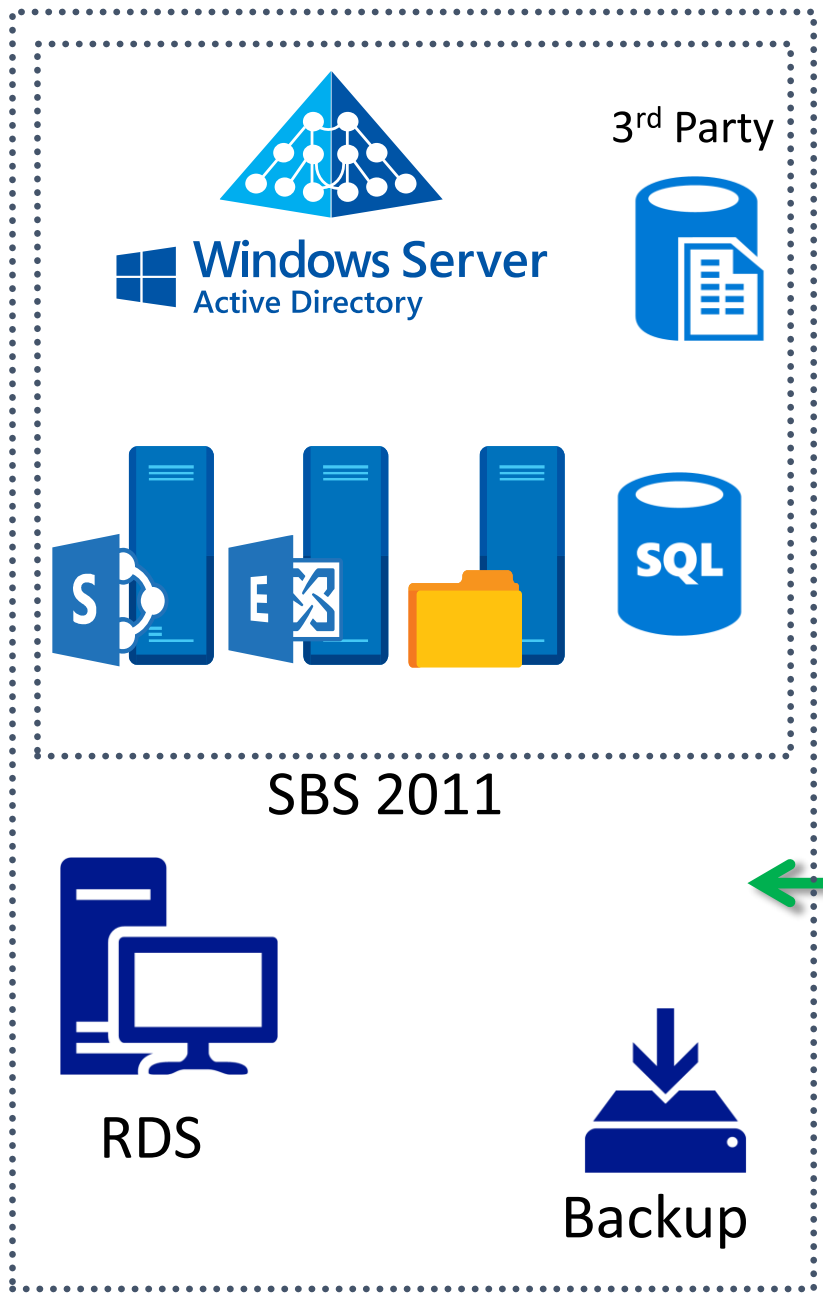


## Security & Management

Log analytics  
Backup  
Site Recovery  
Security Center

Office 365

On Prem



# On Prem



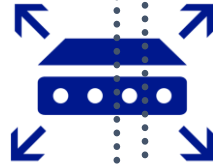
10.0.0.4

SBS 2011



10.0.0.200

192.168.0.6



192.168.0.1

10.0.0.0/24

# Azure

Gateway

Subnet

10.2.200.0/29

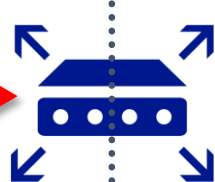
10.2.0.0/24

10.2.0.0/16

On Prem



SBS 2011

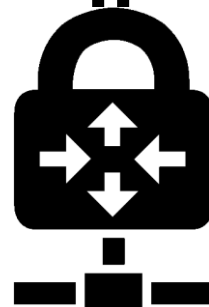


VPN



Azure

Gateway



Subnet



ServerA



NewDC

# Azure supports multiple VNets

- May require multiple networks to provide segregation for billing, security or administration.
- Vnet cannot span a subscription
- Connect via Site to Site VPN or VNET Peering

# Site to Site VNet

- Can connect to on premises or between VNets
- Requires an Azure Network Gateway
- Requires supported IPSec router on premises
- Uses a shared secret for encryption

# VNet Peering

- Doesn't require Network Gateway
- Traffic does not travel over public internet
- Low latency, high bandwidth
- No network bandwidth restrictions
- Gateway transit is a peering property that enables one virtual network to utilize the VPN gateway in the peered virtual network for cross-premises or VNet-to-VNet connectivity.

# Virtual Machine Networking



## IPv4 and IPv6 Support

Support for multiple network interfaces for routing and firewalls

Private and/or Public IP addresses (static or dynamic)

Network Security Groups for traffic isolation

Automatic assignment of DNS servers from virtual network or from Azure DNS

Accelerated Networking

MAC Persistence



# Load Balancing



Load Balancer



Application Gateway with WAF



Traffic Manager



3<sup>rd</sup> Party Solutions from Marketplace

# Connectivity Options to Azure

Compute



Storage











Networking

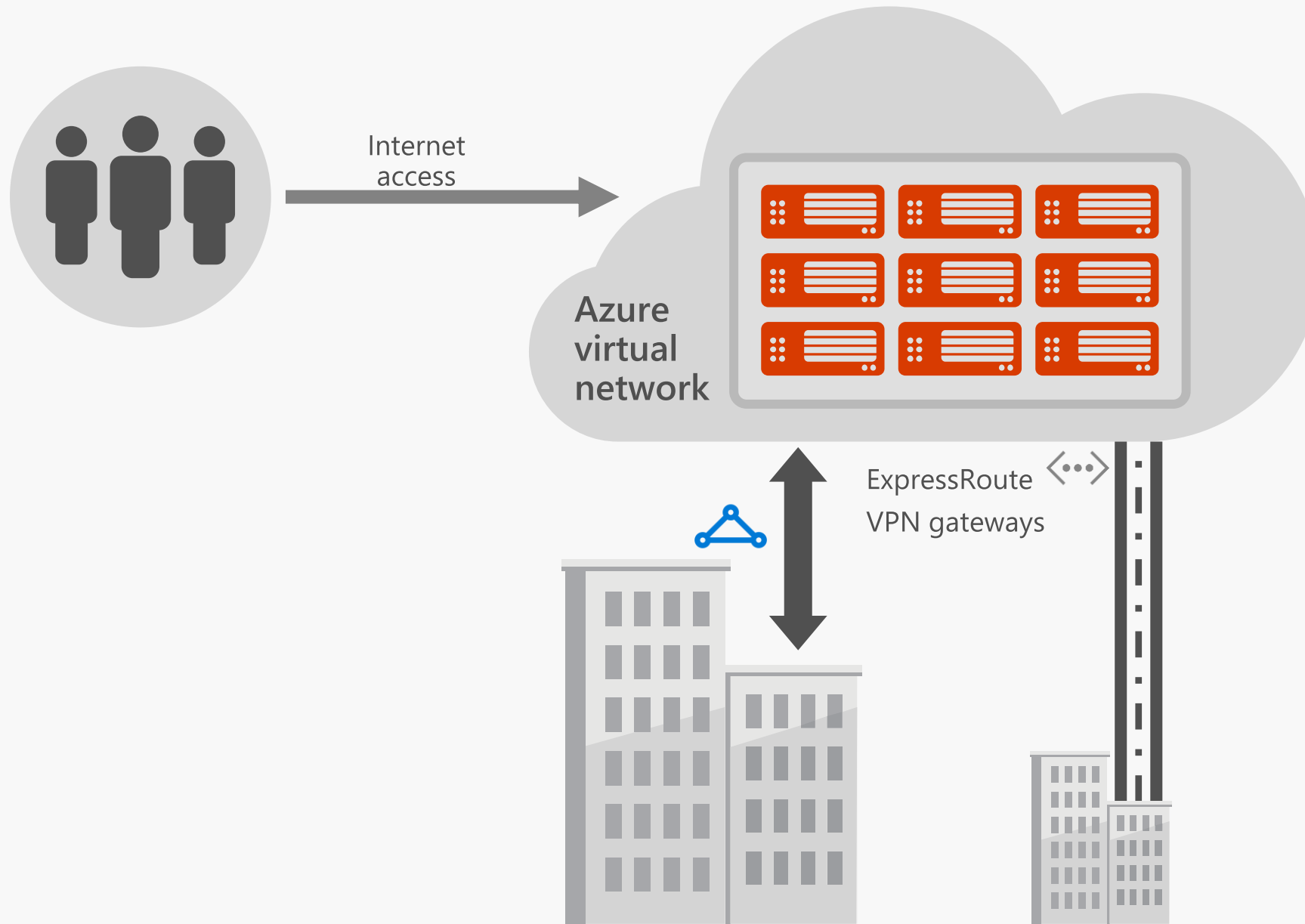


Management



	Secure point-to-site connectivity		<ul style="list-style-type: none"><li>• POC Efforts</li><li>• Small scale deployments</li><li>• Connect from anywhere</li></ul>
	Secure site-to-site VPN connectivity		<ul style="list-style-type: none"><li>• Connect to Azure compute from on-premises or another Azure region</li></ul>
	VNet Peering within region		<ul style="list-style-type: none"><li>• In-region VNet-to-VNet connectivity</li><li>• Direct VM-to-VM connectivity</li><li>• Peer VNets for routing and transit</li></ul>
	ExpressRoute private connectivity		<ul style="list-style-type: none"><li>• Private connectivity from your on-premises data center to Azure virtual networks and PaaS Services</li></ul>

# Azure Networking



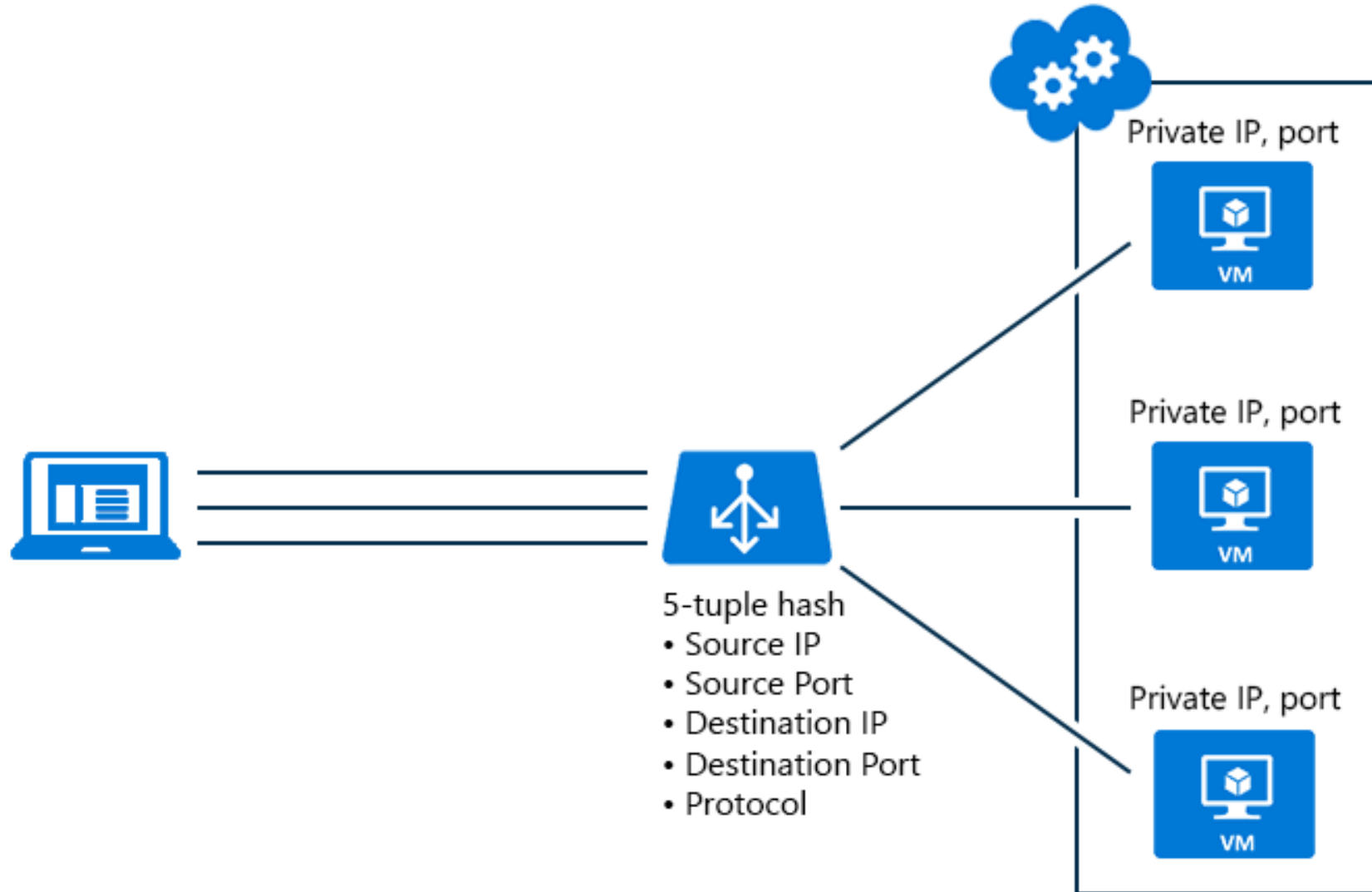
## Virtual network

- Private IP addresses, Network-level isolation
- Segment with subnets and security groups
- Control traffic flow with user-defined routes

## Hybrid connectivity

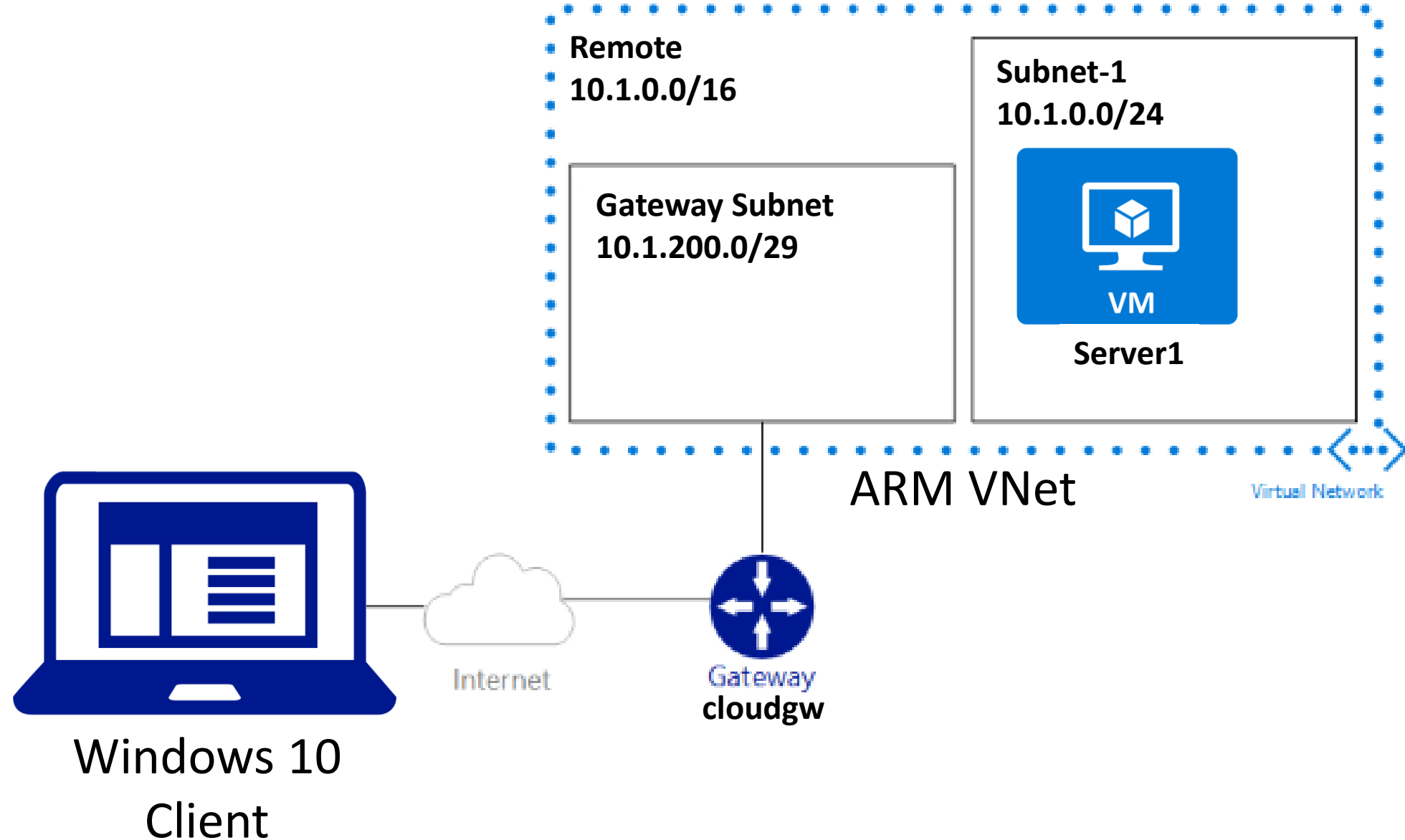
- Point-to-site for dev/test
- VPN gateways for secure site-to-site connectivity
- ExpressRoute for private enterprise grade connectivity
- Domain-join with on-premises

# Load balancer



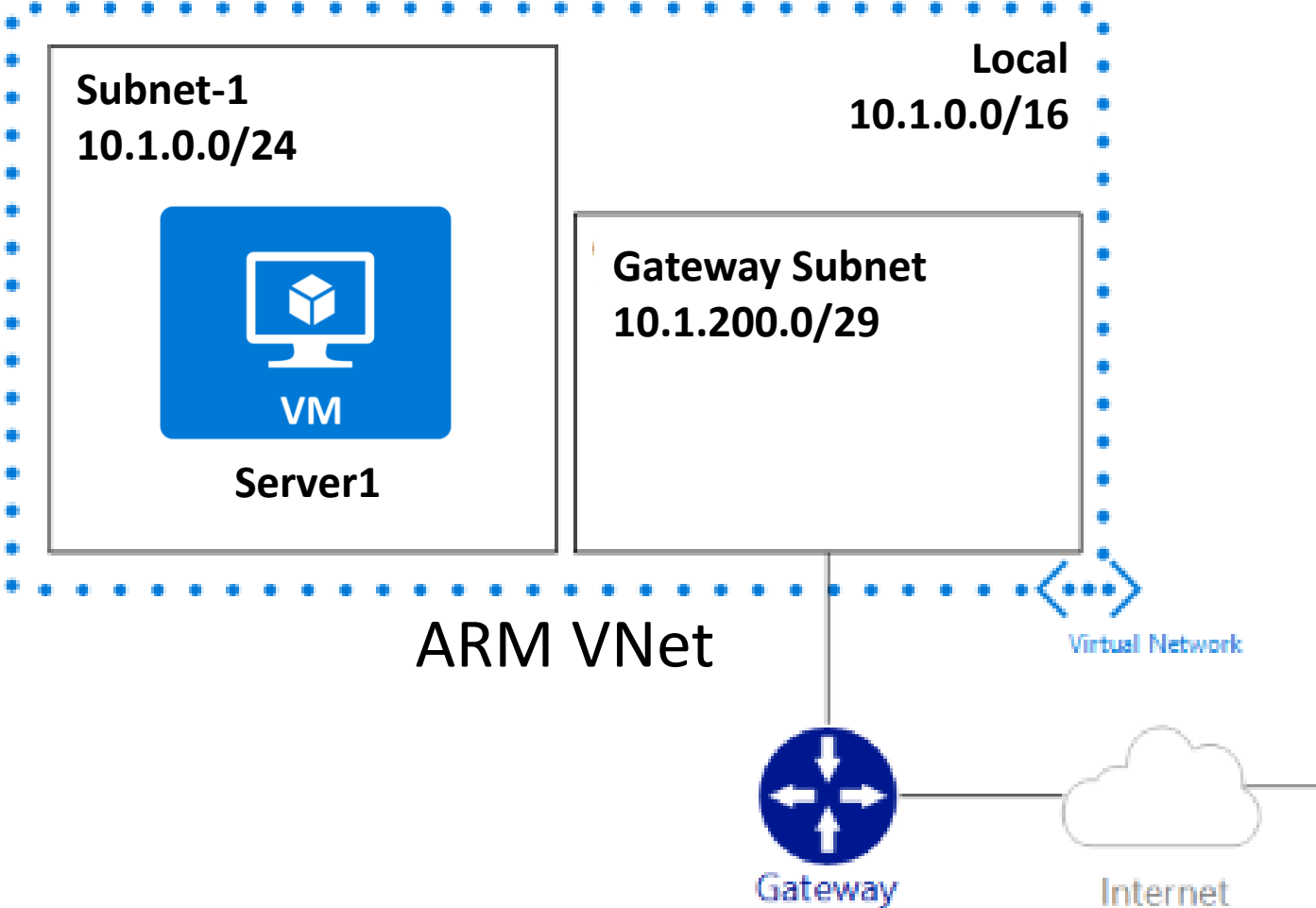
Point to Site VPN

# Azure Resource Manager



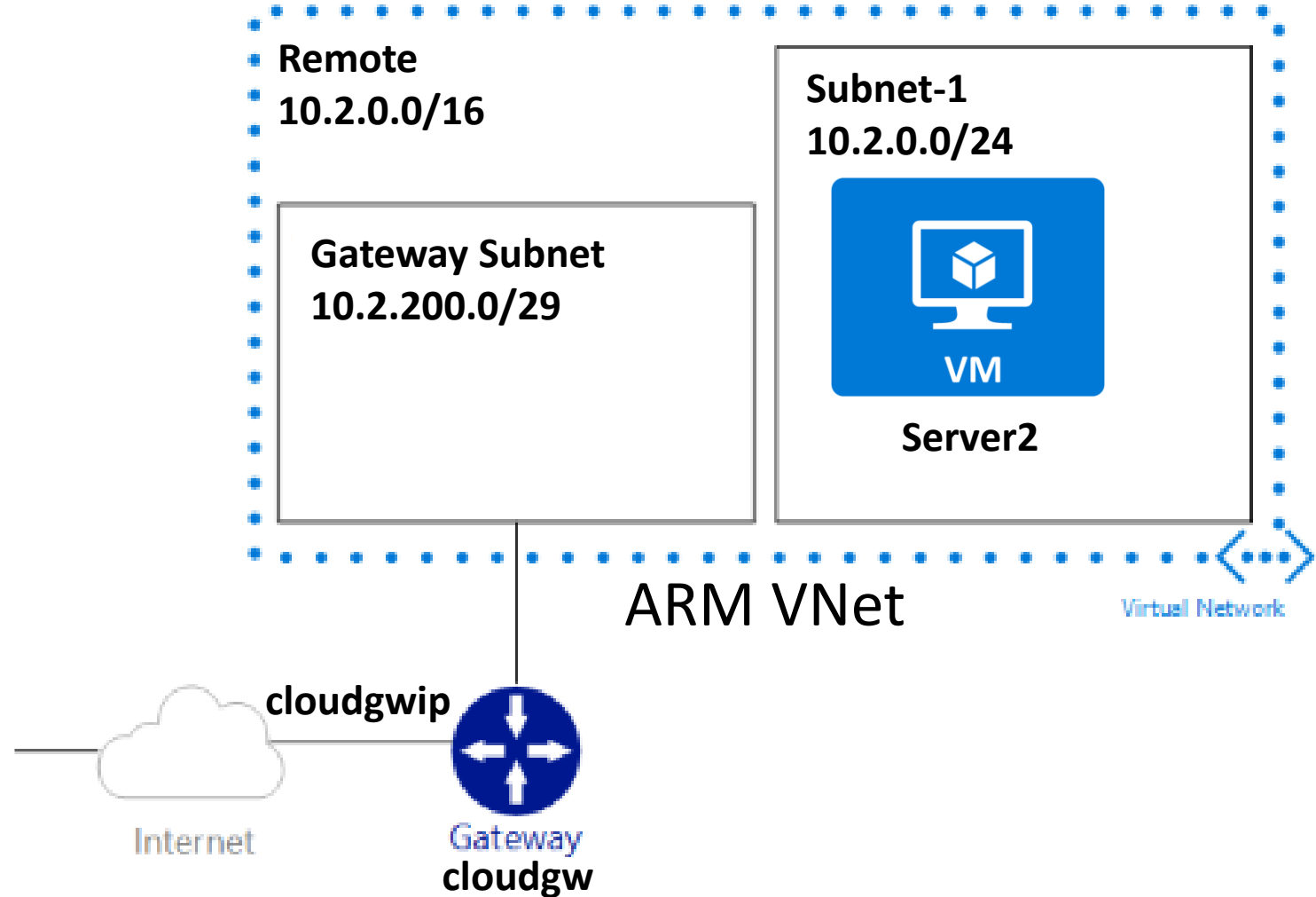
Site to Site VPN

# Azure Service Manager

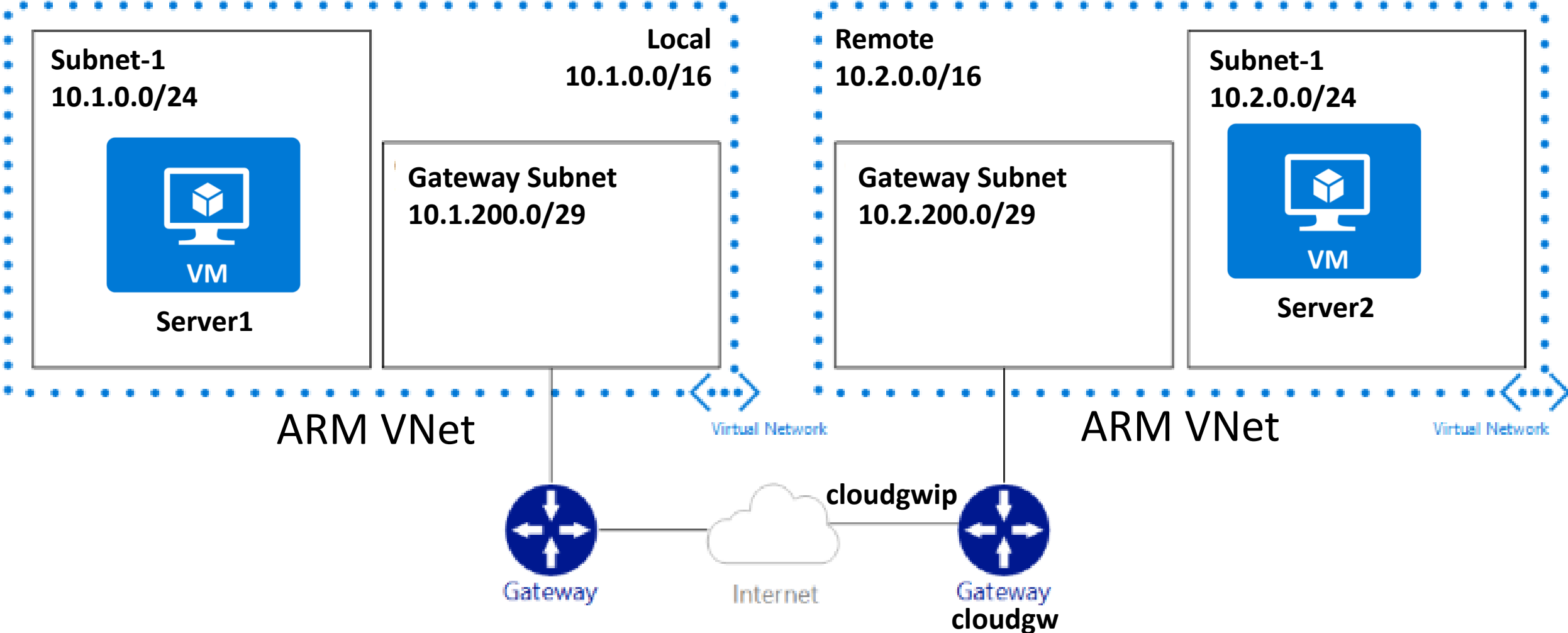




# Azure Resource Manager

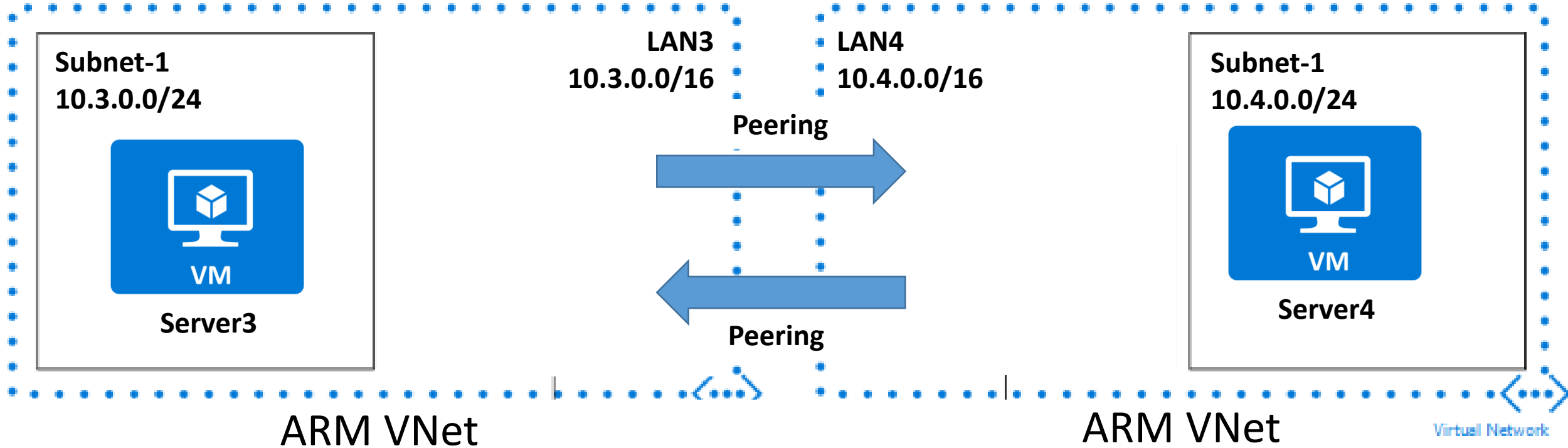


# Site to Site VPN



# Azure VNet Peering

# Azure Resource Manage Vnet Peering



# Vnet Peering

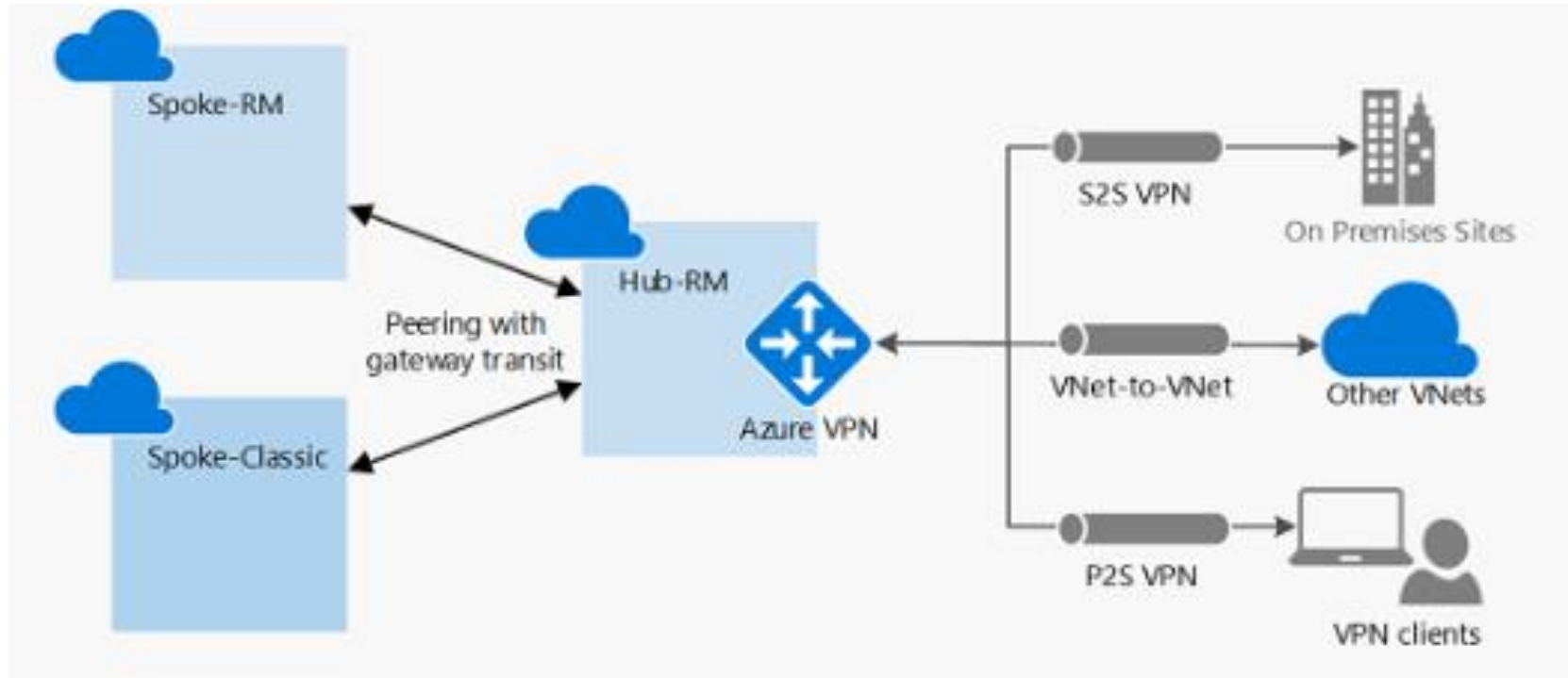
The traffic between virtual machines in the peered virtual networks is routed through the Microsoft backbone infrastructure, much like traffic is routed between virtual machines in the same virtual network, through private IP addresses only. Azure supports:

- VNet peering - connecting VNets within the same Azure region
- Global VNet peering - connecting VNets across Azure regions

The benefits of using virtual network peering, whether local or global, include:

- Network traffic between peered virtual networks is private. Traffic between the virtual networks is kept on the Microsoft backbone network. No public Internet, gateways, or encryption is required in the communication between the virtual networks.
- A low-latency, high-bandwidth connection between resources in different virtual networks.
- The ability for resources in one virtual network to communicate with resources in a different virtual network, once the virtual networks are peered.
- The ability to transfer data across Azure subscriptions, deployment models, and across Azure regions.
- The ability to peer virtual networks created through the Azure Resource Manager or to peer one virtual network created through Resource Manager to a virtual network created through the classic deployment model. To learn more about Azure deployment models, see [Understand Azure deployment models](#).
- No downtime to resources in either virtual network when creating the peering, or after the peering is created.

# VNet Peering – Gateway transit

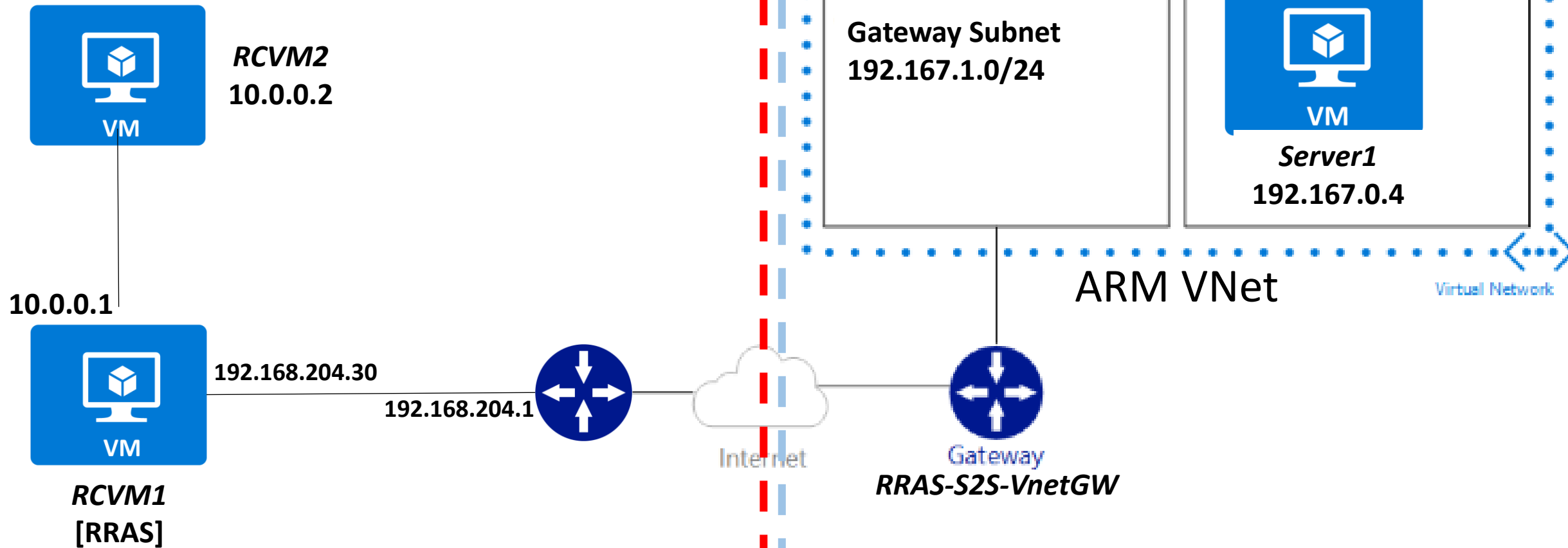


In the diagram, gateway transit allows the peered virtual networks to use the Azure VPN gateway in Hub-RM. Connectivity available on the VPN gateway, including S2S, P2S, and VNet-to-VNet connections, applies to all three virtual networks.

Windows RRAS  
Site To Site VPN

# On-Premises

# Azure





# Azure network watcher

Topology	Network Diagnostics	Metric	Logs
Visualize your network topology	Diagnostic tools for networking related issues	Measure and view your network performance and health	Provide network diagnostic logs

# Network Security Groups

# What is a Network Security Group?

A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets, individual VMs, or individual network interfaces (NIC) attached to VMs.

When an NSG is associated to a subnet, the rules apply to all resources connected to the subnet. Traffic can further be restricted by also associating an NSG to a VM or NIC.

# Network Security Group

The screenshot displays the Azure portal interface for a Network Security Group (NSG) named 'nested-nsg'. The left-hand navigation pane includes sections for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, and Monitoring. The 'Settings' section is expanded to show 'Inbound security rules' and 'Outbound security rules'. The main content area shows the 'Essentials' section with two tables of rules.

**nested-nsg**  
Network security group

Search (Ctrl+/)    Move    Delete    Refresh

**Essentials**

### Inbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
1000	default-allow-rdp	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBal...	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