Microsoft

Azure MI Platform and Network Security

Module 3

CONDITIONS AND TERMS OF USE:

Learning Units covered in this Module

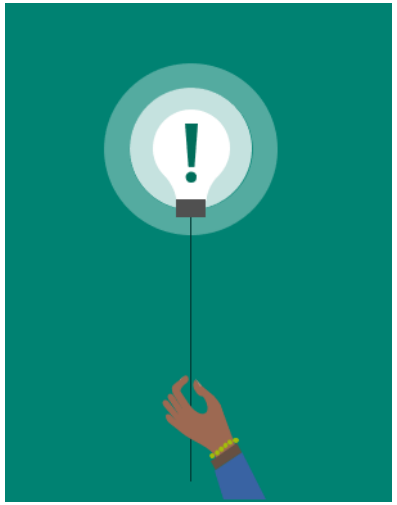
- Lesson 1: Overview of Azure SQL MI security
- Lesson 2: Isolation and Connectivity
- Lesson 3: Azure Virtual Network and Security Rules
- Lesson 4: Network Peering

Lesson 1: Overview of Azure SQL MI Security

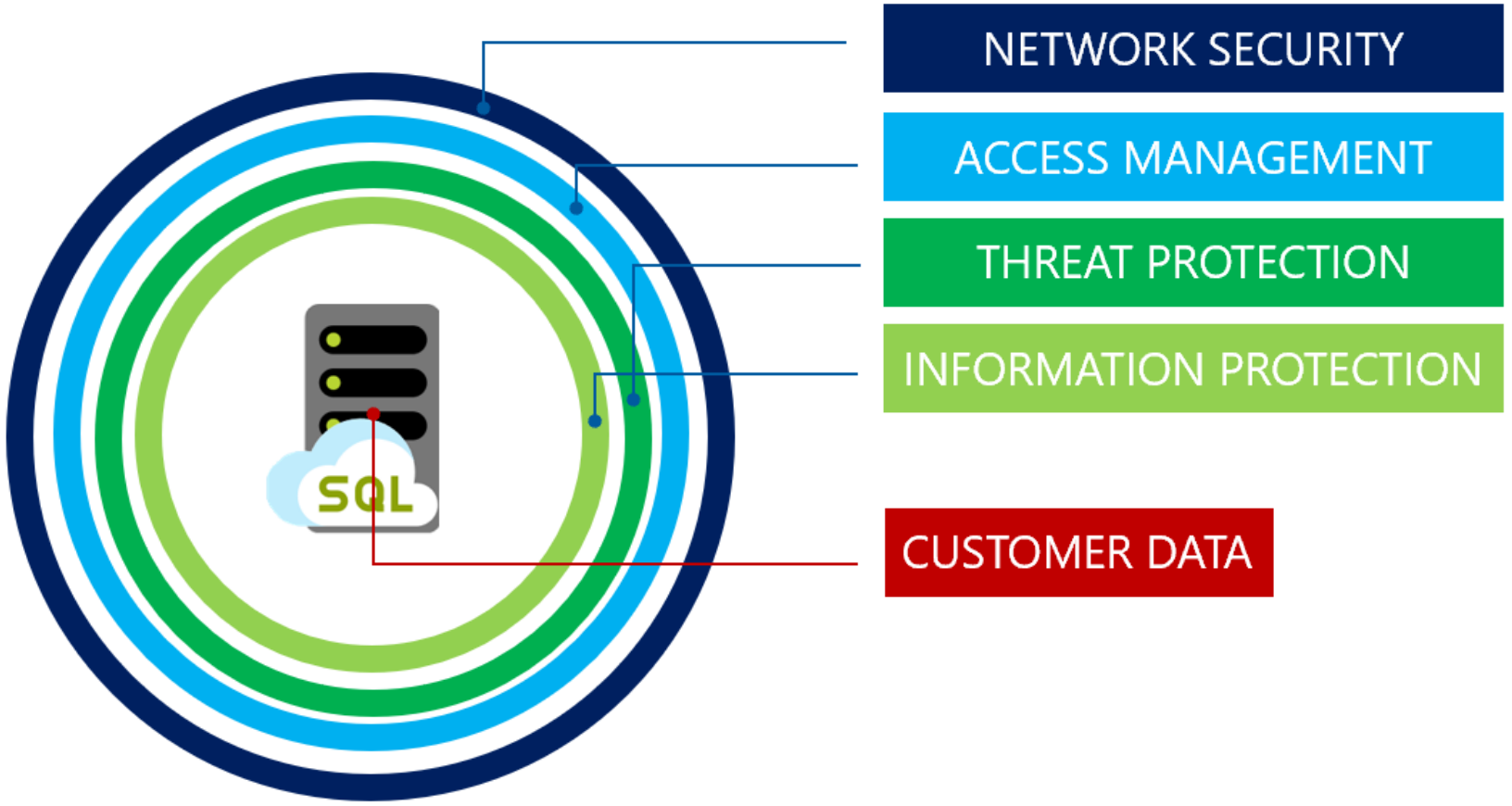
Objectives

After completing this learning, you will be able to:

- Learn the various security options in Azure SQL Managed Instance as high level.
- Understand the security lifecycle about how to secure your databases in Azure SQL MI.



Overview of Azure SQL Managed Instance Security Capabilities



Enterprise Security that is Easy-to-Use

Authentication & Access Management

- Azure Active Directory
- Multi-Factor Authentication (MFA)
- Role-based Access Control (RBAC)
- SQL Authentication
- Row/Column-level Security

Data protection

- Encryption-in-flight (TLS)
- Encryption-in-use (Always Encrypted
- Encryption-at-rest (TDE)
- Dynamic Data Masking

Network security

- VNet injection for managed instances
- Private Link for SQL databases
- Firewall Rules
- Network Security Groups (NSG)

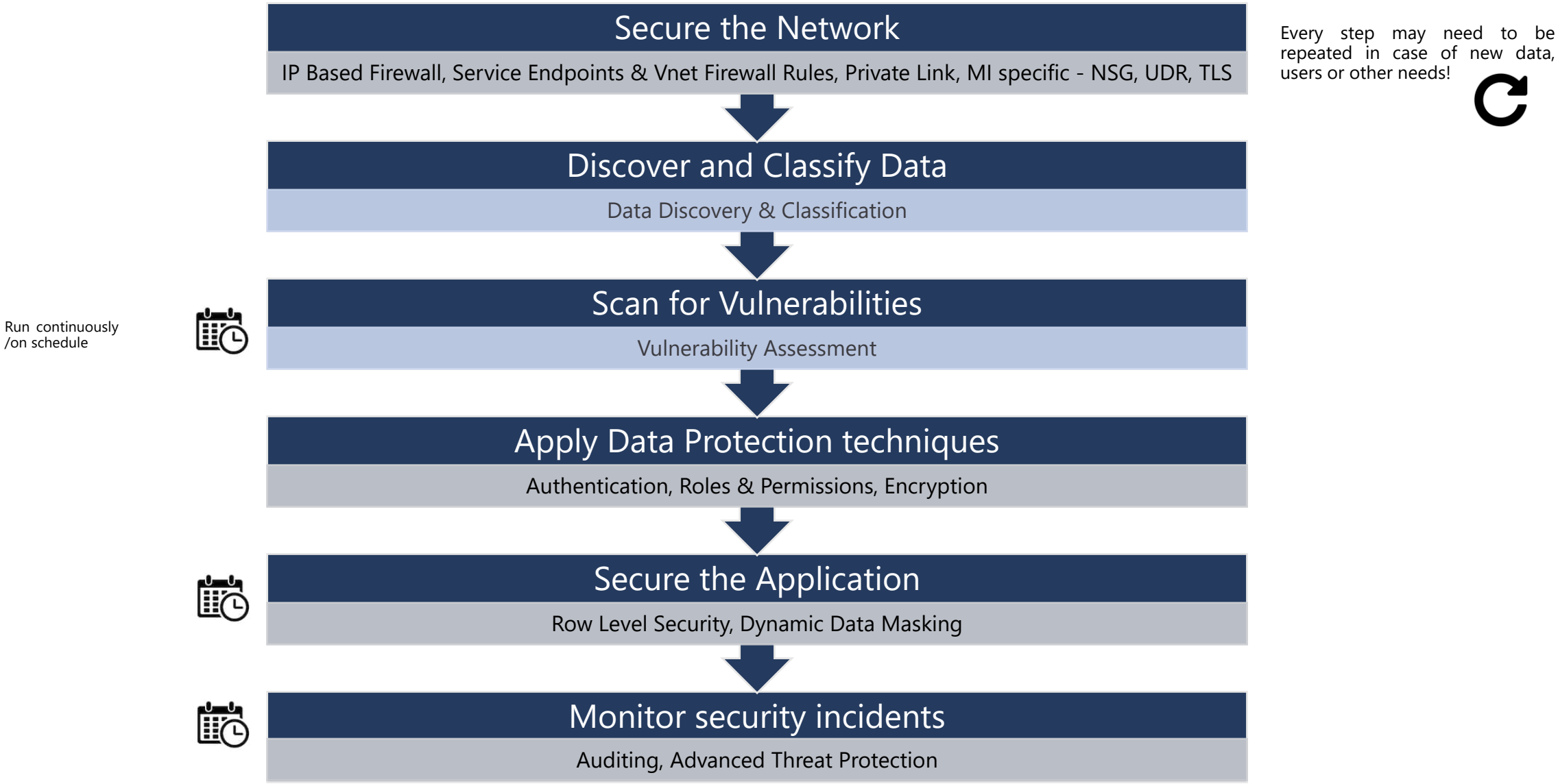
Monitoring, Logging & Auditing

- Advanced Threat Protection
- SQL Audit
- Audit Integration with Log Analytics

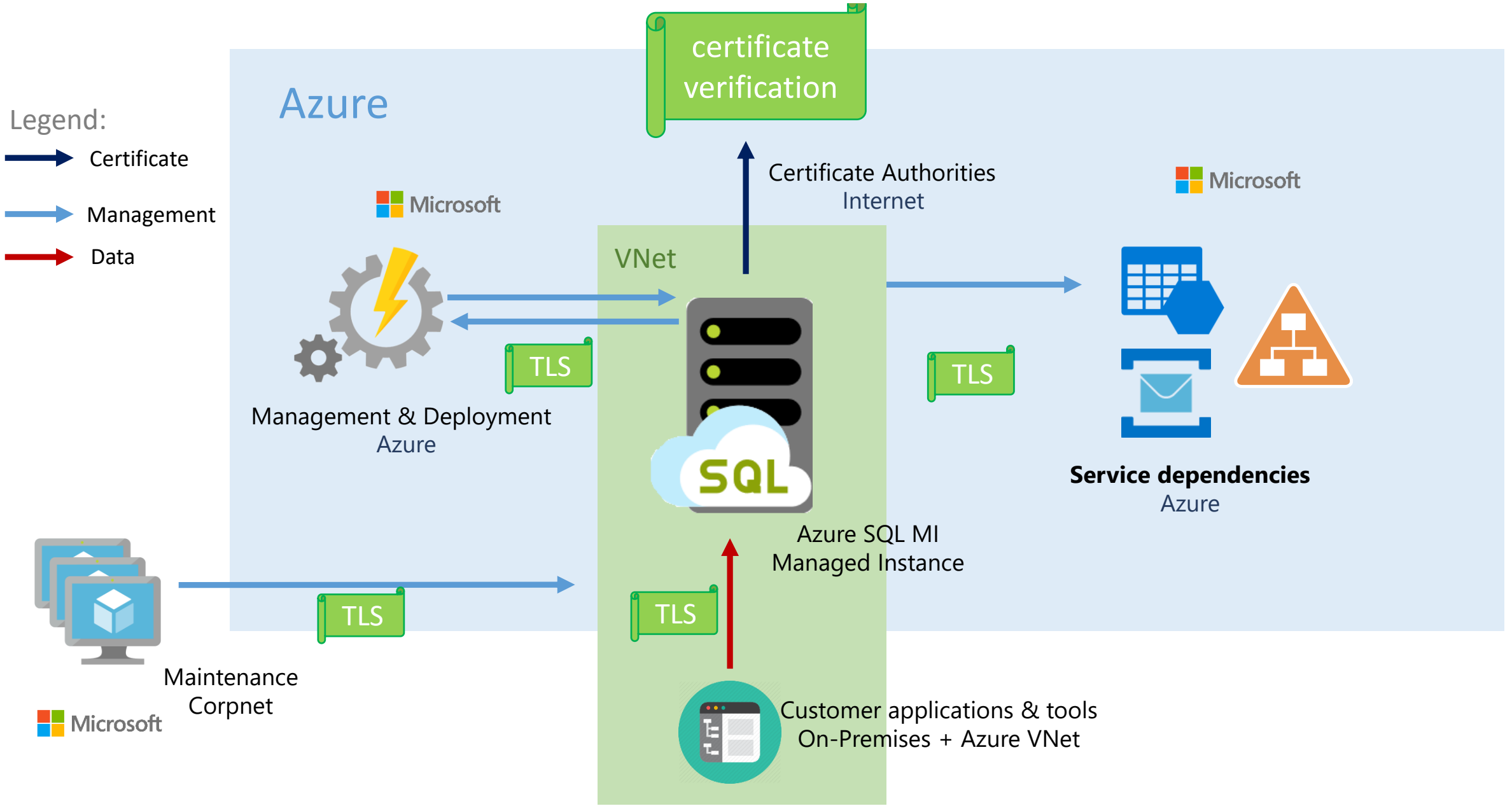
Security management

- Vulnerability Assessment
- Integration with Azure Security Center
- Data Discovery & Classification

Securing your databases in Azure SQL MI (Security Lifecycle)



Azure MI Network Communications



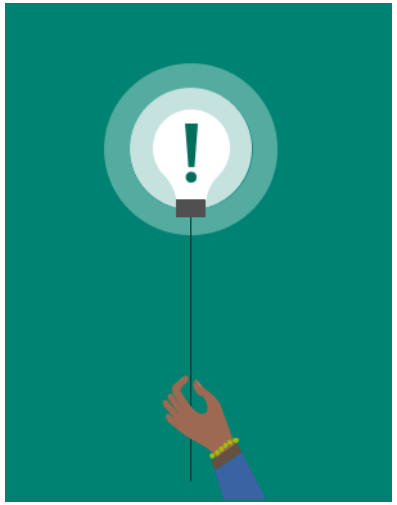
Questions?

Lesson 2: Isolation and Connectivity

Objectives

After completing this learning, you will be able to:

- Learn the different connectivity options for Azure SQL MI.

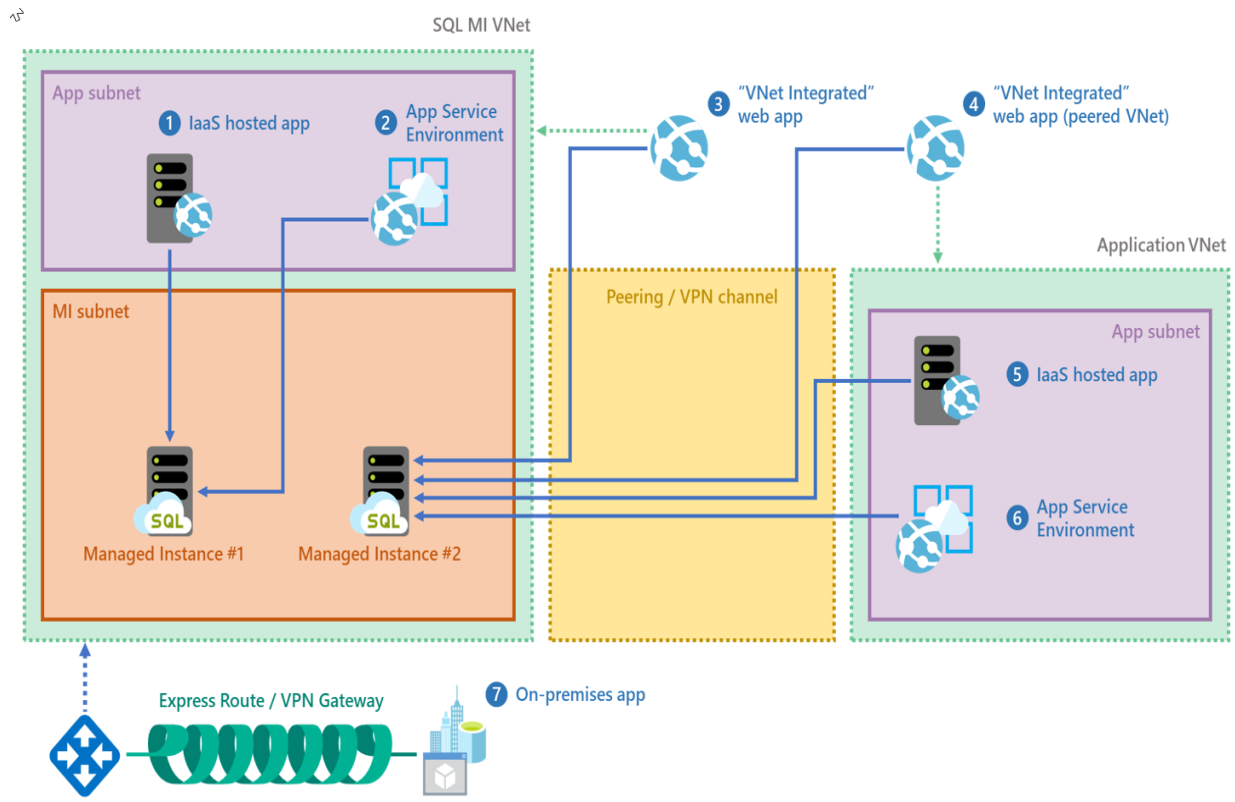


MI Security Isolation

Full isolation from other tenants without resource sharing

Promote secure communication over private IP addresses with native VNET integration

Connectivity from on-premises environment using Azure Express Route or VPN Gateway



High Level Connectivity Architecture

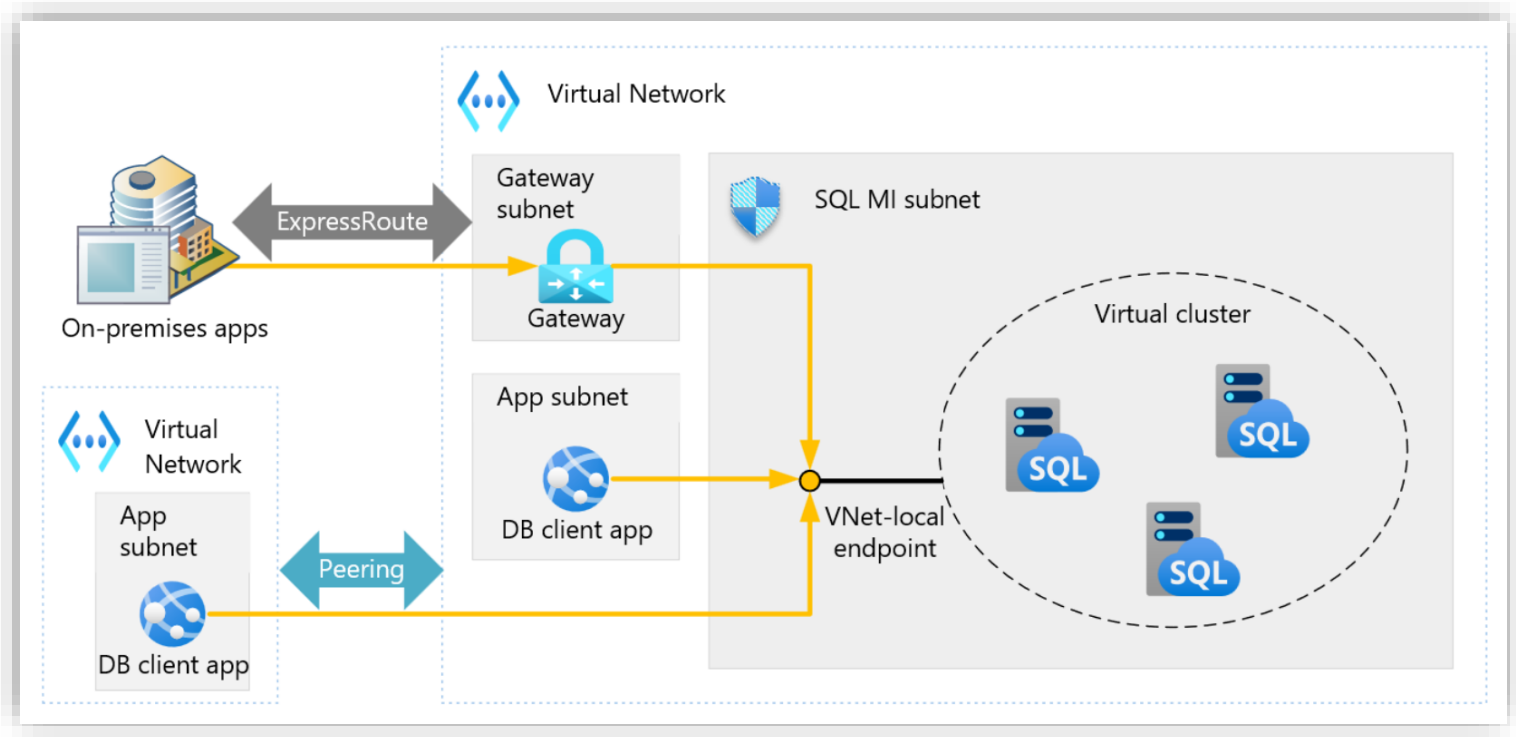
MI is set of Service Components

Hosted on a dedicated/isolated VMs

VMs run inside virtual network subnet

These machines form a virtual cluster

TDS endpoint to connect to MI

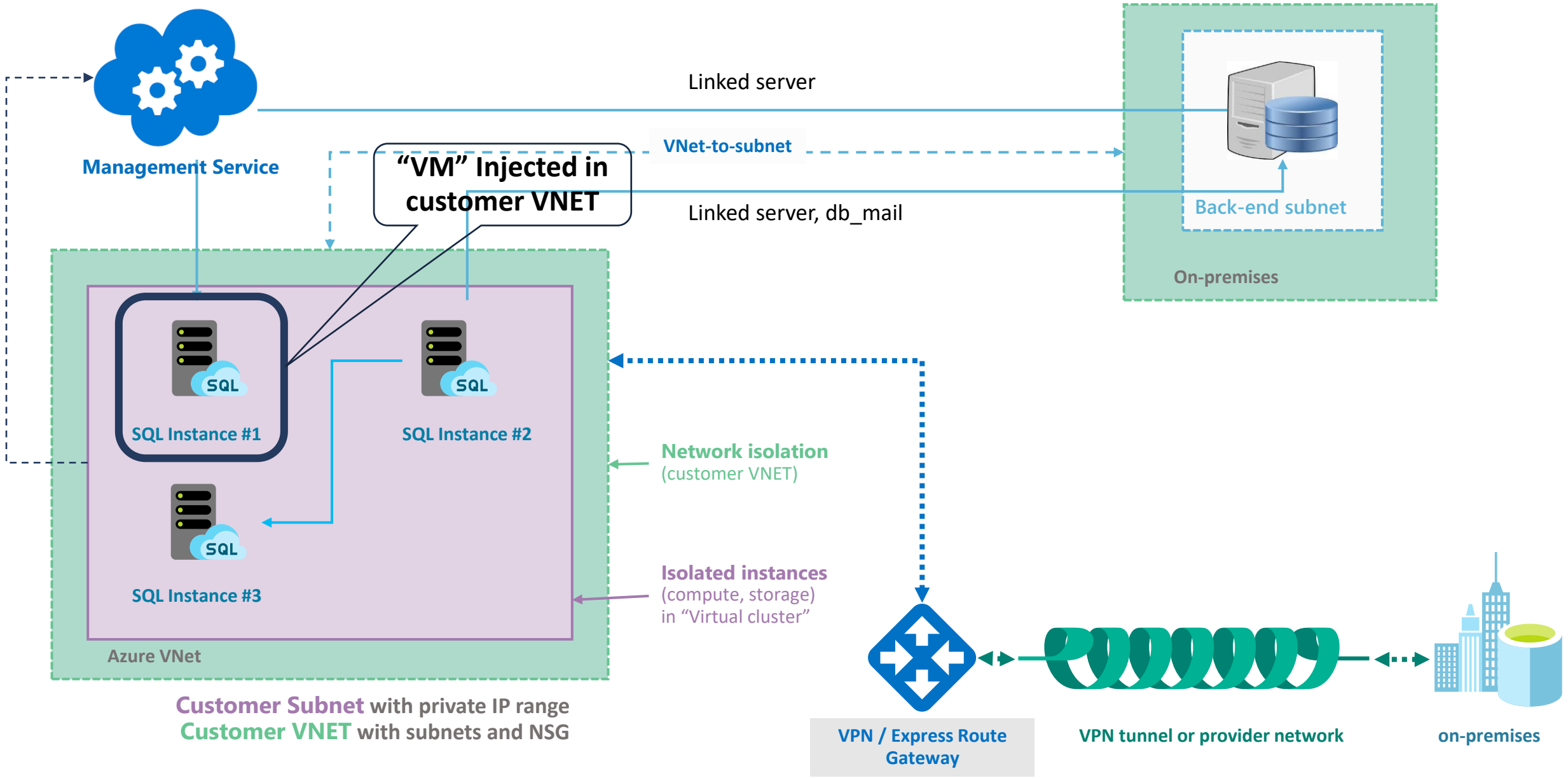


Demonstration

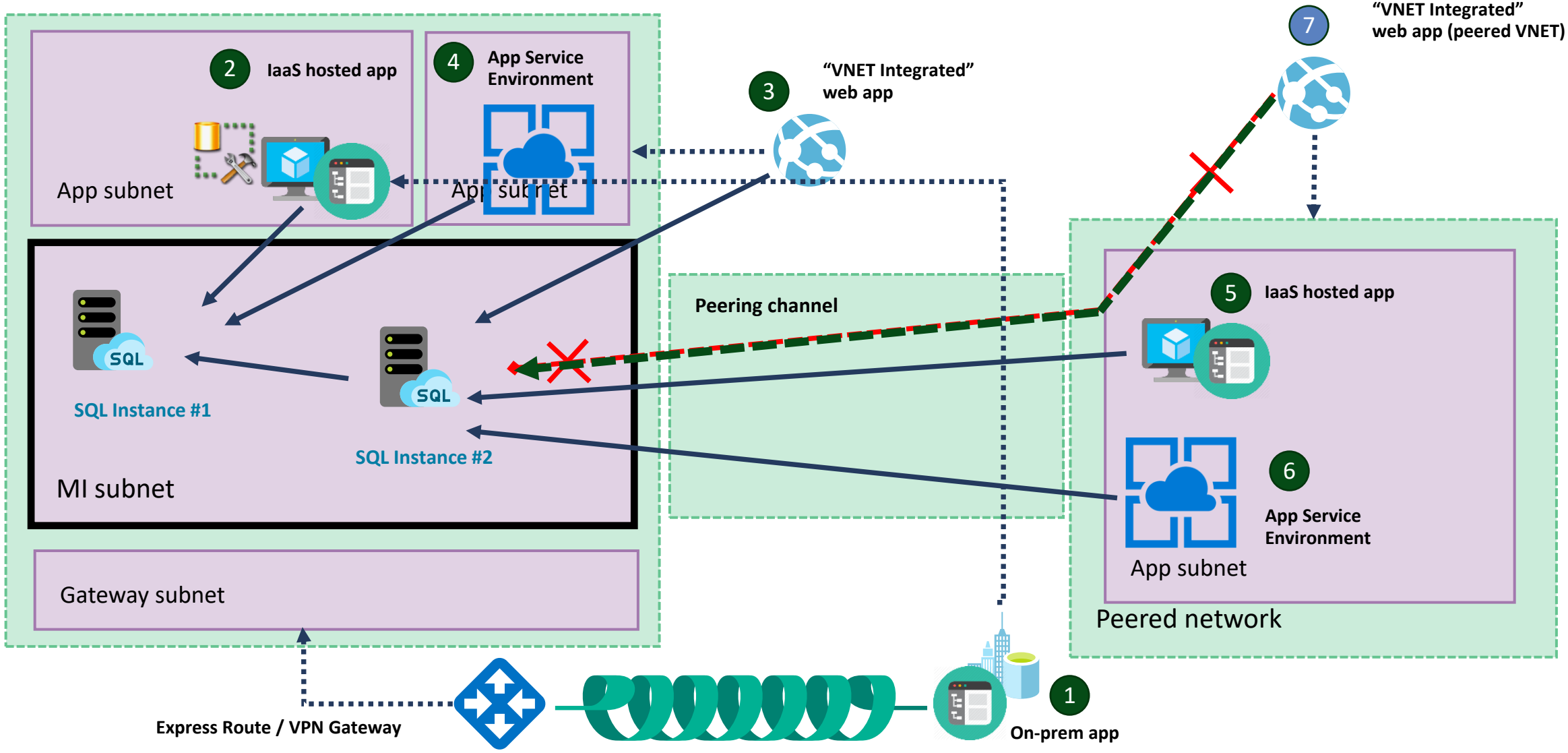
Review Managed Instance Components

- Show the resources created and Network specific components.

Removing security & isolation concerns



App integration and network security



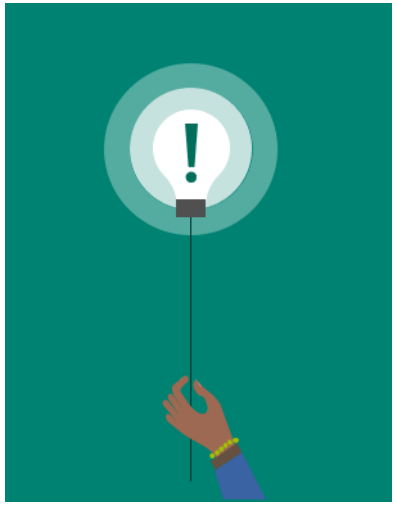
Questions?

Lesson 3: Azure Virtual Network and Security Rules

Objectives

After completing this learning, you will be able to:

- Learn the virtual network concepts in Azure SQL MI.



The Azure Virtual Network

SQL Managed Instance is placed inside the Azure virtual network and the subnet is dedicated to managed instances.	A secure private IP address.
	The ability to connect an on-premises network to SQL Managed Instance.
	The ability to connect SQL Managed Instance to a linked server or another on-premises data store.
	The ability to connect SQL Managed Instance to Azure resources.
	IP address blocks, DNS settings, security policies, and route tables within a VNet can be controlled.

Dedicated subnet inside VNet

Deploy SQL Managed Instance in a dedicated subnet inside the virtual network. The subnet must have these characteristics:	No other cloud services, except MI, allowed in subnet
	Subnet delegation to Microsoft.Sql/managedInstances resource provider
	Network Security Group (NSG) - must define inbound/outbound security rules
	User Route Table (UDR) - communicate with the Azure Management Service
	Sufficient IP Address

Network Security Groups (NSG)

Filter network traffic to and from Azure resources in an Azure virtual network with a network security group. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.	An NSG needs to be associated with the SQL Managed Instance subnet.
	NSG to control access to SQL MI by filtering traffic on port 1433 and ports 11000-11999 for redirect connections.
	The service will automatically provision and keep current rules required to allow uninterrupted flow of management traffic.

Azure Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

It is a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability

Centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks

Uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network

Network Security Group Inbound/Outbound Rules

Inbound/Outbound security rules are required to direct Internet or other virtual networks traffic to MI

- Mandatory inbound rules

Name	Port	Protocol	Source	Destination	Action
management	9000, 9003, 1438, 1440, 1452	TCP	SqlManagement	MI SUBNET	Allow
	9000, 9003	TCP	CorpnetSaw	MI SUBNET	Allow
	9000, 9003	TCP	CorpnetPublic	MI SUBNET	Allow
mi_subnet	Any	Any	MI SUBNET	MI SUBNET	Allow
health_probe	Any	Any	AzureLoadBalancer	MI SUBNET	Allow

- Mandatory outbound rules

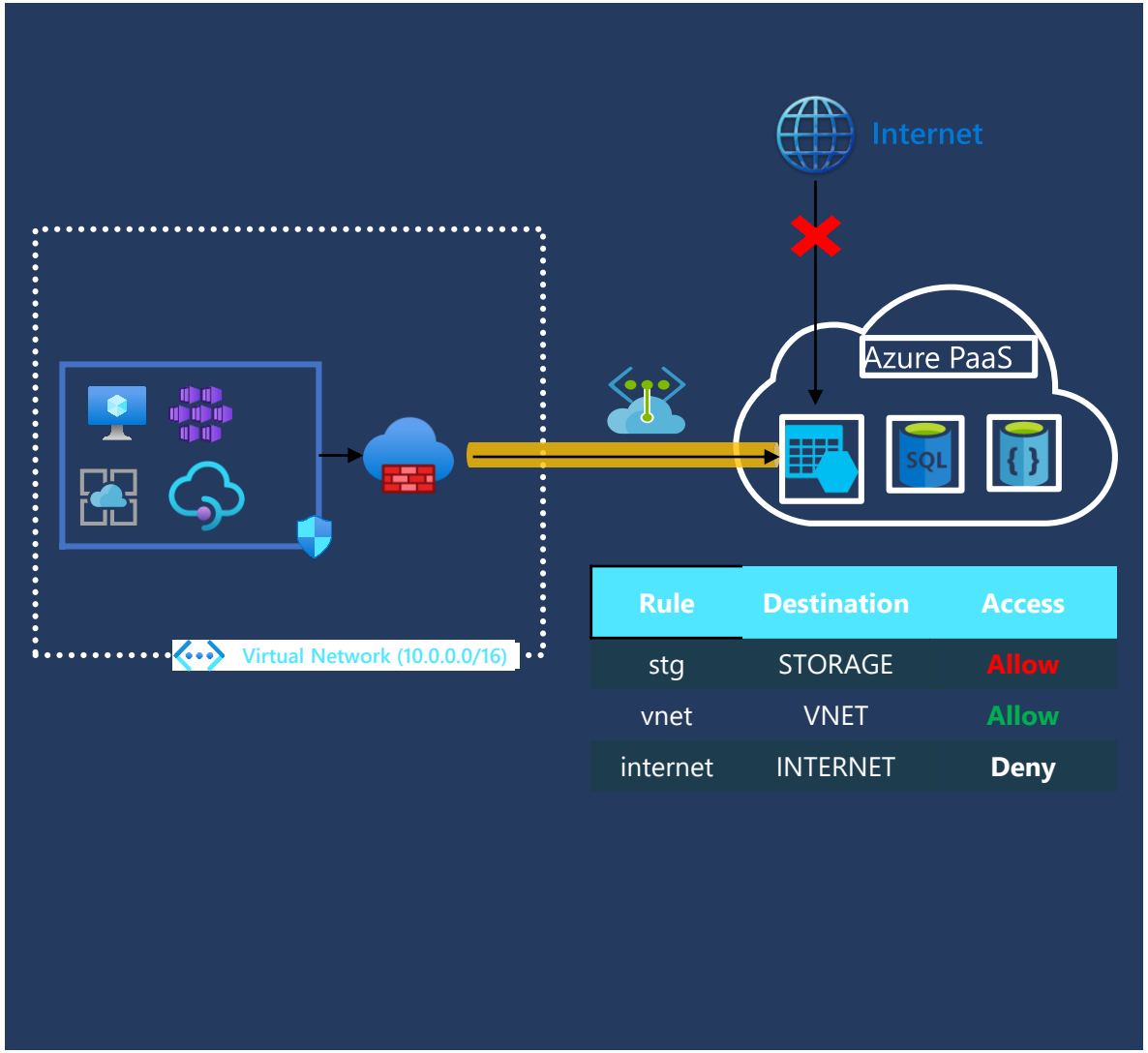
Name	Port	Protocol	Source	Destination	Action
management	443, 12000	TCP	MI SUBNET	AzureCloud	Allow
mi_subnet	Any	Any	MI SUBNET	MI SUBNET	Allow

Virtual Network Service Endpoints

Virtual Network (VNet) service endpoints extend your virtual network private address space and the identity of your VNet to the Azure services, over a direct connection.

Endpoints allow you to secure your critical Azure service resources to only your virtual networks.

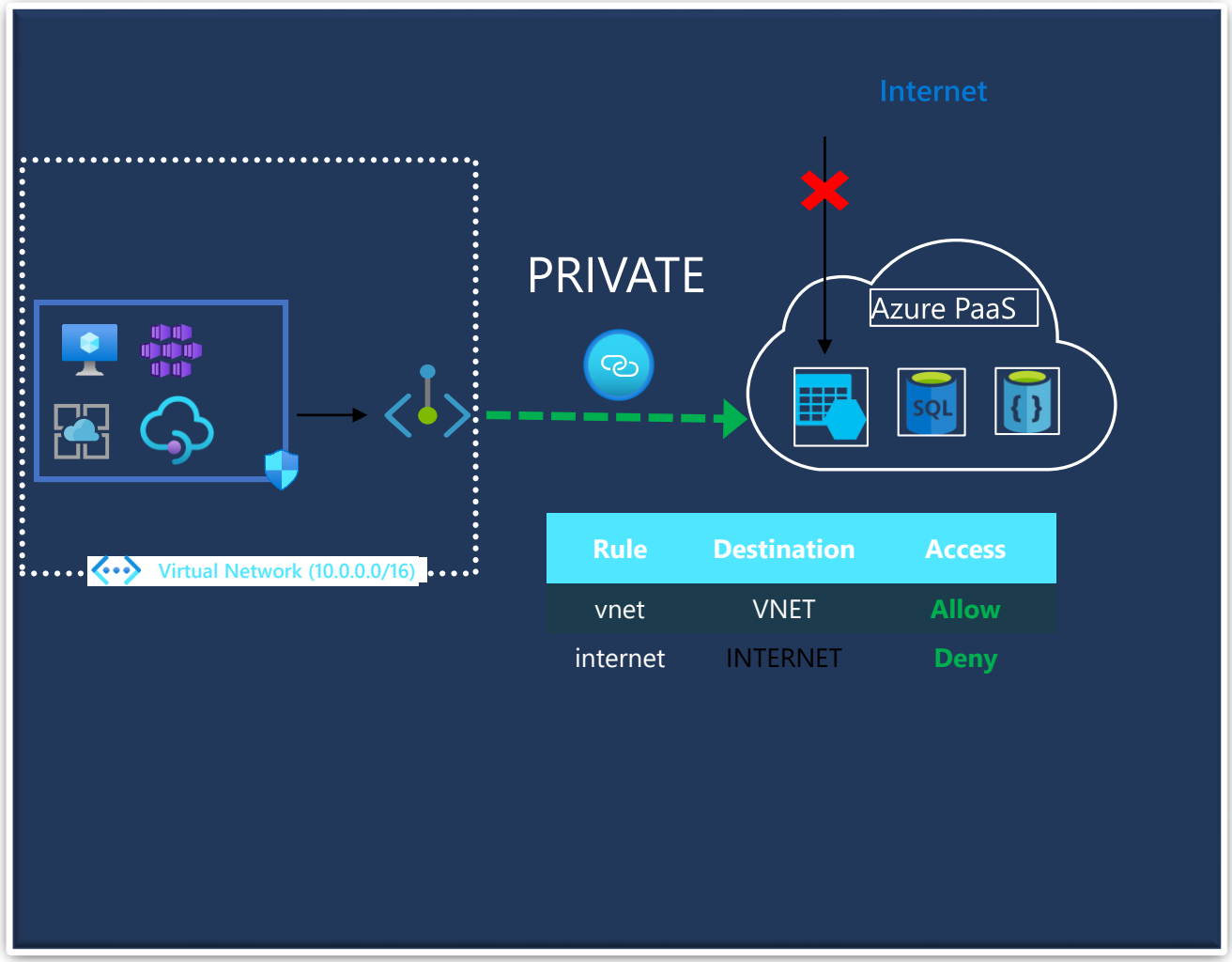
Traffic from your virtual network to the Azure service always remains on the Microsoft Azure backbone network.



Azure Private Link

Azure Private Link enables you to access Azure PaaS Services and Azure hosted customer-owned/partner services over a private endpoint in your virtual network.

- PaaS resource mapped to Private IP Address. NSGs restricted to VNet space
- VNet PaaS via the Microsoft backbone
- In-built data exfiltration protection
- Access only to mapped PaaS resource



MI with Public Endpoint

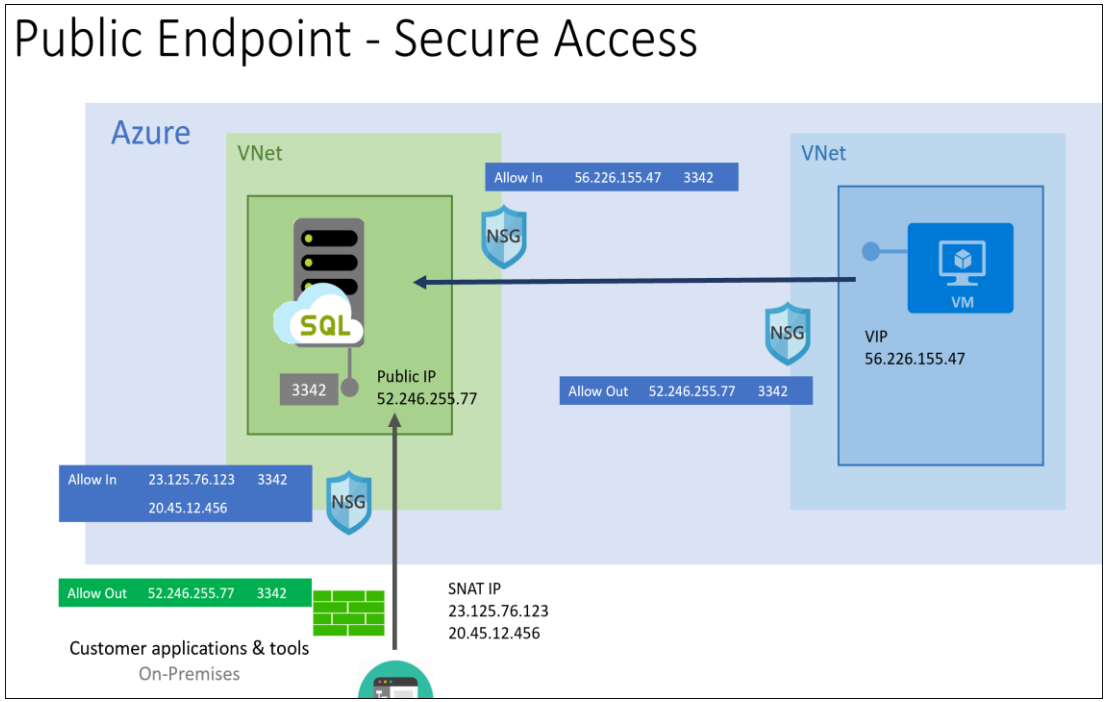
Connect to Managed Instance from the Internet without the VPN

Simultaneously coexist with the private endpoint

Access MI from **multi-tenant** Azure like Power BI, Azure app services.

NSG with port 3342 open for inbound traffic

Public endpoint host name <mi_name>.public.<dns_zone>.database.windows .net. Port 3342



Demonstration

Configure public endpoint

- Show how to configure public endpoint for your Managed Instance

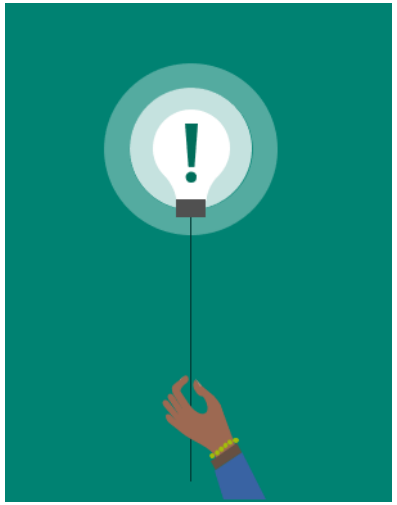
Questions?

Lesson 4: Network Peering

Objectives

After completing this learning, you will be able to:

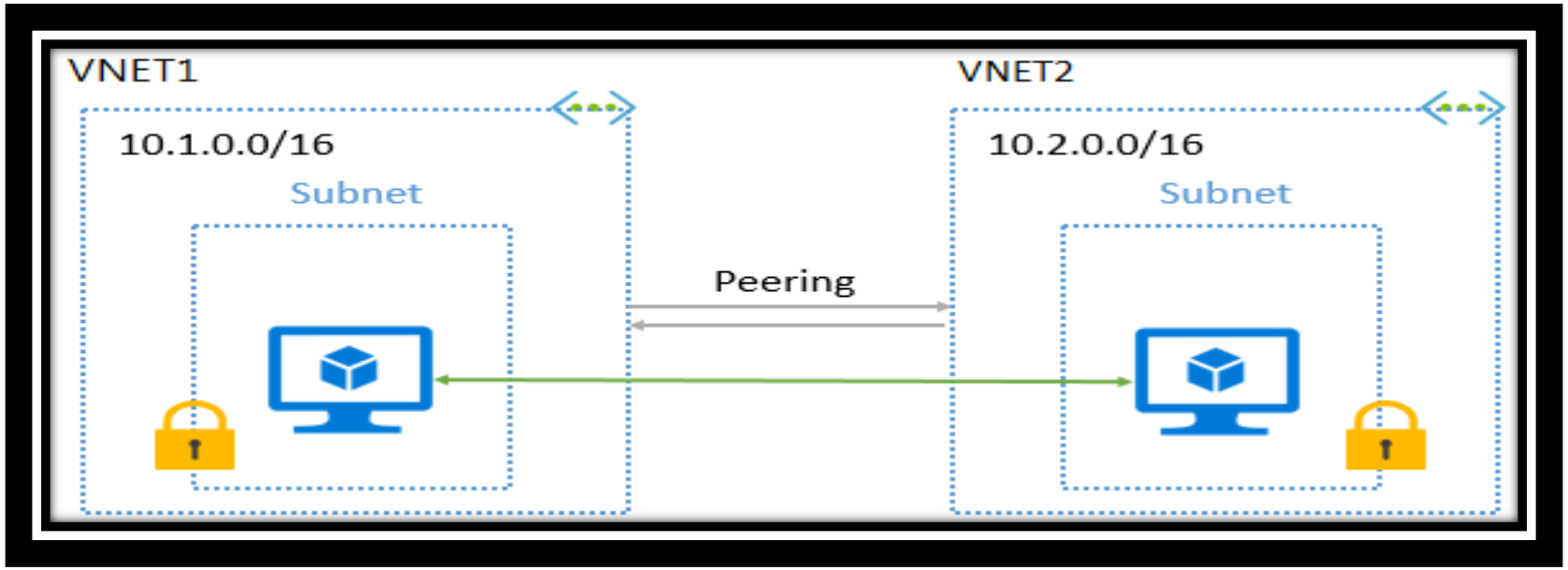
- Learn the network peering in Azure SQL MI.



Virtual Network to Virtual Network (VNet Peering)

Virtual network peering enables you to seamlessly connect two Azure virtual networks. Once peered, the virtual networks appear as one, for connectivity purposes

- VNet peering - Connecting VNets within the same Azure region.
- Global VNet peering - Connectivity across Azure regions.



Virtual Network Peering Features:

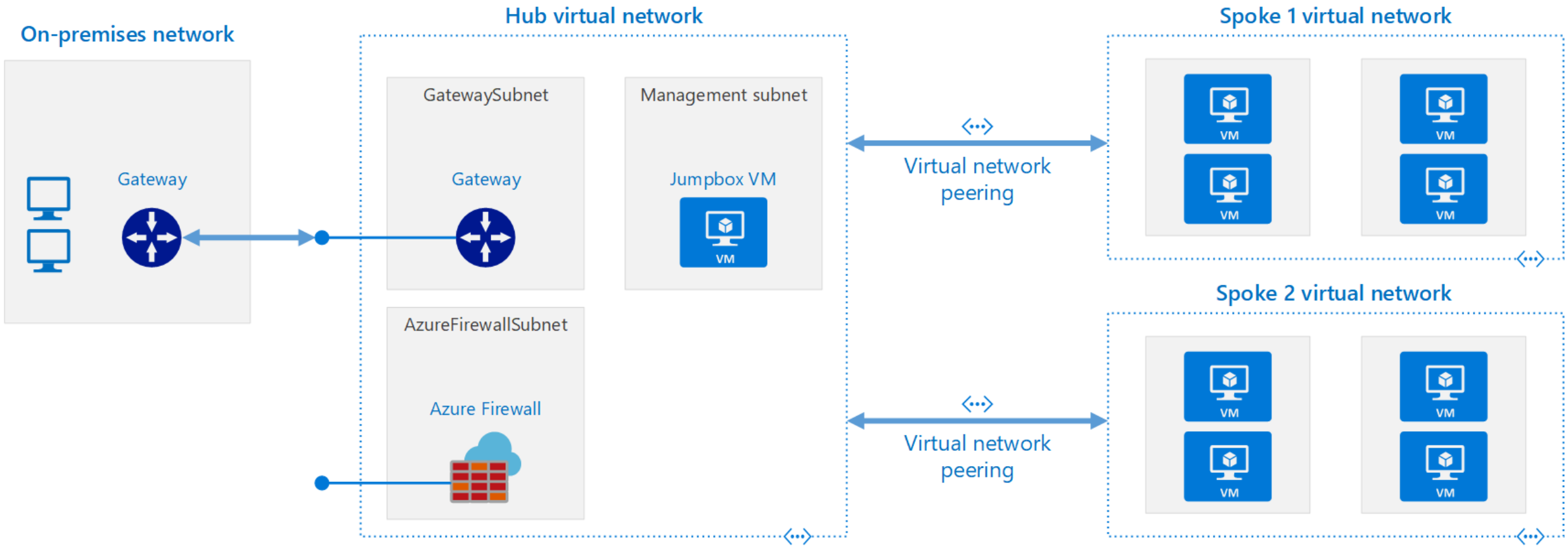
A low-latency, high-bandwidth connection between resources in different virtual networks

No public Internet, gateways, or encryption is required in the communication between the virtual networks

The ability to transfer data across Azure subscriptions, deployment models, and across Azure regions.

No downtime to resources in either virtual network when creating the peering, or after the peering is created.

Hub & Spoke Architecture



Questions?

Module Summary

Overview of Azure SQL MI security

Isolation and Connectivity

Azure Virtual Network, Security Rules

Network Peering