# Microsoft Azure Security Engineer: Implement Advanced Network Security

## SECURING CONNECTIONS BETWEEN VMS AND AZURE SERVICES

**Gabriel McNeilly**
CLOUD & QA ENGINEER

@gmcneilly  software-tester.io

# Securing Connections between VMs and Azure Services

Configuring Network Security Groups and Application Security Groups


Configuring a firewall on a Storage Account, Azure SQL, Key Vault or App Service

Implementing Service Endpoints

Configuring Azure Bastion

# Securing Web Applications Hosted in Azure

Configuring Azure Front Door as an application gateway

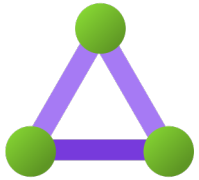
Configuring a Web Application Firewall on Azure Application Gateway

Creating and configuring Azure Firewall

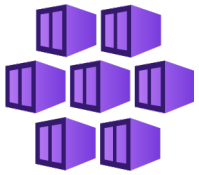
Implementing DDoS Protection

# Securing Connections to Virtual Networks

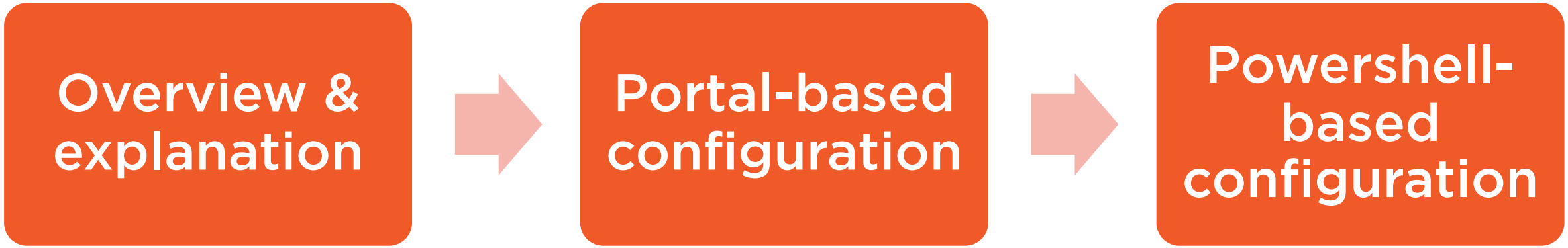
**VPNs**



**Azure ExpressRoute**



**Integrating Azure Kubernetes Service with virtual networks**


Overview & explanation
Portal-based configuration
Powershell-based configuration

# Network Security Groups and Application Security Groups

# Network Security Group (NSG)

A basic stateful packet filtering firewall

Allows you to control network traffic via security rules

Does not provide application layer inspection or authenticated access controls

# Default Security Rules

Inbound security rules

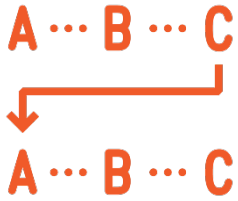
| Priority | Name | Port | Protocol | Source | Destination | Action |
|---|---|---|---|---|---|---|
| 65000 | AllowVnetInBound | Any | Any | VirtualNetwork | VirtualNetwork | Allow |
| 65001 | AllowAzureLoadBalancerInBound | Any | Any | AzureLoadBalancer | Any | Allow |
| 65500 | DenyAllInBound | Any | 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 |

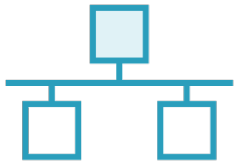
# NSG Security Rules

Name




Priority

Source & Destination



Source & Destination Ports

Protocol

Action

# Sources and Destinations

Any

IP address

Application Security Group

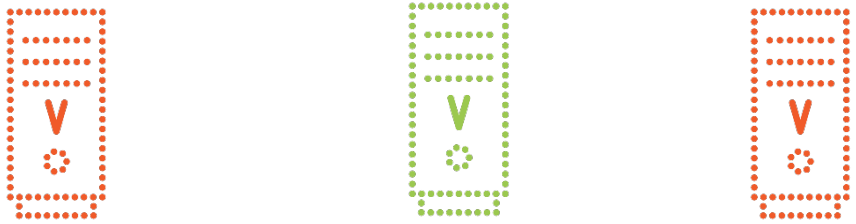
Service Tag

# Application Security Group

A method of logically grouping virtual machines in order to minimise the effort required to define and maintain NSG security rules

Subnet 1

10.0.0.1 10.0.0.2 10.0.0.3



App-Vm1 Sales-Vm1 App-Vm2

NSG

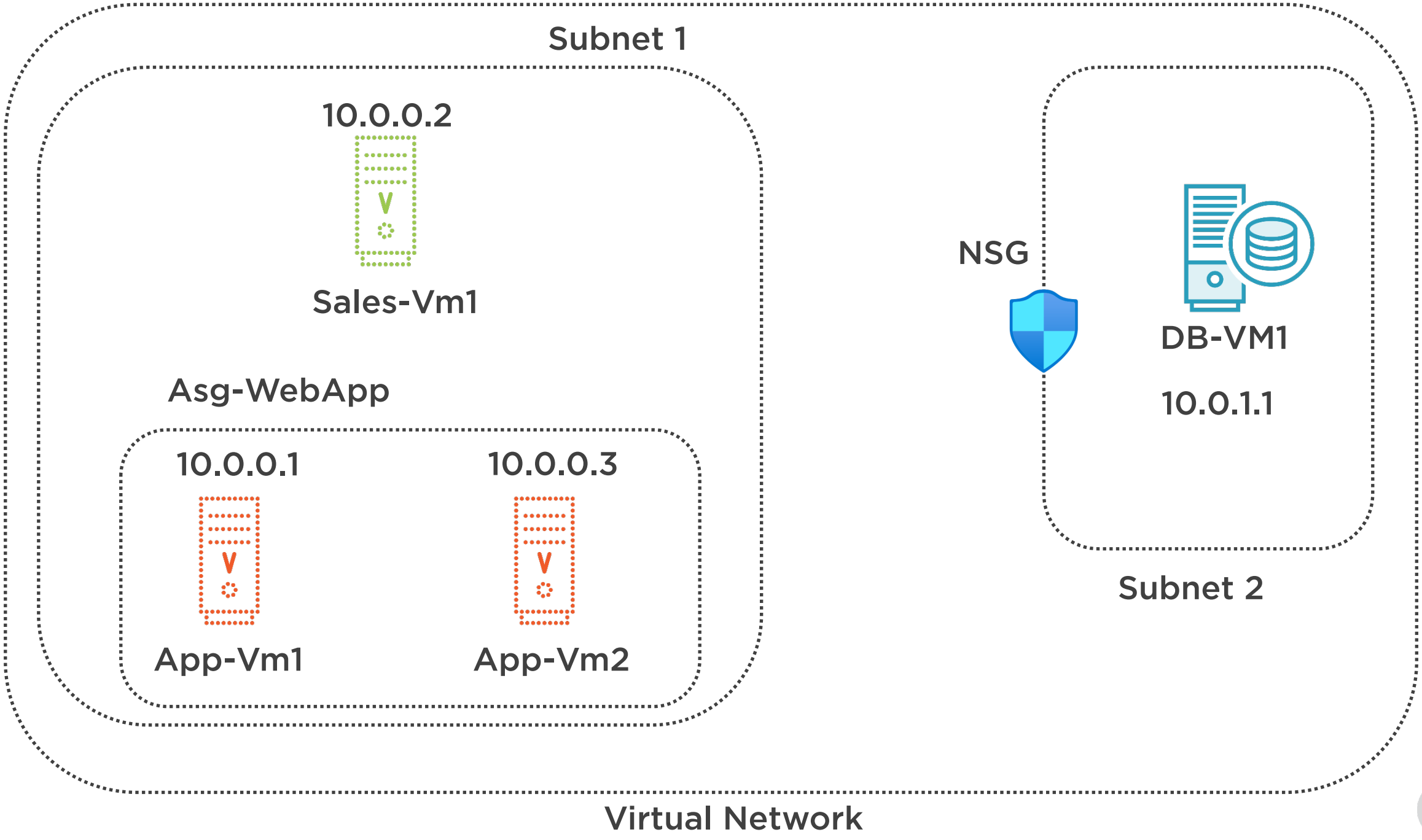
DB-VM1

10.0.1.1

Subnet 2

1. Allow inbound traffic from Subnet 1
2. Allow inbound traffic from each IP address
3. Allow inbound traffic from an ASG

Virtual Network


Subnet 1
10.0.0.2
Sales-Vm1
Asg-WebApp
10.0.0.1
App-Vm1
10.0.0.3
App-Vm2
NSG
DB-VM1
10.0.1.1
Subnet 2
Virtual Network

# Application Security Groups

Reduce maintenance of NSG security rules

Can be used as the source and destination for a security rule

You cannot use ASGs with NICs in different virtual networks if you are using them as the source and destination

You cannot add NICs from different virtual networks to the same ASG

You cannot specify multiple ASGs as the source or destination

# Demo

Add an NSG to a subnet

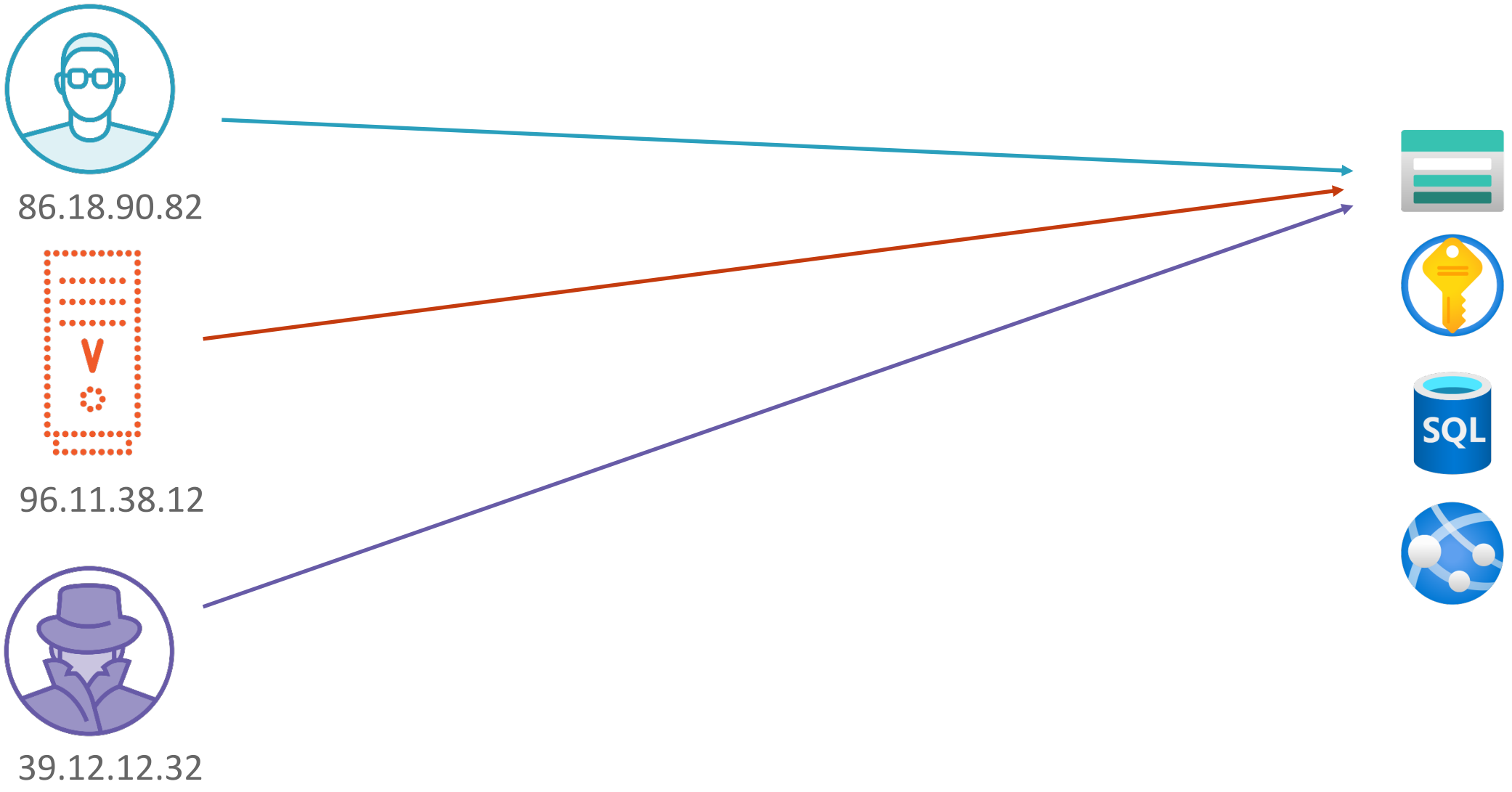
Allow RDP access to the subnet

Create an ASG

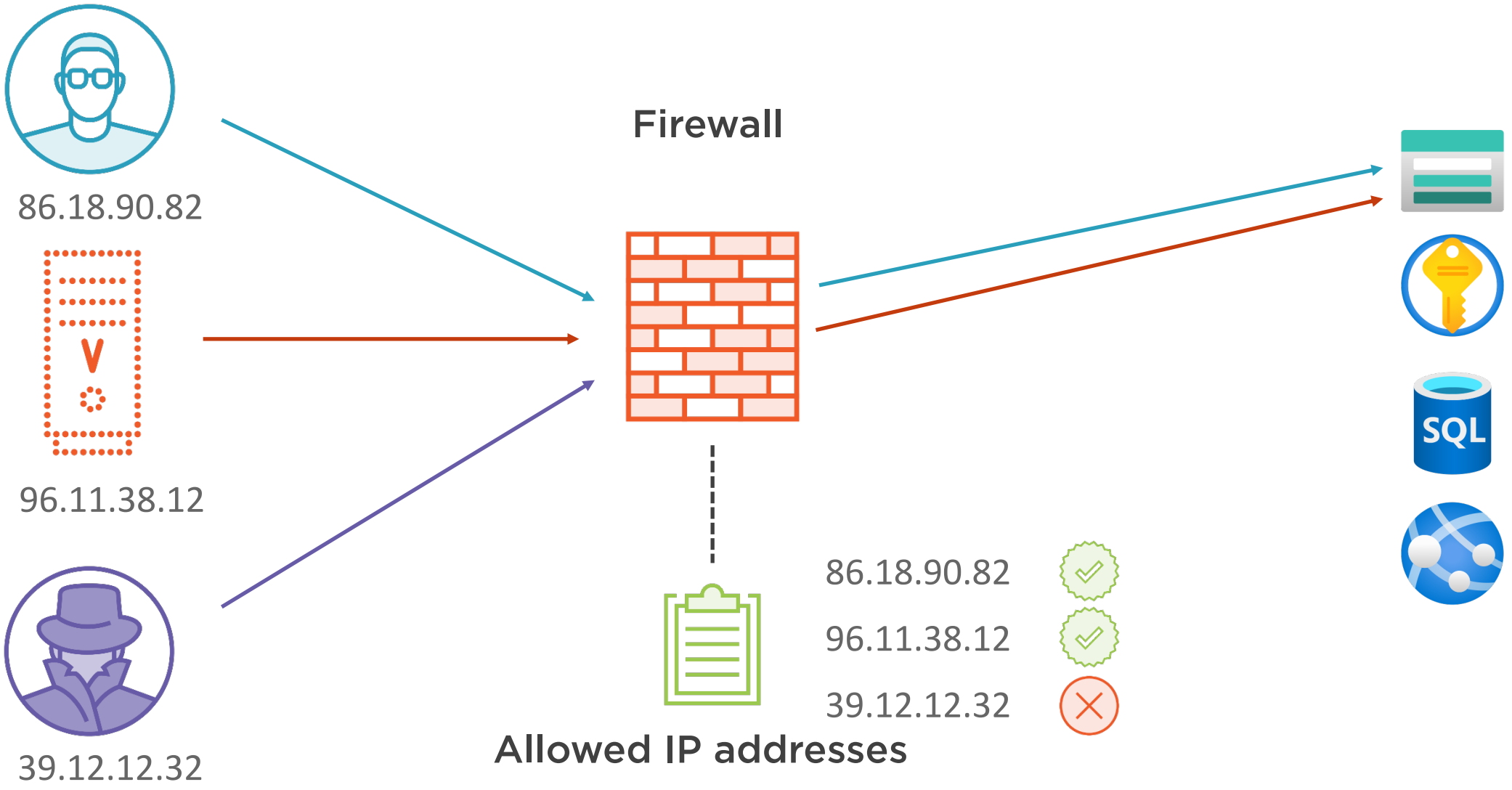
Allow HTTP traffic from a VM on the subnet to the ASG

# Firewalls on a Storage Account, Azure SQL, Key Vault or App Service

# IP-based Firewalls



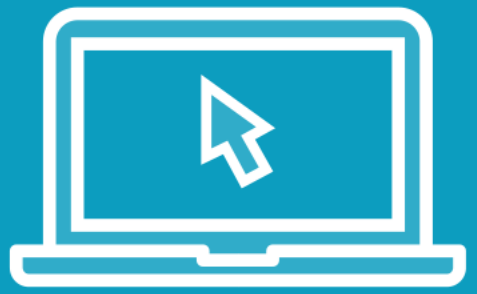
# IP-based Firewalls



# Default Firewalls for Resource Types

| Allow All | Deny All |
| --- | --- |
| Azure Storage | Azure SQL |
| Azure Key Vault | |
| Azure App Service | |

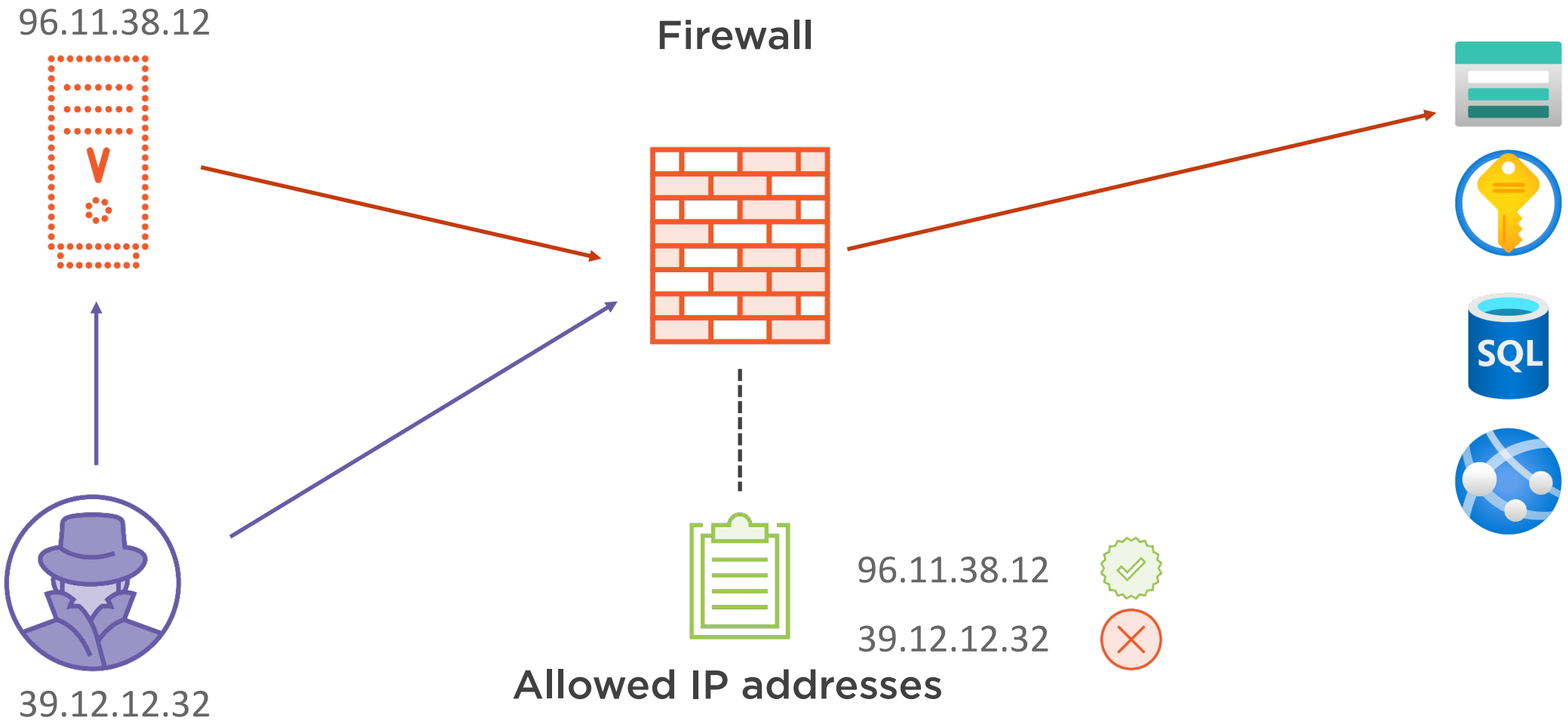
# Demo



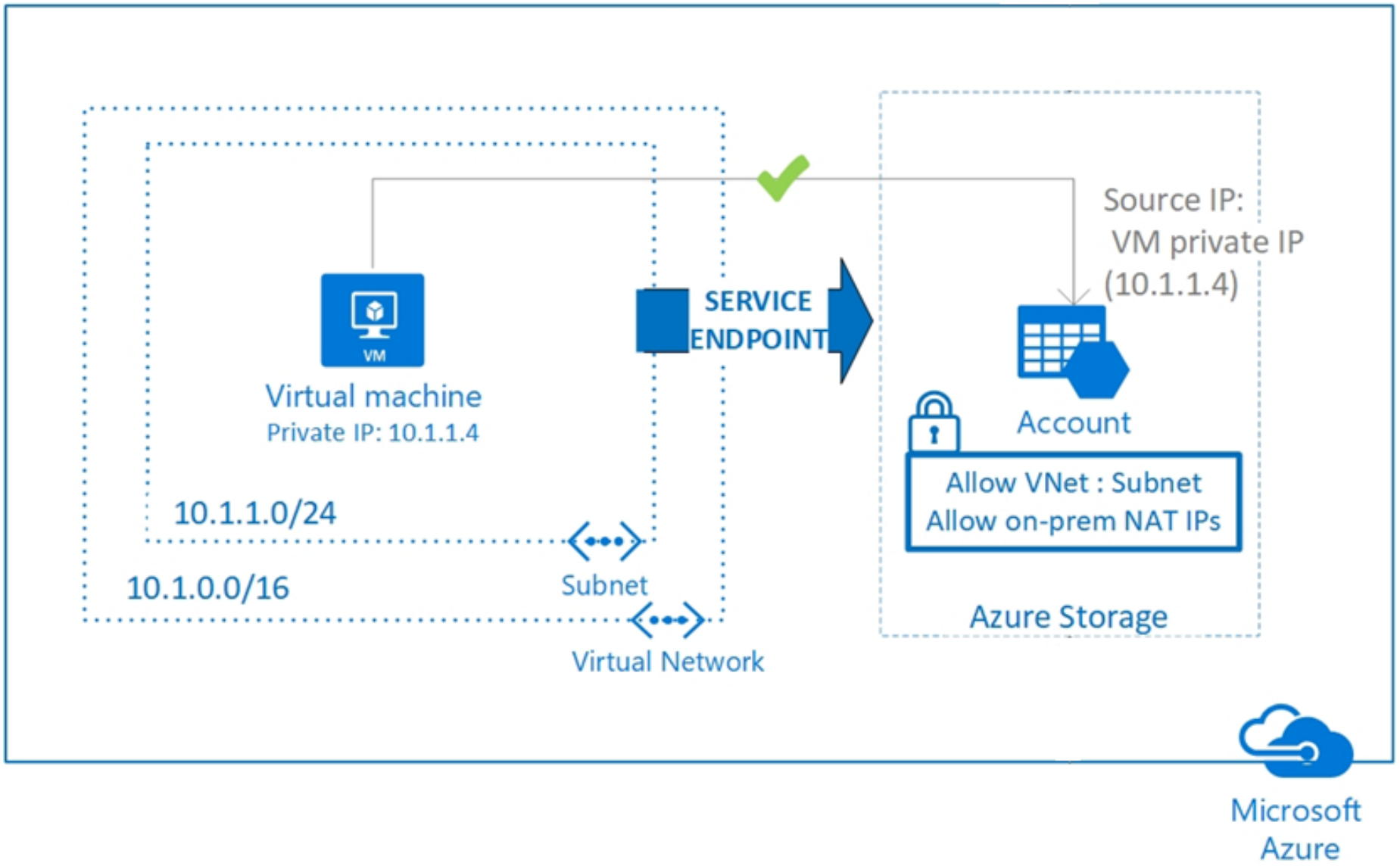
- Configure a firewall for a SQL DB
- Configure a firewall for a storage account
- Configure a firewall for a key vault
- Configure a firewall for an app service

# Service Endpoints

# The Problem with IP-based Firewalls

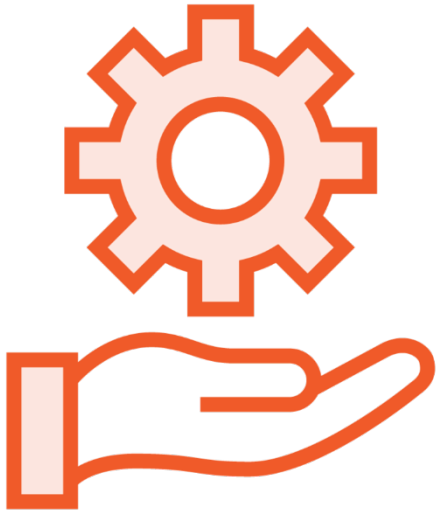


# Service Endpoints



# Benefits of Service Endpoints

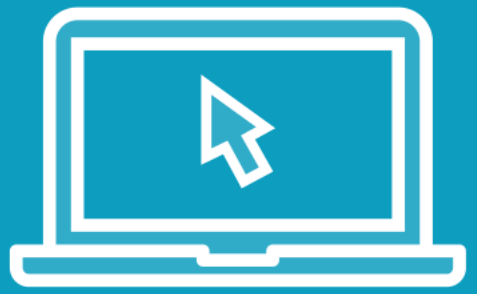
**Improved Security**



**Reduced Maintenance**

**Improved Performance**

# Demo



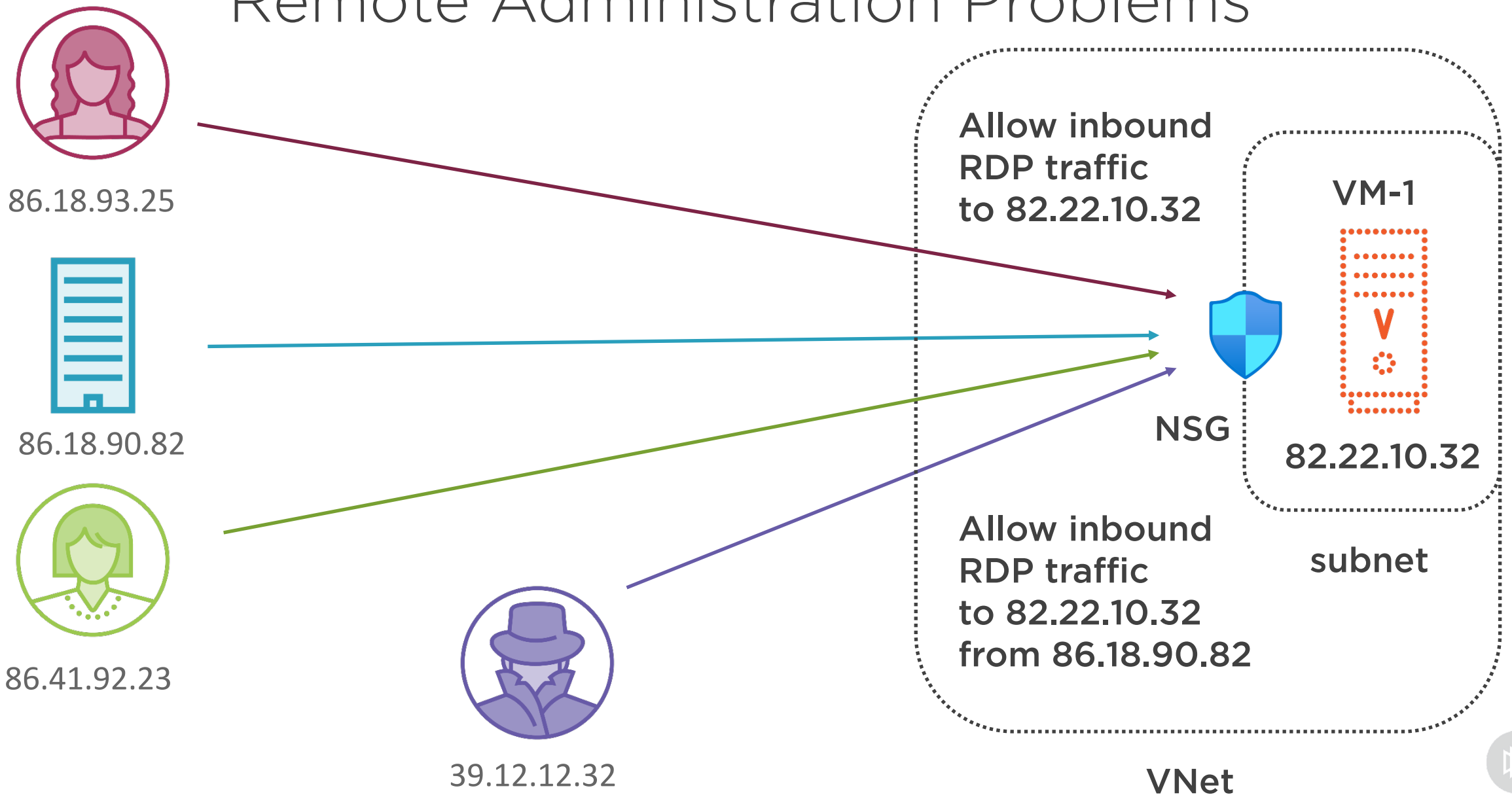
Add a service endpoint for a storage account

Configure NSG rules

Restrict network access to the storage account

# Azure Bastion

# Remote Administration Problems

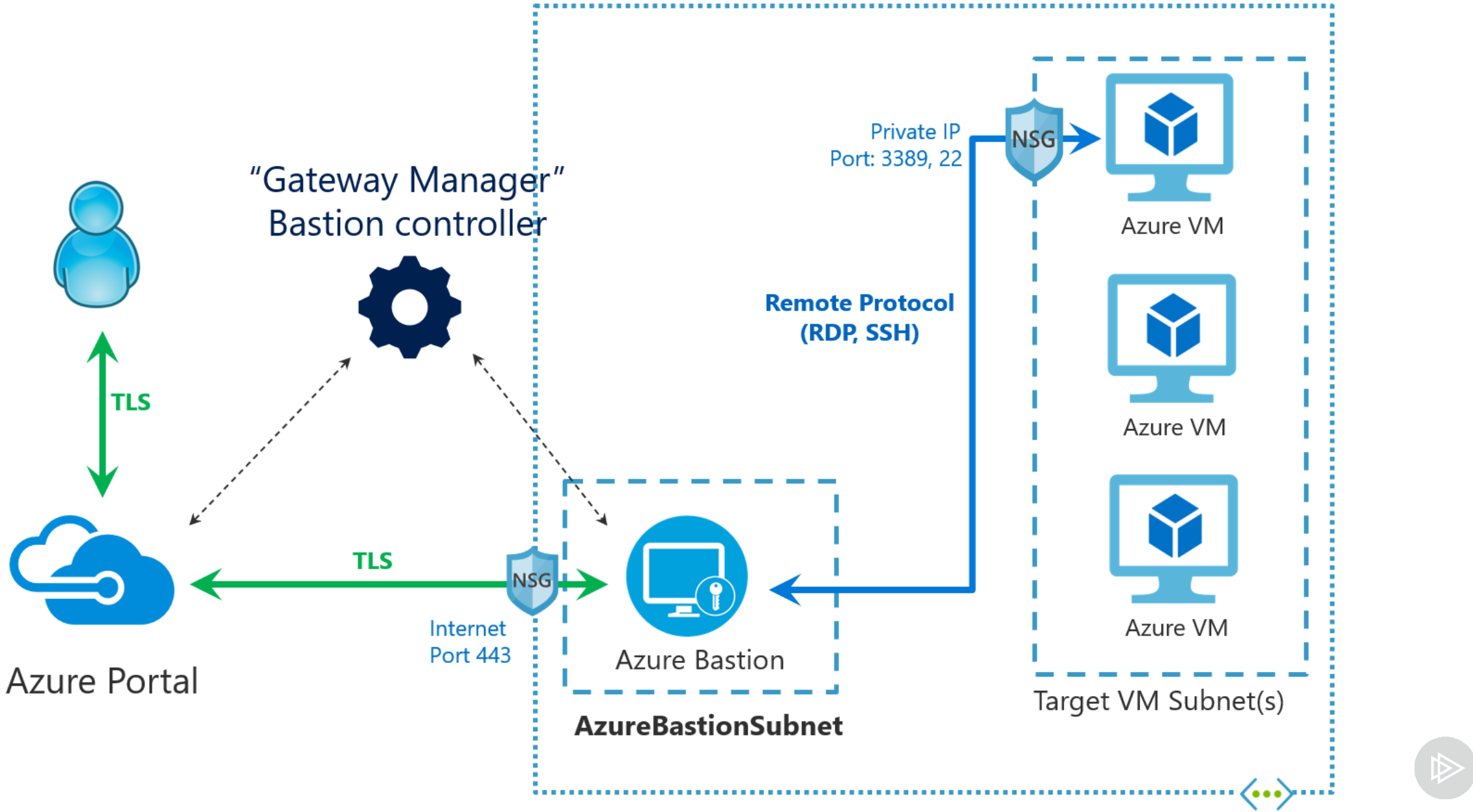


# Azure Bastion

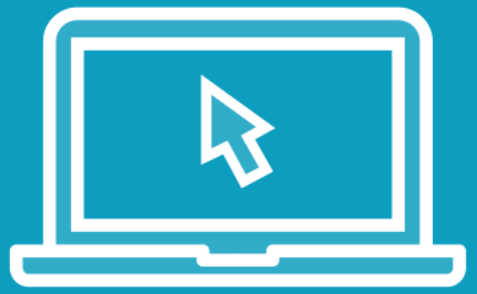
You can start an RDP or SSH session on your Azure VMs via the portal

You can allow RDP or SSH traffic from only the Azure Bastion

Your VMs do not require public IP addresses


"Gateway Manager"
Bastion controller
TLS
Azure Portal
TLS
NSG
Internet
Port 443
Azure Bastion
AzureBastionSubnet
Private IP
Port: 3389, 22
NSG
Remote Protocol
(RDP, SSH)
Azure VM
Azure VM
Azure VM
Target VM Subnet(s)

# Demo



Deploy an Azure Bastion

Create the required NSG security rules

Connect to a VM via the Bastion