**Microsoft Azure Fundamentals: Azure Secure Networks**

**Azure Network Security Groups (NSGs)**

* Used to filter network traffic
* Filter traffic between Azure resources in a virtual network

Ein Bild, das Screenshot, Kreis, Logo, Grafiken enthält.

KI-generierte Inhalte können fehlerhaft sein.

**Security Rules**

Ein Bild, das Text, Stecker enthält.

KI-generierte Inhalte können fehlerhaft sein.

**How Security Rules Work**

* Security rules are evaluated based on five-tuple information
* Only a single rule can be created with same priority and direction
* Flow records are created for existing connections
* Communication is permitted based on the connection state of the flow record

**Security Rule Properties**

* Name
* Priority
* Source or destination
* Protocol

Ein Bild, das Text, Stecker, Design enthält.

KI-generierte Inhalte können fehlerhaft sein.

**Augmented Security Rules**

* Service tags
* Application security groups

**Managing NSGs Using the Azure Portal**

Network security groups 🡪 Create

Network security groups 🡪 „sbdemo1803“ 🡪 Inbound security rules 🡪 Add (AllowHttp Port 80)

Network security groups 🡪 „sbdemo1803“ 🡪 Outbound security rules

**Managing NSGs Using the Command Line Interface (CLI)**

Az login

Cls

Az network nsg list

Az network nsg create -g sbdemo1803 -n sbdemo1804

Cls

Az network nsg rule create -g sbdemo1803 --nsg-name sbdemo1804 -n AllowHttp --direction inbound --destination-port-ranges 80 --access allow --priority 100

Az network nsg show -g sbdemo1803 -n sbdemo1804

**Managing NSGs Using PowerShell**

Connect-AzAccount

Cls

Get-AzNetworkSecurityGroup

New-AzNetworkSecurityGroup -ResourceGroupName sbdemo1803 -Name sbdemo1805 -Location „westus“

$nsg = NetworkSecurityGroup -ResourceGroupName sbdemo1803 -Name sbdemo1804

$nsg | Add-NetworkSecurityRuleConfig -Name AllowHttp -Direction Inbound -DestinationPortRange 80 -Access -Priority 100 -Protocol TCP -SourcePortRange \* -SourceAddressPrefix \* -DestinationAddressPrefix \* | Set-AzNetworkSecurityGroup

Get-AzNetworkSecurityGroup -ResourceGroupName sbdemo1803 -Name sbdemo1805

**Azure Firewall**

* Cloud-native intelligent firewall service
* Cloud workload threat protection

Ein Bild, das Text, Schrift, Screenshot, Kreis enthält.

KI-generierte Inhalte können fehlerhaft sein.

**Azure Firewall Basic**

* Threat Intel alert mode only
* Fixed scale unit for two VM instances
* 250 Mbps throughput recommended

**Azure Firewall Standard**

* L3-L7 filtering and threat intelligence
* Alerts and denies traffic to or from known malicious sites

**Azure Firewall Premium**

* Signature-based intrusion detection and prevention system (IDPS)
* Pattern-based rapid detection

**Azure Firewall Manager**

Central mamagement of Azue Firewalls

Support for VNet and Virtual WAN environment firewalls

**Managing Azure Firewall Application Rules**

Firewalls 🡪 Create

Firewalls 🡪 „sbdemo1807“ 🡪 Firewall Policy 🡪 Add a rule collection

**Managing Azure Firewall Network Rules**

Firewalls 🡪 „sbdemo1807“ 🡪 Firewall Policy 🡪 Application rules

Firewalls 🡪 „sbdemo1807“ 🡪 Firewall Policy 🡪 Network rules 🡪 Add a rule collection

**Managing Azure Firewall Network Address Translation (NAT) Rules**

Firewalls 🡪 „sbdemo1807“ 🡪 Public IP (copy)

Firewalls 🡪 „sbdemo1807“ 🡪 Firewall Policy 🡪 DNAT rules 🡪 Add a rule collection