**Microsoft Azure Fundamentals: Azure VNet Peering & VPNs**

**Virtual Network (VNet) Peering**

* Improved network performance
* Private IP connectivity

**VNet Peering**

**Ein Bild, das Text, Diagramm, Schrift, Reihe enthält.

KI-generierte Inhalte können fehlerhaft sein.**

. VNets can be within or spread among Azure subscriptions

. VNets can be within or spread among Azure regions

· Peering is completed when the peering status says "Connected"

. VNet peering is not transitive (VNet1 <- >VNet2, VNet2 <- >VNet3 -VNet1 is not peered to VNet3)

**VNet Peering - Azure Portal**

Virtual Networks 🡪 Vnet1 🡪 Peerings

**Peering VNets Using the Azure Portal**

Virtual Networks 🡪 Vnet1 🡪 Peerings

**Peering VNets Using the Command Line Interface (CLI)**

VNet1=$(az network vnet show --resource-group east --name vnet1 --query id --out tsv)

Echo $VNet1

VNet3=$(az network vnet show --resource-group east --name vnet3 --query id --out tsv)

Echo $VNet1

Az network vnet peering create --name Vnet1ToVnet3 --resource-group east --vnet-name VNet1 --remote-vnet $VNet3 --allow-vnet-access

Az network vnet peering create --name Vnet3ToVnet1 --resource-group east --vnet-name VNet3 --remote-vnet $VNet1 --allow-vnet-access

**Peering VNets Using PowerShell**

$vnet1 = Get-AzVirtualNetwork -Name VNet1 -ResourceGroupName east

$vnet1

$vnet3 = Get-AzVirtualNetwork -Name VNet3 -ResourceGroupName east

$vnet3

$vnet3 | get-member -type property

$vnet3.id

$vnet1.id

Add-AzVirtualNetworkPeering -Name VNet1-Vnet3 -VirtualNetwork $vnet1 -RemoteVirtualNetworkId $vnet3.Id | Out-Null

Add-AzVirtualNetworkPeering -Name Vnet3-VNet1 -VirtualNetwork $vnet3 -RemoteVirtualNetworkId $vnet1.Id | Out-Null

**Virtual Private Networks (VPNs)**

* Remote access to a private network over an untrusted network such as the Internet
* Encrypted network tunnel (encryption of data in transit) linking both VPN endpoints

**Common VPN Protocols**

· Point-to-Point Tunneling Protocol (PPTP)

. Not considered secure

. Layer 2 Tunneling Protocol (L2TP)

. Normally uses Internet Protocol Security (IPsec)

. Secure Sockets Layer (SSL)/Transport Layer Security (TLS)

. Firewall friendly, Transmission Control Protocol (TCP) 443

. Users access remote network resources through a web browser

**Client-to-site VPN**

* Links a single client device over the Internet to a private network located elsewhere
* VPN clients are assigned an IP address from a preconfigured IP address pool
* Additional IP configurations show up on a client device
* Client authentication can use multi-factor authentication (MFA), for example, one-time codes, public key infrastructure (PKI) certificates, or biometrics in addition to a username and password

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

KI-generierte Inhalte können fehlerhaft sein.

**Site-to-site VPN**

* Links networks together over the Internet
* IPsec, Secure Socket Tunneling Protocol (SSTP), OpenVPN SSL/TLS
* Client device VPN software not required
* Allows connectivity of resources between networks

Ein Bild, das Text, Diagramm, Schrift, Reihe enthält.

KI-generierte Inhalte können fehlerhaft sein.

**Point-to-site VPN Clients**

* VPN client software
* VPN client configuartion file (.zip)
* Client certificate authentication

**Generating Self-signed Certificates Using PowerShell**

Get-command \*certificate\*

#Create self-signed root certificate

$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature

-Subject „CN-RootCert“ -KeyExportPolicy Exportable

-Hashalgorithm sha256 -KeyLength 2048

-CertStoreLocation „CertStoreLocation „Cert:\CurrentUser\My“ -KeyUsageProperty Sign -KeyUsage -CertSign

#Create client certificate using the self-signed root certificate from above

New-selfsignedCertificate -Type Custom -DnsName ClientCert -KeySpec Signature

-Subject „CN=ClientCert“ -KeyExportPolicy Exportable

-HashAlgorithm sha256 -KeyLength 2048

-CertStoreLocation „Cert:\CurrentUser\My“

-Signer $cert -TextExtension @(„2.5.29.37={text}1.3.6.1.5.5.7.3.2“)

**Configuring a Site-to-site VPN**

Create a resource 🡪 virtual network gateway

Create a resource 🡪 local network gateway (public IP from virtual network gateway)

LocalNetworkGatewayCreate-20…🡪 onprem\_site1\_vpn 🡪 Connections

**Configuring a Point-to-site VPN**

VPN-Gateway needed

All resources 🡪 azure\_vpn\_east (Gateway) 🡪 Point-to-site configuration

Certificate from windows management console 🡪 Export public key (Base64)

**Azure ExpressRoute**

* Private dedicated wide area network (WAN) circuit (does not use the Internet)
* Link on-premises network to the Azure cloud through a dedicated WAN connection

**ExpressRoute**

* Requires an Azure subscription
* ExpressRoute circuit is an Azure cloud resource
* Router technician configures on-premises router

**ExpressRoute Configuration**

* Provider (TELUS, Bell Canada, British Telecom, and more)
* Peering location (city)
* Bandwidth (50 Mbps-10 Gbps)

**Provisioning ExpressRoute**

* ExpressRoute circuit globally unique identifier (GUID) is the service key
* Example: 02fc90da-c6f6-43d6-be36-56bfb077bd54
* Unique service key is provided to the service provider

1. Create ExpressRoute resource
2. Provide unique service key to provider
3. Provider status changes to "Provisioned"
4. Link VNets to the ExpressRoute circuit

**ExpressRoute Direct**

* Designed for large amounts of data transfer
* From 10 Gbps up to 100 Gbps dual links
* Private dedicated network