Microsoft Azure Administrator: Integrate On-Premises Networks with Azure Virtual Networks

CONFIGURING AN AZURE VIRTUAL PRIVATE NETWORK

Tim Warner
AUTHOR EVANGELIST, PLURALSIGHT

@TechTrainerTim   TechTrainerTim.com

Overview

Differentiate Azure VPN types

Create and configure VPNs
- Site-to-Site (S2S)
- Point-to-Site (P2S)

Exercise Files

Exercise Files

microsoft-azure-ad-privileged-identity-management-configuring-m4-links.t...

File   Edit   Selection   View   Go   Debug   ...

microsoft-azure-ad-privileged-identity-management-configuring-m4-links.txt

C: ▸ Users ▸ Tim ▸ Desktop ▸ microsoft-azure-ad-privileged-identity-management-configuring-m4-links.txt

```
 1   Module 4: Organize and Perform Azure AD PIM Access Reviews
 2
 3   Microsoft Azure
 4   https://azure.microsoft.com/en-us/
 5
 6   Azure Documentation
 7   https://docs.microsoft.com/en-us/azure/
 8
 9   Azure AD Privileged Identity Management (PIM) documentation | Microsoft Docs
10   https://docs.microsoft.com/en-us/azure/active-directory/
     privileged-identity-management/
11
12   Identity Governance - Azure Active Directory | Microsoft Docs
13   https://docs.microsoft.com/en-us/azure/active-directory/governance/
     identity-governance-overview
14
15   Create an access review of Azure resource roles in PIM - Azure Active Directory |
     Microsoft Docs
16   https://docs.microsoft.com/en-us/azure/active-directory/
     privileged-identity-management/pim-resource-roles-start-access-review
17
18   Review access to Azure AD roles in PIM - Azure Active Directory | Microsoft Docs
19   https://docs.microsoft.com/en-us/azure/active-directory/
     privileged-identity-management/pim-how-to-perform-security-review
20
21   View audit history for Azure AD roles in PIM - Azure Active Directory | Microsoft
     Docs
22   https://docs.microsoft.com/en-us/azure/active-directory/
     privileged-identity-management/pim-how-to-use-audit-log
```

⊗ 0 ⚠ 0   Spaces: 4   UTF-8   CRLF   Plain Text

C:\Users\Tim\Downloads\azur

File   Edit   View   Favorites   Too

Add   Extract   Test   Copy   Mo

C:\Users\Tim\Downloads

Name
📁 02
📁 03
📁 04
📁 05
📁 06

0 / 5 object(s) selected

02\demos\

Size   Pac
1 298
359

Microsoft Azure Administrator

Objective Domain

Exam AZ-104: Microsoft Azure Administrator – Skills Measured

Functional Group

Configure and manage virtual networking (30-35%)

Integrate an on-premises network with an Azure virtual network

Objective

- create and configure Azure VPN Gateway
- create and configure VPNs
- configure ExpressRoute
- configure Azure Virtual WAN

Skills

Azure VPN Types

Virtual Private Network (VPN)

A secure, encrypted connection over an unsecure communications medium (typically the public Internet)

Azure VPN Value Proposition

Extend local network to Azure	**Manage local systems from Azure**	**Manage Azure systems from local network**
Fully embrace hybrid cloud deployments	**Compliance**	**High availability**

Site-to-Site VPN (S2S VPN)
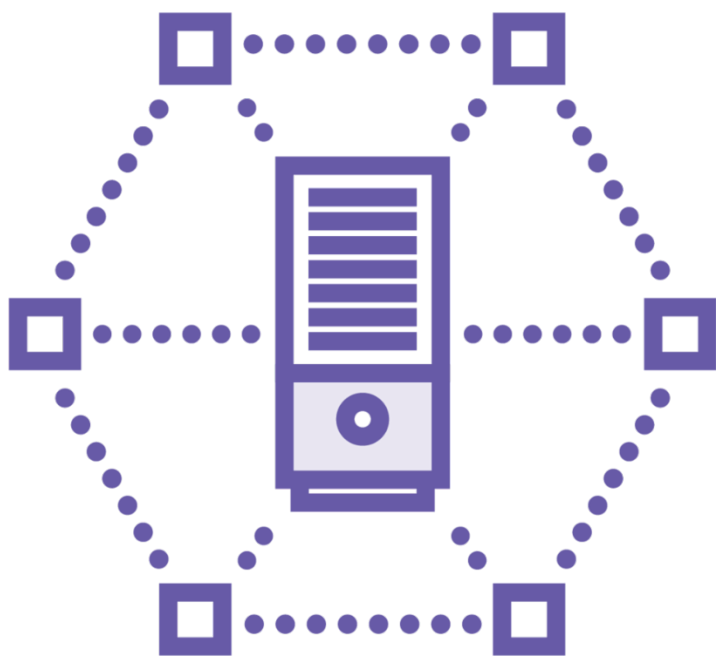
"Always on" VPN using IPSec and IKE protocols

Supports Policy Based (static) or Route Based (dynamic) routing methods

Active-Active or Active-passive HA

Number of tunnels and max bandwidth depend on SKUs

S2S VPN Topology

On-premises network

Gateway

Hub virtual network

GatewaySubnet

Gateway

Management subnet

Jumpbox VM

AzureFirewallSubnet

Azure Firewall

Virtual network peering

Virtual network peering

Spoke 1 virtual network

VM VM VM VM

Spoke 2 virtual network

VM VM VM VM

https://timw.info/bb61b
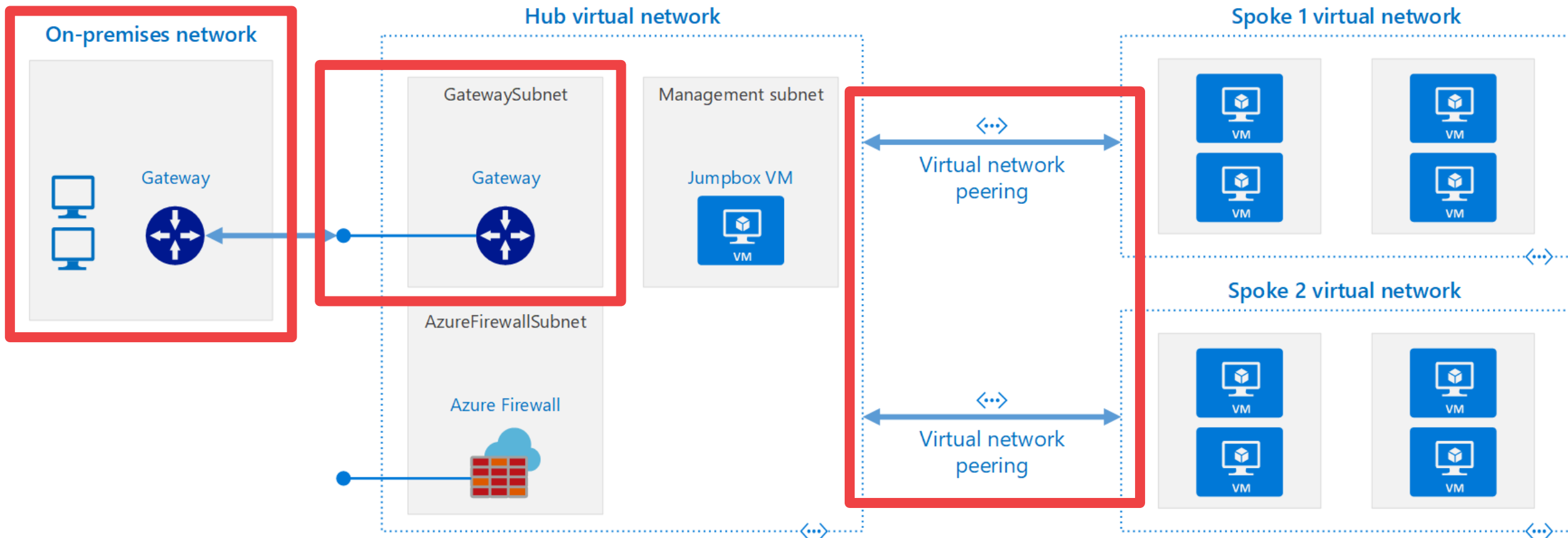
VNet-to-VNet VPN
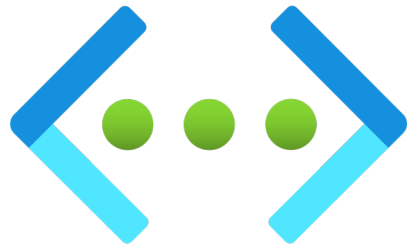
Before global VNet peering, this was once the only way to link VNets in different regions

Same IPSec/IKE secure tunnel used in S2S VPN

Local network gateways are automatically created and populated
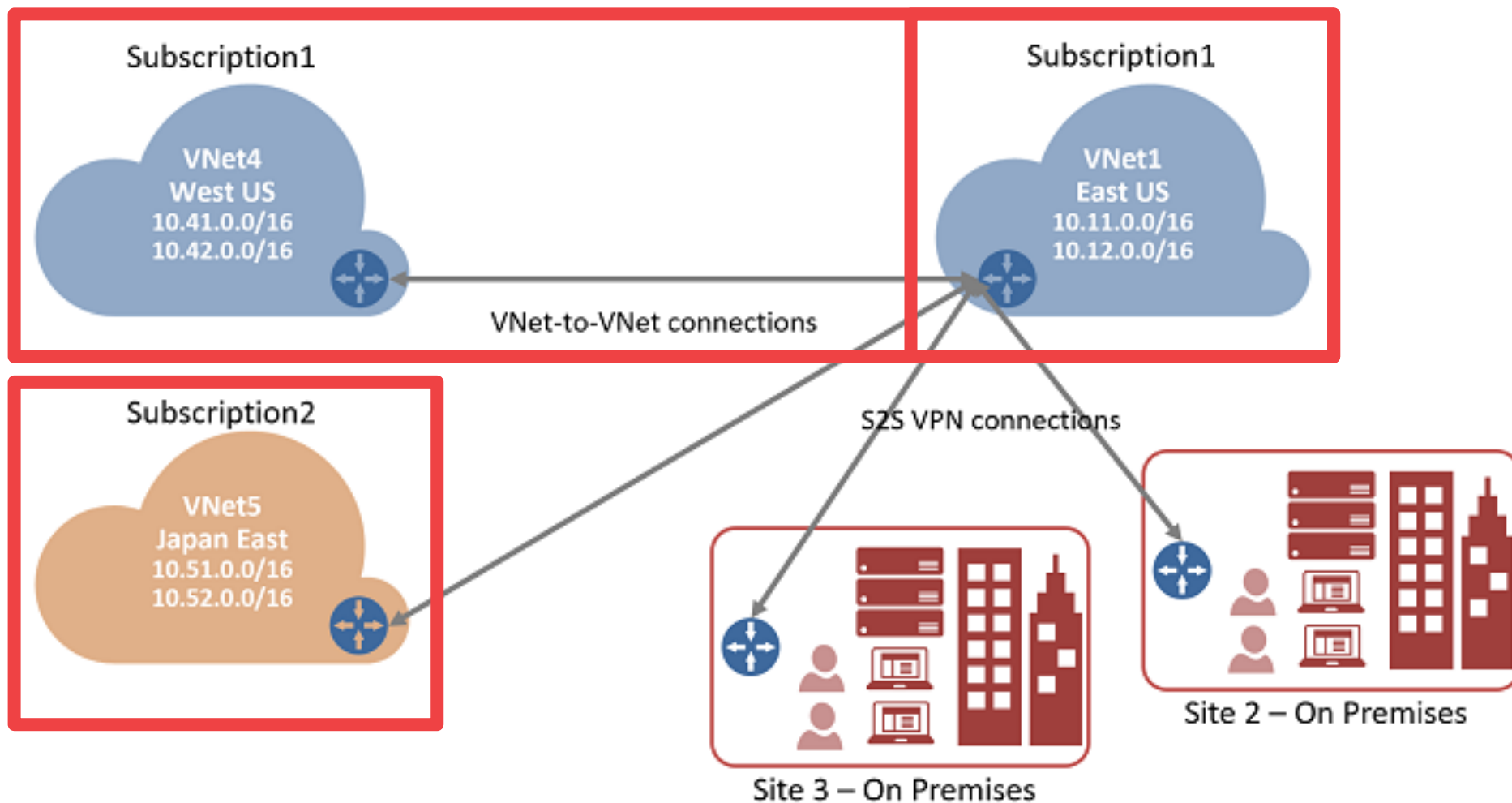
Benefit: isolation, security, administrative boundary

VNet-to-VNet VPN Topology

https://timw.info/53e5e

Point-to-Site VPN (P2S VPN)

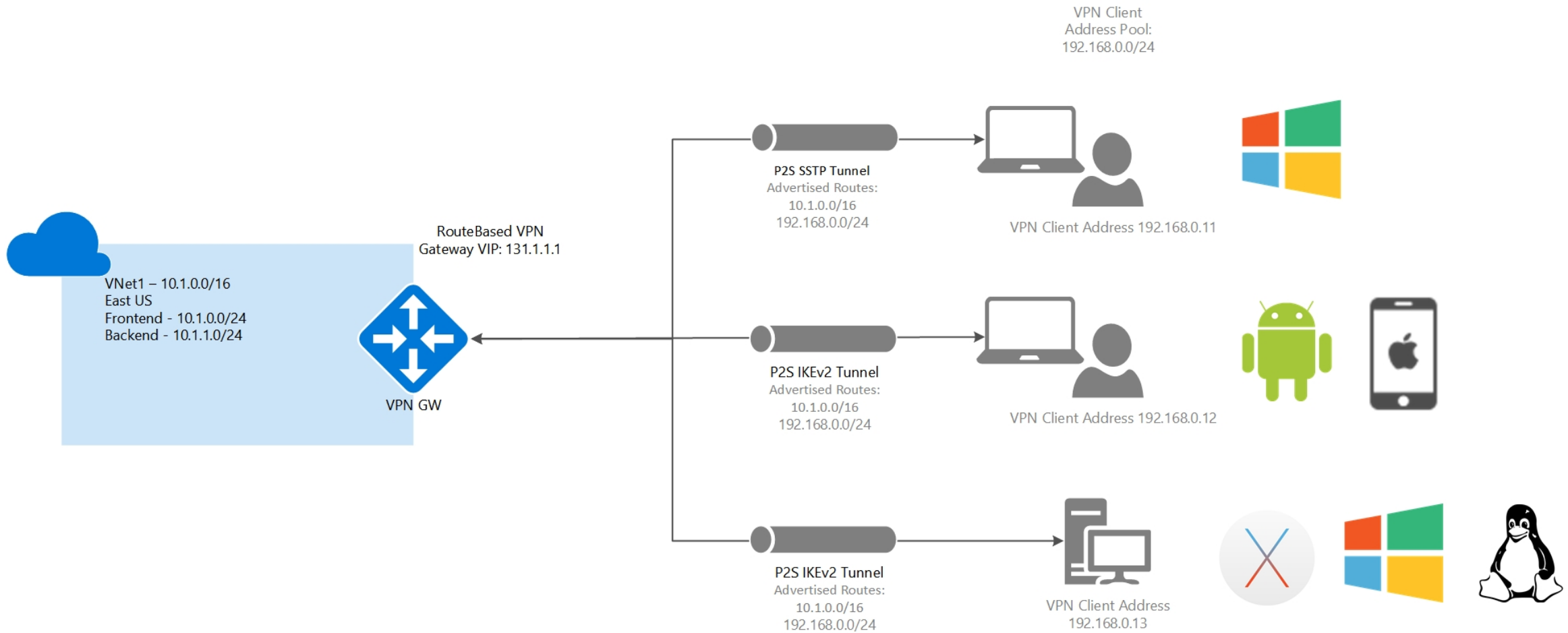**Individual VPN tunnels to the virtual network**

Standards-based protocols: OpenVPN, SSTP, IKEv2 VPN

Proof of concept deployments, remote workers

Certificate and Azure AD authentication options

P2S VPN Topology

VPN Client
Address Pool:
192.168.0.0/24

P2S SSTP Tunnel
Advertised Routes:
10.1.0.0/16
192.168.0.0/24

VPN Client Address 192.168.0.11

RouteBased VPN
Gateway VIP: 131.1.1.1

VNet1 – 10.1.0.0/16
East US
Frontend - 10.1.0.0/24
Backend - 10.1.1.0/24

VPN GW

P2S IKEv2 Tunnel
Advertised Routes:
10.1.0.0/16
192.168.0.0/24

VPN Client Address 192.168.0.12

P2S IKEv2 Tunnel
Advertised Routes:
10.1.0.0/16
192.168.0.0/24

VPN Client Address
192.168.0.13
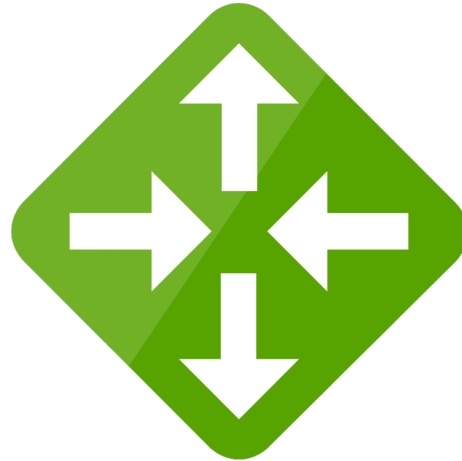
Create and Configure Azure VPNs

Azure S2S VPN Components

VPN Gateway

Azure VNet endpoint

IPSec/IKE

Local Gateway

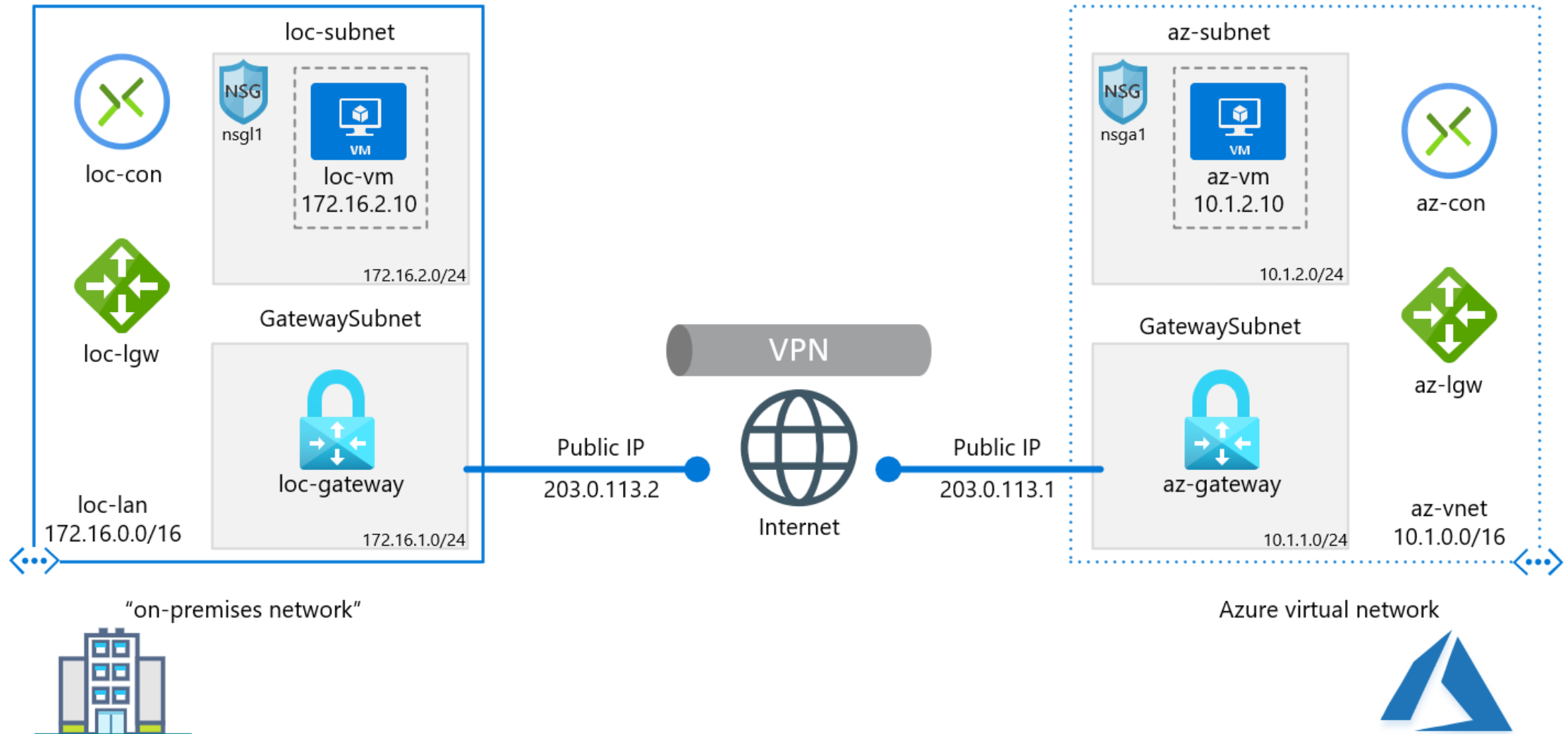Public IP address of local VPN device

Local LAN ranges

Connection

Ties together the VPN Gateway and the Local Gateway

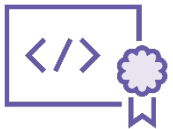# Lab Topology

Demo

1

Build S2S VPN

Test client connectivity

Azure P2S VPN Components

- VPN Gateway
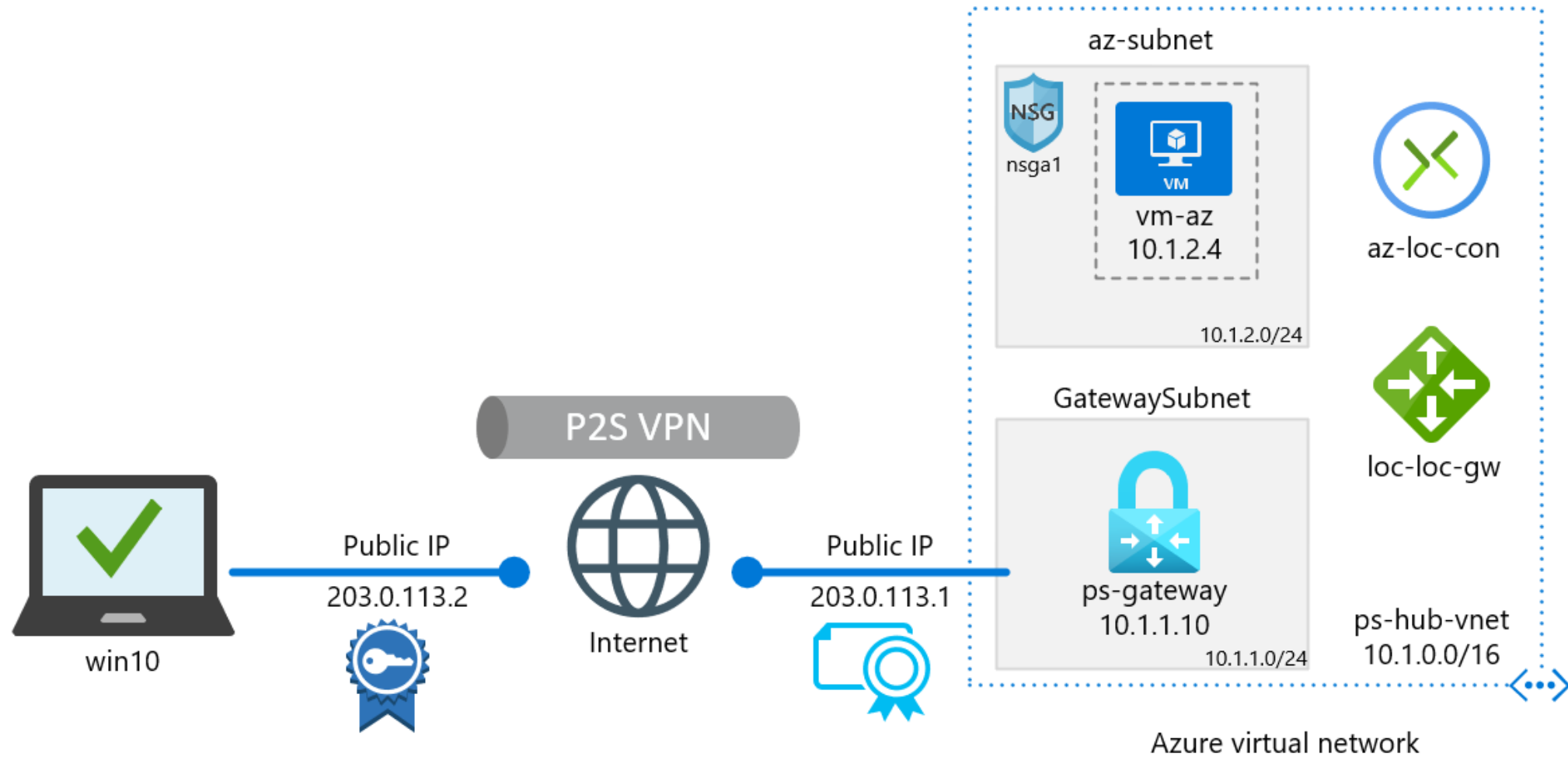- Server certificate
- Client certificate
- VPN client

Lab Topology

Demo

2

Set up a P2S VPN

Test from the client

Summary

The S2S VPN is the most straightforward method to extend your local network(s) into Azure

The P2S VPN is a flexible approach to secure Azure VNet connections

Next module: Configuring ExpressRoute and Azure Virtual WAN