

# Design, Implement, and Manage a P2S VPN Connection

---



**Tim Warner**

Author Evangelist, Pluralsight

@TechTrainerTim   TechTrainerTim.com



# Overview



**Select an appropriate virtual network gateway SKU**

**Plan and configure authentication**

- RADIUS
- Certificate-based
- OpenVPN

**Implement a VPN client configuration file**

**Diagnose and resolve client-side and authentication issues**



# Relevant Exam AZ-700 Skills

## **Exam AZ-700: Designing and Implementing Microsoft Azure Networking Solutions – Skills Measured**

### **Design, Implement, and Manage Hybrid Networking (10–15%)**

#### **Design, implement, and manage a point-to-site VPN connection**

- select an appropriate virtual network gateway SKU
- plan and configure RADIUS authentication
- plan and configure certificate-based authentication
- plan and configure OpenVPN authentication
- plan and configure Azure Active Directory (Azure AD) authentication
- implement a VPN client configuration file
- diagnose and resolve client-side and authentication issues

# Point-to-Site VPN Basics

---



## Azure P2S VPN



**You might have services bound to an Azure VNet**

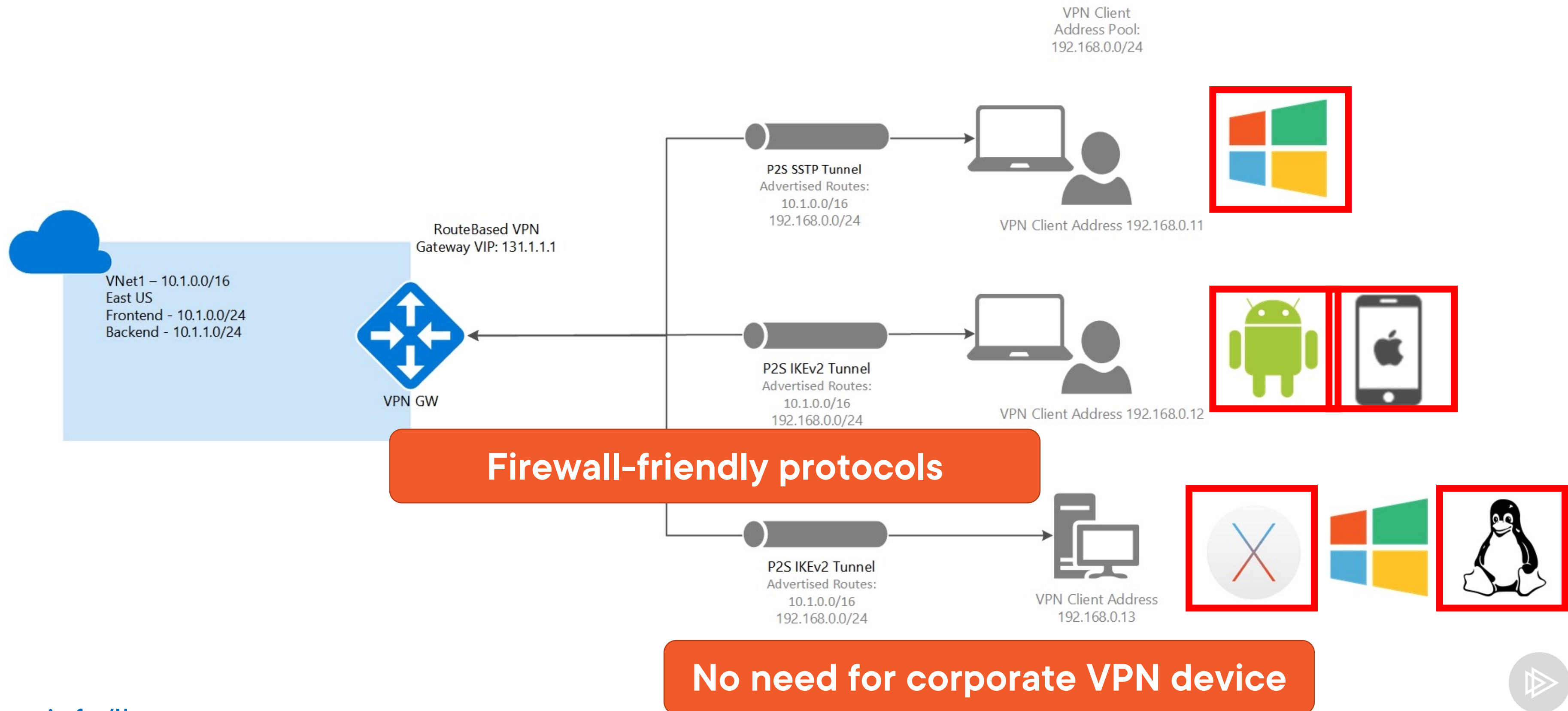
**You might have telecommuters or very few Azure users**

**You don't need or want the overhead of a S2S VPN or ExpressRoute circuit**





# Point-to-Site VPN Topology



# Configure P2S VPN Connections

---



# P2S VPN Tunnel Types



**SSTP (SSL)** - Proprietary. Supports only Windows devices



**OpenVPN (SSL)** - Open standard. Supports Windows, Linux, macOS, iOS, and Android

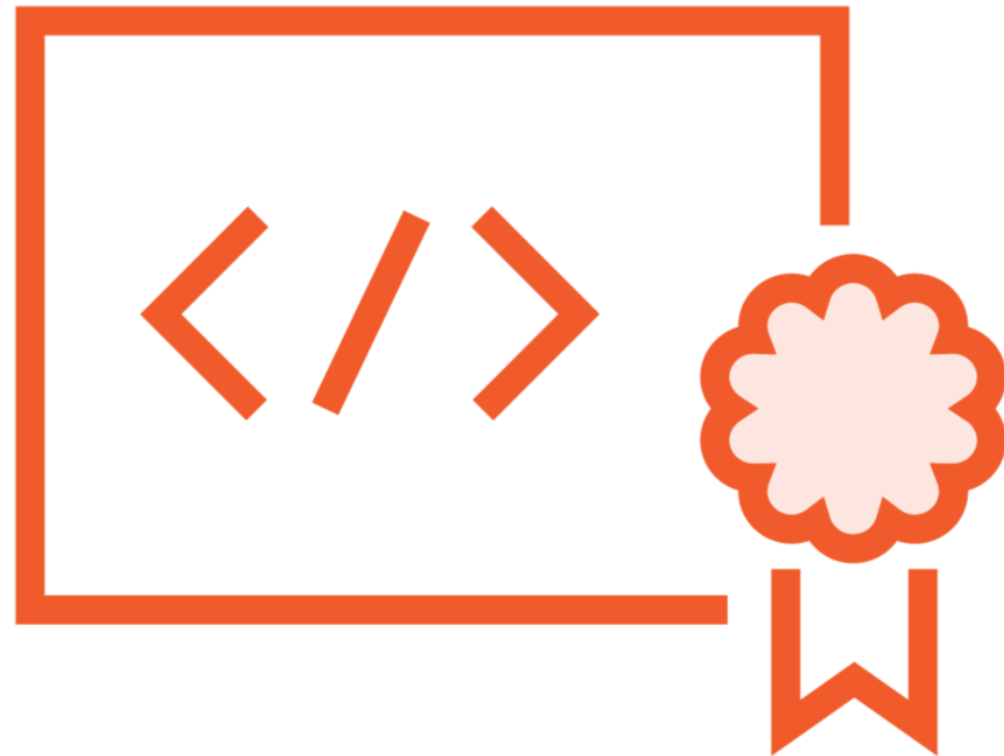


**IKEv2** - Standards-based IPSec VPN solution. Supports macOS





# P2S VPN Authentication Types



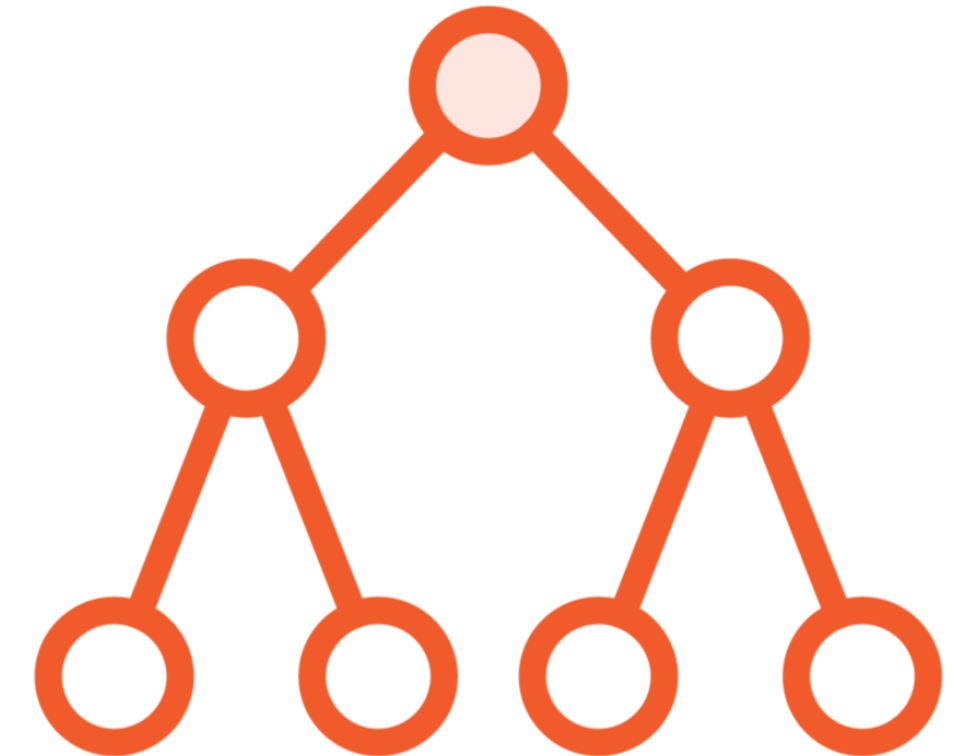
## **Azure certificate**

Client certificate  
Upload trusted root  
certificate to gateway



## **Azure AD**

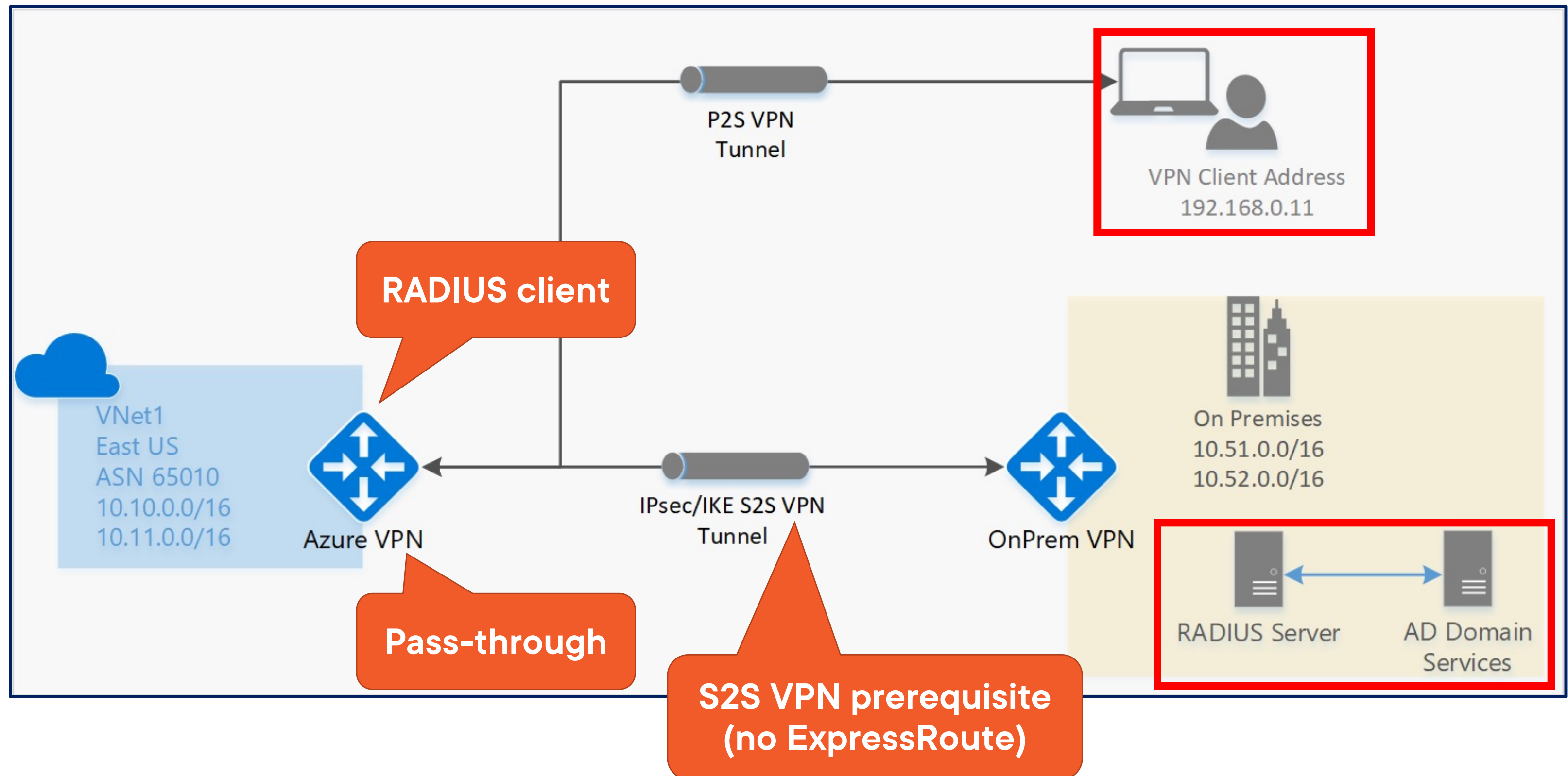
Supported only for  
Windows 10 with  
OpenVPN and Azure  
VPN Client



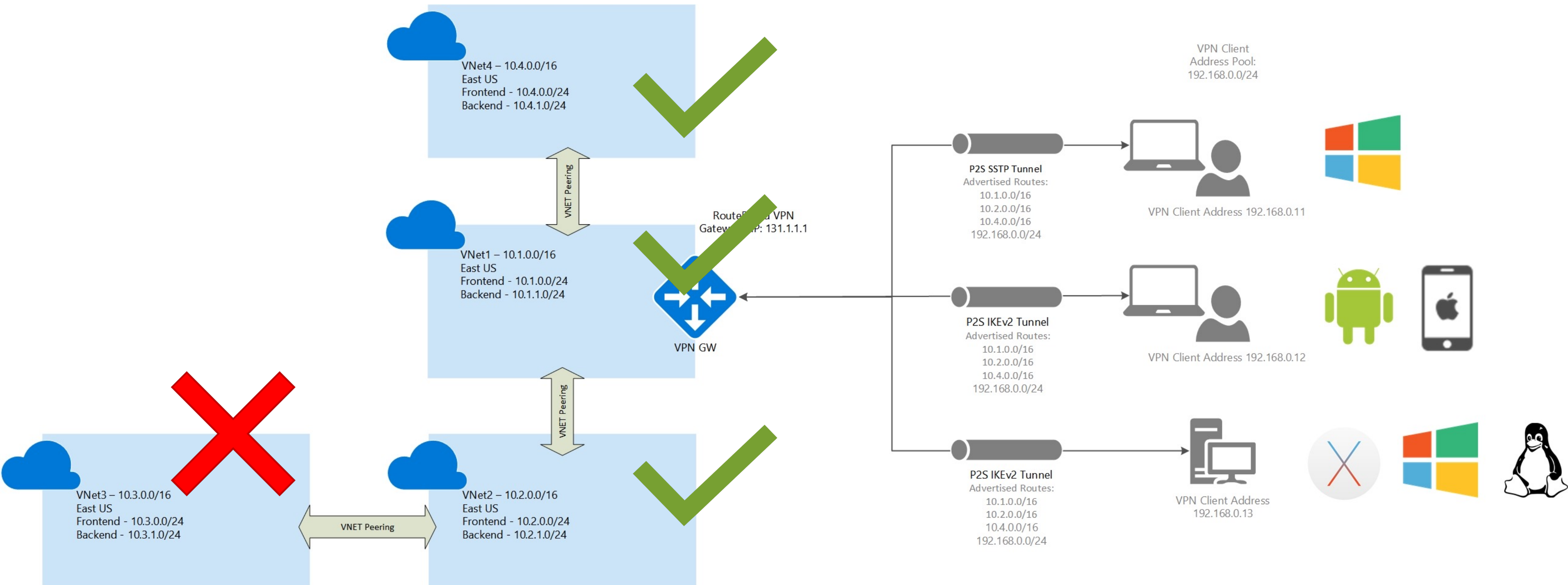
## **RADIUS**

Integrate with AD DS  
domain controllers  
Network Policy Server  
(NPS)

# Azure P2S RADIUS Authentication



# Azure P2S Routing with VNet Peering



# Configure the P2S VPN Client

Azure VPN Client

VPN Connections

Connection Name: Contoso Cert VPN

VPN Server: [Empty field]

Server Validation

Certificate Information: DigiCert Global Root CA

Server Secret: [Masked field]

Client Authentication

Authentication Type: Certificate

Client Certificate: P2SChildCert

Save Cancel

Azure VPN Client

VPN connections Home Refresh

Connection Name: Contoso VPN

VPN Server: azuregateway-4e6a0032-7aad-4e72-a46d-0c78

Server Validation

Certificate Information: DigiCert Global Root CA

Server Secret: [Masked field]

Client Authentication

Authentication Type: Azure Active Directory

Tenant: https://login.microsoftonline.com/72f988bf-86f1

Audience: 41b23e61-6c1e-4545-b367-cd054e0ed4b4

Issuer: https://sts.windows.net/72f988bf-86f1-41af-91al

Clear Saved Account

Save Cancel

Azure VPN Client



# Demo



# 1

**Set up P2S VPN**

**Test on Windows 10 client**



# Troubleshoot P2S VPN Connections

---



# Troubleshoot Azure P2S Connections

**Double-check root, server, and client certificates**

**Do you need to redeploy/reinstall the VPN client?**

**Double-check protocol selection against client OSes in use**

**Run Azure VPN Client and Azure VPN gateway diagnostics**





## Summary



### You may not need a P2S VPN tunnel

- Azure Cloud Shell
- Azure portal mobile apps (iOS, Android)

What if you have need for a persistent Azure connection that bypasses the public Internet?

**Next module:** *Design, Implement, and Manage Azure ExpressRoute*

