

Infrastructure Planning



Richard Hicks

Richard M. Hicks Consulting, Inc.

@richardhicks www.richardhicks.com



Overview



Infrastructure Planning

Overview

- VPN and RADIUS server options
- Networking considerations
- VPN protocols
- PKI and certificates
- Provisioning and management



VPN and RADIUS Servers



VPN Server



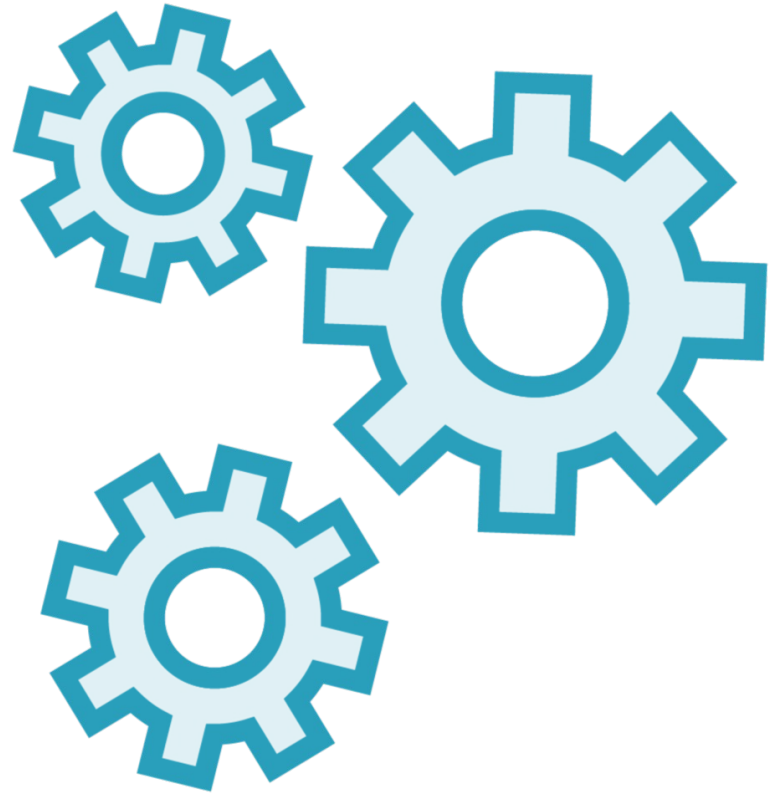
Windows Server

- Routing and Remote Access Service (RRAS)

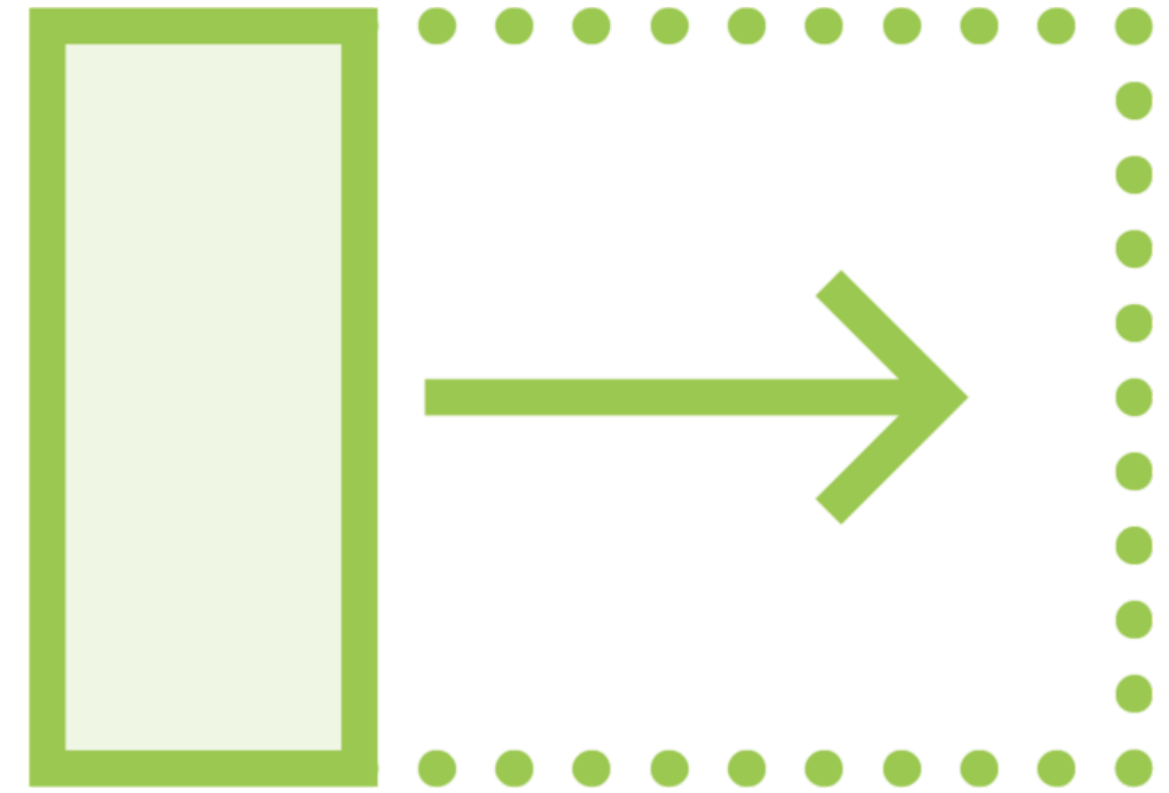
Non-Microsoft security device

- Cisco, Palo Alto, Checkpoint, Fortinet, etc.

Non-Microsoft VPN Requirements

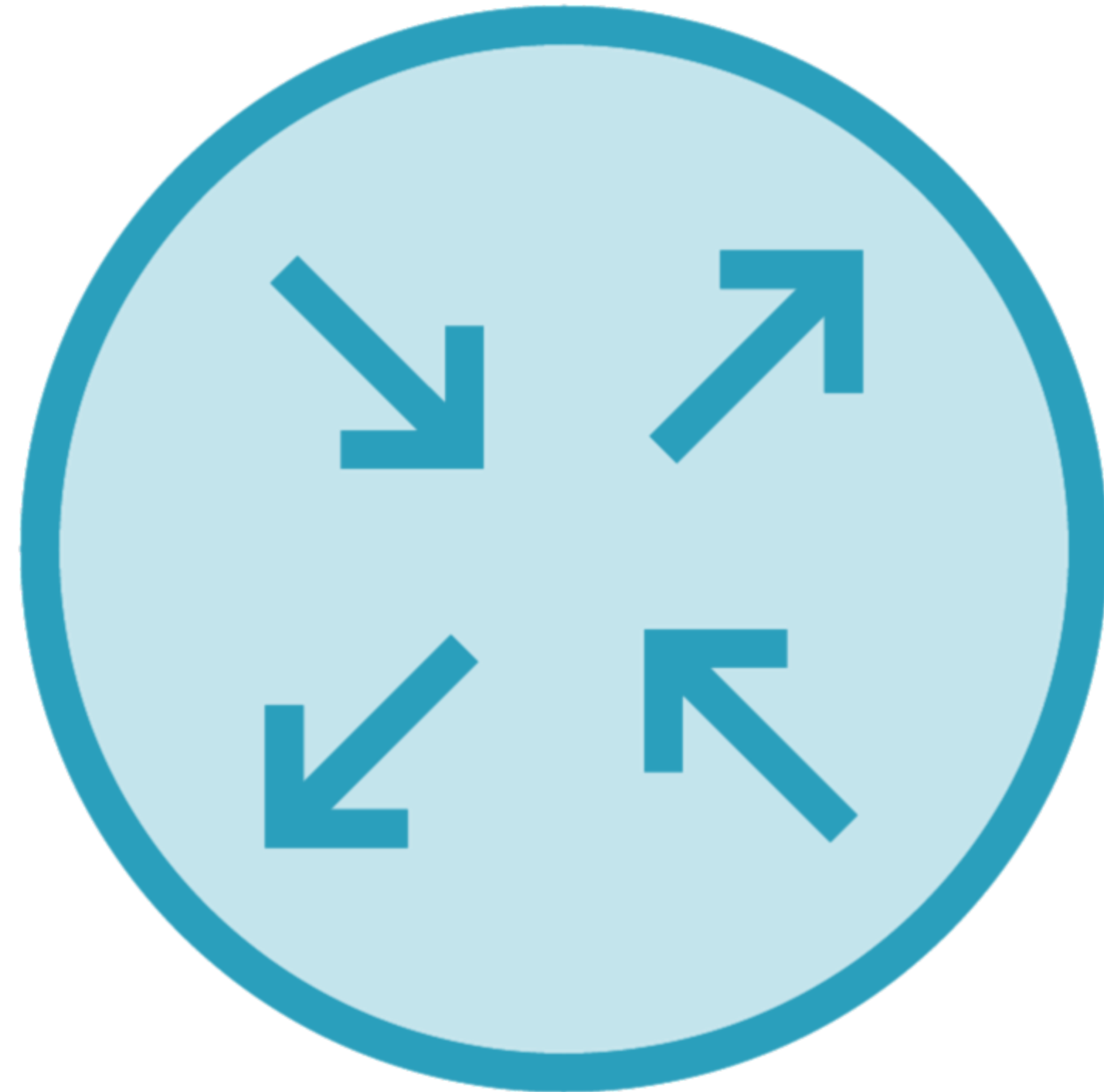


Native VPN client
Built-in to Windows
Requires IKEv2



Plug-in VPN client
Available in Microsoft store
Uses TLS

F5
Cisco
Palo Alto
Azure VPN Client
Pulse Secure
Check Point
SonicWall



RADIUS Server



Windows Server

- Network Policy and Access Service (NPAS)

Non-Microsoft RADIUS server

- Cisco, PulseSecure, open source



Server Requirements

VPN Server

**Windows Server 2019
(minimum)**

Domain-join optional

Server GUI or Core

NPS Server

**Any supported version of
Windows Server**

Domain-join required

Server GUI only!



Networking Considerations



Networking Considerations

Network placement

LAN, DMZ

Network interfaces

Single NIC, multihome

VPN client addressing

DHCP, static pool

VPN client IP subnet

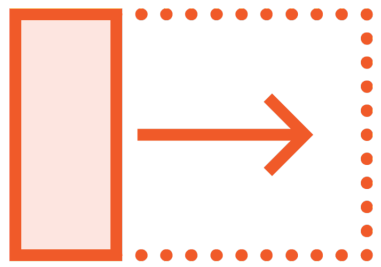
Allocation, routing

Edge firewall

ACL, NAT



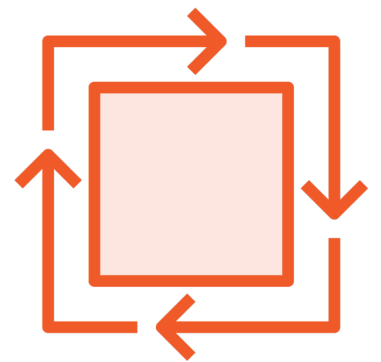
VPN Server Network Placement



LAN – domain-joined, single network interface



DMZ – domain-join optional, single network interface



Multihome – domain-join optional, two network interfaces



VPN Client IP Addressing

DHCP

Not recommended
Limited addressing
options

Static pool

Preferred
Unique IP subnet
Overprovision

IPv6

Static pool only
Unique prefix



Internal network routes are
required for VPN client IP
subnets



Edge Firewall

ACL

Inbound TCP 443 (SSTP)

**Inbound UDP 500, 4500
(IKEv2)**

NAT

To VPN server IP address

Destination NAT only!



Split Tunnel vs. Force Tunnel

Split Tunnel

Only internal traffic routed over VPN

Best user experience

Recommended configuration

Force Tunnel

All traffic including Internet routed over VPN

Provides visibility and control for all client activity

Poor user experience

Requires more resources

Not recommended

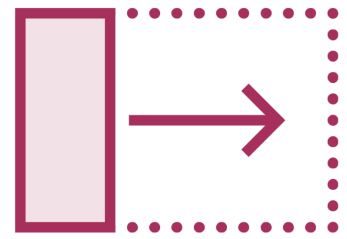
Alternative methods



VPN Protocols



VPN Protocols



Internet Key Exchange version 2 (IKEv2)



Secure Socket Tunneling Protocol (SSTP)



Layer Two Tunneling Protocol (L2TP)



Point-to-Point Tunneling Protocol (PPTP)



IKEv2



Open standard protocol



Uses IPsec for protection



UDP ports 500, 4500



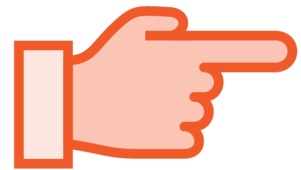
Has operational limitations



Known performance issues



SSTP



Microsoft proprietary



Uses Transport Layer Security (TLS) for protection



TCP port 443



Firewall friendly



Offers best performance



L2TP and PPTP



L2TP

Deprecated in favor of IKEv2



PPTP

Deprecated as insecure

IKEv2 or SSTP?



IKEv2

Device tunnel
Non-Microsoft VPN devices
Highest security required



SSTP

User tunnel
RRAS/Azure VPN gateway
Very good security

PKI and Certificates



Certificates



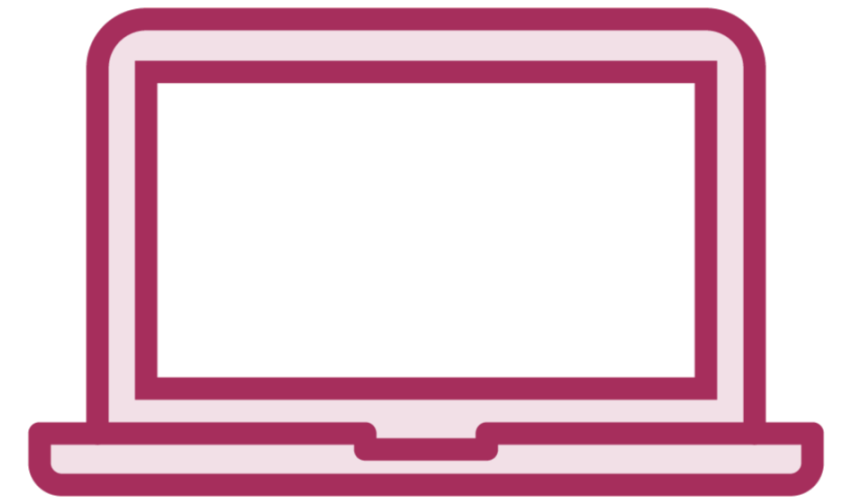
VPN server



NPS server



VPN users



VPN devices





VPN server

- IKEv2 (internal certificate)
- SSTP (public certificate)
- Server authentication EKU
- IP security IKE intermediate EKU (IKEv2)

NPS server

- Server authentication EKU

VPN users

- Client authentication EKU

VPN devices

- Client authentication EKU

Enroll certificates with TPM on mobile endpoints



Provisioning and Management



Client Provisioning and Management



Microsoft Endpoint Manager
Best administrative experience
Greatest scalability



PowerShell
Testing and evaluation
Small deployments
SCCM

Summary



Infrastructure Planning

Summary

- Infrastructure requirements
- IP addressing and firewall configuration
- Protocol selection
- Certificate requirements
- Client provisioning



Up Next:
Prepare the Infrastructure

