Why You Can Benefit From Using Always On VPN

TechTarget

In this handbook:

Why You Can Benefit From Using Always On VPN

BRIEN POSEY, MICROSOFT MVP

Increased latency and other performance issues are some common VPN issues, but recent updates to this technology in Windows Server can overcome these speed bumps.

A VPN gives workers remote access to enterprise resources in a secure way. While there are multiple VPN vendors to choose from, the Windows Remote Access services in Windows Server include the option to configure a VPN host. If you want to optimize remote connections, then you can deploy Always On VPN, which overcomes some of the drawbacks of a traditional VPN and introduces several benefits for the IT staff.

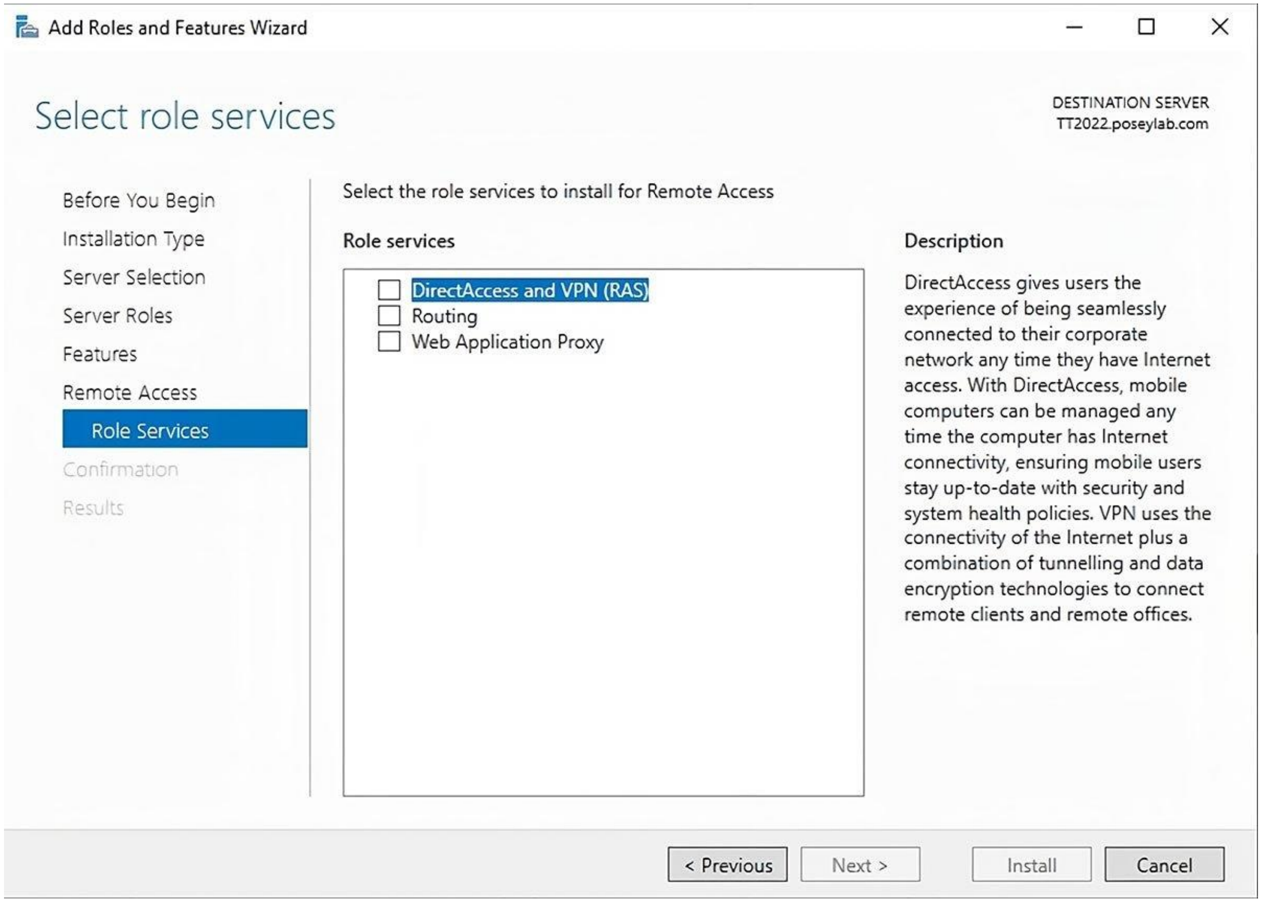
What is Always On VPN?

At a high level, deploying Always On VPN is similar to configuring a standard Windows Server VPN. When you install the Windows Remote Access services, Windows Server asks you which role services you want to deploy. There is no option listed for Always On VPN because Always On VPN is a configuration, not a role.

In this handbook:

Why You Can Benefit From Using Always On VPN

If you want to create an Always On VPN, then deploy the Windows Server VPN in the usual way, and then configure your clients with an Always On VPN profile.



Select role services

DESTINATION SERVER
TT2022.poseylab.com

Select the role services to install for Remote Access

Role services

- □ DirectAccess and VPN (RAS)
- □ Routing
- □ Web Application Proxy

Description

DirectAccess gives users the experience of being seamlessly connected to their corporate network any time they have Internet access. With DirectAccess, mobile computers can be managed any time the computer has Internet connectivity, ensuring mobile users stay up-to-date with security and system health policies. VPN uses the connectivity of the Internet plus a combination of tunnelling and data encryption technologies to connect remote clients and remote offices.

How does Always On VPN differ from DirectAccess?

Even though Always On VPN uses the same software components as a standard Windows Server remote access VPN, it is functionally more like DirectAccess. DirectAccess enables remote clients to remain continuously joined to a network without initiating a VPN connection. Clients using DirectAccess can be managed as though they are local to the network.

Microsoft positions Always On VPN as a better alternative to DirectAccess and recommends the use of Always On VPN whenever possible. However, Always On VPN requires clients to run Windows 10 or higher, which might not be an option in environments that need to support older Windows OSes or non-Windows clients. Also, Always On VPN is not compatible with Azure VMs.

What are the benefits of Always On VPN?

Always On VPN has features that go beyond the simple on/off state of a VPN, such as triggered connectivity. Always On VPN does not need to use a static connection. You can configure Windows to automatically establish an Always On VPN connection in response to various conditions. For example, you can configure Always On VPN to start when a user launches a specific application or attempts to access a resource within your domain.

You can also set up Always On VPN so that it does not connect if a user is attached to a particular network. The trusted network detection feature boosts security, but it also has a more practical use.

For example, users at the corporate office who connect to your organization's wireless network do not need the Always On VPN connection. They have far better performance if they access the various network resources directly rather than through the Always On VPN connection since they are already on the network. This feature streamlines the connection experience so a user doesn't have to manually turn on and switch off the VPN.

On a similar note, Always On VPN offers application-specific split tunneling. The idea behind split-tunnel VPNs is that not every application needs to be -- or even should be -- accessed through the corporate VPN.

For example, a remote user who always uses their VPN and needs to access a Microsoft 365 application through their browser runs all their traffic across the VPN. When the user attempts to access Microsoft 365, a request is sent first to the organization's VPN gateway host and then on to Microsoft, using the organization's internet connection. This is fine for a situation where the user needs to access

In this handbook:

sensitive information, but a request to a SaaS application through a VPN connection only diminishes the user's performance and congests the organization's VPN gateway. The split-tunnel feature in Always On VPN allows specific requests to go directly to their destination without passing through the VPN tunnel.

A benefit of DirectAccess is it enables you to manage clients as though they are local to the network. Always On VPN has a similar feature but with a few improvements to ease device administration.

One problem with remote client management is the inability to administer a device if it's not connected to the network. Always On VPN differs from a traditional VPN by supporting the simultaneous use of two tunnels: one for users and one for devices. As the name indicates, the user tunnel connects the user to the corporate network after they log in. The device tunnel is a low-level tunnel you can configure to automatically connect any time the machine turns on, regardless of whether the user is signed in or not.

The user tunnel supports domain-joined, Azure-joined and workgroup devices, but device tunnels only work with domain-joined devices running Windows 10 version 1709 or higher. Also, Microsoft only supports using Enterprise and Education editions with device tunnels.

Microsoft introduced Always On VPN in Windows Server 2016 and continues to add new capabilities and upgrade existing functionality. In Windows Server 2022, Always On VPN includes support for the Internet Key Exchange version 2 VPN protocol for improved performance and security; Microsoft Entra ID (formerly Azure Active Directory) for conditional access policy integration; and XML profile configuration via PowerShell, Microsoft Endpoint Configuration Manager (formerly System Center Configuration Manager) and other administration tools.

As handy as these and other features are, there is another compelling reason to use Always On VPN instead of a legacy VPN. Unlike most VPNs, Always On VPN supports multifactor authentication when used with RADIUS services and Network Policy Server extensions. It also works with Windows Hello for Business, meaning that users can connect seamlessly without needing to enter a password.

Brien Posey is a 15-time Microsoft MVP with two decades of IT experience. He has served as a lead network engineer for the U.S. Department of Defense and as a network administrator for some of the largest insurance companies in America.