Tipps & Tricks

Windows 10 als VPN-Client oder Server einrichten

Dieser Praxisbeitrag erklärt, wie man VPN unter Windows 10 einrichtet, sowohl für den Client- als auch für den Server-Betrieb. Dies ist wichtig zu wissen, falls externe Systeme sicher auf den Windows-10-Rechner zugreifen sollen.

Auch wenn Windows und Windows Server mittlerweile zahlreiche Möglichkeiten bieten, sich von unterwegs in das Netzwerk einzuwählen oder auf Cloud-Lösungen zuzugreifen, verwenden viele Unternehmen noch immer herkömmliche VPN-Verbindungen. Aus diesem Grund hat Microsoft in Windows 10 auch weiterhin den VPN-Client integriert. Dieser ist mittlerweile leichter steuerbar und kann auch auf Tablets eingesetzt werden. Neben den Möglichkeiten, Windows 10 als VPN-Client zu nutzen, können Sie auch einen VPN-Server auf Basis eines Windows-10-Rechners erstellen. Dadurch erhalten externe Rechner die Möglichkeit, per VPN auf einen Windows-10-Rechner zuzugreifen.

Windows 10 als VPN-Client nutzen

Sie können den Assistenten zum Aufbau einer VPN-Verbindung über den Link „Neue Verbindung oder neues Netzwerk einrichten“ im Netzwerk- und Freigabe-Center starten. Wählen Sie im Anschluss die Option „Verbindung mit dem Arbeitsplatz herstellen“. Sodann startet der Assistent zur Einrichtung eines VPN mit dem Arbeitsplatz. Hier geben Sie die Daten des VPN-Servers ein, den Sie verwenden wollen. Anschließend wählen Sie die Option „Die Internetverbindung (VPN) verwenden“, um eine Verbindung über Ihre bestehende Internetverbindung mit dem VPN-Server aufzubauen.

› Im Netzwerk- und Freigabecenter richten Sie neue VPN-Verbindungen ein.

› Sie können eine Wählleitung für den Verbindungsaufbau zum VPN verwenden, oder eine existierende Internetverbindung.

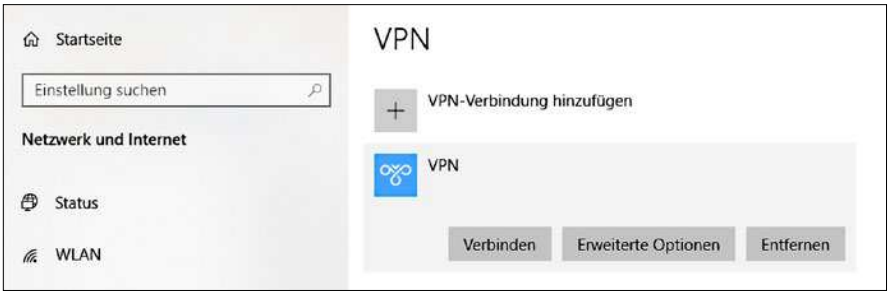
Auf der nächsten Seite geben Sie die IP-Adresse des Servers oder Windows-10-Rechners ein, zu dem Sie eine Verbindung aufbauen wollen. Soll die Verbindung über das Internet hergestellt werden, müssen Sie auf der Firewall/dem DSL-Router eine Weiterleitung einrichten und einen dynamischen DNS-Dienst oder eine statische IP-Adresse verwenden. Mit Fritzboxen ist das kein Problem. Sobald die Verbindung erstellt ist, steht diese über die Netzwerkverbindungen zur Verfügung. Diese erreichen Sie am schnellsten, wenn Sie nach „ncpa.cpl“ im Suchfeld der Taskleiste suchen. Bauen Sie eine Verbindung auf, können Sie die Anmeldedaten auch speichern lassen. Alternativ können Sie die Anmeldedaten jederzeit wieder eingeben.

VPNs mit der Einstellungs-App erstellen

Auf Tablets, oder auch wenn Sie lieber die Einstellungs-App von Windows 10 nutzen wollen, finden Sie den Assistenten zum Erstellen neuer VPN-Verbindungen über „Einstellungen / Netzwerk und Internet / VPN“.

› In der neuen Einstellungs-App können Sie ebenfalls VPN-Verbindungen erstellen.

Klicken Sie dazu zunächst auf „VPN-Verbindung hinzufügen". Anschließend startet der Assistent zum Einrichten der Verbindung. Hier geben Sie alle notwendigen Verbindungsdaten ein und klicken danach auf „Speichern". Sobald Sie die VPN erstellt haben, wird diese im Fenster angezeigt. Klicken Sie auf die Verbindung, können Sie eine Verbindung aufbauen, die Verbindung bearbeiten oder sie löschen.



› Nach der ersten Einrichtung lassen sich in den erweiterten Einstellungen der VPN-Verbindungen auch professionelle Einstellungen vornehmen.

In den Einstellungen können Sie alle Konfigurationsschritte durchführen, die Sie auch bei der Erstellung der Verbindung durchgeführt haben. Außerdem können Sie die Anmeldedaten löschen und automatische Konfigurations-Skripte laden lassen.

Allerdings können Sie in der Einstellungs-App nicht alle wichtigen Einstellungen anpassen. Um alle Einstellungen von VPN-Verbindungen zu konfigurieren, rufen Sie die Eigenschaften der VPN-Verbindung im Netzwerk- und Freigabecenter oder über „ncpa.cpl" auf. Hier können Sie auf verschiedenen Registerkarten mehr Einstellungen vornehmen. Vor allem auf der Registerkarte „Sicherheit" verstecken sich viele Einstellungen, mit denen Sie Probleme beim Verbindungsaufbau lösen können.

Windows 10 als VPN-Server nutzen

Windows 10 kann also so eingerichtet werden, dass eine Einwahl per VPN auf den Rechner erfolgen kann. Damit können Sie über das Internet oder ein internes Netzwerk eine gesicherte Netzwerkverbindung zu Ihrem PC herstellen. Um die Einrichtung vorzunehmen, gehen Sie folgendermaßen vor:

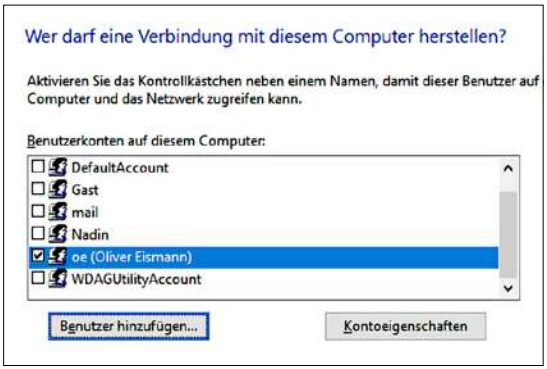
Öffnen Sie die „Netzwerk- und Interneteinstellungen" per Rechtsklick auf das Netzwerksymbol in der Taskleiste und einem Klick auf „Netzwerk- und Interneteinstellungen öffnen". Wechseln Sie zu „Ethernet" oder „WLAN" und klicken Sie anschließend auf „Adapteroptionen ändern". Diesen Bereich erreichen Sie auch, indem Sie „ncpa.cpl"

in das Suchfeld der Taskleiste eingeben. Öffnen Sie mit der (Alt)-Taste die Menüleiste und klicken Sie auf „Datei / Neue eingehende Verbindung“.

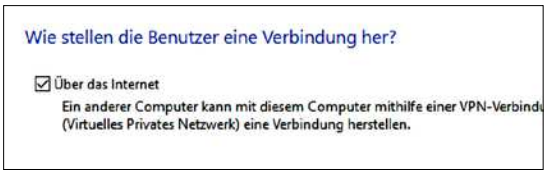
› In Windows 10 erstellen Sie relativ einfach eingehende Verbindungen auf VPN-Basis.

Anschließend öffnet sich ein neues Fenster, in dem Sie auswählen, welchen lokalen Benutzern Sie die Einwahl gestatten wollen. Über „Benutzer hinzufügen“ können Sie einen eigenen Benutzer für die Einwahl festlegen. Auf der nächsten Seite des Assistenten aktivieren Sie die Option „Über das Internet“. Dadurch wird sichergestellt, dass Anwender per VPN eine Verbindung mit dem Rechner aufbauen können.

Im nächsten Fenster belassen Sie die Standardauswahl der Protokolle und bestätigen das Erstellen der Verbindung. Anschließend wird die VPN-Verbindung angezeigt. Die Einstellungen können jederzeit über die Eigenschaften der Verbindung angepasst werden.



› Legen Sie fest, welche Benutzer auf die neue Verbindung zugreifen dürfen.



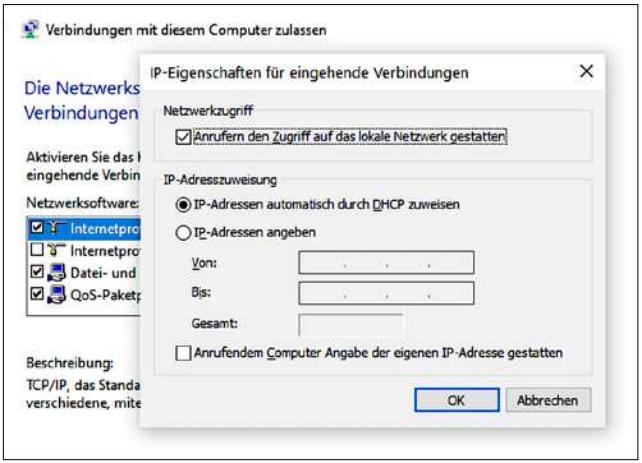
› Geben Sie nun noch an, dass die Verbindung mit dem Computer per VPN „Über das Internet“ hergestellt wird.

Anpassen einer VPN-Verbindung

Damit die Einwahl per VPN funktioniert, muss noch festgelegt werden, welche IP-Adresse die VPN-Clients erhalten sollen. Standardmäßig verwendet Windows 10 DHCP, verteilt die Adressen also automatisch. Diese Einstellungen lassen sich aber auch manuell vorgeben. Sie können dazu den Assistenten fortführen oder nach der Einrichtung die Einstellung auch manuell anpassen.

Rufen Sie die Eigenschaften der eingehenden Verbindung auf. Wechseln Sie zur Registerkarte „Netzwerk“. Rufen Sie die Eigenschaften von „Internetprotokoll Version 4“ auf. Aktivieren Sie die Option „IP-Adressen angeben“.

Anschließend geben Sie den Adress-Pool an, der den VPN-Clients zugewiesen wird. Achten Sie aber darauf, nur Adressen zu verwenden, die nicht bereits intern genutzt werden. Sie haben hier auch die Möglichkeit, die Zuteilung der Adresse den Clients zu überlassen. Wenn Sie sich selbst an Ihrem Rechner einwählen, können Sie persönlich steuern, welche IP-Adresse Sie verwenden.



› Legen Sie hier den Bereich für IP-Adressen fest, die den VPN-Clients bei Verbindung zugewiesen werden sollen.

Firewall-Einstellungen beachten

Mit PPTP sollten Sie das IP-Protokoll 47 und den TCP-Port 1723 für VPN-Zugriffe auf dem Router und der Firewall öffnen. Verwenden Sie L2TP, müssen Sie die UDP-Ports 500 und 1701 sowie das IP-Protokoll 50 aktivieren. Sobald die Verbindung aufgebaut ist, können Sie über das Netzwerk und das VPN mit dem Explorer auf die Verzeichnisse des anderen VPN-Servers oder auf andere Ressourcen im internen Netzwerk des VPN-Servers zugreifen.

Da die Verschlüsselung und der Transport der einzelnen VPN-IP-Pakete in den meisten Fällen durch das GRE-Protokoll (Generic Routing Encapsulation) durchgeführt werden, müssen Sie darauf achten, dass die Hardware Firewall beziehungsweise der DSL-Router, den Sie vor dem PC im Internet platzieren, dieses Protokoll beherrscht. Bei vielen preisgünstigen Modellen ist das nicht der Fall. In diesem Fall können Sie kein PPTP-VPN mit einem Windows-10-PC aufbauen.

Sie sollten daher bereits den Erwerb der Hardware Firewall, die vor dem PC im Internet steht, in die Planung einbeziehen. Windows 10 verwendet das Point-To-Point-Tunneling-Protocol (PPTP) für den VPN-Aufbau. Bei PPTP werden einzelne PTP-Pakete (Point-To-Point) in sogenannten GRE-Paketen (Generic Routing Encapsulation) verpackt und verschickt. Die meisten Experten stufen PPTP als sicher ein, auch wenn die Verschlüsselung nicht so stark ist wie die von L2TP. PPTP ermöglicht die verschlüsselte Einkapselung verschiedener Netzwerkprotokolle.

Nachdem die Authentifizierung durchgeführt ist, wird die Verbindung verschlüsselt. Die Verschlüsselung baut auf dem Kennwort der Authentifizierung auf. Je komplexer das Kennwort ist, umso besser ist die Verschlüsselung. PPTP nutzt zwei Kommunikationskanäle, einen zur Verwaltung und einen zum Datenaustausch. Der Verwaltungs-Channel ist eine TCP-Verbindung zum Port 1723 auf den PC. Der Datenkanal nutzt GRE (Generic Routing Encapsulation) auf TCP/UDP-Port 47. Aus diesem Grund sollten Sie auf dem Router auch diese beiden Ports an den PC weiterleiten lassen.

Thomas Joos

Thomas Joos ist freiberuflicher IT-Consultant und seit 20 Jahren in der IT tätig. Er schreibt praxisnahe Fachbücher und veröffentlicht in zahlreichen IT-Publikationen wie TecChannel.de und PC Welt.