VPN Zugang

Übersicht über die untergeordneten Dokumente

Inhalt

Wozu benötige ich einen VPN-Tunnel?

Befindet sich der dienstliche Rechner im Firmennetzwerk, kann auf alle Ressourcen (z.B. Laufwerke, E-Mails, etc.) zugegriffen werden, die dienstlich zur Verfügung stehen. Wird dieser Rechner (z.B. ein Notebook) außerhalb des Firmennetzwerks, z.B. im Homeoffice oder beim Kunden, eingesetzt und mit dem Internet verbunden, stehen diese Ressourcen nicht zur Verfügung. Um sich auch aus der Ferne mit dem Firmennetzwerk zu verbinden, kann ein virtuelles privates Netz (VPN) in die Firma aufgebaut werden. Die Daten, die in diesem VPN transportiert werden, sind verschlüsselt. Somit kann eine VPN-Verbindung als sicher eingestuft werden.

In diesem Artikel werden nur sogenannte User-to-Site-VPN-Tunnel behandelt, also VPN-Tunnel, die von einem Endgerät in das MSP-Netzwerk aufgebaut werden.

Für dauerhafte Kopplungen zwischen Firmennetzen können auch Site-to-Site-Tunnel eingerichtet werden, die Ressourcen zwischen Firmen über einen gesicherten Tunnel ohne Verwendung von Software auf Clientseite teilen.

Wie bekomme ich einen Zugang zum VPN-Tunnel?

Jeder VPN-Tunnel muss im **MSP JIRA Kundenportal** beantragt werden und durch einen Vorgesetzten bei MSP oder bei einem MSP Kunden genehmigt werden. (Siehe VPN-Benutzer im JIRA Kundenportal beantragen)

Sobald diese Genehmigung vorliegt, kann der Zugang erstellt werden. Die Zugangsdaten werden ausschließlich dem Nutzer des Tunnels auf einem sicheren Weg zur Verfügung gestellt. Nach dem Ablauf der Nutzungsanforderung werden die Zugangsdaten automatisch invalidiert. Das Ablaufdatum wird durch den Genehmiger (Vorgesetzter) festgelegt.

Welche VPN-Software wird verwendet?

Um eine VPN-Verbindung aufzubauen, muss eine entsprechende Software auf dem Endgerät installiert sein. Auf allen mobil einsetzbaren Geräten (Notebooks, Tablets, etc.) ist dieses der Fall.

Checkpoint Client (IPSec)

Standard ist auf von MSP verwalteten Geräten der *Checkpoint-IPSec-Client*. Dieser wird auf die Geräte durch die Softwareverteilung installiert und aktuell gehalten. Sollte die Software doch einmal fehlen, ist die Installation durch ein JIRA Ticket anzufordern. Die Authentifizierung erfolgt über Windows ActiveDirectory (AD), Anmeldename und ein entsprechendes Kennwort werden benötigt. Diese Zugangsdaten entsprechen bei internen Mitarbeitern der bekannten Windows Anmeldung am Endgerät. Hinweise zur Bedienung des Checkpoint-IPSec-Clients finden sich im untergeordneten Dokument (Checkpoint IPSec-Client verwenden).

Externe Dienstleister

MSP unterstützt generell nur Windows-Systeme. Andere Betriebssysteme wie MacOS oder Linux bieten zwar die Möglichkeit, VPN-Verbindungen zu konfigurieren. Dies geschieht ohne Support der MSP.

Hinweis für externe Dienstleister: Diese installieren die VPN-Software auf eigene Verantwortung in Absprache mit ihrer IT.

Checkpoint Client (IPSec)

Für externe Dienstleister wird der Checkpoint Client (IPSec) zusammen mit den Zugangsdaten bereitgestellt. Die Installation erfolgt wie üblich bei Windows-Software. Der von MSP bereitgestellte Client ist für die Verbindung zur MSP-Firewall vorkonfiguriert. MSP aktualisiert den Checkpoint-IPSec-Client regelmäßig, sobald eine neuere Version vom Hersteller bereitgestellt wird. Externe Dienstleister müssen den VPN-Client auf ihren PCs selbstständig über den Download-Link einmal im Jahr aktualisieren.

Die Zugangsdaten werden über ein JIRA-Ticket beim jeweiligen MSP-Ansprechpartner angefordert und auf gesichertem Weg übermittelt. Die Anmeldedaten werden nur für die VPN-Verbindung sowie weitere von MSP betreute Systeme (JIRA) benötigt. Für welche Systeme die Zugangsdaten ebenfalls gelten, teilt der Ansprechpartner von MSP ihnen mit. Hinweise zur Bedienung des Checkpoint-IPSec-Clients finden sich im untergeordneten Dokument (Checkpoint IPSec-Client verwenden).