VPN für Institute

Beschreibt den Dienst "Instituts-VPN", der auf dem allgemeinen VPN-Dienst aufsetzt.

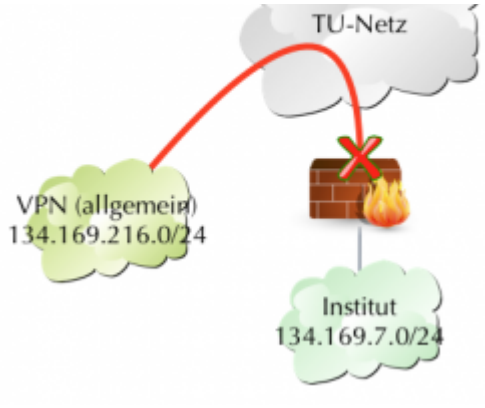
Was ist "Instituts-VPN" ?

Die Einwahl über den VPN-Dienst der TU (vpngate.tu-braunschweig.de) erlaubt zunächst grundsätzlich die verschlüsselte Übertragung von Daten aus einem möglicherweise unsicheren (mobilen) Netz bis zur TU, wo der Verkehr entschlüsselt und die Daten normal über das Internet weiterverteilt werden. Darüberhinaus erhält der Nutzer durch die im VPN vergebene TU-interne IP-Adresse Zugriff auf Dienste der TU, die nur TU-intern freigegeben sind. Im Kombination mit entsprechenden Regeln auf den Instituts-Firewalls, die die Netze aller Einrichtungen auch innerhalb der TU noch mal voreinander schützen, erweitert der Dienst "Instituts-VPN" letzteren Vorteil gewissermaßen auf die Netze und internen Dienste innerhalb einzelner Einrichtungen.

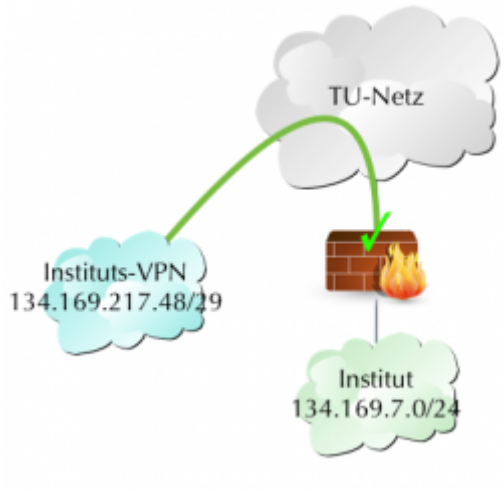
Das Angebot "Instituts-VPN" baut dazu auf dem allgemeinen VPN-Angebot auf, stellt aber den Nutzern einzelner Einrichtungen jeweils einen eigenen VPN-Adress-Pool bereit, der im KDD unter Datennetz->IPv4 eingesehen werden kann. Nutzer des Dienstes "Instituts-VPN" erhalten bei der VPN-Einwahl entsprechend keine IP-Adresse aus einem öffentlichen VPN-IP-Adressbereich der TU sondern eine IP-Adresse aus dem VPN-Adressbereich, der nur ihrer Einrichtung gehört und nur von Mitarbeitenden der Einrichtungen genutzt werden kann. Welche Mitarbeitenden (mit welcher Benutzerkennung) den Dienst nutzen können, stellt der DV-Koordinator dazu im KDD ein. Entsprechende Einstellungen werden unter „Personen zu Netzwerk“ im KDD durchgeführt und sind ca. 30 Minuten später (ggf. nach Neu-Einwahl im VPN) aktiv. Nach Aufbau der VPN-Verbindung kann in den "Statistics" des Anyconnect-Clients oder wahlweise über z.B. die Website https://www.wieistmeineip.de überprüft werden, ob eine IP-Adresse aus dem für die Einrichtung reservierten Adressbereich vergeben wurde.

Parallel dazu wird die Firewall der Einrichtung so konfiguriert, dass Einrichtungs-interne Dienste von den speziellen VPN-IP-Adressen aus zugreifbar werden. Wie weitreichend diese Firewall-Freischaltungen sein sollen, richtet sich nach Ihren Anforderungen.

Die folgenden zwei Bilder verdeutlichen beispielhaft den Unterschied zwischen der Nutzung des allgemeinen VPN-Dienstes und der Nutzung von Instituts-VPN im Hinblick auf Instituts-interne Dienste:



ohne VPN



mit VPN

Technische Umsetzung

Für die technische Realisierung des Dienstes "Instituts-VPN" vergeben wir an jede Einrichtung einen Pool von maximal acht öffentlichen IP-Adressen im VPN und richten zur Nutzung dieses Adresspools für Ihre Einrichtung ein spezielles Verbindungsprofil auf unserem VPN-Gateway ("vpngate.tu-braunschweig.de) ein. Durch Zuordnung des entsprechenden Netzes zur Benutzerkennung eines Mitarbeitenden (im KDD unter „Personen zu Netz“) wird bei der Anmeldung dieser Benutzerkennung am VPN-Gateway eine Information übermittelt, die für genau diese Benutzerkennung das Profil und damit den Adresspool für Ihr Institut auswählt. Dadurch brauchen weder Sie noch Ihre Kollegen Änderungen an Ihren VPN-Clients bzw. deren Konfiguration vorzunehmen. **Sie installieren und konfigurieren den Client genau wie zur Nutzung des allgemeinen VPN-Angebots.**

Die IP-Adressen Ihres VPN-Pools werden dynamisch zugeordnet. Eine feste Zuweisung von IP-Adressen im VPN an einzelne Benutzer ist nicht möglich. Entsprechend der Größe des VPN-Adressspools können gleichzeitige VPN-Verbindungen aufgebaut werden. Sofern dies nicht ausreicht, teilen Sie (als DV-Koordinator) bitte mit, dass es einen erhöhten Bedarf gibt. Dann werden wir zusätzlich eine Lösung konfigurieren, die mithilfe von NAT/PAT die Anzahl der gleichzeitig möglichen Verbindungen bis auf ca. 260 gleichzeitige Verbindungen erweitert, ohne dass auf den Clients etwas geändert werden muss. Bei dieser Lösung wird zusätzlich zu den bereits vergebenen öffentlichen IP-Adressen ein Netz von 255 privaten Adressen (aus dem Adressraum 10.0.*.*) konfiguriert und dynamisch auf die letzte der öffentlichen IPs übersetzt.

Instituts-VPN beantragen und Benutzerkonten konfigurieren

Instituts-VPN beantragen

Im Modul "Datennetz" des KDD sind die Netzbereiche aufgelistet, die teilweise oder vollständig Ihrer Einrichtung zugeordnet sind. Neben den Namen der Adressbereiche befinden sich Spalten für weitere Dienste, die zu den Adressbereichen aktiv oder verfügbar sind. Zum Beantragen von Instituts-VPN klicken Sie auf "Beantragen" in der entsprechenden Spalte. Bitte beachten Sie, dass wir den Dienst in der Regel nur für einen Adressbereich einer Einrichtung einrichten. Näheres zur Netzübersicht finden Sie auch in der Dokumentation des KDD-Datennetzmoduls.

Ist Instituts-VPN bereits aktiv, wird dies (neben dem entsprechenden grünen Haken in der Spalte neben dem Adressbereich) in der Rubrik "Übersicht anderer Adressbereiche" weiter unten angezeigt. Dort wird jedoch nur der übergeordnete Adressbereich aufgelistet, aus dem Ihrer Einrichtung einzelne IP-Adressen zugeteilt wurden. Welche IP-Adressen dies genau sind, erfahren Sie durch Klick auf den Adressbereich.

Benutzerkonten für Instituts-VPN konfigurieren

In der Rubrik "Personen zu Netzwerk" werden alle Mitarbeitenden, die der Einrichtung zugeordnet sind, mit Ihren jeweiligen Benutzerkonten aufgelistet. Markieren Sie einen Mitarbeiter durch Klick und gehen Sie unten auf [**Auswählen**]. In der folgenden Ansicht können Sie pro Benutzerkennung des Mitarbeitenden über ein Drop-Down-Menü wählen, ob diese bei der VPN-Einwahl im öffentlichen Netz ("Public") oder in einem der Einrichtung zugeordneten VPN-Adressbereich landen sollen. Bestätigen Sie die Änderung durch Klick auf die entsprechende Schaltfläche. Es kann bis zu

30 Minuten dauern, bis die Änderung im System aktiv wird. Danach muss außerdem eine neue Anmeldung am VPN erfolgen.