Zertifikatsprobleme mit Anyconnect unter Android/Linux

01.07.2025 20:58:47

FAQ-Artikel-Ausdruck

Kategorie:	Zugang ins TU-Netz	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	de	**Letzte Aktualisierung:**	12:17:56 - 07.02.2025

Schlüsselwörter

VPN Anyconnect Zertifikat Probleme Android Linux

Symptom (öffentlich)

Der Anyconnect-Client kann sich mit dem VPN-Server "vpngate.tu-braunschweig.de" nicht verbinden. Es wird angezeigt, dass das Zertifikat nicht vertrauenswürdig sei.

Problem (öffentlich)

Hin und wieder kommt es vor, dass der Anyconnect-Client, obwohl er nach Anleitung ordentlich installiert wurde, dem Zertifikat des VPN-Servers nicht vertrauen möchte. Dies ist besonders unter Android häufiger der Fall.
Teilweise kommt es auch unter normalem Linux vor.

Lösung (öffentlich)

Die Lösung für dieses Problem ist der Import des Server-Zertifikats in den Zertifikatsspeicher des Anyconnect-Clients. Dazu geht man unter Android wie folgt vor:

1) Öffnen der Einstellungen im Anyconnect Client. Einmaliges deaktivieren der Einstellung "Nicht vertrauenswürdige Server blockieren"
2) Verbindung zu vpngate.tu-braunschweig.de aufbauen. Man erhält dann eine Warnung, dass das Zertifikat nicht vertrauenswürdig sei. Klick auf Details.

3) Vergleichen der Detail-Informationen mit den Informationen des Zertifikats und sollten die Informationen übereinstimmen, dann auf "Import and Continue" klicken. Damit wird dem Zertifikat dauerhaft das Vertrauen ausgesprochen.
4) Beenden der VPN-Verbindung. Einstellungen erneut öffnen und erneut das Häkchen bei "Nicht vertrauenswürdige Server blockieren" wieder setzen.

Anschließend kann unter "Diagnostik --> Zertifikatsverwaltung" im Anyconnect-Client bei "Server" angezeigt werden, dass das Zertifikat in den Client importiert wurde. Es kann dort auch jederzeit wieder gelöscht werden. Bei zukünftigen Verbindungen zu vpngate.tu-braunschweig.de sollte keine Warnung mehr erscheinen.

Unter Linux kann man den gleichen Weg ausprobieren. Falls das nicht zum Erfolg führt, kann man die Zertifikatskette auch manuell im Filesystem hinterlegen. Dazu die Zertifikatskette [1]hier herunterladen und (als Root) unter

/opt/.cisco/certificates/ca

ablegen.

[1] https://pki.pca.dfn.de/dfn-ca-global-g2/pub/cacert/chain.txt