

Problem mit Split-VPN, DNS und Routing (Beispiel: Moodle)

Bei Nutzung des **Split-VPN** kann es zu Verbindungsproblemen kommen, wenn interne Clients einen **externen DNS-Server** verwenden und dadurch eine **externe IP-Adresse** für einen eigentlich internen Dienst erhalten.

Hintergrund

Beim **Split-VPN** wird nur bestimmter Netzwerkverkehr über das VPN geroutet (z. B. interne Netze). Der restliche Verkehr wird direkt über das lokale Netzwerk bzw. das Internet gesendet.

Wenn ein Client jedoch **externen DNS** verwendet, kann Folgendes passieren:

1. Die Domain wird **auf eine externe IP-Adresse aufgelöst**.
2. Der Client versucht diese externe Adresse zu erreichen.
3. Diese Adresse ist **aus dem internen Netz nicht erreichbar**.
4. Die Verbindung schlägt daher fehl, obwohl der Dienst intern verfügbar ist.

Beispiel: Moodle

Die Adresse `moodle.bszn-da.de` kann auf zwei verschiedene IP-Adressen zeigen:

- **Intern:** `172.31.200.11`
- **Extern:** `130.83.90.135`

Wird ein **interner DNS-Server** verwendet, erhält der Client die interne Adresse und kann den Dienst direkt erreichen.

Wird jedoch ein **externer DNS-Server** genutzt, erhält der Client die externe Adresse. Da diese aus dem internen Netz **nicht erreichbar ist**, schlägt die Verbindung fehl.

Ping-Tests

Auflösung über internen DNS

[09:52] moodle.bszn-da.de → 172.31.200.11 (intern) 6 Pakete, 0% loss | min/avg/max = 2.5 / 6.7 / 18.3 ms

Auflösung über externen DNS

[10:27] moodle.bszn-da.de → 130.83.90.135 (docker2.da.schule.hessen.de, extern) 8 Pakete, 0% loss | min/avg/max = 31.4 / 40.7 / 58.0 ms

Direkte Tests

[10:28] Direkt → 172.31.200.11 (intern) 7 Pakete, 0% loss | min/avg/max = 2.8 / 4.0 / 5.0 ms

[10:28] Direkt → 130.83.90.135 (extern) — kein Ergebnis

Ursache

Der Fehler entsteht durch die Kombination aus:

- **Split-VPN**
- **externem DNS**
- einer **externen Adresse, die intern nicht erreichbar ist**

Der Client versucht den Dienst über eine Adresse zu erreichen, die aus dem aktuellen Netzwerkpfad **nicht geroutet werden kann**.

Lösungsmöglichkeiten

Folgende Maßnahmen verhindern das Problem:

- Verwendung des **internen DNS-Servers**
- **Split-DNS** für interne Dienste
- Eintrag der internen Adresse in der **Hosts-Datei**

172.31.200.11 moodle.bszn-da.de

- Sicherstellen, dass interne Clients **interne Adressen bevorzugt nutzen**

Damit wird verhindert, dass interne Systeme versuchen, einen intern gehosteten Dienst über eine nicht erreichbare externe Adresse aufzurufen.

Version #3

Erstellt: 2026-03-09 21:29:25 UTC von Björn Wiskamp

Zuletzt aktualisiert: 2026-03-09 21:39:10 UTC von Björn Wiskamp