14.6

VPN-Fehlersuche in der Praxis

VPN-Probleme wirken oft so, als wäre „das Netzwerk kaputt“.

Tatsächlich können VPN-Fehler an vielen Stellen entstehen:

- Internetverbindung
- VPN-Client
- VPN-Gateway
- Benutzeranmeldung
- MFA
- Zertifikat
- Routing
- DNS
- Firewall
- NAT
- Zielsystem
- Host-Firewall
- Berechtigungen
- MTU
- Performance

Merksatz:

> VPN-Fehlersuche ist nie nur Tunnelprüfung.

Grundidee der VPN-Fehlersuche

Ein VPN-Zugriff besteht aus mehreren Schritten.

Vereinfacht:

1. Client erreicht VPN-Gateway.
2. Benutzer oder Gerät authentifiziert sich.
3. Tunnel wird aufgebaut.
4. Client erhält VPN-Konfiguration.

5. Routen werden gesetzt.
6. DNS wird gesetzt.
7. Firewall erlaubt Zugriff.
8. Zielsystem antwortet.
9. Anwendung erlaubt Zugriff.

Wenn ein Schritt fehlschlägt, funktioniert der Zugriff nicht vollständig.

Merksatz:

VPN funktioniert nur,
wenn alle Schritte der Zugriffskette passen.

VPN-Fehlersuche nach Fehlerbild

Wichtige erste Frage:

Was genau funktioniert nicht?

Typische Fehlerbilder:

VPN verbindet gar nicht.

VPN verbindet,
aber interne IPs gehen nicht.

VPN verbindet,
aber interne Namen gehen nicht.

VPN verbindet,
aber nur bestimmte Dienste gehen nicht.

VPN verbindet,
aber Zugriff ist langsam.

VPN verbindet,
aber bricht ab.

VPN funktioniert nur für manche Benutzer.

VPN funktioniert nur aus manchen Netzen.

Merksatz:

Das Fehlerbild entscheidet,
wo man zuerst sucht.

Fehlerbild 1: VPN verbindet gar nicht

Wenn VPN gar nicht verbindet, liegt der Fehler vor oder während des Tunnelaufbaus.

Mögliche Ursachen:

falsche VPN-Serveradresse
Internetverbindung gestört
VPN-Gateway nicht erreichbar
Port oder Protokoll blockiert
Benutzername falsch
Passwort falsch
Konto gesperrt
MFA schlägt fehl
Zertifikat ungültig
Clientversion veraltet
Lizenzproblem
VPN-Dienst auf Gateway gestoppt

Merksatz:

Wenn VPN nicht verbindet,
zuerst Erreichbarkeit,
Anmeldung,
MFA
und Zertifikate prüfen.

Prüfung: Ist das VPN-Gateway erreichbar?

Vor der VPN-Anmeldung muss der Client das Gateway erreichen.

Prüfen:

```
DNS-Name des VPN-Gateways korrekt?
öffentliche IP erreichbar?
richtiger Port offen?
TCP oder UDP korrekt?
Firewall oder Provider blockiert?
Gateway online?
Wartungsfenster aktiv?
Zertifikat gültig?
```

Typische Fehler:

```
falscher Hostname
alte öffentliche IP
DNS zeigt auf falsches Ziel
Port am Gateway nicht offen
UDP im fremden Netz blockiert
```

Merksatz:

```
Ohne erreichbares Gateway kein VPN-Tunnel.
```

Prüfung: DNS-Name des VPN-Gateways

Viele VPN-Clients verbinden sich zu einem Namen.

Beispiel:

```
vpn.firma.de
```

Wenn dieser Name falsch auflöst, verbindet sich der Client zum falschen Ziel oder gar nicht.

Prüfen:

```
liefert DNS die richtige öffentliche IP?
gibt es alte DNS-Einträge?
```

ist der DNS-Cache veraltet?

funktioniert Auflösung intern und extern gleich?

wird IPv4 oder IPv6 verwendet?

Merksatz:

> VPN-Gateway-Namen immer aus Sicht des Clients prüfen.

Prüfung: Port und Protokoll

Je nach VPN-Protokoll müssen andere Ports oder Protokolle erreichbar sein.

Beispiele:

VPN-Technik	häufig relevant
IPsec IKE	UDP 500
IPsec NAT-T	UDP 4500
IPsec ESP	IP-Protokoll 50
OpenVPN	häufig UDP 1194 oder konfiguriert
WireGuard	häufig UDP 51820
TLS-VPN	häufig TCP 443

Wichtig:

> UDP und TCP nicht verwechseln.

Merksatz:

> VPN-Fehlersuche braucht Kenntnis von Port und Protokoll.

Fehlerbild 2: Anmeldung schlägt fehl

Wenn das Gateway erreichbar ist, aber die Anmeldung fehlschlägt, liegt der Fehler eher bei Identität oder Richtlinie.

Mögliche Ursachen:

Benutzername falsch
Passwort falsch
Konto gesperrt
Konto deaktiviert
Passwort abgelaufen
MFA nicht bestätigt
MFA nicht eingerichtet
Benutzer nicht in VPN-Gruppe
Login nur von verwaltetem Gerät erlaubt
Conditional Access blockiert
Zertifikat fehlt oder ungültig
Zeitabweichung

Merksatz:

Anmeldefehler sind meistens Authentifizierung oder Zugriffsrichtlinie.

Authentifizierung und Autorisierung trennen

Authentifizierung:

Wer bist du?

Autorisierung:

Was darfst du?

Beispiel:

Benutzer meldet sich korrekt an,
ist aber nicht in der VPN-Gruppe.

Dann ist die Identität korrekt, aber der VPN-Zugriff nicht erlaubt.

Merksatz:

Erfolgreiche Anmeldung heißt nicht automatisch:
VPN-Zugriff erlaubt.

Fehlerbild 3: MFA schlägt fehl

Mögliche Ursachen:

Benutzer bestätigt nicht
falsches Gerät registriert
Authenticator-App nicht eingerichtet
Uhrzeit falsch
Push-Anfrage kommt nicht an
Benutzer ist gesperrt
Richtlinie verlangt anderen Faktor
Number Matching falsch
Angreifer löst Push-Fatigue aus

Prüfen:

MFA-Log
Benutzerstatus
registrierte Faktoren
Uhrzeit
Richtlinie
Fehlermeldung

Merksatz:

MFA-Probleme immer mit Authentifizierungslogs prüfen.

Fehlerbild 4: Zertifikatsfehler

VPN-Zertifikate können auf Client- oder Serverseite Probleme verursachen.

Mögliche Ursachen:

```
Serverzertifikat abgelaufen
Clientzertifikat abgelaufen
Zertifikatskette unvollständig
CA nicht vertrauenswürdig
Name passt nicht
Zertifikat widerrufen
privater Schlüssel fehlt
falsches Zertifikat ausgewählt
Systemzeit falsch
```

Merksatz:

```
Zertifikatsfehler mit Name,
Gültigkeit,
CA,
Schlüssel
und Zeit prüfen.
```

Fehlerbild 5: VPN verbindet, aber interne IPs gehen nicht

Wenn VPN verbunden ist, aber interne IP-Adressen nicht erreichbar sind, liegt der Fehler meist nach dem Tunnelaufbau.

Mögliche Ursachen:

```
Route zum Zielnetz fehlt
Rückroute fehlt
Firewall-Regel fehlt
Zielsystem offline
Host-Firewall blockiert
VPN-Gruppe darf Ziel nicht erreichen
Adresskonflikt mit Heimnetz
NAT falsch
falscher VPN-Adresspool
falsches Zielnetz
```

Merksatz:

```
VPN verbunden,
aber IP nicht erreichbar:
Route,
Firewall,
Rückweg
und Zielsystem prüfen.
```

Prüfung: VPN-IP erhalten?

Ein VPN-Client bekommt häufig eine Adresse aus einem VPN-Adresspool.

Beispiel:

```
VPN-IP:
10.8.0.25
```

Prüfen:

```
Hat der Client eine VPN-IP bekommen?
Liegt sie im richtigen Pool?
Passt der Pool zur Benutzergruppe?
Gibt es doppelte Adressen?
Ist der Pool voll?
Wird die IP in Logs angezeigt?
```

Merksatz:

```
Ohne korrekte VPN-IP können Regeln und Routen nicht passen.
```

Prüfung: Route zum Zielnetz

Der Client braucht eine Route zum internen Zielnetz.

Beispiel:

```
Zielnetz:
192.168.20.0/24
```

```
Route:
über VPN-Tunnel
```

Fehlt diese Route, sendet der Client Pakete nicht durch VPN.

Merksatz:

```
Route zum Zielnetz ist Pflicht.
```

Prüfung: Rückroute

Das Zielsystem oder dessen Gateway muss wissen, wie es zum VPN-Client zurückkommt.

Beispiel:

```
VPN-Pool:
10.8.0.0/24

Servernetz:
192.168.20.0/24
```

Das Servernetz braucht einen Rückweg zu:

```
10.8.0.0/24
```

Merksatz:

```
Ohne Rückroute sieht der Client keine Antwort.
```

Prüfung: Firewall zwischen VPN und Ziel

Auf dem Weg können mehrere Firewalls beteiligt sein.

Beispiele:

```
VPN-Gateway-Firewall
Core-Firewall
Servernetz-Firewall
```

Host-Firewall auf dem Zielsystem

Prüfen:

Quelle ist VPN-Pool?
Ziel ist korrekt?
Port ist korrekt?
TCP oder UDP korrekt?
Benutzergruppe korrekt?
Richtung korrekt?
Logs zeigen Allow oder Deny?
NAT verändert Quelle oder Ziel?

Merksatz:

Alle Filterstellen auf dem Weg prüfen.

Prüfung: Host-Firewall

Auch wenn das Netz den Zugriff erlaubt, kann das Zielsystem blockieren.

Beispiele:

Windows Firewall erlaubt RDP nur aus lokalem Subnetz.

Linux-Firewall erlaubt SSH nur aus Adminnetz.

Dienst erlaubt keine VPN-Quelladressen.

Merksatz:

Zielsystem-Firewall ist Teil der VPN-Fehlersuche.

Fehlerbild 6: VPN verbindet, aber interne Namen gehen nicht

Wenn IP-Adressen funktionieren, aber Namen nicht, ist DNS sehr wahrscheinlich betroffen.

Mögliche Ursachen:

interner DNS wird nicht gesetzt
DNS-Suffix fehlt
Split DNS falsch
DNS-Anfragen gehen lokal raus
DNS-Server über VPN nicht erreichbar
Firewall blockiert UDP/TCP 53
falscher DNS-Record
DNS-Cache veraltet
IPv6-Antwort zeigt falschen Weg

Merksatz:

IP geht,
Name nicht:
DNS prüfen.

Prüfung: DNS aus Sicht des VPN-Clients

Wichtig ist nicht, was der Administrator auf dem Server sieht.

Wichtig ist:

Was sieht der VPN-Client?

Prüfen:

Welche DNS-Server nutzt der Client?
Welche Suchdomäne ist gesetzt?
Wird Split DNS verwendet?
Welche Antwort liefert DNS?
Wird A oder AAAA genutzt?
Ist der interne DNS erreichbar?
Gibt es DNS-Leaks?

Merksatz:

DNS immer dort prüfen,
wo der Fehler auftritt.

Fehlerbild 7: Nur bestimmte Dienste gehen nicht

Wenn nur ein Dienst nicht funktioniert, ist der VPN-Tunnel wahrscheinlich grundsätzlich aktiv.

Beispiele:

```
Intranet geht,
aber RDP nicht.

DNS geht,
aber SMB nicht.

Ping geht,
aber HTTPS nicht.
```

Mögliche Ursachen:

```
Port nicht erlaubt
Dienst läuft nicht
Host-Firewall blockiert
Benutzer nicht berechtigt
Anwendung lehnt VPN-Quelle ab
Zertifikat oder TLS-Problem
falscher Port
falsches Protokoll
```

Merksatz:

```
Ein Dienst betroffen:
Port,
Dienst,
Berechtigung
und Anwendung prüfen.
```

Dienstprüfung über VPN

Bei einem einzelnen Dienst prüft man:

```
Zielname korrekt?
Ziel-IP korrekt?
Port korrekt?
TCP oder UDP?
Dienst lauscht?
Firewall erlaubt?
Host-Firewall erlaubt?
Anwendung antwortet?
Benutzer berechtigt?
Logs vorhanden?
```

Merksatz:

```
Dienstprüfung ist mehr als Ping.
```

Fehlerbild 8: VPN funktioniert nur für manche Benutzer

Wenn der Zugriff nur bei bestimmten Benutzern funktioniert, liegt der Fehler häufig bei Gruppen, Rollen oder Profilen.

Mögliche Ursachen:

```
falsche VPN-Gruppe
Benutzer nicht berechtigt
andere Routen
andere DNS-Einstellungen
andere Firewall-Regeln
anderes VPN-Profil
MFA-Richtlinie unterschiedlich
Gerätestatus unterschiedlich
Konto gesperrt
Rolle fehlt
```

Merksatz:

```
Manche Benutzer betroffen:
Gruppen,
Profile
```

und Rechte vergleichen.

Vergleichsmethode bei Benutzerproblemen

Vergleiche:

```
funktionierender Benutzer
mit
fehlerhaftem Benutzer
```

Prüfen:

```
gleiche Gruppe?
gleiches VPN-Profil?
gleiche Routen?
gleiche DNS-Server?
gleiche Firewall-Zone?
gleiche MFA-Richtlinie?
gleiches Endgerät?
gleiche Zielrechte?
```

Merksatz:

```
Vergleich zeigt,
was beim fehlerhaften Benutzer anders ist.
```

Fehlerbild 9: VPN funktioniert nur aus manchen Netzen

Wenn VPN aus einem Heimnetz funktioniert, aus einem anderen aber nicht, liegt der Fehler oft außerhalb der Firma.

Mögliche Ursachen:

```
lokales Heimnetz überschneidet sich
lokaler Router blockiert VPN
Hotel-WLAN blockiert UDP
Mobilfunk nutzt CGNAT
Provider blockiert Ports
```

```
DNS im Fremdnetz fehlerhaft
IPv6 nimmt anderen Weg
restriktives Gastnetz
captive portal aktiv
```

Merksatz:

```
Fremde Netze können VPN-Protokolle blockieren oder stören.
```

Adresskonflikt mit Heimnetz erkennen

Typisches Problem:

```
Heimnetz:
192.168.1.0/24

Firmennetz:
192.168.1.0/24
```

Symptom:

```
VPN verbunden,
aber Ziel im Firmennetz nicht erreichbar.
```

Ursache:

```
Client hält Ziel für lokal
und sendet nicht durch den Tunnel.
```

Merksatz:

```
Gleiche Netze auf beiden Seiten sind ein klassischer VPN-Fehler.
```

Fehlerbild 10: VPN langsam

VPN-Langsamkeit kann viele Ursachen haben.

Mögliche Ursachen:

hohe Latenz
Paketverlust
schlechte WLAN-Verbindung
Full Tunnel überlastet
VPN-Gateway ausgelastet
zentrale Internetleitung ausgelastet
MTU-Problem
TCP-over-TCP
Proxy langsam
schwacher Client
Server langsam
Datenbank langsam

Merksatz:

Langsam ist nicht gleich nicht erreichbar.

Performance prüfen

Bei VPN-Performance prüft man:

Latenz
Paketverlust
Bandbreite
Auslastung des Gateways
Auslastung des Clients
WLAN-Qualität
MTU
Tunnelart
Full Tunnel oder Split Tunnel
Zielserver
Anwendung
Tageszeit

Merksatz:

VPN-Performance braucht Messwerte,
nicht Bauchgefühl.

Fehlerbild 11: VPN bricht ab

Mögliche Ursachen:

```
instabile Internetverbindung
WLAN-Roaming
Mobilfunkwechsel
NAT-Timeout
Firewall-Timeout
VPN-Clientfehler
Token läuft ab
Zertifikat läuft ab
Gateway überlastet
Energiesparmodus
MTU-Problem
Keepalive fehlt
```

Merksatz:

```
VPN-Abbrüche mit Zeitbezug,
Logs
und Verbindungsmessung prüfen.
```

MTU-Probleme bei VPN

VPN fügt zusätzliche Header hinzu.

Dadurch kann die effektive Paketgröße sinken.

Typische Symptome:

```
kleine Webseiten gehen
große Webseiten hängen
Downloads brechen ab
VPN wirkt instabil
RDP friert ein
SSH hängt bei viel Ausgabe
große Dateiübertragung bricht ab
```

Merksatz:

```
Kleine Daten gehen,
große nicht:
MTU prüfen.
```

TCP-over-TCP bei VPN

Wenn ein VPN über TCP läuft und darin TCP-Verkehr transportiert wird, kann Performance schlechter werden.

Besonders bei Paketverlust stören sich die Steuerungsmechanismen.

Typisch:

```
langsame Dateiübertragung
stockende Verbindungen
hohe Latenz
Wiederholungen
```

Merksatz:

```
TCP im TCP-Tunnel kann bremsen.
```

NAT-Timeout

Viele Router und Firewalls löschen inaktive NAT-Zuordnungen nach einiger Zeit.

Folge:

```
VPN-Verbindung wirkt verbunden,
aber Daten fließen nicht mehr.
```

Oder:

```
Tunnel bricht ab.
```

Lösungsideen:

Keepalive
passende Timeout-Werte
stabile Verbindung
geeignete VPN-Konfiguration

Merksatz:

NAT-Timeout kann VPN-Verbindungen still abbrechen lassen.

VPN-Logs richtig auswerten

VPN-Logs können zeigen:

Verbindungsversuch
Benutzer
Quell-IP
Gateway
Authentifizierung
MFA-Ergebnis
Zertifikatsprüfung
zugewiesene IP
zugewiesene Gruppe
Routen
Trennungsgrund
Fehlercode
Phase-1- oder Phase-2-Fehler bei IPsec

Merksatz:

VPN-Logs zeigen,
an welchem Schritt die Verbindung scheitert.

Client-Logs

VPN-Client-Logs sind wichtig, weil der Client oft mehr Details zum Fehler sieht.

Sie zeigen zum Beispiel:

```
DNS-Auflösung des Gateways
Verbindungsversuch
Zertifikatsfehler
Authentifizierungsfehler
gesetzte Routen
gesetzte DNS-Server
Tunnelstatus
Abbruchgrund
```

Merksatz:

```
Client-Logs zeigen die Sicht des Endgeräts.
```

Gateway-Logs

VPN-Gateway-Logs zeigen die Sicht der Gegenstelle.

Sie zeigen zum Beispiel:

```
kommt der Client an?
wird Benutzer erkannt?
schlägt MFA fehl?
wird Zertifikat akzeptiert?
wird eine VPN-IP vergeben?
welche Gruppe wird angewendet?
welche Richtlinie greift?
warum wird Verbindung getrennt?
```

Merksatz:

```
Gateway-Logs zeigen,
was das VPN-System entschieden hat.
```

Firewall-Logs bei VPN

Firewall-Logs helfen nach dem Tunnelaufbau.

Sie zeigen:

```
Quelle aus VPN-Pool
Zielsystem
Port
Protokoll
erlaubte Verbindung
blockierte Verbindung
Regelname
Zone
NAT
Rückverkehr
```

Merksatz:

```
Firewall-Logs zeigen,
ob VPN-Verkehr wirklich erlaubt wird.
```

Paketmitschnitt bei VPN

Ein Paketmitschnitt kann helfen, wenn Logs nicht ausreichen.

Mögliche Mitschnittorte:

```
VPN-Client
VPN-Gateway außen
VPN-Gateway innen
interne Firewall
Zielserver
```

Fragen:

```
sendet der Client?
kommt Verkehr am Gateway an?
verlässt Verkehr das Gateway intern?
kommt Verkehr am Ziel an?
antwortet das Ziel?
kommt Antwort zurück?
```

Merksatz:

Mehrere Mitschnittpunkte zeigen,
wo Pakete verschwinden.

VPN-Fehlersuche nach OSI-Modell

Schicht	VPN-Prüfung
1	Internetverbindung, WLAN, Kabel
2	lokales Netz, WLAN, VLAN
3	IP, Routing, VPN-Pool, Rückroute
4	TCP/UDP, Ports, Firewall
5	Session, Tunnelstabilität, Timeout
6	TLS, Zertifikate, Verschlüsselung
7	Login, MFA, DNS, Anwendung, Rechte

Merksatz:

Auch VPN-Probleme lassen sich nach OSI eingrenzen.

Praktische Prüfreihenfolge

Eine gute Reihenfolge:

1. Fehlerbild genau aufnehmen.
2. VPN-Art und Protokoll bestimmen.
3. Client-Internet prüfen.
4. VPN-Gateway-Erreichbarkeit prüfen.
5. Authentifizierung und MFA prüfen.
6. Zertifikate prüfen.
7. VPN-IP prüfen.
8. Routen prüfen.
9. DNS prüfen.
10. Firewall-Regeln prüfen.
11. Zielsystem und Host-Firewall prüfen.
12. Logs vergleichen.
13. Performance und MTU prüfen.
14. Ergebnis dokumentieren.

Merksatz:

```
Erst Tunnel,
dann Route,
dann DNS,
dann Dienst.
```

Checkliste: VPN verbindet nicht

```
Gateway-Name korrekt?
Gateway-IP korrekt?
Internetverbindung vorhanden?
Port und Protokoll erreichbar?
VPN-Gateway online?
Benutzerkonto aktiv?
Passwort korrekt?
MFA erfolgreich?
Zertifikat gültig?
Clientversion passend?
Uhrzeit korrekt?
Logs geprüft?
```

Merksatz:

```
Bei Verbindungsfehlern vorne in der Kette suchen.
```

Checkliste: VPN verbunden, aber kein Zugriff

```
VPN-IP erhalten?
richtige Gruppe?
Route zum Zielnetz vorhanden?
Rückroute vorhanden?
DNS korrekt?
Firewall erlaubt?
Host-Firewall erlaubt?
Zielsystem online?
Dienst läuft?
```

Berechtigung vorhanden?

Logs geprüft?

Merksatz:

Bei Zugriffproblemen nach dem Tunnel suchen.

Checkliste: VPN langsam

Latenz gemessen?

Paketverlust gemessen?

Bandbreite geprüft?

WLAN geprüft?

Full Tunnel oder Split Tunnel?

Gateway ausgelastet?

Client ausgelastet?

MTU geprüft?

TCP-over-TCP möglich?

Zielserver langsam?

Anwendung langsam?

Tageszeit oder Lastspitzen?

Merksatz:

Langsamkeit mit Messwerten belegen.

Checkliste: VPN bricht ab

Abbruchzeitpunkt bekannt?

Client-Log geprüft?

Gateway-Log geprüft?

Internetverbindung stabil?

WLAN-Wechsel?

Mobilfunkwechsel?

NAT-Timeout?

Keepalive aktiv?

Zertifikat oder Token abgelaufen?

Gateway überlastet?

Energiesparmodus aktiv?

MTU-Problem möglich?

Merksatz:

Abbrüche brauchen Zeitbezug und Logs.

Typische Prüfungsfragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Warum reicht ein verbundener VPN-Tunnel nicht aus?
- Welche Schritte prüft man bei VPN-Fehlersuche?
- Warum sind Routen bei VPN wichtig?
- Warum ist der Rückweg wichtig?
- Warum können interne Namen trotz VPN nicht funktionieren?
- Warum ist DNS bei VPN häufig eine Fehlerquelle?
- Warum kann ein Dienst trotz VPN-Verbindung nicht erreichbar sein?
- Warum können unterschiedliche Benutzer unterschiedliche VPN-Rechte haben?
- Warum verursachen gleiche Netze auf beiden Seiten Probleme?
- Was sind typische Ursachen für langsame VPN-Verbindungen?
- Warum können MTU-Probleme bei VPN auftreten?
- Welche Logs sind bei VPN wichtig?
- Wie hilft ein Paketmitschnitt bei VPN-Fehlern?

Typische Prüfungsfallen

VPN verbunden heißt nicht:
alles funktioniert.

VPN-Status grün heißt nicht:
Routen stimmen.

Login erfolgreich heißt nicht:
Zugriff erlaubt.

Authentifizierung ist nicht Autorisierung.

IP geht,
Name nicht:
DNS prüfen.

Ping geht,
Dienst nicht:
Port und Anwendung prüfen.

Ein Dienst betroffen:
nicht ganzes VPN kaputt.

Manche Benutzer betroffen:
Gruppen und Profile vergleichen.

Manche Heimnetze betroffen:
Adresskonflikt prüfen.

Gleiche Netze auf beiden Seiten sind problematisch.

Route zum Ziel reicht nicht,
Rückroute muss auch stimmen.

Host-Firewall kann blockieren.

DNS-Suffix und Split DNS beachten.

UDP und TCP nicht verwechseln.

MTU bei großen Datenproblemen prüfen.

VPN-Logs und Firewall-Logs gemeinsam auswerten.

Client-Sicht und Gateway-Sicht vergleichen.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung

VPN-Fehlersuche	systematische Analyse von VPN-Problemen
VPN-Gateway	Gegenstelle für VPN-Verbindungen
VPN-Client	Endgerät oder Software des Benutzers
VPN-IP	Adresse aus dem VPN-Adresspool
VPN-Profil	Konfiguration für VPN-Zugriff
VPN-Gruppe	Gruppe zur Steuerung von Rechten
Route	Weg zu einem Zielnetz
Rückroute	Antwortweg zurück zum VPN-Client
Split DNS	getrennte DNS-Auflösung
DNS-Leak	DNS-Anfragen gehen falschen Weg
Host-Firewall	Firewall auf Zielsystem
MTU	maximale Paketgröße
NAT-Timeout	Ablauf einer NAT-Zuordnung
Keepalive	regelmäßiges Paket zum Offenhalten
Client-Log	Log aus Sicht des Endgeräts
Gateway-Log	Log aus Sicht des VPN-Systems
Firewall-Log	Log über erlaubten oder blockierten Verkehr
TCP-over-TCP	TCP-Verkehr in TCP-Tunnel
Adresskonflikt	gleiche Netze auf beiden Seiten

IHK-sichere Kurzformulierung

Bei der VPN-Fehlersuche muss zuerst das genaue Fehlerbild bestimmt werden. Ein VPN kann bereits beim Verbindungsaufbau, bei der Authentifizierung, bei MFA, bei Zertifikaten, beim Routing, bei DNS, bei Firewall-Regeln, beim Rückweg, beim Zielsystem oder bei Berechtigungen scheitern. Ein verbundener VPN-Tunnel bedeutet nicht automatisch, dass interne Ressourcen erreichbar sind. Der Client benötigt eine gültige VPN-IP, passende Routen, interne DNS-Einstellungen und die nötigen Firewall- und Benutzerrechte. Bei Performanceproblemen sind Latenz, Paketverlust, Bandbreite, MTU, Full Tunnel, Gateway-Auslastung und Client-Verbindung zu prüfen. Logs auf Client, VPN-Gateway, Firewall und Zielsystem helfen, den Fehler einzugrenzen.

Merksätze

VPN-Fehlersuche ist mehr als Tunnelprüfung.

Erst Fehlerbild klären.

VPN-Art bestimmen.

VPN-Protokoll bestimmen.

Gateway muss erreichbar sein.

Port und Protokoll müssen passen.

UDP und TCP nicht verwechseln.

Authentifizierung prüft Identität.

Autorisierung prüft Rechte.

MFA-Logs bei MFA-Problemen prüfen.

Zertifikate mit Name,
CA,
Gültigkeit
und Zeit prüfen.

VPN-IP muss korrekt sein.

Route zum Zielnetz muss vorhanden sein.

Rückroute muss vorhanden sein.

Firewall-Regeln müssen VPN-Quelle erlauben.

Host-Firewall nicht vergessen.

IP geht,
Name nicht:
DNS prüfen.

Interne Namen brauchen internes DNS.

Nur ein Dienst betroffen:
Port,

Dienst
und Rechte prüfen.

Manche Benutzer betroffen:
Gruppen und Profile prüfen.

Manche Heimnetze betroffen:
Adresskonflikt prüfen.

VPN langsam:
Latenz,
Paketverlust,
MTU
und Auslastung prüfen.

VPN bricht ab:
Logs und Zeitbezug prüfen.

Client-Logs zeigen Endgerätesicht.

Gateway-Logs zeigen VPN-Systemsicht.

Firewall-Logs zeigen Zugriffspfad.

Paketmitschnitt zeigt,
wo Pakete verschwinden.

Erst Tunnel,
dann Route,
dann DNS,
dann Dienst.