14.4

VPN-Routing, DNS und Firewall-Regeln

Ein VPN-Tunnel allein reicht nicht aus, damit interne Dienste erreichbar sind.

Zusätzlich müssen passen:

```
- IP-Adressbereiche
- Routing
- DNS
- Firewall-Regeln
- NAT-Regeln
- Berechtigungen
- Rückwege
- Client-Konfiguration
```

Merksatz:

```
VPN verbunden heißt nicht automatisch:
Ziel erreichbar.
```

Warum Routing bei VPN wichtig ist

Routing entscheidet, über welchen Weg ein Paket geschickt wird.

Wenn ein Client per VPN verbunden ist, muss sein System wissen:

```
Welche Ziele liegen im VPN?
Welche Ziele liegen im lokalen Netz?
Welche Ziele gehen direkt ins Internet?
```

Fehlt eine passende Route, geht der Verkehr nicht durch den VPN-Tunnel.

Merksatz:

```
Ohne Route kein Weg durch den Tunnel.
```

VPN-Routing einfach erklärt

Beispiel:

```
VPN-Client:
10.8.0.20

Firmennetz:
192.168.10.0/24
```

Damit der Client das Firmennetz erreicht, braucht er eine Route:

```
Zielnetz 192.168.10.0/24
über VPN-Tunnel
```

Wenn diese Route fehlt, sendet der Client die Pakete eventuell an sein lokales Gateway.

Merksatz:

```
Der Client muss wissen,
welche Netze über VPN erreichbar sind.
```

Routingtabelle

Eine Routingtabelle enthält Wege zu Netzwerken.

Sie beantwortet:

```
Wohin schicke ich Pakete für dieses Zielnetz?
```

Typische Einträge:

```
Standardroute
lokale Netzroute
VPN-Route
Hostroute
spezifische Netzroute
```

Merksatz:

```
Routingtabelle = Wegweiser für IP-Pakete.
```

Standardroute

Die Standardroute wird genutzt, wenn keine spezifischere Route passt.

Sie zeigt meist zum lokalen Internetrouter.

Beispiel:

```
0.0.0.0/0
über lokales Gateway
```

Bei Full Tunnel kann die Standardroute über VPN gesetzt werden.

Merksatz:

```
Standardroute ist der Weg für alles,
was nicht genauer bekannt ist.
```

Spezifischere Route gewinnt

Routing arbeitet nach dem Prinzip:

```
die genaueste passende Route gewinnt.
```

Beispiel:

```
0.0.0.0/0
über lokales Gateway

192.168.10.0/24
über VPN
```

Wenn Ziel 192.168.10.50 ist, gewinnt die spezifische VPN-Route.

Merksatz:

Genauere Route gewinnt vor allgemeiner Route.

Split Tunnel

Split Tunnel bedeutet:

Nur bestimmte Netze gehen durch VPN.

Beispiel:

Firmennetze:
durch VPN

normales Internet:
direkt lokal

Vorteile:

weniger Last auf VPN
weniger Bandbreitenbedarf in der Firma
oft bessere Performance für normale Internetdienste

Nachteile:

weniger zentrale Kontrolle
Sicherheitsrichtlinien schwieriger einheitlich durchsetzbar

Merksatz:

Split Tunnel leitet nur ausgewählten Verkehr durch VPN.

Full Tunnel

Full Tunnel bedeutet:

Der gesamte Verkehr läuft durch VPN.

Auch Internetverkehr geht zuerst zum Unternehmen.

Vorteile:

```
zentrale Kontrolle
zentrale Filterung
einheitliche Sicherheitsrichtlinien
bessere Protokollierung
```

Nachteile:

```
mehr Last
höhere Latenz
mehr Bandbreite nötig
VPN-Gateway wird kritischer
```

Merksatz:

```
Full Tunnel leitet alles durch VPN.
```

Split Tunnel und Full Tunnel vergleichen

Merkmal	Split Tunnel	Full Tunnel
Firmennetze	über VPN	über VPN
Internetverkehr	direkt lokal	über VPN
Last auf VPN	geringer	höher
zentrale Kontrolle	geringer	höher
Performance	oft besser	abhängig vom VPN
Sicherheitspolitik	schwieriger	zentraler

Merksatz:

```
Split Tunnel spart Last.
Full Tunnel gibt mehr Kontrolle.
```

VPN-Adresspool

Der VPN-Adresspool ist der IP-Bereich, aus dem VPN-Clients ihre VPN-Adresse bekommen.

Beispiel:

```
10.8.0.0/24
```

Ein Client erhält dann zum Beispiel:

```
10.8.0.20
```

Diese Adresse wird in Firewall-Regeln, Routing und Logs verwendet.

Merksatz:

```
VPN-Adresspool bestimmt,
aus welchem Netz VPN-Clients kommen.
```

VPN-Adresspool darf sich nicht überschneiden

Der VPN-Adresspool darf sich nicht mit anderen Netzen überschneiden.

Problematisch:

```
VPN-Pool:
192.168.1.0/24

Heimnetz des Benutzers:
192.168.1.0/24
```

Dann ist unklar, ob 192.168.1.50 lokal oder über VPN erreichbar ist.

Merksatz:

```
Überlappende Netze verursachen VPN-Routingprobleme.
```

Adresskonflikt mit Heimnetz

Ein sehr häufiger VPN-Fehler:

```
Firmennetz:
192.168.1.0/24

Heimnetz:
192.168.1.0/24
```

Der Client denkt dann oft:

```
192.168.1.x ist lokal
```

und sendet Pakete nicht durch den VPN-Tunnel.

Folge:

```
interne Systeme sind nicht erreichbar.
```

Merksatz:

```
Häufige Heimnetzbereiche im Firmennetz vermeiden.
```

Typische problematische Heimnetzbereiche

Viele Heimrouter nutzen Standardnetze wie:

```
192.168.0.0/24
192.168.1.0/24
192.168.2.0/24
192.168.178.0/24
```

Wenn Unternehmen dieselben Netze intern nutzen, kann VPN-Zugriff aus dem Homeoffice Probleme machen.

Merksatz:

```
Für Firmennetze möglichst eindeutige,
weniger typische Adressbereiche planen.
```

Route fehlt

Fehlt eine VPN-Route, kann der Tunnel verbunden sein, aber interne Netze sind trotzdem nicht erreichbar.

Typisches Fehlerbild:

```
VPN zeigt verbunden.
Internet geht.
interne IPs gehen nicht.
interne Namen gehen nicht.
nur VPN-Gateway erreichbar.
```

Mögliche Ursache:

```
Route zu internem Netz wurde nicht verteilt.
```

Merksatz:

```
VPN-Status grün heißt nicht:
Routen stimmen.
```

Route zum Zielnetz fehlt

Beispiel:

```
Ziel:
10.20.30.50
```

Benötigte Route:

```
10.20.30.0/24
über VPN
```

Wenn nur 192.168.10.0/24 über VPN geroutet wird, ist 10.20.30.50 nicht erreichbar.

Merksatz:

```
Jedes gewünschte Zielnetz braucht eine passende Route.
```

Rückroute fehlt

Nicht nur der Client braucht eine Route zum Ziel.

Auch das Zielnetz muss wissen, wie es zum VPN-Client zurückkommt.

Beispiel:

```
VPN-Client:
10.8.0.20

Server:
192.168.10.50
```

Der Server oder sein Gateway braucht einen Rückweg zu:

```
10.8.0.0/24
```

Merksatz:

```
VPN braucht Hinweg und Rückweg.
```

Asymmetrisches Routing bei VPN

Asymmetrisches Routing bedeutet:

```
Hinweg und Rückweg laufen über unterschiedliche Wege.
```

Bei Firewalls kann das problematisch sein, weil Stateful Firewalls den Verbindungszustand verfolgen.

Wenn die Antwort einen anderen Weg nimmt, kann sie blockiert werden.

Merksatz:

```
Stateful Firewalls brauchen passenden Hin- und Rückweg.
```

VPN und NAT

Manchmal wird NAT auch bei VPN genutzt.

Beispiele:

```
überlappende Netze müssen übersetzt werden
VPN-Clients sollen mit bestimmter Quell-IP erscheinen
Partnernetz darf interne echte Adressen nicht sehen
Cloud-Netz erwartet bestimmte Adressbereiche
```

Aber:

```
NAT macht Fehlersuche komplizierter.
```

Merksatz:

```
NAT im VPN kann helfen,
aber erschwert Analyse und Dokumentation.
```

NAT bei überlappenden Netzen

Wenn zwei Seiten dasselbe Netz verwenden, kann NAT eine technische Umgehung sein.

Beispiel:

```
Standort A:
192.168.1.0/24

Standort B:
192.168.1.0/24
```

Eine Seite wird für den Tunnel in ein anderes Netz übersetzt.

Aber:

```
Das ist meist komplizierter als saubere IP-Planung.
```

Merksatz:

```
NAT kann Adresskonflikte umgehen,
ersetzt aber keine gute Netzplanung.
```

VPN-DNS

VPN-DNS sorgt dafür, dass interne Namen korrekt aufgelöst werden.

Beispiele:

```
intranet.firma.local
fileserver.firma.local
wiki.intern
dc01.firma.local
```

Dafür erhält der VPN-Client meist:

```
interne DNS-Server
DNS-Suffix
Suchdomäne
Split-DNS-Regeln
```

Merksatz:

```
VPN braucht oft interne DNS-Konfiguration.
```

DNS-Server über VPN

Der VPN-Client kann interne DNS-Server zugewiesen bekommen.

Beispiel:

```
DNS-Server:
192.168.10.10
```

Damit kann er interne Namen auflösen.

Wenn der interne DNS-Server nicht erreichbar ist, funktioniert Namensauflösung trotz VPN nicht.

Merksatz:

```
Interner DNS muss über VPN erreichbar und erlaubt sein.
```

DNS-Suffix

Ein DNS-Suffix ergänzt kurze Namen.

Beispiel:

```
Benutzer gibt ein:
fileserver
```

Mit DNS-Suffix wird daraus:

```
fileserver.firma.local
```

Fehlt das DNS-Suffix, funktionieren kurze interne Namen eventuell nicht.

Merksatz:

```
DNS-Suffix hilft bei kurzen internen Namen.
```

Split DNS

Split DNS bedeutet:

```
interne Namen werden über interne DNS-Server aufgelöst

externe Namen werden normal oder öffentlich aufgelöst
```

Beispiel:

```
firma.local
über VPN-DNS

öffentliche Webseiten
über normalen DNS
```

Merksatz:

```
Split DNS trennt interne und externe Namensauflösung.
```

Fehlerbild: Interne Namen gehen nicht

Mögliche Ursachen:

```
- interner DNS wird nicht verteilt
- DNS-Suffix fehlt
- DNS-Anfragen gehen nicht durch VPN
- DNS-Server über VPN nicht erreichbar
- Firewall blockiert UDP/TCP 53
- Split DNS falsch
- falscher DNS-Server antwortet
- lokale DNS-Cache-Einträge sind alt
```

Merksatz:

```
VPN-Namensprobleme sind oft DNS- oder Split-DNS-Probleme.
```

Fehlerbild: IP geht, Name nicht

Wenn interne IP-Adresse funktioniert, aber interner Name nicht, liegt der Fehler meist bei DNS.

Beispiel:

```
192.168.10.50 funktioniert.

fileserver.firma.local funktioniert nicht.
```

Prüfen:

```
DNS-Server
DNS-Suffix
DNS-Record
Firewall für DNS
Split DNS
```

```
Cache
```

Merksatz:

```
IP geht,
Name nicht:
DNS prüfen.
```

VPN und Firewall-Regeln

Ein VPN-Tunnel bedeutet nicht automatisch, dass alle Ziele erlaubt sind.

Die Firewall muss regeln:

```
Welche VPN-Gruppe darf wohin?
Welche Ports sind erlaubt?
Welche Protokolle sind erlaubt?
Welche Richtung gilt?
Welche Zone ist beteiligt?
Wird der Zugriff protokolliert?
```

Merksatz:

```
VPN braucht gezielte Firewall-Regeln.
```

VPN-Zone

VPN-Verkehr sollte in eigene Firewall-Zonen eingeordnet werden.

Beispiele:

```
VPN-Mitarbeiter
VPN-Admin
VPN-Dienstleister
VPN-Partner
Site-to-Site-Partner
Cloud-VPN
```

Vorteil:

```
Regeln können gezielt und übersichtlich erstellt werden.
```

Merksatz:

```
VPN-Zonen verhindern pauschale Vermischung mit LAN.
```

Regelprinzip für VPN

Nicht gut:

```
VPN → LAN any allow
```

Besser:

```
VPN-Mitarbeiter → Intranet HTTPS erlauben

VPN-Support → bestimmte Clients RDP erlauben

VPN-Admin → Managementnetz SSH/RDP erlauben

VPN-Dienstleister → Wartungsserver erlauben
```

Merksatz:

```
VPN-Zugriff nach Rolle,
Ziel
und Dienst begrenzen.
```

VPN und Least Privilege

Least Privilege bedeutet:

```
nur notwendige Rechte und Zugriffe erlauben.
```

Bei VPN heißt das:

```
nicht alle Netze
nicht alle Ports
nicht alle Benutzer
nicht dauerhaft
nicht ohne Protokollierung
```

Merksatz:

```
VPN-Zugang so eng wie möglich freigeben.
```

VPN und Gruppen

VPN-Zugriffe werden oft über Gruppen gesteuert.

Beispiele:

```
VPN-Mitarbeiter
VPN-Support
VPN-Admins
VPN-Externe
VPN-Cloud-Admins
```

Gruppen steuern:

```
Routen
Firewall-Regeln
DNS
Zugriff auf Anwendungen
MFA-Anforderungen
```

Merksatz:

```
Gruppen machen VPN-Zugriff verwaltbar.
```

VPN und Benutzerrechte

VPN-Zugang allein gibt noch keine Anwendungsrechte.

Beispiel:

```
Benutzer erreicht Dateiserver per VPN.
```

Trotzdem braucht er:

```
gültige Anmeldung
Freigaberecht
Dateisystemrecht
Gruppenmitgliedschaft
```

Merksatz:

```
Netzwerkzugang ist nicht dasselbe wie Anwendungsberechtigung.
```

VPN und Host-Firewall

Auch wenn die zentrale Firewall Zugriff erlaubt, kann die lokale Firewall des Zielsystems blockieren.

Beispiele:

```
Windows Defender Firewall blockiert RDP.

Linux-Firewall blockiert SSH.

Server erlaubt nur internes LAN,
aber nicht VPN-Pool.
```

Merksatz:

```
Zielsystem-Firewall muss VPN-Quellen ebenfalls erlauben.
```

VPN und Serverdienste

Der Zielserver muss auf dem richtigen Port lauschen.

Prüfen:

```
Dienst läuft?
Dienst lauscht auf richtiger IP?
Dienst lauscht auf richtigem Port?
Dienst erlaubt VPN-Quellen?
Anwendung erlaubt Benutzer?
Logs zeigen Fehler?
```

Merksatz:

```
VPN erreicht nur Dienste,
die auch wirklich laufen und erreichbar sind.
```

VPN und Rückweg über Gateway

Ein Server antwortet meist über sein Standardgateway.

Wenn das Gateway keine Route zum VPN-Adresspool kennt, geht die Antwort falsch.

Beispiel:

```
Server will zu 10.8.0.20 antworten.
Gateway kennt 10.8.0.0/24 nicht.
```

Folge:

```
Antwort kommt nicht zurück.
```

Merksatz:

```
Zielnetz muss den VPN-Pool zurückrouten können.
```

VPN und interne Firewalls

In größeren Netzen gibt es oft mehrere Firewalls.

Beispiel:

```
VPN-Gateway
→ Core-Firewall
→ Servernetz-Firewall
→ Host-Firewall
```

Jede dieser Stellen kann blockieren.

Merksatz:

```
Bei VPN-Zugriff alle Filterstellen auf dem Weg prüfen.
```

VPN und VLANs

VPN-Benutzer können Zugriff auf bestimmte VLANs erhalten.

Beispiele:

```
Client-VLAN
Server-VLAN
Management-VLAN
DMZ-VLAN
```

Wichtig:

```
VPN-Zugriff auf Management-VLAN besonders stark begrenzen.
```

Merksatz:

```
VLAN-Zugriff über VPN bewusst steuern.
```

VPN und DMZ

VPN-Gateways können in einer DMZ stehen.

Warum?

```
Sie sind von außen erreichbar
und sollten vom internen LAN getrennt sein.
```

Nach erfolgreichem VPN-Aufbau dürfen Benutzer nur über definierte Regeln weiter ins interne Netz.

Merksatz:

```
VPN-Gateway in DMZ,
Zugriff ins LAN nur geregelt.
```

VPN und Extranet

Bei Extranet-Zugängen gilt besonders:

```
externe Benutzer nur auf benötigte Systeme
keine pauschale LAN-Freigabe
eigene Benutzerkonten
MFA
Ablaufdatum
Protokollierung
regelmäßige Prüfung
```

Merksatz:

```
Extranet-VPN braucht besonders enge Regeln.
```

VPN und Cloud-Netze

Bei Cloud-VPN müssen beide Seiten passen.

Lokale Seite:

```
Routen
Firewall
NAT
DNS
```

Cloud-Seite:

```
Routing Table
Security Group
Network Security Group
Cloud Firewall
Subnetze
DNS
```

Merksatz:

```
Cloud-VPN braucht Regeln und Routen auf beiden Seiten.
```

VPN und IPv6

VPN kann IPv4, IPv6 oder beides transportieren.

Wichtig:

```
Wenn IPv6 aktiv ist,
müssen auch IPv6-Routen und IPv6-Firewall-Regeln stimmen.
```

Problem:

```
IPv4 funktioniert über VPN,
aber IPv6 nimmt anderen Weg.
```

Merksatz:

```
Dual Stack bedeutet:
IPv4 und IPv6 prüfen.
```

VPN-Leak

Ein VPN-Leak bedeutet:

```
Verkehr geht unerwartet außerhalb des VPN-Tunnels.
```

Beispiele:

DNS-Leak:
DNS-Anfragen gehen an lokalen Provider statt internen DNS.

IPv6-Leak:
IPv6-Verkehr geht direkt ins Internet statt durch VPN.

Split-Tunnel-Fehlkonfiguration:
sensible Ziele gehen nicht durch VPN.

Merksatz:

VPN-Leak bedeutet:
Verkehr nimmt unerwartet den falschen Weg.

DNS-Leak

Ein DNS-Leak liegt vor, wenn DNS-Anfragen nicht wie vorgesehen über den VPN-DNS laufen.

Folgen:

interne Namen funktionieren nicht
Provider sieht DNS-Anfragen
Sicherheitsrichtlinien werden umgangen
falsche Antworten werden genutzt

Merksatz:

DNS-Leak betrifft Namensauflösung außerhalb des gewünschten Weges.

IPv6-Leak

Ein IPv6-Leak kann entstehen, wenn VPN nur IPv4 tunnelt, aber der Client weiterhin IPv6 direkt nutzt.

Folge:

Verkehr kann außerhalb des VPNs laufen.

Lösung:

```
IPv6 korrekt tunneln
oder
IPv6 bewusst regeln
```

Merksatz:

```
IPv6 bei VPN nicht vergessen.
```

VPN und Proxy

Manche Unternehmen kombinieren VPN mit Proxy.

Beispiele:

```
Full Tunnel plus Webproxy
Split Tunnel plus Cloudproxy
Proxy nur für bestimmte Anwendungen
PAC-Datei für Browser
```

Fehlerquellen:

```
falsche Proxy-Einstellungen
Proxy nicht über VPN erreichbar
Authentifizierung am Proxy schlägt fehl
falsche Ausnahmen
```

Merksatz:

```
VPN und Proxy müssen zusammenpassen.
```

VPN und Zertifikate

Zertifikate können für VPN wichtig sein.

Beispiele:

```
Serverzertifikat des VPN-Gateways
Clientzertifikat auf Endgerät
Zertifikatskette
interne CA
Zertifikatswiderruf
Ablaufdatum
```

Fehler:

```
Zertifikat abgelaufen
Name passt nicht
CA nicht vertraut
Clientzertifikat fehlt
CRL oder OCSP nicht erreichbar
```

Merksatz:

```
VPN-Zertifikate mit Name,
Vertrauen,
Gültigkeit
und Widerruf prüfen.
```

VPN und Zeit

Korrekte Zeit ist wichtig für:

```
Zertifikate
Kerberos
MFA
Tokens
Logs
Sicherheitsprüfungen
```

Wenn die Uhrzeit stark abweicht, können Anmeldungen oder Zertifikate fehlschlagen.

Merksatz:

```
VPN-Fehler können durch falsche Uhrzeit entstehen.
```

VPN-Fehlersuche: Grundreihenfolge

Eine sinnvolle Reihenfolge:

1. VPN-Art bestimmen.
2. VPN-Protokoll bestimmen.
3. Verbindungsstatus prüfen.
4. Authentifizierung prüfen.
5. VPN-IP prüfen.
6. Routen prüfen.
7. DNS prüfen.
8. Firewall-Regeln prüfen.
9. Zielsystem prüfen.
10. Rückweg prüfen.
11. Logs prüfen.
12. MTU und Performance prüfen.

Merksatz:

VPN-Fehlersuche braucht Tunnel,
Route,
DNS,
Firewall
und Zielsystem.

Fehlerbild: VPN verbunden, aber Ziel-IP nicht erreichbar

Mögliche Ursachen:

- Route fehlt
- Firewall blockiert
- Zielsystem offline
- Rückroute fehlt
- Host-Firewall blockiert
- VPN-Gruppe darf Ziel nicht erreichen
- Adresskonflikt
- NAT falsch
- falsches Zielnetz

Prüfen:

```
VPN-IP
Routingtabelle
Firewall-Logs
Zielsystem
Rückweg
```

Merksatz:

```
Ziel-IP nicht erreichbar:
Route,
Firewall
und Rückweg prüfen.
```

Fehlerbild: VPN verbunden, interner Name nicht erreichbar

Mögliche Ursachen:

```
- DNS-Server nicht gesetzt
- DNS-Suffix fehlt
- Split DNS falsch
- DNS-Server nicht erreichbar
- Firewall blockiert DNS
- falscher Record
- Cache veraltet
```

Prüfen:

```
DNS-Server
DNS-Antwort
DNS-Suffix
UDP/TCP 53
Split DNS
```

Merksatz:

Interner Name nicht erreichbar:
DNS prüfen.

Fehlerbild: Nur ein Dienst nicht erreichbar

Mögliche Ursachen:

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

Prüfen:

Porttest
Dienststatus
Firewall-Log
Serverlog
Berechtigungen

Merksatz:

Ein Dienst betroffen:
Port,
Dienst
und Anwendung prüfen.

Fehlerbild: Zugriff geht nur für manche Benutzer

Mögliche Ursachen:

- unterschiedliche VPN-Gruppen
- unterschiedliche Routen

- unterschiedliche Firewall-Regeln
- Benutzerrechte fehlen
- MFA-Richtlinie unterschiedlich
- Clientprofil unterschiedlich
- Gerätestatus unterschiedlich
- Rolle fehlt

Prüfen:

Gruppenmitgliedschaft
VPN-Profil
Routen
Rechte
Logs

Merksatz:

Unterschiedliche Benutzer:
Gruppen,
Rollen
und Profile prüfen.

Fehlerbild: Zugriff geht nur von manchen Heimnetzen nicht

Mögliche Ursachen:

- Adresskonflikt mit Heimnetz
- lokaler Router blockiert VPN
- restriktives WLAN
- Provider blockiert
- CGNAT oder NAT-Probleme
- IPv6 nimmt anderen Weg
- DNS des Heimnetzes stört

Merksatz:

Manche Heimnetze betroffen:
lokale Netze,

NAT,
DNS
und IPv6 prüfen.

Fehlerbild: VPN langsam oder instabil

Mögliche Ursachen:

- hohe Latenz
- Paketverlust
- MTU-Problem
- WLAN-Probleme
- Full Tunnel überlastet
- VPN-Gateway ausgelastet
- TCP-over-TCP
- schwache Clientleistung
- Providerproblem
- Sicherheitsprüfung oder Proxy langsam

Merksatz:

VPN-Performance mit Latenz,
Paketverlust,
MTU
und Auslastung prüfen.

Checkliste: VPN-Routing

VPN-IP erhalten?
Route zum Zielnetz vorhanden?
genaueste Route korrekt?
Standardroute verändert?
Split Tunnel oder Full Tunnel?
Zielnetz überschneidet sich?
Rückroute vorhanden?
mehrere Gateways beteiligt?
Routing auf Cloud-Seite korrekt?

Routing auf Servernetz-Seite korrekt?

Merksatz:

VPN-Routing immer auf Client,
Gateway
und Zielnetz prüfen.

Checkliste: VPN-DNS

interner DNS gesetzt?
DNS-Suffix gesetzt?
Split DNS korrekt?
UDP 53 erlaubt?
TCP 53 erlaubt?
interner DNS über VPN erreichbar?
liefert DNS richtige IP?
A und AAAA prüfen?
Cache geleert oder geprüft?
interner und externer DNS verglichen?

Merksatz:

DNS bei VPN immer aus Sicht des VPN-Clients prüfen.

Checkliste: VPN-Firewall

VPN-Zone korrekt?
Quelle VPN-Pool korrekt?
Benutzergruppe korrekt?
Zielnetz korrekt?
Zielhost korrekt?
Port korrekt?
TCP oder UDP korrekt?
Richtung korrekt?
Host-Firewall korrekt?
Rückverkehr erlaubt?

Logs zeigen Treffer?

Merksatz:

Firewall-Regeln für VPN genau wie andere Regeln prüfen.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Warum reicht ein aufgebauter VPN-Tunnel allein nicht aus?
- Warum ist Routing bei VPN wichtig?
- Was ist ein VPN-Adresspool?
- Warum sind überlappende Netze problematisch?
- Was ist Split Tunneling?
- Was ist Full Tunnel?
- Warum ist DNS bei VPN wichtig?
- Was ist Split DNS?
- Was ist ein DNS-Leak?
- Was ist ein IPv6-Leak?
- Warum braucht VPN Firewall-Regeln?
- Warum sollte VPN-Zugriff nach Rollen begrenzt werden?
- Warum kann eine Host-Firewall VPN-Zugriffe blockieren?
- Warum ist der Rückweg wichtig?
- Wie geht man bei VPN-Fehlersuche systematisch vor?

Typische Prüfungsfallen

VPN verbunden heißt nicht:
alles erreichbar.

Route fehlt:
Ziel nicht erreichbar.

Rückroute fehlt:
Antwort kommt nicht zurück.

Genaueste Route gewinnt.

Split Tunnel leitet nur ausgewählten Verkehr.

Full Tunnel leitet alles durch VPN.

VPN-Adresspool muss eindeutig sein.

Heimnetz und Firmennetz dürfen sich nicht überschneiden.

DNS ist bei VPN häufige Fehlerquelle.

IP geht,
Name nicht:
DNS prüfen.

Interner DNS muss über VPN erreichbar sein.

DNS-Suffix kann für kurze Namen nötig sein.

Split DNS trennt interne und externe Namensauflösung.

DNS-Leak bedeutet DNS außerhalb des gewünschten Weges.

IPv6-Leak nicht vergessen.

VPN braucht Firewall-Regeln.

VPN-Zugriff nicht pauschal ins LAN erlauben.

Host-Firewall auf Zielsystem prüfen.

VPN-Gruppe beeinflusst Zugriff.

Netzwerkzugang ist nicht Anwendungsberechtigung.

Cloud-VPN braucht Regeln auf beiden Seiten.

Zertifikate,
Zeit

und Logs bei VPN prüfen.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
VPN-Routing	Wege für Netze über VPN
Routingtabelle	Tabelle mit Wegen zu Zielnetzen
Standardroute	Route für alle nicht genauer bekannten Ziele
spezifische Route	genauere Route zu bestimmtem Netz
Split Tunnel	nur ausgewählter Verkehr über VPN
Full Tunnel	gesamter Verkehr über VPN
VPN-Adresspool	IP-Bereich für VPN-Clients
Adresskonflikt	gleiche Netze auf beiden Seiten
Rückroute	Antwortweg zurück zum VPN-Client
asymmetrisches Routing	Hin- und Rückweg unterschiedlich
VPN-DNS	DNS-Einstellungen für VPN-Clients
DNS-Suffix	Ergänzung für kurze Namen
Split DNS	getrennte DNS-Auflösung
DNS-Leak	DNS-Anfrage geht falschen Weg
IPv6-Leak	IPv6-Verkehr geht außerhalb VPN
VPN-Zone	Firewall-Zone für VPN-Verkehr
VPN-Gruppe	Gruppe zur Steuerung von VPN-Rechten
Host-Firewall	Firewall auf dem Zielsystem
Cloud-VPN	Verbindung zu Cloud-Netz
Rückweg	Antwortpfad zum Absender

IHK-sichere Kurzformulierung

Ein aufgebauter VPN-Tunnel allein reicht nicht aus, damit interne Ressourcen erreichbar sind. Zusätzlich müssen Routing, DNS, Firewall-Regeln, Rückwege und Berechtigungen stimmen. Der VPN-Client benötigt passende Routen zu den internen Zielnetzen. Bei Split Tunneling wird nur ausgewählter Verkehr durch das VPN geleitet, während bei Full Tunnel der gesamte Verkehr durch den VPN-Tunnel läuft. Der VPN-Adresspool darf sich nicht mit lokalen oder internen Netzen überschneiden, da sonst Routingprobleme entstehen. Für interne Namen müssen interne DNS-Server, DNS-Suffixe oder Split-DNS-Regeln korrekt gesetzt sein. VPN-Zugriffe sollten über eigene Firewall-Zonen, Gruppen und Least-Privilege-Regeln gesteuert werden.

Merksätze

VPN verbunden heißt nicht:
Zugriff funktioniert.

Ohne Route kein Weg.

Ohne Rückroute keine Antwort.

Genaueste Route gewinnt.

Standardroute gilt nur,
wenn nichts Spezifischeres passt.

Split Tunnel leitet ausgewählten Verkehr.

Full Tunnel leitet gesamten Verkehr.

VPN-Adresspool muss eindeutig sein.

Überlappende Netze vermeiden.

Heimnetzkonflikte sind häufig.

Jede Zielroute muss bekannt sein.

NAT im VPN macht Analyse schwieriger.

VPN-DNS ist wichtig für interne Namen.

DNS-Suffix hilft bei Kurznamen.

Split DNS trennt interne und externe Auflösung.

IP geht,
Name nicht:
DNS prüfen.

VPN braucht Firewall-Regeln.

VPN-Zonen schaffen Übersicht.

VPN-Zugriff nach Rollen begrenzen.

Least Privilege gilt auch im VPN.

Netzwerkzugang ist nicht Anwendungsrecht.

Host-Firewall mitprüfen.

Zielsystem muss Dienst bereitstellen.

Rückweg über Gateway prüfen.

Cloud-VPN braucht Regeln beidseitig.

IPv6 bei VPN nicht vergessen.

DNS-Leak bedeutet falscher DNS-Weg.

IPv6-Leak bedeutet falscher IPv6-Weg.

Zertifikate und Zeit können VPN beeinflussen.

VPN-Fehlersuche braucht Tunnel,
Route,
DNS,
Firewall,
Zielsystem
und Logs.