20.9 Trainer – VPN, Intranet, Extranet und sicherer Fernzugriff

Diese Trainer-Seite wiederholt VPN, Intranet, Extranet, VPN-Arten, VPN-Protokolle, VPN-Routing, DNS und typische Fehler beim sicheren Fernzugriff.

Ziel ist, typische Prüfungsfragen zu verschlüsseltem Zugriff, Standortvernetzung, Remote-Arbeit und VPN-Fehlersuche sicher zu beantworten.

Merksatz:

> VPN verbindet sicher über unsichere Netze.
> Intranet ist intern.
> Extranet ist kontrollierter Zugriff für Externe.

Lernziele

Nach dieser Seite solltest du sicher können:

- VPN erklären
- Intranet und Extranet unterscheiden
- Remote-Access-VPN und Site-to-Site-VPN unterscheiden
- VPN-Protokolle grob einordnen
- Split-Tunneling und Full-Tunneling erklären
- VPN-Routing und VPN-DNS verstehen
- typische VPN-Fehler erkennen
- Sicherheitsmaßnahmen für VPN nennen
- VPN von normaler Portweiterleitung unterscheiden

Kurzüberblick

Begriff	Bedeutung
VPN	verschlüsselte Verbindung über ein unsicheres Netz
Remote-Access-VPN	einzelner Benutzer verbindet sich ins Firmennetz
Site-to-Site-VPN	zwei Standorte oder Netze werden verbunden
Intranet	internes Netz einer Organisation
Extranet	kontrollierter Zugriff für externe Partner

Begriff	Bedeutung
Split-Tunneling	nur bestimmter Verkehr läuft durch VPN
Full-Tunneling	gesamter Verkehr läuft durch VPN
VPN-Gateway	Gegenstelle für VPN-Verbindungen

Merksatz:

```
VPN ist der Tunnel.
Intranet ist intern.
Extranet ist kontrolliert extern.
```

Aufgabe 1

Was ist ein VPN?

Antwort anzeigen

VPN steht für:

```
Virtual Private Network
```

Ein VPN stellt eine geschützte Verbindung über ein unsicheres Netz her, zum Beispiel über das Internet.

Typische Ziele:

```
Vertraulichkeit

Integrität

Authentifizierung

sicherer Fernzugriff
```

Merksatz:

```
VPN = verschlüsselter Tunnel über unsicheres Netz.
```

Aufgabe 2

Warum nutzt man VPN?

Antwort anzeigen

VPN wird genutzt für:

```
sicheren Fernzugriff

Homeoffice

Standortvernetzung

Zugriff auf interne Dienste

geschützte Administration

sichere Kommunikation über das Internet
```

Merksatz:

```
VPN ermöglicht sicheren Zugriff auf interne Ressourcen.
```

Aufgabe 3

Was ist ein Intranet?

Antwort anzeigen

Ein Intranet ist ein internes Netzwerk oder internes Informationssystem einer Organisation.

Typische Inhalte:

```
interne Webseiten

interne Dokumente
```

```
interne Anwendungen

interne Dateiablagen

interne Kommunikation
```

Zugriff:

```
normalerweise nur für berechtigte interne Benutzer.
```

Merksatz:

```
Intranet = internes Netz oder internes Informationssystem.
```

Aufgabe 4

Was ist ein Extranet?

Antwort anzeigen

Ein Extranet ist ein kontrollierter Zugriff auf interne Dienste für externe Personen oder Organisationen.

Beispiele:

```
Lieferantenportal

Kundenportal

Partnerzugang

externer Dienstleisterzugriff
```

Wichtig:

Zugriff ist begrenzt und kontrolliert.

Merksatz:

Extranet = kontrollierter Zugriff für Externe.

Aufgabe 5

Was ist der Unterschied zwischen Intranet und Extranet?

Antwort anzeigen

Intranet:

internes Netzwerk oder interne Dienste für eigene Organisation

Extranet:

kontrollierter Zugriff für externe Partner,
Kunden
oder Dienstleister

Merksatz:

Intranet intern.
Extranet kontrolliert extern.

Aufgabe 6

Was ist ein Remote-Access-VPN?

Antwort anzeigen

Remote-Access-VPN bedeutet:

Ein einzelner Benutzer oder Client verbindet sich von außen sicher ins Firmennetz.

Typische Nutzung:

Homeoffice

Außendienst

Administratorzugriff

Zugriff auf interne Anwendungen

Merksatz:

Remote-Access-VPN = einzelner Benutzer ins Netz.

Aufgabe 7

Was ist ein Site-to-Site-VPN?

Antwort anzeigen

Site-to-Site-VPN bedeutet:

Zwei Netzwerke oder Standorte werden über einen VPN-Tunnel verbunden.

Beispiele:

Hauptstandort zu Filiale

Rechenzentrum zu Cloud-Netz

Firma zu Partnernetz

Merksatz:

Site-to-Site-VPN = Netz zu Netz.

Aufgabe 8

Ordne zu.

VPN-Art	Bedeutung
Remote-Access-VPN	?
Site-to-Site-VPN	?

Antwort anzeigen

VPN-Art	Bedeutung
Remote-Access-VPN	einzelner Benutzer verbindet sich ins Firmennetz
Site-to-Site-VPN	zwei Standorte oder Netze werden verbunden

Merksatz:

Remote Access = Benutzer.

Site-to-Site = Standort.

Aufgabe 9

Was ist ein VPN-Gateway?

Antwort anzeigen

Ein VPN-Gateway ist die Gegenstelle, an der VPN-Verbindungen aufgebaut werden.

Beispiele:

Firewall

Router

VPN-Server

Cloud-VPN-Gateway

Aufgabe:

VPN-Tunnel terminieren

Benutzer oder Gegenstelle authentifizieren

Verkehr entschlüsseln und weiterleiten

Merksatz:

VPN-Gateway = Eingangspunkt des VPN-Tunnels.

Aufgabe 10

Was bedeutet Tunnel bei VPN?

Antwort anzeigen

Ein Tunnel bedeutet:

Daten werden in eine geschützte Verbindung eingepackt
und über ein anderes Netz transportiert.

Der eigentliche Datenverkehr ist dabei für das unsichere Netz geschützt.

Merksatz:

Tunnel = geschützter Transportweg durch ein anderes Netz.

Aufgabe 11

Welche Schutzziele unterstützt VPN besonders?

Antwort anzeigen

VPN unterstützt besonders:

Vertraulichkeit

Integrität

Authentizität

Begründung:

Daten werden verschlüsselt,
Manipulationen können erkannt werden
und Gegenstellen werden authentifiziert.

Merksatz:

VPN schützt nicht nur den Weg,
sondern auch Identität und Datenintegrität.

Aufgabe 12

Was ist Split-Tunneling?

Antwort anzeigen

Split-Tunneling bedeutet:

Nur bestimmter Verkehr läuft durch den VPN-Tunnel.

Beispiel:

Zugriff auf Firmennetz läuft durch VPN.

normaler Internetverkehr läuft direkt ins Internet.

Vorteil:

```
weniger Last auf VPN-Gateway

oft bessere Internetgeschwindigkeit
```

Risiko:

```
weniger zentrale Kontrolle des gesamten Verkehrs
```

Merksatz:

```
Split-Tunneling = nur ausgewählter Verkehr durch VPN.
```

Aufgabe 13

Was ist Full-Tunneling?

Antwort anzeigen

Full-Tunneling bedeutet:

```
Der gesamte Netzwerkverkehr des Clients läuft durch den VPN-Tunnel.
```

Beispiel:

```
interne Dienste

Internetzugriff

DNS

Webverkehr
```

alles wird über das Firmennetz geleitet.

Vorteil:

zentrale Kontrolle

einheitliche Sicherheitsrichtlinien

Nachteil:

mehr Last auf VPN-Infrastruktur

Merksatz:

Full-Tunneling = gesamter Verkehr durch VPN.

Aufgabe 14

Vergleiche Split-Tunneling und Full-Tunneling.

Merkmal	Split-Tunneling	Full-Tunneling
Verkehr durch VPN	?	?
Last auf VPN	?	?
zentrale Kontrolle	?	?
typisches Risiko	?	?

Antwort anzeigen

Merkmal	Split-Tunneling	Full-Tunneling
Verkehr durch VPN	nur ausgewählter Verkehr	gesamter Verkehr
Last auf VPN	geringer	höher
zentrale Kontrolle	geringer	stärker
typisches Risiko	weniger Kontrolle über Direktverkehr	VPN-Gateway stärker belastet

Merksatz:

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

Aufgabe 15

Was ist IPsec?

Antwort anzeigen

IPsec ist eine Protokollfamilie zur Absicherung von IP-Kommunikation.

Typische Nutzung:

```
Site-to-Site-VPN

Remote-Access-VPN
```

Eigenschaften:

```
Verschlüsselung

Integritätsschutz

Authentifizierung
```

Merksatz:

```
IPsec sichert IP-Verkehr.
```

Aufgabe 16

Was ist IKEv2?

Antwort anzeigen

IKEv2 steht für:

```
Internet Key Exchange Version 2
```

Aufgabe:

```
Aufbau und Aushandlung von IPsec-Verbindungen unterstützen.
```

IKEv2 wird häufig zusammen mit IPsec genutzt.

Merksatz:

```
IKEv2 hilft beim Aufbau von IPsec-VPNs.
```

Aufgabe 17

Was ist OpenVPN?

Antwort anzeigen

OpenVPN ist eine VPN-Lösung, die häufig TLS zur Absicherung verwendet.

Typische Nutzung:

```
Remote-Access-VPN

flexible VPN-Szenarien
```

Eigenschaften:

```
weit verbreitet

zertifikatsbasiert möglich

über TCP oder UDP betreibbar
```

Merksatz:

```
OpenVPN nutzt häufig TLS und ist flexibel einsetzbar.
```

Aufgabe 18

Was ist WireGuard?

Antwort anzeigen

WireGuard ist ein modernes VPN-Protokoll.

Eigenschaften:

```
schlank

vergleichsweise einfach konfigurierbar

nutzt moderne Kryptografie

häufig gute Performance
```

Merksatz:

```
WireGuard ist ein schlankes modernes VPN-Protokoll.
```

Aufgabe 19

Was ist ein TLS-VPN?

Antwort anzeigen

Ein TLS-VPN nutzt TLS zur Absicherung der Verbindung.

Typisch:

Zugriff über VPN-Client

teilweise Zugriff über Browserportal

sichere Verbindung über bekannte Web-Techniken

Merksatz:

TLS-VPN nutzt TLS für geschützte Kommunikation.

Aufgabe 20

Ordne die VPN-Protokolle grob zu.

Begriff	Einordnung
IPsec	?
IKEv2	?
OpenVPN	?
WireGuard	?
TLS-VPN	?

Antwort anzeigen

Begriff	Einordnung
IPsec	Sicherung von IP-Kommunikation
IKEv2	Aushandlung und Aufbau von IPsec
OpenVPN	flexible VPN-Lösung, häufig TLS-basiert
WireGuard	modernes schlankes VPN-Protokoll
TLS-VPN	VPN über TLS-gesicherte Verbindung

Merksatz:

IPsec sichert IP.
IKEv2 handelt IPsec aus.

OpenVPN und TLS-VPN nutzen TLS-Techniken.

WireGuard ist modern und schlank.

Aufgabe 21

Warum braucht ein VPN Authentifizierung?

Antwort anzeigen

VPN muss prüfen, wer oder was sich verbinden darf.

Mögliche Verfahren:

Benutzername und Passwort

MFA

Zertifikate

Schlüssel

Geräteprüfung

Ziel:

nur berechtigte Benutzer oder Standorte dürfen Zugriff erhalten.

Merksatz:

VPN ohne starke Authentifizierung ist ein hohes Risiko.

Aufgabe 22

Warum ist MFA bei VPN sinnvoll?

Antwort anzeigen

MFA schützt, wenn ein Passwort gestohlen wurde.

Ohne MFA reicht ein gestohlenes Passwort eventuell für VPN-Zugriff.

Mit MFA wird zusätzlich ein zweiter Faktor benötigt.

Merksatz:

```
VPN plus MFA schützt besser gegen Passwortmissbrauch.
```

Aufgabe 23

Welche Risiken entstehen bei offenem VPN-Zugang ohne MFA?

Antwort anzeigen

Risiken:

```
Passwortmissbrauch

Brute-Force-Angriffe

Credential Stuffing

unberechtigter Zugriff ins interne Netz

laterale Bewegung nach erfolgreichem Login

Datenabfluss
```

Merksatz:

```
VPN-Zugang ist ein Eingang ins Netz und muss stark geschützt werden.
```

Aufgabe 24

Was ist VPN-Routing?

Antwort anzeigen

VPN-Routing bestimmt, welche Zielnetze über den VPN-Tunnel erreichbar sind.

Beispiele:

```
10.10.0.0/16 über VPN

192.168.50.0/24 über VPN
```

Wichtig:

```
Routen müssen auf Client,
VPN-Gateway
und Gegenseite passen.
```

Merksatz:

```
VPN-Tunnel allein reicht nicht.
Die Routen müssen stimmen.
```

Aufgabe 25

Ein VPN verbindet sich erfolgreich, aber interne Server sind nicht erreichbar.

Welche Ursachen sind wahrscheinlich?

Antwort anzeigen

Mögliche Ursachen:

```
fehlende VPN-Route

falsche Route
```

```
Firewall-Regel blockiert

DNS löst falsch auf

Benutzer hat keine Berechtigung

Zielnetz nicht erlaubt

Rückroute fehlt

IP-Adresskonflikt
```

Merksatz:

```
VPN verbunden heißt nicht automatisch,
dass alle internen Dienste erreichbar sind.
```

Aufgabe 26

Was ist ein IP-Adresskonflikt bei VPN?

Antwort anzeigen

Ein IP-Adresskonflikt entsteht, wenn das lokale Netz des Benutzers denselben IP-Bereich nutzt wie das entfernte Firmennetz.

Beispiel:

```
Heimnetz:
192.168.1.0/24

Firmennetz:
192.168.1.0/24
```

Problem:

```
Der Client kann nicht eindeutig entscheiden,
ob ein Ziel lokal oder über VPN erreichbar ist.
```

Merksatz:

```
Gleiche Netze auf beiden Seiten verursachen VPN-Routingprobleme.
```

Aufgabe 27

Warum ist DNS bei VPN wichtig?

Antwort anzeigen

Interne Dienste werden oft über interne Namen angesprochen.

Beispiele:

```
intranet.firma.local

fileserver.intern

app.firma.de intern
```

VPN muss häufig passende DNS-Server oder DNS-Suffixe bereitstellen.

Merksatz:

```
VPN braucht oft internes DNS.
```

Aufgabe 28

VPN ist verbunden. Zugriff per interner IP funktioniert, aber per Name nicht.

Was ist wahrscheinlich?

Antwort anzeigen

Wahrscheinlich:

```
DNS-Problem im VPN
```

Mögliche Ursachen:

```
falscher DNS-Server

DNS-Server nicht über VPN erreichbar

DNS-Suffix fehlt

Split-DNS falsch

DNS-Cache veraltet
```

Merksatz:

```
VPN-IP ja,
VPN-Name nein:
VPN-DNS prüfen.
```

Aufgabe 29

Was ist Split-DNS bei VPN?

Antwort anzeigen

Split-DNS bedeutet:

```
interne und externe DNS-Auflösung liefern unterschiedliche Antworten.
```

Beispiel:

```
intern über VPN:
app.firma.de zeigt auf private IP
```

```
extern:
app.firma.de zeigt auf öffentliche IP
```

Merksatz:

```
Split-DNS sorgt dafür,
dass interne Namen über VPN passend aufgelöst werden.
```

Aufgabe 30

Warum kann eine Firewall VPN-Verkehr blockieren?

Antwort anzeigen

Firewalls können VPN-Verkehr blockieren, wenn benötigte Protokolle oder Ports nicht erlaubt sind.

Außerdem können Regeln nach erfolgreichem VPN-Aufbau den Zugriff auf interne Ziele blockieren.

Prüfen:

```
VPN-Aufbau erlaubt?

Zielnetz erlaubt?

Benutzergruppe erlaubt?

Port zum Ziel erlaubt?

Richtung korrekt?

Logs prüfen.
```

Merksatz:

VPN braucht Regeln für Tunnelaufbau und Zielzugriff.

Aufgabe 31

Warum ist ein VPN sicherer als eine direkte Portweiterleitung auf RDP?

Antwort anzeigen

Bei direkter Portweiterleitung ist RDP direkt aus dem Internet erreichbar.

Risiken:

Brute Force

Exploits

Credential Stuffing

Bei VPN:

RDP ist nicht direkt öffentlich erreichbar.

Erst nach VPN-Authentifizierung ist Zugriff möglich.

Zusätzlich sinnvoll:

MFA

Firewall-Regeln

Logging

Zugriff nur für Adminnetz oder Benutzergruppen

Merksatz:

VPN schützt Adminzugriffe besser als direkt veröffentlichte Ports.

Aufgabe 32

Ist VPN automatisch sicher?

Antwort anzeigen

Nein.

VPN muss sicher konfiguriert werden.

Wichtige Maßnahmen:

MFA

starke Authentifizierung

aktuelle VPN-Software

sichere Verschlüsselung

Rechtebegrenzung

Logging

Zugriff nach Gruppen

Geräteprüfung

keine unnötigen Zielnetze freigeben

Merksatz:

VPN ist nur so sicher wie seine Konfiguration.

Aufgabe 33

Was ist Least Privilege bei VPN?

Antwort anzeigen

Least Privilege bei VPN bedeutet:

```
Benutzer erhalten nur Zugriff auf die Netze und Dienste,
die sie wirklich benötigen.
```

Beispiele:

```
Dienstleister nur auf einen Server

Mitarbeiter nur auf benötigte Anwendungen

Adminzugriff nur aus Adminrollen
```

Merksatz:

```
VPN-Zugang nicht pauschal ins gesamte Netz erlauben.
```

Aufgabe 34

Was sollte bei VPN protokolliert werden?

Antwort anzeigen

Sinnvolle Logs:

```
erfolgreiche Anmeldungen

fehlgeschlagene Anmeldungen

Benutzername
```

```
Quell-IP

Zeitpunkt

zugewiesene VPN-IP

verwendete Authentifizierung

getrennte Verbindungen

auffällige Loginversuche

Zugriff auf Zielsysteme je nach System
```

Merksatz:

```
VPN-Logs sind wichtig für Sicherheit und Fehlersuche.
```

Aufgabe 35

Was ist ein Site-to-Site-VPN zwischen Firma und Cloud?

Antwort anzeigen

Ein Site-to-Site-VPN zwischen Firma und Cloud verbindet:

```
lokales Firmennetz

mit

Cloud-Netzwerk
```

Beispiel:

```
internes Rechenzentrum
```

zu

Cloud-VPC oder virtuellem Netzwerk

Ziel:

private Kommunikation zwischen Standorten und Cloud-Ressourcen.

Merksatz:

Site-to-Site kann auch On-Premises und Cloud verbinden.

Aufgabe 36

Ein Site-to-Site-VPN ist aufgebaut, aber nur eine Richtung funktioniert.

Welche Ursachen sind möglich?

Antwort anzeigen

Mögliche Ursachen:

Rückroute fehlt

Firewall blockiert Rückverkehr

falsche Phase-2-Netze bei IPsec

NAT-Regel greift falsch

asymmetrisches Routing

Security Group oder Cloud-Firewall blockiert

lokale ACL blockiert

Merksatz:

```
Kommunikation braucht Hinweg und Rückweg.
```

Aufgabe 37

Was ist ein VPN-Client?

Antwort anzeigen

Ein VPN-Client ist die Software oder Funktion auf dem Endgerät, die eine VPN-Verbindung zum VPN-Gateway aufbaut.

Beispiele:

```
Firmenlaptop mit VPN-Software

Smartphone mit VPN-Profil

Betriebssystemeigener VPN-Client
```

Merksatz:

```
VPN-Client baut den Tunnel zum Gateway auf.
```

Aufgabe 38

Welche Antwort ist besser?

Aufgabe:

```
VPN ist verbunden,
aber interne Namen funktionieren nicht.
Was prüfen Sie?
```

Antwort A:

```
Internet ist kaputt.
```

Antwort B:

Da interne IP-Adressen erreichbar sind,
interne Namen aber nicht,
sollte die DNS-Konfiguration des VPN geprüft werden,
insbesondere interner DNS-Server,
DNS-Suffix,
Split-DNS
und Erreichbarkeit des DNS-Servers.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort leitet die Prüfung aus dem Fehlerbild ab
und unterscheidet IP-Erreichbarkeit von Namensauflösung.

Merksatz:

IP ja,
Name nein:
DNS.

Aufgabe 39

Welche Antwort ist besser?

Aufgabe:

Warum sollte ein Dienstleister über VPN nicht automatisch Zugriff auf das gesamte Netz erhalten?

Antwort A:

Weil Dienstleister extern sind.

Antwort B:

> Nach dem Least-Privilege-Prinzip sollte ein Dienstleister nur Zugriff auf die Systeme und Dienste erhalten, die er für seine Aufgabe benötigt.
> Dadurch wird das Risiko bei kompromittierten Zugangsdaten oder Fehlverhalten begrenzt.

Antwort anzeigen

B ist besser.

Begründung:

> Die Antwort nennt das Prinzip
> und erklärt die Sicherheitswirkung.

Merksatz:

> Sicherheitsantwort:
> Risiko,
> Maßnahme,
> Wirkung.

Aufgabe 40

Welche Antwort ist besser?

Aufgabe:

> Warum ist VPN besser als RDP direkt ins Internet weiterzuleiten?

Antwort A:

> VPN klingt sicherer.

Antwort B:

Bei direkter RDP-Portweiterleitung ist der RDP-Dienst öffentlich erreichbar und damit Angriffen ausgesetzt.
Bei VPN muss sich der Benutzer zuerst am VPN authentifizieren.
Erst danach kann der Zugriff auf RDP zusätzlich per Firewall,
MFA
und Berechtigungen eingeschränkt werden.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort nennt das konkrete Risiko
und beschreibt die bessere Schutzwirkung.

Merksatz:

Nicht Adminports veröffentlichen,
sondern sicheren Zugang davor setzen.

Mini-Prüfung: schnelle Zuordnung

Frage	Antwort
Wofür steht VPN?	Virtual Private Network
Was macht ein VPN?	verschlüsselte Verbindung über unsicheres Netz
Was ist Remote-Access-VPN?	Benutzer verbindet sich ins Firmennetz
Was ist Site-to-Site-VPN?	Netz verbindet sich mit Netz
Was ist Intranet?	internes Netz oder interne Dienste
Was ist Extranet?	kontrollierter Zugriff für Externe
Was ist Split-Tunneling?	nur bestimmter Verkehr durch VPN
Was ist Full-Tunneling?	gesamter Verkehr durch VPN
Was ist ein VPN-Gateway?	Gegenstelle des VPN-Tunnels
Warum MFA bei VPN?	Passwort allein reicht nicht
Warum VPN-DNS?	interne Namen auflösen
Was ist IP-Adresskonflikt?	gleiche Netze lokal und remote

Mini-Prüfung: Fehlerbild erkennen

Fehlerbild	Wahrscheinliches Thema
VPN verbindet nicht	Zugangsdaten, MFA, Gateway, Netzwerk, Firewall
VPN verbunden, aber kein internes Ziel erreichbar	Route, Firewall, Berechtigung, Zielnetz
interne IP geht, Name nicht	VPN-DNS
nur ein internes Netz erreichbar	VPN-Routen oder Berechtigungen
Verbindung bricht regelmäßig ab	Timeout, Netzwerk, WLAN, Client, Gateway
Site-to-Site nur in eine Richtung	Rückroute oder Firewall
Heimnetz und Firmennetz gleich	IP-Adresskonflikt
Dienstleister sieht zu viele Systeme	Least Privilege fehlt
RDP direkt offen	Sicherheitsrisiko
VPN-Loginversuche sehr häufig	Brute Force oder Credential Stuffing

IHK-sichere Kurzformulierung

Ein VPN ist ein virtuelles privates Netzwerk, das eine geschützte Verbindung über ein unsicheres Netz wie das Internet herstellt. Remote-Access-VPN verbindet einzelne Benutzer sicher mit einem Firmennetz, während Site-to-Site-VPN zwei Netzwerke oder Standorte verbindet. Intranet bezeichnet interne Dienste einer Organisation, Extranet kontrollierten Zugriff für externe Partner oder Dienstleister. Split-Tunneling leitet nur bestimmten Verkehr durch den VPN-Tunnel, Full-Tunneling den gesamten Verkehr. Für VPN-Sicherheit sind starke Authentifizierung, MFA, aktuelle Software, passende Firewall-Regeln, Logging und Least Privilege wichtig. Eine erfolgreiche VPN-Verbindung bedeutet nicht automatisch, dass Routing, DNS und Zugriffsrechte korrekt funktionieren.

Merksätze

VPN = Virtual Private Network.

VPN verbindet sicher über unsichere Netze.

Remote-Access-VPN = Benutzer ins Netz.

Site-to-Site-VPN = Netz zu Netz.

Intranet = intern.

Extranet = kontrolliert extern.

VPN-Gateway = Gegenstelle des Tunnels.

Tunnel = geschützter Transportweg.

Split-Tunneling = nur ausgewählter Verkehr über VPN.

Full-Tunneling = gesamter Verkehr über VPN.

IPsec sichert IP-Kommunikation.

IKEv2 hilft beim IPsec-Aufbau.

OpenVPN nutzt häufig TLS.

WireGuard ist schlank und modern.

TLS-VPN nutzt TLS.

VPN braucht starke Authentifizierung.

MFA schützt VPN-Zugang.

VPN ist ein Eingang ins Netz.

VPN verbunden heißt nicht:
alle Dienste funktionieren.

VPN braucht passende Routen.

VPN braucht oft internes DNS.

IP ja,
Name nein:
DNS.

Gleiche Netze lokal und remote verursachen Routingprobleme.

Kommunikation braucht Hinweg und Rückweg.

Dienstleisterzugriff nach Least Privilege begrenzen.

VPN-Logs sind wichtig.

RDP nicht direkt ins Internet weiterleiten.

Adminzugriffe besser über VPN,
MFA
und Firewall beschränken.

VPN ist nur so sicher wie seine Konfiguration.