Neue Seite

Merksätze und Prüfungswissen zu VPN, Intranet und Extranet

Diese Seite fasst die wichtigsten Inhalte zu VPN, Intranet, Extranet, VPN-Arten, VPN-Protokollen, Routing, DNS, Firewall-Regeln, Sicherheit und Fehlersuche zusammen.

Dieses Kapitel ist besonders prüfungsrelevant, weil VPN nicht nur Verschlüsselung bedeutet, sondern auch Routing, Berechtigungen, DNS, Firewall, Authentifizierung und Sicherheit betrifft.

Merksatz:

> VPN ist nicht nur ein Tunnel.
> VPN ist ein Zugriffskonzept mit Technik,
> Regeln
> und Sicherheit.

Grundbegriffe

Begriff	Bedeutung
Internet	öffentliches weltweites Netzwerk
Intranet	internes Netzwerk oder internes Portal einer Organisation
Extranet	kontrollierter Zugriff für externe Berechtigte
VPN	geschützter Tunnel über ein fremdes oder unsicheres Netz

Merksatz:

> Internet öffentlich.
> Intranet intern.
> Extranet kontrolliert extern.
> VPN sicherer Tunnel.

Intranet

Ein Intranet ist ein internes Netzwerk oder internes Informationssystem.

Typische Inhalte:

internes Wiki
Mitarbeiterportal
Ticketsystem
Zeiterfassung
Dateiablage
interne Anwendungen
interne APIs
Monitoring
interne Dokumentation

Wichtig:

Ein Intranet ist nicht automatisch öffentlich erreichbar.

Merksatz:

Intranet nutzt oft Webtechnik,
ist aber intern beschränkt.

Extranet

Ein Extranet stellt ausgewählten externen Personen oder Organisationen kontrollierten Zugriff bereit.

Beispiele:

Lieferantenportal
Kundenportal
Partnerportal
Dienstleisterzugang
gemeinsamer Projektraum
Wartungszugang

Wichtig:

Externe bekommen nur Zugriff auf bestimmte Ressourcen,
nicht auf das ganze interne Netz.

Merksatz:

```
Extranet = ausgewählter externer Zugriff.
```

VPN

VPN steht für:

```
Virtual Private Network
```

Ein VPN baut über ein fremdes oder unsicheres Netz einen geschützten Tunnel auf.

Typische Zwecke:

```
Homeoffice
Standortvernetzung
Fernwartung
Zugriff auf interne Dienste
Cloud-Anbindung
Adminzugriff
Extranet-Zugriff
```

Merksatz:

```
VPN verbindet entfernte Benutzer oder Netze sicher mit geschützten Ressourcen.
```

VPN-Tunnel

Ein VPN-Tunnel transportiert Daten geschützt durch ein anderes Netz.

Dabei werden Daten:

```
eingepackt
verschlüsselt
übertragen
am Ziel wieder ausgepackt
```

Das nennt man:

```
Tunneling
```

Merksatz:

```
Tunneling bedeutet:
Daten werden in eine geschützte Verbindung eingepackt.
```

VPN schützt nicht automatisch alles

Ein VPN schützt vor allem den Übertragungsweg.

Es ersetzt nicht:

```
Firewall-Regeln
Benutzerrechte
MFA
Gerätesicherheit
Protokollierung
Segmentierung
Patchmanagement
Anwendungsberechtigungen
```

Merksatz:

```
VPN schützt den Tunnel,
aber nicht automatisch jedes Zielsystem.
```

Remote-Access-VPN

Remote-Access-VPN verbindet einzelne Benutzer mit internen Ressourcen.

Typische Beispiele:

```
Homeoffice-Mitarbeiter
Außendienst
Administrator
mobiler Benutzer
Support
```

```
Dienstleister
```

Merksatz:

```
Remote-Access-VPN = Benutzer verbindet sich aus der Ferne.
```

Client-to-Site-VPN

Client-to-Site-VPN ist praktisch eine andere Bezeichnung für Remote-Access-VPN.

Beispiel:

```
Notebook
→ VPN-Gateway
→ Firmennetz
```

Merksatz:

```
Client-to-Site verbindet einen einzelnen Client mit einem Netz.
```

Site-to-Site-VPN

Site-to-Site-VPN verbindet ganze Netzwerke miteinander.

Beispiele:

```
Hauptstandort ↔ Niederlassung
Firma ↔ Rechenzentrum
Firma ↔ Cloud-Netz
Unternehmen ↔ Partnernetz
```

Merksatz:

```
Site-to-Site-VPN = Netz verbindet sich mit Netz.
```

Remote-Access und Site-to-Site unterscheiden

Merkmal	Remote-Access-VPN	Site-to-Site-VPN
verbindet	einzelner Benutzer	ganze Netze
Endpunkte	Client und Gateway	Gateway und Gateway
typischer Zweck	Homeoffice	Standortvernetzung
Steuerung	Benutzer, Gruppen, Profile	Netze, Routen, Firewall
Fehlerquellen	Client, MFA, DNS, Routen	Phase 1/2, Routing, Netze, Firewall

Merksatz:

```
Remote-Access ist benutzerbezogen.
Site-to-Site ist netzbezogen.
```

Weitere VPN-Arten

VPN-Art	Zweck
Host-to-Host-VPN	zwei einzelne Systeme verbinden
Extranet-VPN	externer Partnerzugriff
Cloud-VPN	lokales Netz mit Cloud-Netz verbinden
Admin-VPN	besonders geschützter Adminzugang
Fernwartungs-VPN	zeitlich begrenzter Supportzugang
Always-On-VPN	automatisch dauerhaft verbunden
On-Demand-VPN	startet bei Bedarf
Per-App-VPN	nur bestimmte Apps nutzen VPN

Merksatz:

```
VPN-Art richtet sich nach Einsatzzweck.
```

VPN-Protokolle

VPN ist ein Oberbegriff.

Technische Umsetzungen können sein:

```
IPsec
IKEv2
```

```
OpenVPN
WireGuard
TLS-VPN
L2TP/IPsec
```

Veraltet:

```
PPTP
```

Merksatz:

```
VPN ist der Zweck.
Protokoll ist die technische Umsetzung.
```

IPsec

IPsec steht für:

```
Internet Protocol Security
```

IPsec schützt IP-Kommunikation.

Typische Einsätze:

```
Site-to-Site-VPN
Cloud-VPN
Standortvernetzung
Remote-Access-VPN
```

IPsec arbeitet nah an Schicht 3, weil IP-Pakete geschützt werden.

Merksatz:

```
IPsec schützt IP-Kommunikation auf Netzwerkebene.
```

IKE und IKEv2

IKE steht für:

Internet Key Exchange

IKE handelt bei IPsec Schlüssel und Sicherheitsparameter aus.

IKEv2 ist die modernere Variante.

Merksatz:

IKE handelt aus,
wie IPsec abgesichert wird.

IPsec Phase 1 und Phase 2

Phase	Bedeutung
Phase 1	sichere Verbindung zwischen VPN-Gegenstellen aufbauen
Phase 2	geschützte Netze oder Datenströme festlegen

Typische Einordnung:

Phase-1-Fehler:
Tunnel kommt oft gar nicht hoch.

Phase-2-Fehler:
Tunnel steht eventuell,
aber Daten fließen nicht richtig.

Merksatz:

Phase 1 verbindet Gateways.
Phase 2 schützt Netze.

ESP und AH

ESP steht für:

Encapsulating Security Payload

ESP kann bieten:

```
Verschlüsselung
Integrität
Authentifizierung
```

AH steht für:

```
Authentication Header
```

AH bietet Integrität und Authentifizierung, aber keine Verschlüsselung des Inhalts.

Merksatz:

```
ESP schützt Daten.
AH verschlüsselt nicht.
```

Wichtige IPsec-Ports und Protokolle

Zweck	Port oder Protokoll
IKE	UDP 500
NAT-Traversal	UDP 4500
ESP	IP-Protokoll 50
AH	IP-Protokoll 51

Wichtig:

```
ESP und AH sind keine TCP- oder UDP-Ports.
```

Merksatz:

```
IPsec ist nicht nur ein einzelner Port.
```

OpenVPN

OpenVPN ist eine flexible TLS-basierte VPN-Lösung.

Eigenschaften:

```
nutzt TLS
kann UDP oder TCP verwenden
kann Zertifikate nutzen
ist flexibel konfigurierbar
wird für Remote-Access und Site-to-Site genutzt
```

Merksatz:

```
OpenVPN ist flexibel und TLS-basiert.
```

WireGuard

WireGuard ist ein modernes, schlankes VPN-Protokoll.

Wichtige Begriffe:

```
Peer
öffentlicher Schlüssel
privater Schlüssel
Allowed IPs
Endpoint
Persistent Keepalive
```

WireGuard nutzt typischerweise UDP.

Merksatz:

```
WireGuard arbeitet mit Peers,
Schlüsseln
und Allowed IPs.
```

Allowed IPs bei WireGuard

Allowed IPs bestimmen bei WireGuard:

```
welche Zielnetze über einen Peer gehen
```

und gleichzeitig:

```
welche Quelladressen von diesem Peer erwartet werden
```

Merksatz:

```
Allowed IPs sind bei WireGuard Routing und Zuordnung zugleich.
```

TLS-VPN

TLS-VPN nutzt TLS als Grundlage.

Es wird oft noch SSL-VPN genannt.

Typische Eigenschaften:

```
häufig TCP 443
oft firewallfreundlich
häufig für Remote-Access
teilweise portalbasiert
teilweise clientbasiert
```

Merksatz:

```
SSL-VPN meint in der Praxis meistens TLS-VPN.
```

PPTP

PPTP steht für:

```
Point-to-Point Tunneling Protocol
```

PPTP ist veraltet und gilt nicht mehr als sicher.

Merksatz:

```
PPTP kennen,
aber nicht mehr einsetzen.
```

Split Tunnel

Split Tunnel bedeutet:

```
Nur bestimmter Verkehr läuft durch das VPN.
```

Beispiel:

```
Firmennetze:
durch VPN

normales Internet:
direkt lokal
```

Vorteile:

```
weniger Last
oft bessere Performance
```

Nachteile:

```
weniger zentrale Kontrolle
höhere Anforderungen an Sicherheitskonzept
```

Merksatz:

```
Split Tunnel leitet nur ausgewählten Verkehr durch VPN.
```

Full Tunnel

Full Tunnel bedeutet:

```
Der gesamte Clientverkehr läuft durch das VPN.
```

Auch Internetverkehr geht dann zuerst durch das Unternehmensnetz.

Vorteile:

zentrale Kontrolle
einheitliche Filterung
zentrale Protokollierung

Nachteile:

mehr Last
höhere Latenz
mehr Bandbreitenbedarf

Merksatz:

Full Tunnel leitet alles durch VPN.

Split Tunnel und Full Tunnel vergleichen

Merkmal	Split Tunnel	Full Tunnel
Firmennetze	über VPN	über VPN
Internetverkehr	lokal direkt	über VPN
VPN-Last	geringer	höher
zentrale Kontrolle	geringer	höher
Performance	oft besser	abhängig von Gateway und Leitung

Merksatz:

Split Tunnel spart Last.
Full Tunnel erhöht zentrale Kontrolle.

VPN-Routing

VPN braucht passende Routen.

Der Client muss wissen:

Welche Netze liegen hinter dem VPN?

Beispiel:

```
Zielnetz:
192.168.10.0/24

Route:
über VPN-Tunnel
```

Fehlt die Route, geht Verkehr eventuell ins lokale Netz oder ins Internet.

Merksatz:

```
Ohne Route kein Weg durch VPN.
```

Rückroute

Nicht nur der Client braucht eine Route zum Ziel.

Das Zielnetz braucht auch einen Weg zurück zum VPN-Client.

Beispiel:

```
VPN-Pool:
10.8.0.0/24

Servernetz:
192.168.10.0/24
```

Das Servernetz muss wissen, wie es zu 10.8.0.0/24 zurückkommt.

Merksatz:

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

VPN-Adresspool

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

Beispiel:

```
10.8.0.0/24
```

Ein Client bekommt zum Beispiel:

```
10.8.0.25
```

Diese Adresse ist wichtig für:

```
Routing
Firewall-Regeln
Logs
Gruppenregeln
Fehlersuche
```

Merksatz:

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

Adresskonflikte

Ein häufiger VPN-Fehler:

```
Firmennetz:
192.168.1.0/24

Heimnetz:
192.168.1.0/24
```

Dann weiß der Client nicht eindeutig, ob eine Adresse lokal oder über VPN erreichbar ist.

Merksatz:

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

VPN-DNS

VPN-Benutzer brauchen oft interne Namensauflösung.

Beispiele:

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

Dafür werden benötigt:

```
interner DNS-Server
DNS-Suffix
Split DNS
Firewall-Regeln für DNS
korrekte DNS-Records
```

Merksatz:

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

Split DNS

Split DNS bedeutet:

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

und:

```
öffentliche Namen werden normal oder extern aufgelöst
```

Beispiel:

```
firma.local
→ interner DNS

öffentliche Webseiten
```

→ normaler DNS

Merksatz:

Split DNS trennt interne und externe Namensauflösung.

DNS-Leak

Ein DNS-Leak bedeutet:

DNS-Anfragen gehen unerwartet außerhalb des VPNs.

Mögliche Folgen:

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

Merksatz:

DNS-Leak = DNS nimmt den falschen Weg.

IPv6-Leak

Ein IPv6-Leak kann entstehen, wenn VPN nur IPv4 tunnelt, aber IPv6 direkt am VPN vorbei ins Internet geht.

Wichtig:

IPv6 bewusst tunneln
oder
IPv6 bewusst filtern und regeln

Merksatz:

IPv6 bei VPN nicht vergessen.

VPN-Firewall-Regeln

Ein VPN-Tunnel darf nicht automatisch Zugriff auf alles geben.

Firewall-Regeln sollten festlegen:

```
Quelle
Ziel
Port
Protokoll
Richtung
Zone
Benutzergruppe
Zweck
Logging
```

Merksatz:

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

VPN-Zonen

VPN-Verkehr sollte in eigene Sicherheitszonen eingeordnet werden.

Beispiele:

```
VPN-Mitarbeiter
VPN-Support
VPN-Admin
VPN-Dienstleister
VPN-Partner
Cloud-VPN
```

Vorteil:

```
Zugriffe können sauber getrennt werden.
```

Merksatz:

VPN-Zonen verhindern pauschale LAN-Freigaben.

Least Privilege beim VPN

Least Privilege bedeutet:

nur die Rechte,
die wirklich nötig sind.

Beim VPN heißt das:

keine pauschale LAN-Freigabe
keine unnötigen Ports
keine unnötigen Zielnetze
keine Dauerzugänge für Externe
keine Sammelkonten

Merksatz:

VPN-Zugriff so eng wie möglich,
so weit wie nötig.

Authentifizierung

Authentifizierung beantwortet:

Wer bist du?

Beim VPN möglich durch:

Benutzername und Passwort
Zertifikat
MFA
Token
Smartcard
Gerätezertifikat

SSO

Merksatz:

Authentifizierung prüft Identität.

Autorisierung

Autorisierung beantwortet:

Was darfst du?

Beispiele:

Darf Benutzer ins VPN?
Darf Benutzer ins Servernetz?
Darf Benutzer RDP nutzen?
Darf Benutzer auf Dateiablage?
Darf Dienstleister Wartungsserver erreichen?

Merksatz:

Autorisierung prüft Berechtigung.

Authentifizierung und Autorisierung unterscheiden

Begriff	Frage	Beispiel
Authentifizierung	Wer bist du?	Login mit Passwort und MFA
Autorisierung	Was darfst du?	Zugriff auf bestimmtes Netz erlaubt

Merksatz:

Anmeldung ist nicht automatisch Berechtigung.

MFA bei VPN

MFA steht für:

```
Multi-Faktor-Authentifizierung
```

Warum wichtig?

```
VPN ist oft aus dem Internet erreichbar.
Passwörter können gestohlen werden.
Phishing ist häufig.
VPN-Zugang führt oft zu internen Ressourcen.
```

Merksatz:

```
VPN-Zugänge sollten mit MFA geschützt werden.
```

Zertifikate bei VPN

VPN kann Zertifikate verwenden für:

```
Serverauthentifizierung
Clientauthentifizierung
Gerätezulassung
stärkere Identitätsprüfung
```

Wichtig:

```
Zertifikate müssen gültig sein,
widerrufen werden können
und zur richtigen CA gehören.
```

Merksatz:

```
Zertifikate erhöhen Sicherheit,
brauchen aber Verwaltung.
```

Gerätesicherheit

Ein VPN-Client bringt ein entferntes Gerät näher an interne Systeme.

Deshalb wichtig:

```
aktuelles Betriebssystem
Updates
Gerätemanagement
Festplattenverschlüsselung
Schutzsoftware
kein kompromittiertes Gerät
sichere Konfiguration
Posture Check
```

Merksatz:

```
Unsicheres Gerät plus VPN ist ein Risiko.
```

BYOD und VPN

BYOD bedeutet:

```
Bring Your Own Device
```

Private Geräte im VPN sind kritisch, wenn sie nicht verwaltet werden.

Risiken:

```
unklarer Patchstand
keine Kontrolle
Malware
Datenabfluss
fehlende Trennung privat/geschäftlich
```

Merksatz:

```
BYOD-VPN braucht klare Regeln und technische Kontrolle.
```

Dienstleisterzugang

Dienstleisterzugänge müssen besonders eng geregelt werden.

Wichtig:

```
eigenes Konto pro Person
keine Sammelkonten
MFA
Zugriff nur auf Zielsystem
zeitliche Begrenzung
Protokollierung
Deaktivierung nach Projektende
```

Merksatz:

```
Externe niemals pauschal ins interne Netz lassen.
```

Admin-VPN

Admin-VPN braucht besonderen Schutz.

Wichtig:

```
separate Admin-Konten
MFA
Zertifikate
verwaltete Geräte
Zugriff nur auf Managementnetze
Bastion Host oder Jump Server
Protokollierung
Alarmierung
```

Merksatz:

```
Admin-VPN ist Hochrisiko-Zugang.
```

Bastion Host und Jump Server

Ein Bastion Host oder Jump Server ist ein besonders geschützter Zwischenserver.

Zweck:

```
Adminzugriffe bündeln
direkte Zugriffe vermeiden
Protokollierung verbessern
Zugriffspfade kontrollieren
```

Merksatz:

```
Jump Server kontrolliert den Weg zu kritischen Systemen.
```

VPN-Logging

VPN-Logs sollten zeigen:

```
Benutzer
Gerät
Quell-IP
Zeitpunkt
VPN-IP
MFA-Ergebnis
Gruppe
Verbindungserfolg
Fehlergrund
Trennungsgrund
Zielzugriffe je nach System
```

Merksatz:

```
VPN-Zugriffe müssen nachvollziehbar sein.
```

VPN-Monitoring

VPN-Infrastruktur sollte überwacht werden.

Wichtige Werte:

```
Tunnelstatus
aktive Benutzer
```

CPU
RAM
Bandbreite
Fehlversuche
Zertifikatsablauf
Latenz
Paketverlust
Gateway-Verfügbarkeit

Merksatz:

VPN ist kritische Infrastruktur.

VPN-Fehlersuche Grundreihenfolge

Sinnvolle Reihenfolge:

1. Fehlerbild aufnehmen.
2. VPN-Art bestimmen.
3. VPN-Protokoll bestimmen.
4. Internetverbindung prüfen.
5. VPN-Gateway prüfen.
6. Authentifizierung und MFA prüfen.
7. Zertifikate prüfen.
8. VPN-IP prüfen.
9. Routen prüfen.
10. DNS prüfen.
11. Firewall prüfen.
12. Zielsystem prüfen.
13. Host-Firewall prüfen.
14. Logs prüfen.
15. MTU und Performance prüfen.

Merksatz:

Erst Tunnel,
dann Route,
dann DNS,

dann Dienst.

Typische VPN-Fehlerbilder

Fehlerbild	wahrscheinliche Richtung
VPN verbindet nicht	Gateway, Port, Login, MFA, Zertifikat
VPN verbunden, IP geht nicht	Route, Firewall, Rückweg, Zielsystem
IP geht, Name nicht	DNS, Split DNS, DNS-Suffix
nur ein Dienst geht nicht	Port, Dienst, Host-Firewall, Rechte
nur manche Benutzer betroffen	Gruppen, Profile, Rollen
nur manche Heimnetze betroffen	Adresskonflikt, NAT, Provider, IPv6
VPN langsam	Latenz, Paketverlust, Bandbreite, MTU
VPN bricht ab	NAT-Timeout, WLAN, Keepalive, Token, Gateway

Merksatz:

Fehlerbild gibt die Richtung der Fehlersuche vor.

VPN und MTU

VPN fügt zusätzliche Header hinzu.

Dadurch kann die nutzbare Paketgröße sinken.

Typische Symptome:

kleine Daten funktionieren
große Downloads brechen ab
Webseiten laden teilweise
VPN wirkt instabil
RDP friert ein
SSH hängt bei viel Ausgabe

Merksatz:

Kleine Daten gehen,
große nicht:

MTU prüfen.

TCP-over-TCP

TCP-over-TCP kann entstehen, wenn ein TCP-basierter VPN-Tunnel TCP-Verkehr transportiert.

Problem:

zwei TCP-Schichten versuchen gleichzeitig,
Paketverlust und Stau zu regeln.

Folge:

schlechtere Performance bei Verlusten oder instabiler Verbindung

Merksatz:

TCP im TCP-Tunnel kann bremsen.

NAT-Traversal

NAT-Traversal hilft VPN-Verbindungen, durch NAT-Geräte zu funktionieren.

Besonders relevant bei:

IPsec
Heimnetzen
Mobilfunk
Hotel-WLAN
Provider-NAT

Merksatz:

NAT-Traversal hilft VPN durch NAT-Umgebungen.

CGNAT

CGNAT steht für:

Carrier Grade NAT

Dabei teilt der Provider öffentliche IPv4-Adressen zwischen vielen Kunden.

Problem:

eingehende Verbindungen zum eigenen VPN-Gateway sind schwierig oder unmöglich.

Remote-Access vom Client nach außen ist oft weniger problematisch, wenn das Gateway öffentlich erreichbar ist.

Merksatz:

CGNAT stört besonders,
wenn das VPN-Gateway von außen erreichbar sein muss.

Intranet, Extranet und VPN unterscheiden

Aussage	richtig?	Erklärung
Intranet ist intern	ja	internes Netz oder internes Portal
Extranet ist öffentlich	nein	nur kontrolliert für Externe
Internet ist öffentlich	ja	grundsätzlich öffentlich erreichbar
VPN ist ein Tunnel	ja	geschützte Verbindung
VPN ist dasselbe wie Extranet	nein	Extranet ist Zugriffskonzept, VPN mögliche Technik
VPN ersetzt Firewall	nein	Firewall-Regeln bleiben nötig
VPN ersetzt Rechte	nein	Anwendung und Benutzerrechte bleiben nötig

Merksatz:

Begriffe sauber trennen.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was ist ein VPN?
- Wofür steht VPN?
- Was ist ein VPN-Tunnel?
- Was ist ein Intranet?
- Was ist ein Extranet?
- Was ist der Unterschied zwischen Intranet, Extranet und Internet?
- Was ist der Unterschied zwischen Remote-Access-VPN und Site-to-Site-VPN?
- Was ist Split Tunneling?
- Was ist Full Tunnel?
- Warum braucht VPN Routing?
- Warum ist DNS bei VPN wichtig?
- Was ist Split DNS?
- Warum sind überlappende Netze problematisch?
- Warum sollte VPN mit MFA geschützt werden?
- Was ist der Unterschied zwischen Authentifizierung und Autorisierung?
- Was ist IPsec?
- Was ist IKE?
- Was bedeuten Phase 1 und Phase 2 bei IPsec?
- Was ist WireGuard?
- Was sind Allowed IPs?
- Warum ist PPTP veraltet?
- Wie geht man bei VPN-Fehlersuche vor?

Typische Prüfungsfallen

VPN heißt Virtual Private Network.

VPN ist nicht automatisch ein vollständiges Sicherheitskonzept.

VPN schützt den Tunnel,
aber nicht automatisch alle Zielsysteme.

VPN ersetzt keine Firewall.

VPN ersetzt keine Berechtigungen.

Remote-Access verbindet Benutzer.

Site-to-Site verbindet Netze.

Client-to-Site ist praktisch Remote-Access.

Intranet ist intern.

Extranet ist kontrolliert extern.

Internet ist öffentlich.

Extranet ist nicht dasselbe wie VPN.

Split Tunnel leitet nur ausgewählten Verkehr.

Full Tunnel leitet alles durch VPN.

VPN braucht Routen.

VPN braucht Rückrouten.

VPN braucht oft internes DNS.

IP geht,
Name nicht:
DNS prüfen.

Überlappende Netze vermeiden.

Heimnetzkonflikte sind häufig.

Authentifizierung ist nicht Autorisierung.

MFA ist bei VPN wichtig.

Dienstleisterzugänge zeitlich begrenzen.

Admin-VPN besonders schützen.

PPTP nicht mehr verwenden.

IPsec Phase 1 und Phase 2 unterscheiden.

ESP ist kein TCP- oder UDP-Port.

WireGuard Allowed IPs genau prüfen.

VPN-Logs und Firewall-Logs gemeinsam auswerten.

VPN verbunden heißt nicht:
alles erreichbar.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Internet	öffentliches weltweites Netzwerk
Intranet	internes Netz oder internes Portal
Extranet	kontrollierter externer Zugriff
VPN	Virtual Private Network
VPN-Tunnel	geschützte logische Verbindung
Tunneling	Daten werden in Tunnelverbindung verpackt
Remote-Access-VPN	Benutzer verbindet sich aus der Ferne
Client-to-Site-VPN	einzelner Client zum Firmennetz
Site-to-Site-VPN	Netz-zu-Netz-Verbindung
VPN-Gateway	Gegenstelle für VPN-Verbindung
VPN-Client	Software oder Gerät des Benutzers
IPsec	Absicherung von IP-Kommunikation
IKE	Schlüsselaushandlung bei IPsec
ESP	IPsec-Bestandteil für Schutz der Daten
AH	IPsec-Bestandteil ohne Inhaltsverschlüsselung
Phase 1	sichere Verbindung zwischen Gateways
Phase 2	Schutz der eigentlichen Netze
OpenVPN	TLS-basierte VPN-Lösung
WireGuard	modernes schlankes VPN-Protokoll
Allowed IPs	Routing- und Peer-Zuordnung bei WireGuard
TLS-VPN	VPN auf TLS-Basis

Begriff	Kurze Erklärung
Split Tunnel	ausgewählter Verkehr durch VPN
Full Tunnel	gesamter Verkehr durch VPN
VPN-Adresspool	IP-Bereich für VPN-Clients
Rückroute	Antwortweg zurück zum VPN-Client
Split DNS	getrennte interne und externe Namensauflösung
DNS-Leak	DNS-Anfragen nehmen falschen Weg
IPv6-Leak	IPv6-Verkehr läuft am VPN vorbei
VPN-Zone	Firewall-Zone für VPN-Verkehr
MFA	Multi-Faktor-Authentifizierung
Least Privilege	minimale notwendige Rechte
Bastion Host	gehärteter Zwischenserver
Jump Server	Sprungserver für Adminzugriffe
MTU	maximale Paketgröße
NAT-Traversal	VPN durch NAT ermöglichen
CGNAT	Provider-NAT für viele Kunden

IHK-sichere Gesamtformulierung

Ein VPN, also Virtual Private Network, stellt über ein unsicheres oder fremdes Netz einen geschützten Tunnel bereit. Es kann einzelne Benutzer per Remote-Access-VPN oder ganze Netzwerke per Site-to-Site-VPN verbinden. Ein Intranet ist ein internes Netzwerk oder internes Portal einer Organisation, während ein Extranet ausgewählten externen Partnern kontrollierten Zugriff auf bestimmte Ressourcen ermöglicht. Für VPN-Zugriffe sind nicht nur Verschlüsselung, sondern auch Authentifizierung, Autorisierung, MFA, Routing, Rückrouten, DNS, Split DNS, Firewall-Regeln, VPN-Zonen, Gerätesicherheit, Logging und Monitoring wichtig. Ein verbundener VPN-Tunnel bedeutet nicht automatisch, dass interne Ressourcen erreichbar oder erlaubt sind. Die Fehlersuche erfolgt systematisch über Gateway-Erreichbarkeit, Anmeldung, Zertifikate, VPN-IP, Routen, DNS, Firewall, Zielsysteme, Host-Firewall, Logs, MTU und Performance.

Wichtigste Merksätze

```
VPN = Virtual Private Network.

VPN baut einen geschützten Tunnel.

VPN ist nicht automatisch vollständige Sicherheit.
```

VPN ersetzt keine Firewall-Regeln.

VPN ersetzt keine Benutzerrechte.

VPN verbunden heißt nicht:
Zugriff erlaubt.

Intranet ist intern.

Extranet ist kontrolliert extern.

Internet ist öffentlich.

Remote-Access verbindet Benutzer.

Site-to-Site verbindet Netze.

Client-to-Site entspricht praktisch Remote-Access.

VPN-Protokoll ist die technische Umsetzung.

IPsec schützt IP-Kommunikation.

IKE handelt Schlüssel aus.

Phase 1 verbindet Gateways.

Phase 2 schützt Netze.

ESP schützt Daten.

AH verschlüsselt nicht.

OpenVPN ist TLS-basiert.

WireGuard nutzt Peers und Allowed IPs.

TLS-VPN wird oft SSL-VPN genannt.

PPTP ist veraltet.

Split Tunnel leitet ausgewählten Verkehr.

Full Tunnel leitet alles.

VPN braucht Route.

VPN braucht Rückroute.

VPN braucht oft internes DNS.

Split DNS trennt Namensauflösung.

Überlappende Netze vermeiden.

Heimnetzkonflikte sind klassisch.

VPN-Zugriff nach Rollen begrenzen.

MFA für VPN nutzen.

Dienstleisterzugänge zeitlich begrenzen.

Admin-VPN besonders schützen.

Unsichere Endgeräte sind Risiko.

VPN-Logs sind wichtig.

Monitoring gehört zu VPN.

MTU bei großen Datenproblemen prüfen.

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