14.3

VPN-Protokolle: IPsec, IKEv2, OpenVPN, WireGuard und TLS-VPN

VPN ist ein Oberbegriff.

Dahinter können unterschiedliche Protokolle und Techniken stehen.

Die wichtigsten VPN-Protokolle und VPN-Techniken sind:

- IPsec
- IKEv2
- OpenVPN
- WireGuard
- TLS-VPN
- L2TP/IPsec
- PPTP als veraltetes Beispiel

Merksatz:

VPN beschreibt den Zweck.
Das VPN-Protokoll beschreibt die technische Umsetzung.

Warum gibt es verschiedene VPN-Protokolle?

Nicht jedes VPN-Protokoll ist für denselben Zweck ideal.

Unterschiede gibt es bei:

- Sicherheit
- Geschwindigkeit
- Einrichtung
- Firewall-Freundlichkeit
- Betriebssystemunterstützung
- Schlüsselaustausch
- Authentifizierung
- Ports und Protokollen
- Wartbarkeit
- Kompatibilität

Merksatz:

```
Das passende VPN-Protokoll hängt vom Einsatzfall ab.
```

Wichtige Auswahlkriterien

Bei der Auswahl eines VPN-Protokolls fragt man:

```
Soll ein Benutzer oder ein Standort verbunden werden?
Welche Betriebssysteme werden genutzt?
Wird NAT verwendet?
Gibt es Firewalls dazwischen?
Ist hohe Geschwindigkeit wichtig?
Wird MFA benötigt?
Werden Zertifikate genutzt?
Muss das VPN besonders einfach wartbar sein?
Gibt es Unternehmensvorgaben?
Gibt es Compliance-Anforderungen?
```

Merksatz:

```
VPN-Auswahl ist immer eine Kombination aus Sicherheit,
Betrieb
und Kompatibilität.
```

IPsec

IPsec steht für:

```
Internet Protocol Security
```

IPsec ist eine Protokollfamilie, die IP-Kommunikation absichern kann.

IPsec wird häufig verwendet für:

```
- Site-to-Site-VPN
- Standortvernetzung
- Cloud-VPN
```

```
- Remote-Access-VPN
- sichere Kommunikation zwischen Netzen
```

Merksatz:

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

IPsec im OSI-Modell

IPsec arbeitet besonders nah an Schicht 3.

Warum?

```
Es schützt IP-Pakete.
```

Dadurch eignet sich IPsec gut, um ganze Netze miteinander zu verbinden.

Beispiel:

```
Standort A 192.168.10.0/24
↔
Standort B 192.168.20.0/24
```

Merksatz:

```
IPsec passt gut zu Netz-zu-Netz-Verbindungen.
```

IPsec-Grundidee

IPsec kann IP-Pakete schützen durch:

```
- Verschlüsselung
- Integritätsschutz
- Authentifizierung
- Schutz vor Manipulation
- Schutz vor Wiederholungsangriffen
```

Dabei werden Sicherheitsparameter zwischen den VPN-Gegenstellen ausgehandelt.

Merksatz:

```
IPsec schützt nicht nur vor Mitlesen,
sondern auch vor Manipulation.
```

IPsec Tunnel Mode

Beim Tunnel Mode wird das ursprüngliche IP-Paket komplett eingepackt.

Dabei entsteht ein neues äußeres IP-Paket.

Typischer Einsatz:

```
Site-to-Site-VPN
```

Beispiel:

```
internes Paket:
192.168.10.50 → 192.168.20.60

äußeres Paket:
öffentliche IP Standort A → öffentliche IP Standort B
```

Merksatz:

```
Tunnel Mode schützt ganze IP-Pakete zwischen VPN-Gateways.
```

IPsec Transport Mode

Beim Transport Mode wird hauptsächlich die Nutzlast des IP-Pakets geschützt.

Die ursprünglichen IP-Adressen bleiben Teil des äußeren Pakets.

Typischer Einsatz:

```
Host-zu-Host-Kommunikation
```

In der Praxis ist für Standort-VPNs meist der Tunnel Mode wichtiger.

Merksatz:

```
Transport Mode schützt eher direkte Host-Kommunikation.
```

ESP

ESP steht für:

```
Encapsulating Security Payload
```

ESP ist ein wichtiger Bestandteil von IPsec.

ESP kann bieten:

```
- Verschlüsselung
- Integritätsschutz
- Authentifizierung
```

ESP ist für viele IPsec-VPNs zentral.

Merksatz:

```
ESP schützt die Daten bei IPsec.
```

AH

AH steht für:

```
Authentication Header
```

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

In vielen modernen IPsec-VPNs wird häufiger ESP verwendet.

Merksatz:

```
AH schützt Integrität,
aber verschlüsselt nicht den Inhalt.
```

IKE

IKE steht für:

```
Internet Key Exchange
```

IKE wird genutzt, um bei IPsec Schlüssel und Sicherheitsparameter auszuhandeln.

IKE regelt unter anderem:

```
- Authentifizierung der Gegenstellen
- Aushandlung von Verschlüsselung
- Aushandlung von Integritätsschutz
- Schlüsselerzeugung
- Lebensdauer von Sicherheitsbeziehungen
```

Merksatz:

```
IKE handelt aus,
wie IPsec gesichert wird.
```

IKEv1 und IKEv2

IKEv1 ist älter.

IKEv2 ist moderner und wird häufig bevorzugt.

IKEv2 bietet Vorteile wie:

```
stabilere Verbindungen
bessere Unterstützung für Mobilität
bessere Wiederverbindung
einfachere Aushandlung
gute Eignung für Remote-Access
```

Merksatz:

```
IKEv2 ist die modernere Variante von IKE.
```

IPsec Phase 1

Bei IPsec wird häufig von Phase 1 gesprochen.

Phase 1 bedeutet vereinfacht:

```
Die VPN-Gegenstellen bauen eine sichere Steuerverbindung auf.
```

Dabei wird geprüft:

```
Wer ist die Gegenstelle?
Welcher Schlüssel oder welches Zertifikat wird genutzt?
Welche Verschlüsselung wird verwendet?
Welche Integritätsprüfung wird verwendet?
Wie lange gilt die Verbindung?
```

Merksatz:

```
Phase 1 sichert die Verbindung zwischen den VPN-Gateways.
```

IPsec Phase 2

Phase 2 bedeutet vereinfacht:

```
Es wird festgelegt,
welche eigentlichen Daten oder Netze geschützt werden.
```

Beispiele:

```
192.168.10.0/24 ↔ 192.168.20.0/24
```

Oder:

```
bestimmter Host ↔ bestimmter Host
```

Dabei werden Sicherheitsparameter für den eigentlichen Datenverkehr ausgehandelt.

Merksatz:

```
Phase 2 schützt die eigentlichen Nutzdaten oder Netze.
```

Phase 1 und Phase 2 vergleichen

Phase	Aufgabe
Phase 1	sichere Verbindung zwischen VPN-Gegenstellen aufbauen
Phase 2	geschützte Netze oder Datenströme festlegen
Phase 1 Fehler	Tunnel kommt oft gar nicht hoch
Phase 2 Fehler	Tunnel steht teilweise, aber Daten fließen nicht korrekt

Merksatz:

```
Phase 1 verbindet Gateways.
Phase 2 schützt Netze.
```

Security Association

Security Association wird abgekürzt:

```
SA
```

Eine SA beschreibt ausgehandelte Sicherheitsparameter.

Dazu gehören zum Beispiel:

```
- Verschlüsselungsverfahren
- Integritätsverfahren
- Schlüssel
- Lebensdauer
- Gegenstellen
- geschützte Netze
- Richtung der Verbindung
```

Merksatz:

```
SA beschreibt,
wie VPN-Verkehr geschützt wird.
```

Pre-Shared Key

Ein Pre-Shared Key wird abgekürzt:

```
PSK
```

Ein PSK ist ein vorher gemeinsam vereinbarter geheimer Schlüssel.

Er wird häufig bei Site-to-Site-VPNs verwendet.

Risiken:

```
PSK ist zu kurz.
PSK wird mehrfach verwendet.
PSK wird unsicher gespeichert.
PSK wird selten gewechselt.
PSK ist zu vielen Personen bekannt.
```

Merksatz:

```
PSK muss stark,
geheim
und kontrolliert verwaltet werden.
```

Zertifikate bei IPsec

Statt PSK können VPNs Zertifikate verwenden.

Vorteile:

```
bessere Skalierbarkeit
bessere Identitätsprüfung
einzelne Zertifikate können widerrufen werden
keine gemeinsamen Geheimnisse für alle Verbindungen
gut für größere Umgebungen
```

Wichtig:

```
Zertifikate brauchen eine saubere PKI und Verwaltung.
```

Merksatz:

```
Zertifikate sind oft besser skalierbar als gemeinsame PSKs.
```

NAT-Traversal bei IPsec

IPsec kann Probleme mit NAT haben.

Grund:

```
NAT verändert IP-Adressen und manchmal Ports.
```

NAT-Traversal hilft, IPsec durch NAT-Geräte zu transportieren.

Typischer Begriff:

```
NAT-T
```

NAT-T kapselt IPsec-Verkehr so, dass er besser durch NAT-Umgebungen kommt.

Merksatz:

```
NAT-Traversal hilft IPsec durch NAT.
```

Typische Ports und Protokolle bei IPsec

Typisch relevant sind:

Zweck	Port / 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,
sondern eigene IP-Protokolle.
```

Merksatz:

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

OpenVPN

OpenVPN ist eine verbreitete VPN-Lösung.

Eigenschaften:

```
- nutzt TLS
- kann mit Zertifikaten arbeiten
- kann UDP oder TCP verwenden
- flexibel konfigurierbar
- geeignet für Remote-Access und Site-to-Site
- benötigt meist Clientsoftware
```

Merksatz:

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

OpenVPN über UDP

OpenVPN wird häufig über UDP betrieben.

Vorteile:

```
gute Performance
weniger TCP-over-TCP-Probleme
geeignet für VPN-Verkehr
oft stabil bei Paketverlust
```

Merksatz:

OpenVPN über UDP ist häufig performanter.

OpenVPN über TCP

OpenVPN kann auch über TCP betrieben werden.

Vorteile:

kann in manchen Netzen leichter durch Firewalls
TCP 443 wirkt ähnlich wie HTTPS-Verkehr
manchmal nützlich in restriktiven Netzwerken

Nachteile:

TCP-over-TCP kann Performanceprobleme verursachen

Merksatz:

OpenVPN über TCP kann firewallfreundlich,
aber langsamer sein.

TCP-over-TCP-Problem

Wenn ein VPN über TCP läuft und darin TCP-Verkehr transportiert wird, entstehen zwei TCP-Steuerungen übereinander.

Beide versuchen:

Paketverlust zu erkennen
erneut zu senden
Stau zu kontrollieren

Das kann bei Paketverlust zu schlechter Leistung führen.

Merksatz:

TCP im TCP-Tunnel kann bremsen.

WireGuard

WireGuard ist ein modernes VPN-Protokoll.

Eigenschaften:

```
- schlank
- schnell
- vergleichsweise einfache Konfiguration
- moderne Kryptografie
- arbeitet typischerweise über UDP
- gut für Remote-Access und Site-to-Site
- Schlüssel stehen im Mittelpunkt
```

Merksatz:

```
WireGuard ist ein schlankes,
modernes VPN-Protokoll über UDP.
```

WireGuard-Grundidee

WireGuard arbeitet mit öffentlichen und privaten Schlüsseln.

Jeder Peer besitzt:

```
privaten Schlüssel
öffentlichen Schlüssel
```

Die Gegenstelle kennt den öffentlichen Schlüssel.

Zusätzlich werden Allowed IPs definiert.

Allowed IPs bestimmen, welche IP-Adressen über den jeweiligen Peer geroutet werden.

Merksatz:

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

WireGuard Peer

Ein Peer ist eine VPN-Gegenstelle.

Beispiele:

```
Notebook eines Benutzers
Server
Firewall
Router
Standort-Gateway
```

Jeder Peer braucht passende Schlüssel und passende Routing-Angaben.

Merksatz:

```
Peer = WireGuard-Gegenstelle.
```

Allowed IPs bei WireGuard

Allowed IPs haben bei WireGuard zwei wichtige Bedeutungen:

```
Welche Zielnetze gehen über diesen Peer?

Welche Quell-IP-Adressen werden von diesem Peer akzeptiert?
```

Beispiel:

```
AllowedIPs = 10.8.0.2/32
```

für einen einzelnen Client.

Oder:

```
AllowedIPs = 192.168.20.0/24
```

für ein Standortnetz.

Merksatz:

Allowed IPs sind bei WireGuard Routing und Zugriffskontrolle zugleich.

TLS-VPN

TLS-VPN nutzt TLS als Grundlage für den sicheren Tunnel.

Es wird oft auch SSL-VPN genannt, obwohl TLS fachlich der modernere Begriff ist.

Einsatz:

Remote-Access
Webportale
Clientbasierter Zugriff
Zugriff über TCP 443
manchmal browserbasierter Zugriff

Merksatz:

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

TLS-VPN und HTTPS

TLS-VPN kann firewallfreundlich sein, weil es häufig über TCP 443 läuft.

Das ist derselbe Port, der auch für HTTPS genutzt wird.

Vorteil:

funktioniert oft in restriktiven Netzen besser

Nachteil:

Port 443 allein sagt nicht,
ob es normaler Webverkehr oder VPN ist.

Merksatz:

TLS-VPN nutzt häufig Mechanismen ähnlich wie HTTPS.

Clientless VPN

Clientless VPN bedeutet:

```
Benutzer greift über Browser auf ein Portal zu,
ohne klassischen vollständigen VPN-Client.
```

Beispiel:

```
Webportal stellt interne Webanwendung bereit.
```

Vorteile:

```
einfacher Zugriff
weniger Clientinstallation
gut für einzelne Webanwendungen
```

Nachteile:

```
nicht für alle Protokolle geeignet
weniger flexibel als vollständiger Tunnel
```

Merksatz:

```
Clientless VPN ist eher Portalzugriff als kompletter Netzwerktunnel.
```

L2TP/IPsec

L2TP steht für:

```
Layer 2 Tunneling Protocol
```

L2TP selbst bietet keine ausreichende Verschlüsselung.

Deshalb wird es häufig mit IPsec kombiniert.

Einsatz:

ältere oder kompatible VPN-Setups
bestimmte Betriebssystem-Clients
Remote-Access

Merksatz:

L2TP braucht IPsec,
wenn es sicher sein soll.

PPTP

PPTP steht für:

Point-to-Point Tunneling Protocol

PPTP ist veraltet und gilt nicht mehr als sicher.

Es sollte in modernen Umgebungen nicht mehr verwendet werden.

Merksatz:

PPTP kennen,
aber nicht mehr einsetzen.

VPN-Protokolle vergleichen

Protokoll	Typischer Einsatz	Kurzbewertung
IPsec / IKEv2	Site-to-Site, Remote-Access	etabliert, stark, komplexer
OpenVPN	Remote-Access, Site-to-Site	flexibel, weit verbreitet
WireGuard	Remote-Access, Site-to-Site	modern, schnell, schlank
TLS-VPN	Remote-Access	oft firewallfreundlich
L2TP/IPsec	ältere Setups	kompatibel, aber weniger modern
PPTP	veraltet	nicht mehr sicher

Merksatz:

Moderne VPNs bevorzugen IPsec/IKEv2,
OpenVPN,
WireGuard
oder TLS-VPN.

VPN und Ports vergleichen

Technik	typische Ports / Protokolle
IPsec IKE	UDP 500
IPsec NAT-T	UDP 4500
IPsec ESP	IP-Protokoll 50
OpenVPN	oft UDP 1194 oder TCP/UDP konfigurierbar
WireGuard	oft UDP 51820
TLS-VPN	häufig TCP 443
L2TP	UDP 1701 plus IPsec
PPTP	TCP 1723 plus GRE

Wichtig:

Ports können je nach Konfiguration abweichen.

Merksatz:

VPN-Fehlersuche braucht Wissen über verwendete Ports und Protokolle.

VPN und Verschlüsselung

VPN-Protokolle nutzen kryptografische Verfahren für:

Vertraulichkeit
Integrität
Authentizität
Schlüsselaustausch

Wichtig:

Nicht nur das VPN-Protokoll zählt,
sondern auch die konkrete Konfiguration.

Beispiele:

alte Algorithmen vermeiden
schwache Schlüssel vermeiden
unsichere Protokolle abschalten
Zertifikate korrekt prüfen
aktuelle Software nutzen

Merksatz:

Sicheres VPN braucht sicheres Protokoll und sichere Konfiguration.

VPN und Perfect Forward Secrecy

Perfect Forward Secrecy wird oft abgekürzt:

PFS

PFS bedeutet vereinfacht:

Selbst wenn ein langfristiger Schlüssel später kompromittiert wird,
sollen alte Sitzungen nicht einfach nachträglich entschlüsselt werden können.

PFS wird durch geeignete Schlüsselaustauschverfahren erreicht.

Merksatz:

PFS schützt alte Sitzungen besser bei späterem Schlüsselverlust.

VPN und Schlüssel-Lebensdauer

Viele VPNs arbeiten mit Schlüssel- oder SA-Lebensdauern.

Nach Ablauf werden Schlüssel neu ausgehandelt.

Zweck:

```
Sicherheitsverbesserung
Begrenzung der Datenmenge pro Schlüssel
regelmäßige Erneuerung der Sicherheitsparameter
```

Typischer Fehler:

```
Gegenstellen haben stark unterschiedliche Lebensdauern
oder inkompatible Einstellungen.
```

Merksatz:

```
VPN-Gegenstellen müssen bei Sicherheitsparametern zusammenpassen.
```

VPN und Kompatibilität

VPN-Probleme entstehen oft, wenn Gegenstellen unterschiedliche Einstellungen erwarten.

Beispiele:

```
Verschlüsselungsalgorithmus passt nicht.
Hashverfahren passt nicht.
DH-Gruppe passt nicht.
PSK stimmt nicht.
Zertifikat wird nicht vertraut.
Phase-2-Netze passen nicht.
Lebensdauer passt nicht.
NAT-T ist unterschiedlich eingestellt.
```

Merksatz:

```
VPN-Gegenstellen müssen dieselbe Sprache sprechen.
```

Typische IPsec-Fehler

Häufige Fehler:

- falscher Pre-Shared Key
- falsche Peer-Adresse
- Phase 1 passt nicht
- Phase 2 passt nicht
- falsche Netze definiert
- Routing fehlt
- Firewall blockiert UDP 500 oder UDP 4500
- ESP wird blockiert
- NAT-T fehlt
- Zertifikat ungültig
- Uhrzeit falsch

Merksatz:

IPsec-Fehler liegen oft an Parametern,
Routing
oder Firewall.

Typische OpenVPN-Fehler

Häufige Fehler:

- falsche Serveradresse
- falscher Port
- UDP blockiert
- Zertifikat ungültig
- Clientprofil falsch
- Benutzer nicht berechtigt
- Route fehlt
- DNS fehlt
- TLS-Handshake schlägt fehl
- MTU-Problem

Merksatz:

OpenVPN-Fehler mit Profil,
Zertifikat,
Port,

Route
und DNS prüfen.

Typische WireGuard-Fehler

Häufige Fehler:

- falscher öffentlicher Schlüssel
- falscher privater Schlüssel
- Allowed IPs falsch
- Endpoint falsch
- UDP-Port blockiert
- Route fehlt
- NAT oder Firewall blockiert
- kein Persistent Keepalive bei NAT-Szenario
- IP-Adresskonflikt
- Gegenstelle antwortet nicht

Merksatz:

WireGuard-Fehler liegen oft an Schlüsseln,
Allowed IPs,
Endpoint
oder Routing.

Persistent Keepalive bei WireGuard

Persistent Keepalive kann helfen, wenn ein WireGuard-Peer hinter NAT sitzt.

Grund:

NAT-Zuordnungen können nach einiger Zeit ablaufen.

Mit Keepalive sendet der Peer regelmäßig kleine Pakete, damit die NAT-Zuordnung bestehen bleibt.

Merksatz:

Persistent Keepalive hilft WireGuard hinter NAT.

Typische TLS-VPN-Fehler

Häufige Fehler:

- Portal nicht erreichbar
- Zertifikat ungültig
- MFA schlägt fehl
- Benutzer nicht berechtigt
- Clientplugin oder Clientsoftware fehlt
- Richtlinie erlaubt Ziel nicht
- DNS über VPN fehlt
- Session läuft ab
- Browser blockiert Inhalt

Merksatz:

TLS-VPN-Fehler betreffen oft Portal,
Zertifikat,
MFA
oder Richtlinie.

VPN-Protokoll und Firewall

Für VPN-Verbindungen müssen Firewalls den passenden Verkehr erlauben.

Zu prüfen:

Welcher Port?
TCP oder UDP?
Eigenes IP-Protokoll?
NAT beteiligt?
Verbindung von innen nach außen oder von außen nach innen?
Rückverkehr erlaubt?
Provider blockiert etwas?

Merksatz:

VPN funktioniert nur,
wenn Firewall und Protokoll zusammenpassen.

VPN-Protokoll und NAT

Manche VPN-Protokolle kommen besser mit NAT zurecht als andere.

Wichtige Punkte:

NAT verändert Adressen.
Manche Protokolle verwenden eigene IP-Protokolle.
UDP-basierte Protokolle brauchen NAT-Zuordnung.
NAT-Traversal kann nötig sein.
CGNAT kann eingehende Verbindungen verhindern.

Merksatz:

NAT ist bei VPN oft ein wichtiger Fehlerfaktor.

VPN-Protokoll und Betriebssysteme

Nicht jedes Betriebssystem unterstützt jedes VPN gleich gut.

Zu prüfen:

nativer Client vorhanden?
Zusatzsoftware nötig?
MDM-Unterstützung?
Zertifikatsverwaltung möglich?
MFA integrierbar?
Always-On möglich?
Per-App-VPN möglich?
Benutzerfreundlichkeit?

Merksatz:

VPN-Protokoll muss auch zu den Endgeräten passen.

VPN-Protokoll und Sicherheitspolitik

Ein Unternehmen sollte festlegen:

```
Welche VPN-Protokolle sind erlaubt?
Welche sind verboten?
Welche Algorithmen sind erlaubt?
Wie werden Schlüssel verwaltet?
Ist MFA Pflicht?
Wie werden Zertifikate erneuert?
Wie werden Logs gespeichert?
Wer darf VPN nutzen?
Welche Zugriffe sind erlaubt?
```

Merksatz:

```
VPN-Sicherheit braucht technische und organisatorische Vorgaben.
```

Veraltete VPN-Verfahren vermeiden

Veraltete oder schwache Verfahren sollten nicht mehr genutzt werden.

Beispiele:

```
PPTP vermeiden
schwache PSKs vermeiden
alte TLS-Versionen vermeiden
unsichere Algorithmen vermeiden
unsichere Hashverfahren vermeiden
gemeinsame Konten vermeiden
fehlende MFA vermeiden
```

Merksatz:

```
Veraltete VPN-Verfahren sind ein Sicherheitsrisiko.
```

VPN-Protokolle in der Fehlersuche

Bei VPN-Problemen zuerst klären:

Welches VPN-Protokoll wird genutzt?

Welcher Port wird genutzt?

TCP oder UDP?

Welche Gegenstellen?

Remote-Access oder Site-to-Site?

PSK oder Zertifikat?

Welche Netze sollen durch den Tunnel?

Welche Logs gibt es?

Merksatz:

Ohne Protokollwissen ist VPN-Fehlersuche ungenau.

Checkliste: VPN-Protokoll prüfen

1. VPN-Art bestimmen.
2. VPN-Protokoll bestimmen.
3. Ports und Protokolle prüfen.
4. Firewall-Freigaben prüfen.
5. NAT oder CGNAT prüfen.
6. Authentifizierung prüfen.
7. Schlüssel oder Zertifikate prüfen.
8. Routen prüfen.
9. DNS prüfen.
10. Logs prüfen.
11. Sicherheitsparameter vergleichen.
12. Gegenstelle prüfen.

Merksatz:

VPN-Protokoll,
Ports,
Schlüssel,
Routen
und Logs gemeinsam prüfen.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was ist IPsec?
- Was ist IKE?
- Wofür wird IKEv2 genutzt?
- Was ist der Unterschied zwischen IPsec Tunnel Mode und Transport Mode?
- Was ist ESP?
- Was ist AH?
- Was bedeutet Phase 1 bei IPsec?
- Was bedeutet Phase 2 bei IPsec?
- Was ist eine Security Association?
- Was ist ein Pre-Shared Key?
- Warum ist NAT-Traversal bei IPsec wichtig?
- Was ist OpenVPN?
- Was ist WireGuard?
- Was bedeutet Allowed IPs bei WireGuard?
- Was ist TLS-VPN?
- Warum ist PPTP veraltet?
- Warum kann TCP-over-TCP problematisch sein?

Typische Prüfungsfallen

VPN ist Oberbegriff,
nicht ein einzelnes Protokoll.

IPsec arbeitet nah an Schicht 3.

IKE handelt Schlüssel aus.

IKEv2 ist moderner als IKEv1.

ESP schützt Daten bei IPsec.

AH verschlüsselt nicht.

Tunnel Mode ist wichtig für Site-to-Site.

Transport Mode eher für Host-to-Host.

Phase 1 verbindet Gateways.

Phase 2 schützt Netze.

SA beschreibt Sicherheitsparameter.

PSK muss stark und geheim sein.

UDP 500 und UDP 4500 bei IPsec kennen.

ESP ist kein TCP- oder UDP-Port.

OpenVPN kann UDP oder TCP nutzen.

OpenVPN über UDP ist oft performanter.

TCP-over-TCP kann bremsen.

WireGuard nutzt Peers und Schlüssel.

Allowed IPs bei WireGuard sind wichtig.

TLS-VPN wird oft SSL-VPN genannt.

L2TP braucht IPsec für Sicherheit.

PPTP ist veraltet und unsicher.

VPN-Sicherheit hängt auch von Konfiguration ab.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
VPN-Protokoll	technische Umsetzung eines VPN
IPsec	Absicherung von IP-Kommunikation
IKE	Schlüsselaushandlung für IPsec
IKEv2	moderne IKE-Version

Begriff	Kurze Erklärung
Tunnel Mode	gesamtes IP-Paket wird geschützt eingepackt
Transport Mode	Nutzlast wird geschützt
ESP	IPsec-Bestandteil für Verschlüsselung und Integrität
AH	IPsec-Bestandteil für Authentizität und Integrität ohne Verschlüsselung
Phase 1	sichere Verbindung zwischen VPN-Gegenstellen
Phase 2	Schutz der eigentlichen Netze oder Datenströme
SA	Security Association
PSK	Pre-Shared Key
NAT-T	NAT-Traversal
OpenVPN	flexible TLS-basierte VPN-Lösung
WireGuard	modernes schlankes VPN-Protokoll
Peer	VPN-Gegenstelle bei WireGuard
Allowed IPs	Routing- und Zuordnungsangabe bei WireGuard
TLS-VPN	VPN auf Basis von TLS
SSL-VPN	ältere Bezeichnung für TLS-VPN
Clientless VPN	browserbasierter Portalzugriff
L2TP/IPsec	L2TP kombiniert mit IPsec
PPTP	veraltetes VPN-Protokoll
TCP-over-TCP	TCP-Verkehr in TCP-Tunnel
Persistent Keepalive	Keepalive für WireGuard hinter NAT

IHK-sichere Kurzformulierung

VPN ist ein Oberbegriff für verschlüsselte Tunnelverbindungen. Technisch können verschiedene Protokolle eingesetzt werden, zum Beispiel IPsec/IKEv2, OpenVPN, WireGuard oder TLS-VPN. IPsec arbeitet nah an der IP-Schicht und wird häufig für Site-to-Site-VPNs genutzt. IKE handelt dabei Schlüssel und Sicherheitsparameter aus. Bei IPsec beschreibt Phase 1 den Aufbau einer sicheren Verbindung zwischen den VPN-Gegenstellen, während Phase 2 die geschützten Netze oder Datenströme festlegt. OpenVPN ist TLS-basiert und kann über UDP oder TCP betrieben werden. WireGuard arbeitet mit Peers, öffentlichen und privaten Schlüsseln sowie Allowed IPs. TLS-VPN nutzt TLS und wird häufig für Remote-Access eingesetzt. Veraltete Verfahren wie PPTP sollten nicht mehr verwendet werden.

Merksätze

VPN ist ein Oberbegriff.

VPN-Protokoll ist die technische Umsetzung.

IPsec schützt IP-Kommunikation.

IPsec arbeitet nah an Schicht 3.

Tunnel Mode schützt ganze IP-Pakete.

Transport Mode schützt eher Host-Kommunikation.

ESP schützt Daten.

AH verschlüsselt nicht.

IKE handelt Schlüssel aus.

IKEv2 ist moderner als IKEv1.

Phase 1 verbindet Gateways.

Phase 2 schützt Netze.

SA beschreibt Sicherheitsparameter.

PSK muss stark und geheim sein.

Zertifikate sind gut für größere Umgebungen.

NAT-T hilft IPsec durch NAT.

UDP 500 gehört zu IKE.

UDP 4500 gehört zu NAT-T.

ESP ist IP-Protokoll 50.

OpenVPN ist TLS-basiert.

OpenVPN über UDP ist oft performanter.

OpenVPN über TCP kann firewallfreundlich sein.

TCP-over-TCP kann bremsen.

WireGuard ist schlank und modern.

WireGuard arbeitet mit Peers.

Allowed IPs sind bei WireGuard sehr wichtig.

Persistent Keepalive hilft hinter NAT.

TLS-VPN nutzt TLS.

SSL-VPN meint meist TLS-VPN.

Clientless VPN ist Portalzugriff.

L2TP braucht IPsec für Sicherheit.

PPTP ist veraltet.

Sicheres VPN braucht sichere Konfiguration.

VPN-Fehler immer mit Protokoll,
Ports,
Schlüsseln,
Routen
und Logs prüfen.