14.2

VPN-Arten und VPN-Einsatzszenarien

VPN ist nicht immer gleich VPN.

Je nach Zweck, Benutzergruppe und Netzwerkaufbau gibt es unterschiedliche VPN-Arten.

Die wichtigsten Einsatzszenarien sind:

- Remote-Access-VPN
- Site-to-Site-VPN
- Client-to-Site-VPN
- Host-to-Host-VPN
- Extranet-VPN
- Cloud-VPN
- Admin-VPN
- Fernwartungs-VPN

Merksatz:

Die VPN-Art richtet sich danach,
wer oder was sicher verbunden werden soll.

Warum unterscheidet man VPN-Arten?

Nicht jede VPN-Verbindung hat denselben Zweck.

Beispiele:

Ein Mitarbeiter im Homeoffice braucht Zugriff auf interne Anwendungen.

Zwei Firmenstandorte sollen dauerhaft verbunden werden.

Ein externer Dienstleister soll nur einen Wartungsserver erreichen.

Ein Unternehmen verbindet sein lokales Netz mit einem Cloud-Netz.

Ein Administrator braucht sicheren Zugriff auf Managementsysteme.

Diese Fälle haben unterschiedliche Anforderungen.

Merksatz:

> Unterschiedliche VPN-Zwecke brauchen unterschiedliche Konzepte.

Remote-Access-VPN

Remote-Access-VPN verbindet einzelne Benutzer mit dem Unternehmensnetz.

Typische Benutzer:

- Homeoffice-Mitarbeiter
- Außendienst
- Administratoren
- mobile Benutzer
- Support-Mitarbeiter
- externe Dienstleister

Der Benutzer startet meist einen VPN-Client auf seinem Endgerät.

Merksatz:

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

Typischer Ablauf bei Remote-Access-VPN

Ein typischer Ablauf:

1. Benutzer startet VPN-Client.
2. VPN-Client verbindet sich mit VPN-Gateway.
3. Benutzer authentifiziert sich.
4. MFA oder Zertifikat wird geprüft.
5. Tunnel wird aufgebaut.
6. Client erhält VPN-IP-Adresse.
7. Routen und DNS-Einstellungen werden gesetzt.
8. Zugriff auf erlaubte Ressourcen ist möglich.

Merksatz:

Remote-Access braucht Authentifizierung,
Tunnel,
IP,
Routen
und DNS.

Remote-Access-VPN: Vorteile

Vorteile:

- sicherer Zugriff aus dem Homeoffice
- Zugriff auf interne Dienste
- zentrale Kontrolle
- verschlüsselte Verbindung
- flexibel für mobile Benutzer
- oft schnell einrichtbar
- gute Integration mit MFA möglich

Merksatz:

Remote-Access-VPN macht mobile Arbeit mit internen Diensten möglich.

Remote-Access-VPN: Risiken

Risiken:

- gestohlene Zugangsdaten
- unsichere private Endgeräte
- Malware auf Client
- zu breite Zugriffsrechte
- fehlende MFA
- unsichere Split-Tunnel-Regeln
- verlorene Geräte
- veraltete VPN-Clients

Merksatz:

```
Remote-Access ist nur sicher,
wenn Endgerät,
Benutzer
und Rechte kontrolliert werden.
```

Client-to-Site-VPN

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

Dabei verbindet sich ein einzelner Client mit einem Standort oder Unternehmensnetz.

Beispiel:

```
Notebook im Homeoffice
→ VPN-Gateway der Firma
→ internes Netz
```

Merksatz:

```
Client-to-Site = einzelner Client zum Firmennetz.
```

Site-to-Site-VPN

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

Beispiele:

```
Hauptstandort ↔ Niederlassung

Firma ↔ Rechenzentrum

Firma ↔ Cloud-Netz

Unternehmen ↔ Partnernetz
```

Hier verbinden meist Router, Firewalls oder VPN-Gateways die Standorte.

Merksatz:

Site-to-Site-VPN verbindet Netze,
nicht einzelne Benutzer.

Typischer Ablauf bei Site-to-Site-VPN

Ein typischer Ablauf:

1. Gateway A baut Tunnel zu Gateway B auf.
2. Beide Gateways authentifizieren sich.
3. Verschlüsselung und Schlüssel werden ausgehandelt.
4. Netzbereiche werden definiert.
5. Routing wird eingerichtet.
6. Firewall-Regeln erlauben gewünschte Verbindungen.
7. Systeme beider Standorte kommunizieren über den Tunnel.

Merksatz:

Site-to-Site braucht Gateways,
Netze,
Routen
und Firewall-Regeln.

Site-to-Site-VPN: Vorteile

Vorteile:

- dauerhafte Standortverbindung
- keine VPN-Clientsoftware auf jedem Endgerät nötig
- zentrale Netz-zu-Netz-Kommunikation
- gut für Niederlassungen
- gut für Cloud-Anbindung
- transparent für Benutzer

Merksatz:

Site-to-Site verbindet Standorte dauerhaft und zentral.

Site-to-Site-VPN: Risiken

Risiken:

- zu große Netzfreigaben
- falsches Routing
- Überschneidung von IP-Netzen
- kompromittierter Standort erreicht andere Netze
- fehlende Segmentierung
- schwache Schlüssel oder PSKs
- fehlendes Monitoring
- unklare Verantwortlichkeiten zwischen Organisationen

Merksatz:

Site-to-Site darf nicht automatisch alle Netze gegenseitig öffnen.

Remote-Access und Site-to-Site im Vergleich

Merkmal	Remote-Access-VPN	Site-to-Site-VPN
verbindet	Benutzergerät mit Netz	Netz mit Netz
typischer Zweck	Homeoffice, mobiler Zugriff	Standortvernetzung
Endpunkt	Client und Gateway	Gateway und Gateway
Benutzeranmeldung	häufig benutzerbezogen	häufig gatewaybezogen
Clientsoftware	meist notwendig	für Endgeräte meist nicht
Zugriffskontrolle	Benutzer und Gruppen	Netze und Firewall-Regeln
Fehlerquellen	Client, DNS, Routen, MFA	Routing, IP-Überschneidung, Tunnel

Merksatz:

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

Host-to-Host-VPN

Host-to-Host-VPN verbindet zwei einzelne Systeme direkt miteinander.

Beispiel:

```
Server A
↔
Server B
```

Einsatz:

```
besonders schützenswerte Verbindung
Kommunikation zwischen zwei Servern
sichere Verbindung über unsicheres Netz
spezielle Administrationsstrecken
```

Merksatz:

```
Host-to-Host-VPN verbindet einzelne Rechner direkt.
```

Extranet-VPN

Ein Extranet-VPN ermöglicht externen Partnern kontrollierten Zugriff.

Beispiele:

```
Lieferant greift auf Bestellportal zu.

Dienstleister greift auf Wartungsserver zu.

Partnerunternehmen greift auf gemeinsame Projektdaten zu.
```

Wichtig:

```
Zugriff stark begrenzen
eigene Benutzerkonten
MFA
Protokollierung
zeitliche Begrenzung
keine pauschale LAN-Freigabe
```

Merksatz:

```
Extranet-VPN ist VPN-Zugriff für externe Berechtigte.
```

Cloud-VPN

Cloud-VPN verbindet ein lokales Netzwerk mit einem Cloud-Netzwerk.

Beispiel:

```
Unternehmensstandort
↔
Cloud-VPC oder Cloud-VNet
```

Typischer Zweck:

```
Zugriff auf Cloud-Server
Hybrid-Cloud
Datenbankverbindungen
private Cloud-Dienste
Migration
Backup
Standort-zu-Cloud-Kommunikation
```

Merksatz:

```
Cloud-VPN verbindet lokale Infrastruktur mit Cloud-Netzen.
```

Admin-VPN

Ein Admin-VPN ist ein besonders geschützter Zugang für Administratoren.

Ziel:

```
Managementsysteme sicher erreichen
```

Beispiele:

Firewall-Verwaltung
Switch-Management
Serveradministration
Hypervisor
Backup-Systeme
Monitoring
Managementnetz

Wichtig:

MFA
separate Admin-Konten
starke Protokollierung
Zugriff nur auf Managementnetze
keine Nutzung für Alltagsarbeit

Merksatz:

Admin-VPN sollte besonders stark abgesichert sein.

Fernwartungs-VPN

Fernwartungs-VPN wird für Support oder Wartung genutzt.

Beispiele:

Hersteller wartet Anlage.
IT-Dienstleister wartet Server.
externer Techniker greift auf Spezialgerät zu.

Wichtig:

zeitlich begrenzen
nur benötigte Ziele erlauben
Zugriff protokollieren
Benutzer eindeutig zuordnen
nach Wartung deaktivieren
keine gemeinsamen Dauerzugänge

Merksatz:

```
Fernwartung braucht zeitlich und technisch begrenzten Zugriff.
```

VPN für mobile Geräte

Mobile Geräte können ebenfalls VPN nutzen.

Beispiele:

```
Smartphone
Tablet
Außendienstgerät
mobiles Kassensystem
MDM-verwaltetes Gerät
```

Wichtig:

```
Geräteverwaltung
Gerätesperre
Verschlüsselung
Zertifikate
MDM-Richtlinien
App-Schutz
Verlustfall beachten
```

Merksatz:

```
Mobile VPN-Zugänge brauchen Gerätekontrolle.
```

Always-On-VPN

Always-On-VPN bedeutet:

```
Das Gerät baut automatisch eine VPN-Verbindung auf,
sobald es Netzwerkzugang hat.
```

Ziel:

Benutzer muss VPN nicht manuell starten.
Unternehmensrichtlinien greifen dauerhaft.
interne Dienste sind automatisch erreichbar.
Datenverkehr kann zentral kontrolliert werden.

Merksatz:

Always-On-VPN verbindet Geräte automatisch mit dem Unternehmensnetz.

On-Demand-VPN

On-Demand-VPN baut sich nur bei Bedarf auf.

Beispiel:

Benutzer ruft interne Domain auf.
Gerät startet VPN automatisch.

Vorteil:

weniger dauerhafte Verbindung
komfortabel für Benutzer
gezielter Tunnelaufbau

Merksatz:

On-Demand-VPN startet,
wenn eine bestimmte Ressource benötigt wird.

Per-App-VPN

Per-App-VPN bedeutet:

Nur bestimmte Anwendungen nutzen den VPN-Tunnel.

Beispiel:

```
Unternehmens-App nutzt VPN.
private Apps nutzen normales Internet.
```

Vorteil:

```
bessere Trennung zwischen privater und geschäftlicher Nutzung
weniger Tunnelverkehr
gezieltere Kontrolle
```

Merksatz:

```
Per-App-VPN leitet nur ausgewählte Apps durch VPN.
```

VPN für BYOD

BYOD steht für:

```
Bring Your Own Device
```

Dabei nutzen Benutzer private Geräte für berufliche Zwecke.

VPN bei BYOD ist besonders kritisch.

Wichtige Fragen:

```
Ist das Gerät sicher?
Ist es verwaltet?
Gibt es MDM?
Sind Firmendaten getrennt?
Gibt es MFA?
Kann Zugriff bei Verlust entfernt werden?
Darf das private Gerät interne Netze erreichen?
```

Merksatz:

```
BYOD plus VPN braucht klare Sicherheitsregeln.
```

VPN für Dienstleister

Dienstleisterzugang sollte besonders eng geregelt werden.

Besser:

```
eigener VPN-Benutzer
keine Sammelkonten
MFA
nur definierte Ziele
zeitliche Freigabe
Protokollierung
Freigabeprozess
regelmäßige Prüfung
Deaktivierung nach Projektende
```

Merksatz:

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

VPN für Standortvernetzung

Bei Standortvernetzung sind wichtige Punkte:

```
eindeutige IP-Netze
stabile Internetanschlüsse
passende Bandbreite
Routing
Firewall-Regeln
Monitoring
Redundanz
Namensauflösung
Zeitsynchronisation
Dokumentation
```

Merksatz:

```
Standort-VPN braucht saubere Netzplanung.
```

VPN für Cloud-Anbindung

Bei Cloud-VPN sind wichtig:

```
Cloud-Netzbereich
lokaler Netzbereich
Routingtabellen
Security Groups
Network Security Groups
Cloud-Firewall
DNS
Bandbreite
Latenz
Hochverfügbarkeit
Kosten
Monitoring
```

Merksatz:

```
Cloud-VPN braucht Routing und Sicherheitsregeln auf beiden Seiten.
```

VPN und IP-Adressplanung

VPN funktioniert nur sauber, wenn Netze eindeutig sind.

Problematisch:

```
Heimnetz 192.168.1.0/24
und Firmennetz 192.168.1.0/24
```

Oder:

```
Standort A 10.0.0.0/24
und Standort B 10.0.0.0/24
```

Folge:

```
Routing wird uneindeutig.
```

Merksatz:

```
Überlappende Netze verursachen VPN-Probleme.
```

VPN und Namensauflösung

VPN-Benutzer brauchen oft interne DNS-Auflösung.

Beispiele:

```
intranet.firma.local
fileserver.intern
dc01.firma.local
app01.servernetz.local
```

Typische Fehler:

```
VPN ist verbunden,
aber Namen funktionieren nicht.
```

Ursache häufig:

```
interner DNS wird nicht verteilt
DNS-Suffix fehlt
Split DNS falsch
Firewall blockiert DNS
```

Merksatz:

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

VPN und Routingtabellen

Der VPN-Client oder das VPN-Gateway braucht passende Routen.

Beispiel:

```
Zielnetz 10.20.0.0/16
soll über VPN erreichbar sein.
```

Dann muss eine Route existieren:

```
10.20.0.0/16 über VPN-Tunnel
```

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

Merksatz:

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

VPN und Firewall-Zonen

VPN-Verbindungen sollten in eigene Firewall-Zonen eingeordnet werden.

Beispiele:

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

Vorteil:

```
Regeln können gezielt nach Rolle oder Zweck erstellt werden.
```

Merksatz:

```
VPN-Zonen helfen,
Zugriff sauber zu begrenzen.
```

VPN und Gruppen

VPN-Zugriff wird häufig über Gruppen gesteuert.

Beispiele:

```
Gruppe Mitarbeiter:
Zugriff auf Intranet

Gruppe Support:
Zugriff auf Helpdesk-Systeme

Gruppe Admin:
Zugriff auf Managementnetz

Gruppe Dienstleister:
Zugriff nur auf Wartungsserver
```

Merksatz:

```
Gruppen helfen,
VPN-Berechtigungen übersichtlich zu steuern.
```

VPN und Rollenmodell

Ein Rollenmodell beschreibt, welche Rolle welche Zugriffe bekommt.

Beispiel:

Rolle	Zugriff
Mitarbeiter	Intranet, Dateiablage
Support	Ticketsystem, bestimmte Clients
Admin	Managementnetz
Dienstleister	definierter Wartungsserver
Partner	Extranet-Portal

Merksatz:

```
Rollenmodell verhindert pauschale VPN-Freigaben.
```

VPN und MFA nach Risiko

MFA sollte besonders bei externem Zugriff eingesetzt werden.

Bei VPN ist MFA wichtig, weil der Zugang aus unsicheren Netzen kommt.

Besonders kritisch:

```
Admin-VPN
Dienstleister-VPN
Extranet-Zugänge
Zugriff auf Servernetze
Zugriff auf Managementsysteme
```

Merksatz:

```
Je kritischer der Zugriff,
desto stärker die Authentifizierung.
```

VPN und Zertifikatsbasierte Authentifizierung

VPN kann neben Benutzerpasswort auch Zertifikate nutzen.

Vorteile:

```
Gerät kann eindeutig identifiziert werden.
Passwort allein reicht nicht.
verlorene Geräte können durch Zertifikatswiderruf gesperrt werden.
Clientzugriff kann stärker kontrolliert werden.
```

Wichtig:

```
Zertifikate müssen erneuert,
geschützt
und bei Verlust widerrufen werden.
```

Merksatz:

```
Zertifikate binden VPN-Zugriff stärker an Geräte oder Identitäten.
```

VPN und Pre-Shared Key

Ein Pre-Shared Key ist ein vorher gemeinsam vereinbarter geheimer Schlüssel.

Abkürzung:

```
PSK
```

PSK wird häufig bei Site-to-Site-VPNs genutzt.

Risiken:

```
schwacher PSK
PSK wird selten gewechselt
PSK ist mehreren Personen bekannt
PSK wird unsicher dokumentiert
```

Merksatz:

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

VPN und Hochverfügbarkeit

VPN kann kritisch für den Betrieb sein.

Deshalb können sinnvoll sein:

```
zwei VPN-Gateways
redundante Internetanschlüsse
automatische Umschaltung
mehrere Standorte
Monitoring
Backup-Konfiguration
dokumentierter Notfallzugang
```

Merksatz:

Kritische VPN-Zugänge brauchen Redundanz.

VPN und Bandbreite

VPN benötigt Bandbreite.

Besonders relevant bei:

Full Tunnel
vielen Homeoffice-Benutzern
Standortkopplung
Dateiübertragung
Backups
Videokonferenzen
Cloud-Zugriff über Zentrale

Merksatz:

VPN-Leistung hängt auch von Bandbreite und Gateway-Kapazität ab.

VPN und Latenz

Latenz ist die Verzögerung.

VPN kann Latenz erhöhen, weil der Verkehr einen längeren Weg nimmt oder verschlüsselt verarbeitet wird.

Besonders betroffen:

Remote Desktop
VoIP
Datenbankanwendungen
Echtzeitanwendungen
interaktive Webanwendungen

Merksatz:

VPN kann Wege verlängern und Latenz erhöhen.

VPN und Protokollwahl

Die Protokollwahl beeinflusst Betrieb und Leistung.

Beispiele:

```
UDP ist oft besser für VPN-Performance.
TCP über TCP kann bei manchen VPNs ungünstig sein.
TCP 443 ist oft firewallfreundlich.
UDP kann in manchen Netzen blockiert sein.
IPsec braucht passende Ports und Protokolle.
```

Merksatz:

```
VPN-Protokoll muss zu Netzwerk,
Sicherheit
und Betrieb passen.
```

TCP-over-TCP-Problem

Wenn ein VPN über TCP läuft und darin wiederum TCP-Verkehr transportiert wird, können Leistungseinbußen entstehen.

Grundidee:

```
Zwei TCP-Schichten versuchen gleichzeitig,
Verluste und Stau zu regeln.
```

Das kann bei Paketverlust zu schlechter Performance führen.

Merksatz:

```
TCP im TCP-Tunnel kann Performanceprobleme verstärken.
```

VPN und NAT-Traversal

VPN-Verbindungen müssen oft durch NAT-Geräte.

NAT-Traversal hilft, VPN-Verkehr durch NAT zu transportieren.

Besonders relevant bei:

```
IPsec hinter Routern
Heimnetzen
Mobilfunk
Hotel-WLAN
Provider-NAT
```

Merksatz:

```
NAT-Traversal hilft VPNs durch NAT-Umgebungen.
```

VPN und CGNAT

CGNAT kann eingehende Verbindungen erschweren.

Für Remote-Access-VPN ist das oft weniger problematisch, wenn der Client nach außen zum VPN-Gateway verbindet.

Für eigenes VPN-Gateway zuhause oder am kleinen Standort kann CGNAT problematisch sein, weil eingehende Verbindungen nicht direkt möglich sind.

Merksatz:

```
CGNAT stört vor allem,
wenn ein VPN-Gateway von außen erreichbar sein muss.
```

VPN und Logs nach Art unterscheiden

Je nach VPN-Art sind andere Logs wichtig.

Remote-Access:

```
Benutzer
Gerät
MFA
VPN-IP
Gruppen
Routen
```

Site-to-Site:

```
Tunnelstatus
Peer-Adresse
Phase 1 / Phase 2
Schlüssel
Routen
Security Associations
```

Extranet:

```
Partner
Zugriffszeiten
Zielsysteme
Rollen
Ablaufdatum
```

Merksatz:

```
VPN-Logs nach VPN-Art auswerten.
```

Typische Fehler bei Remote-Access-VPN

Häufige Fehler:

```
- Benutzer kann sich nicht anmelden
- MFA schlägt fehl
- Zertifikat fehlt
- VPN-Client veraltet
- Client bekommt keine IP
- interne Namen lösen nicht auf
- Route fehlt
- Zugriff wird durch Gruppe nicht erlaubt
- lokales Heimnetz überschneidet sich
- Endgerät unsicher oder nicht compliant
```

Merksatz:

```
Remote-Access-Fehler betreffen oft Benutzer,
Client,
DNS
und Routen.
```

Typische Fehler bei Site-to-Site-VPN

Häufige Fehler:

```
- Tunnel kommt nicht hoch
- PSK stimmt nicht
- Peer-Adresse falsch
- Phase-1-Parameter falsch
- Phase-2-Parameter falsch
- Netze falsch definiert
- Routing fehlt
- Firewall-Regeln fehlen
- IP-Netze überschneiden sich
- einseitige Erreichbarkeit
- NAT-Regeln stören
```

Merksatz:

```
Site-to-Site-Fehler betreffen oft Parameter,
Netze,
Routing
und Firewall.
```

Phase 1 und Phase 2 bei IPsec

Bei IPsec spricht man häufig von Phase 1 und Phase 2.

Vereinfacht:

```
Phase 1:
sichere Verbindung zwischen den VPN-Gateways aufbauen

Phase 2:
```

festlegen,
welche Netze oder Daten über den Tunnel geschützt werden

Typische Fehler:

Parameter stimmen nicht überein.
PSK falsch.
Netze falsch definiert.
Verschlüsselungsalgorithmen passen nicht.

Merksatz:

Phase 1 verbindet Gateways.
Phase 2 schützt die eigentlichen Netze.

Security Association

Security Association wird oft abgekürzt:

SA

Eine SA beschreibt ausgehandelte Sicherheitsparameter einer VPN-Verbindung.

Dazu gehören zum Beispiel:

Verschlüsselung
Integritätsschutz
Schlüssel
Lebensdauer
beteiligte Gegenstellen
geschützte Netze

Merksatz:

SA beschreibt ausgehandelte VPN-Sicherheitsparameter.

VPN-Fehlersuche nach Art

VPN-Art	zuerst prüfen
Remote-Access	Benutzer, MFA, Client, IP, DNS, Route
Site-to-Site	Tunnelstatus, Peer, PSK, Phase 1/2, Routen
Cloud-VPN	Cloud-Routing, Security Groups, lokale Firewall
Extranet-VPN	Partnerkonto, Rollen, Zielsysteme, Ablaufdatum
Admin-VPN	MFA, Adminrolle, Managementnetz, Logs
Fernwartungs-VPN	Zeitfenster, Zielsystem, Protokollierung

Merksatz:

> Die VPN-Art bestimmt die Fehlersuche.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Welche VPN-Arten gibt es?
- Was ist Remote-Access-VPN?
- Was ist Client-to-Site-VPN?
- Was ist Site-to-Site-VPN?
- Wofür nutzt man Extranet-VPN?
- Wofür nutzt man Cloud-VPN?
- Was ist ein Admin-VPN?
- Warum braucht Fernwartungs-VPN besondere Kontrolle?
- Was ist Always-On-VPN?
- Was ist Per-App-VPN?
- Warum sind überlappende IP-Netze bei VPN problematisch?
- Warum sind VPN-Zonen sinnvoll?
- Warum ist ein Rollenmodell für VPN wichtig?
- Was ist ein Pre-Shared Key?
- Was bedeutet Phase 1 und Phase 2 bei IPsec?
- Was ist eine Security Association?

Typische Prüfungsfallen

VPN ist ein Oberbegriff.

Remote-Access-VPN verbindet Benutzer.

Client-to-Site ist praktisch Remote-Access.

Site-to-Site-VPN verbindet Netze.

Extranet-VPN ist für externe Berechtigte.

Cloud-VPN verbindet lokale und Cloud-Netze.

Admin-VPN besonders schützen.

Fernwartungs-VPN zeitlich begrenzen.

Always-On-VPN startet automatisch.

On-Demand-VPN startet bei Bedarf.

Per-App-VPN gilt nur für bestimmte Apps.

BYOD braucht besondere Gerätekontrolle.

VPN-Zugriff nicht pauschal erlauben.

IP-Netze dürfen sich nicht überschneiden.

VPN braucht DNS und Routing.

VPN-Gruppen steuern Zugriff.

PSK muss stark und geheim sein.

Phase 1 und Phase 2 nicht verwechseln.

VPN-Logs je nach VPN-Art auswerten.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Remote-Access-VPN	Benutzer verbindet sich aus der Ferne
Client-to-Site-VPN	einzelner Client verbindet sich mit Firmennetz
Site-to-Site-VPN	zwei Netze werden verbunden
Host-to-Host-VPN	zwei einzelne Systeme werden verbunden
Extranet-VPN	VPN-Zugriff für externe Berechtigte
Cloud-VPN	Verbindung zwischen lokalem Netz und Cloud-Netz
Admin-VPN	besonders geschützter Adminzugang
Fernwartungs-VPN	Wartungszugang für Support oder Hersteller
Always-On-VPN	VPN startet automatisch dauerhaft
On-Demand-VPN	VPN startet nur bei Bedarf
Per-App-VPN	nur bestimmte Apps nutzen VPN
BYOD	private Geräte im beruflichen Einsatz
VPN-Zone	eigene Firewall-Zone für VPN-Verkehr
VPN-Gruppe	Gruppe zur Steuerung von VPN-Rechten
PSK	Pre-Shared Key
NAT-Traversal	VPN durch NAT ermöglichen
Phase 1	IPsec-Aufbau zwischen Gateways
Phase 2	IPsec-Schutz der eigentlichen Netze
Security Association	ausgehandelte Sicherheitsparameter
Peer	VPN-Gegenstelle
Tunnelstatus	Zustand einer VPN-Verbindung

IHK-sichere Kurzformulierung

VPNs können je nach Einsatzzweck unterschiedlich aufgebaut sein. Remote-Access-VPN oder Client-to-Site-VPN verbindet einzelne Benutzer mit internen Ressourcen, während Site-to-Site-VPN ganze Netzwerke oder Standorte miteinander verbindet. Extranet-VPN ermöglicht externen Partnern kontrollierten Zugriff, Cloud-VPN verbindet lokale Netze mit Cloud-Netzen, und Admin- oder Fernwartungs-VPNs dienen besonders geschützten Administrations- oder Wartungszugängen. Für alle VPN-Arten sind eindeutige IP-Netze, passende Routen, DNS, Firewall-Regeln, starke Authentifizierung, Rollenmodelle, Protokollierung und Monitoring wichtig. Bei IPsec sind Phase 1 und Phase 2 zu unterscheiden: Phase 1 baut die sichere Verbindung zwischen Gateways auf, Phase 2 definiert die geschützten Netze oder Datenströme.

Merksätze

VPN ist ein Oberbegriff.

VPN-Art richtet sich nach Einsatzzweck.

Remote-Access verbindet Benutzer.

Client-to-Site verbindet Client mit Netz.

Site-to-Site verbindet Netze.

Host-to-Host verbindet einzelne Systeme.

Extranet-VPN ist für externe Berechtigte.

Cloud-VPN verbindet lokal mit Cloud.

Admin-VPN besonders absichern.

Fernwartungs-VPN zeitlich begrenzen.

Always-On-VPN startet automatisch.

On-Demand-VPN startet bei Bedarf.

Per-App-VPN gilt nur für bestimmte Apps.

BYOD braucht klare Sicherheitsregeln.

Dienstleisterzugriff nie pauschal erlauben.

Standort-VPN braucht Netzplanung.

Cloud-VPN braucht Regeln auf beiden Seiten.

Überlappende Netze vermeiden.

VPN braucht Routen.

VPN braucht oft internes DNS.

VPN-Zonen trennen Zugriffe.

Gruppen steuern Berechtigungen.

Rollenmodell verhindert Pauschalzugriff.

MFA schützt externe Zugänge.

Zertifikate brauchen Verwaltung.

PSK stark und geheim halten.

Kritische VPNs überwachen.

VPN kann Latenz erhöhen.

TCP-over-TCP kann bremsen.

NAT-Traversal hilft durch NAT.

Phase 1 verbindet Gateways.

Phase 2 schützt Netze.

Security Association beschreibt VPN-Sicherheitsparameter.