14.1 VPN, Intranet und Extranet

VPN, Intranet und Extranet beschreiben verschiedene Möglichkeiten, wie Benutzer und Systeme auf interne oder geschützte Ressourcen zugreifen können.

Diese Begriffe hängen eng zusammen, werden aber nicht gleich verwendet.

Grundidee:

```
Intranet:
internes Netzwerk einer Organisation

Extranet:
kontrollierter Zugriff für externe Partner

VPN:
verschlüsselter Tunnel für Zugriff über ein unsicheres Netz
```

Merksatz:

```
Intranet ist intern.
Extranet ist kontrolliert extern erweitert.
VPN ist ein sicherer Tunnel.
```

Warum ist dieses Kapitel wichtig?

In Unternehmen arbeiten Benutzer nicht immer direkt im Firmennetz.

Beispiele:

```
- Homeoffice
- Außendienst
- externe Dienstleister
- Partnerunternehmen
- mehrere Standorte
- Cloud-Dienste
- mobile Geräte
- Fernwartung
- Zugriff auf interne Anwendungen
```

Dafür braucht man sichere Zugriffskonzepte.

Merksatz:

```
Moderne Netzwerke enden nicht mehr nur am Bürogebäude.
```

Intranet

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

Es ist normalerweise nur für berechtigte interne Benutzer erreichbar.

Typische Inhalte:

```
- interne Webseiten
- Dokumentationen
- Mitarbeiterinformationen
- interne Anwendungen
- Ticketsystem
- Zeiterfassung
- Dateifreigaben
- interne Wikis
- interne Portale
```

Merksatz:

```
Intranet = internes Netz oder internes Portal für die Organisation.
```

Intranet ist nicht automatisch das Internet

Das Internet ist öffentlich.

Das Intranet ist intern.

Beispiel:

```
Internet:
öffentlich erreichbare Webseite einer Firma
```

Intranet:
internes Mitarbeiterportal derselben Firma

Ein Intranet kann Webtechnik nutzen, ist aber nicht automatisch öffentlich erreichbar.

Merksatz:

Intranet nutzt oft Internet-Technik,
ist aber intern beschränkt.

Typische Intranet-Dienste

Typische Dienste im Intranet:

Dienst	Beispiel
internes Wiki	Dokumentation
Dateiablage	SMB, SharePoint, Nextcloud
interne Webanwendung	Zeiterfassung
Ticketsystem	Helpdesk
Monitoring	Systemstatus
Telefonbuch	Mitarbeiterdaten
Authentifizierung	AD, LDAP, SSO
interne APIs	Anwendungskommunikation

Merksatz:

Intranet enthält interne Dienste,
die nicht öffentlich sein sollen.

Schutzbedarf im Intranet

Auch interne Dienste brauchen Schutz.

Warum?

Nicht jeder interne Benutzer darf alles sehen.
Ein kompromittierter Client kann Schaden verursachen.

Gastgeräte dürfen nicht auf interne Systeme.
IoT-Geräte sind nicht automatisch vertrauenswürdig.
Malware kann sich intern ausbreiten.

Merksatz:

Intern heißt nicht automatisch sicher.

Extranet

Ein Extranet erweitert das Intranet kontrolliert für externe Parteien.

Externe Parteien können sein:

- Kunden
- Lieferanten
- Partnerunternehmen
- Dienstleister
- externe Techniker
- Projektpartner

Dabei erhalten sie nur Zugriff auf ausgewählte Ressourcen.

Merksatz:

Extranet = kontrollierter Zugriff für externe Berechtigte.

Beispiel für ein Extranet

Ein Unternehmen stellt einem Lieferanten ein Portal bereit.

Der Lieferant darf dort:

Bestellungen einsehen
Liefertermine bestätigen
Dokumente hochladen
Rechnungen abrufen

Der Lieferant darf aber nicht:

interne Personalakten sehen
interne Server verwalten
alle Kundendaten abrufen
auf das gesamte LAN zugreifen

Merksatz:

Extranet gibt gezielten Zugriff,
nicht vollständigen internen Zugriff.

Intranet und Extranet vergleichen

Begriff	Zugriff	Zielgruppe
Intranet	intern	Mitarbeitende und interne Systeme
Extranet	kontrolliert extern	Partner, Kunden, Lieferanten
Internet	öffentlich	grundsätzlich jeder
VPN	Tunnelzugriff	berechtigte entfernte Benutzer oder Standorte

Merksatz:

Intranet intern,
Extranet ausgewählt extern,
Internet öffentlich.

VPN

VPN steht für:

Virtual Private Network

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

Beispiel:

Benutzer im Homeoffice
→ Internet

→ VPN-Tunnel
→ Firmennetz

Der Verkehr wird dabei verschlüsselt übertragen.

Merksatz:

VPN verbindet entfernte Teilnehmer sicher mit einem Netzwerk.

Warum nutzt man VPN?

VPN wird genutzt, wenn sichere Kommunikation über unsichere Netze benötigt wird.

Typische Gründe:

- Homeoffice-Zugriff
- Standortvernetzung
- Fernwartung
- Zugriff auf interne Server
- verschlüsselte Verbindung über Internet
- Schutz in öffentlichen Netzen
- Zugriff auf interne Anwendungen
- sichere Administration

Merksatz:

VPN schützt den Übertragungsweg durch einen verschlüsselten Tunnel.

VPN-Tunnel

Ein VPN-Tunnel ist eine logische verschlüsselte Verbindung.

Die Daten werden eingepackt, verschlüsselt und über ein anderes Netz transportiert.

Man spricht dabei oft von:

Tunneling

Merksatz:

VPN-Tunnel transportiert geschützte Daten durch ein fremdes Netz.

Tunneling einfach erklärt

Beim Tunneling wird ein Paket in ein anderes Paket verpackt.

Vereinfacht:

```
internes Paket
wird verschlüsselt
und in äußeres Transportpaket eingepackt
```

Das äußere Paket wird über das Internet übertragen.

Am Ziel wird es wieder ausgepackt.

Merksatz:

```
Tunneling bedeutet:
ein Paket wird durch ein anderes Netz getragen.
```

Verschlüsselung beim VPN

VPNs nutzen Verschlüsselung, damit Dritte den Inhalt nicht mitlesen können.

Geschützt werden soll:

```
- Dateninhalt
- Zugangsdaten
- interne Kommunikation
- Dateiübertragungen
- Administrationszugriffe
- Anwendungsdaten
```

Wichtig:

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

Merksatz:

```
VPN verschlüsselt den Transportweg,
ersetzt aber keine Zugriffskontrolle.
```

Authentifizierung beim VPN

Vor dem VPN-Zugriff muss geprüft werden, wer sich verbindet.

Mögliche Verfahren:

```
- Benutzername und Passwort
- Zertifikat
- MFA
- Token
- Smartcard
- Geräteprüfung
- SSO
- Gruppenmitgliedschaft
```

Merksatz:

```
VPN braucht starke Authentifizierung.
```

Autorisierung beim VPN

Nach erfolgreicher Anmeldung muss geprüft werden, was der Benutzer darf.

Beispiele:

```
Support darf auf bestimmte Server.
Externe Dienstleister dürfen nur auf Wartungssysteme.
Mitarbeitende dürfen auf interne Anwendungen.
Admins dürfen ins Managementnetz.
```

Merksatz:

VPN verbunden heißt nicht automatisch:
Zugriff auf alles erlaubt.

Remote-Access-VPN

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

Beispiele:

Homeoffice
Außendienst
Notebook unterwegs
Administrator von extern
mobiler Benutzer

Ablauf:

Benutzer startet VPN-Client.
Benutzer authentifiziert sich.
VPN-Tunnel wird aufgebaut.
Benutzer erhält Zugriff auf erlaubte interne Ressourcen.

Merksatz:

Remote-Access-VPN verbindet einzelne Benutzer.

Site-to-Site-VPN

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

Beispiele:

Hauptstandort ↔ Niederlassung
Firma ↔ Rechenzentrum
Firma ↔ Cloud-Netzwerk
zwei Firewalls miteinander

Dabei baut nicht jeder Benutzer einzeln einen VPN-Client auf.

Die Gateways verbinden die Netze.

Merksatz:

```
Site-to-Site-VPN verbindet Netzwerke.
```

Remote-Access und Site-to-Site vergleichen

Merkmal	Remote-Access-VPN	Site-to-Site-VPN
verbindet	einzelner Benutzer	ganze Netze
typischer Einsatz	Homeoffice	Standortvernetzung
Client nötig	meistens ja	auf Endgerät meist nein
Endpunkt	Benutzergerät zu Gateway	Gateway zu Gateway
Zugriff	benutzerbezogen	netzbezogen

Merksatz:

```
Remote-Access = Benutzer.
Site-to-Site = Standort.
```

VPN-Gateway

Ein VPN-Gateway ist der zentrale Gegenpunkt für VPN-Verbindungen.

Es kann sein:

```
- Firewall
- Router
- VPN-Appliance
- Cloud-Gateway
- Server
- Zero-Trust-Gateway
```

Aufgaben:

```
VPN-Verbindungen annehmen
Benutzer prüfen
```

Tunnel aufbauen
Verschlüsselung aushandeln
Routen verteilen
Zugriff kontrollieren

Merksatz:

VPN-Gateway ist der Zugangspunkt zum geschützten Netz.

VPN-Client

Der VPN-Client läuft auf dem Endgerät des Benutzers.

Beispiele:

Notebook
Smartphone
Tablet
Admin-PC

Aufgaben:

Verbindung zum VPN-Gateway aufbauen
Benutzer anmelden
Tunnel erzeugen
Routen setzen
DNS übernehmen
Verkehr durch Tunnel leiten

Merksatz:

VPN-Client baut den Tunnel vom Endgerät aus auf.

VPN-Protokolle

Häufige VPN-Techniken und Protokolle:

```
- IPsec
- IKEv2
- SSL-VPN / TLS-VPN
- OpenVPN
- WireGuard
- L2TP/IPsec
```

Je nach Umgebung unterscheiden sich:

```
Sicherheit
Geschwindigkeit
Einrichtung
Portnutzung
Betriebssystemunterstützung
Firewall-Freundlichkeit
```

Merksatz:

```
VPN ist ein Oberbegriff,
dahinter können verschiedene Protokolle stehen.
```

IPsec

IPsec ist eine Protokollfamilie zur sicheren Kommunikation auf IP-Ebene.

IPsec kann genutzt werden für:

```
- Site-to-Site-VPN
- Remote-Access-VPN
- verschlüsselte Kommunikation zwischen Netzen
```

IPsec arbeitet besonders nah an Schicht 3.

Merksatz:

```
IPsec schützt IP-Kommunikation.
```

IKE

IKE steht für:

```
Internet Key Exchange
```

IKE dient dazu, bei IPsec die Sicherheitsparameter und Schlüssel auszuhandeln.

IKEv2 ist eine moderne Version.

Merksatz:

```
IKE handelt Schlüssel und Sicherheitsparameter für IPsec aus.
```

SSL-VPN / TLS-VPN

SSL-VPN ist ein älterer Begriff.

Fachlich geht es meist um TLS-VPN.

Dabei wird TLS genutzt, ähnlich wie bei HTTPS.

Vorteile:

```
oft firewallfreundlich
häufig über TCP 443 möglich
gut für Remote-Zugriff
teilweise browserbasiert oder clientbasiert
```

Merksatz:

```
SSL-VPN meint meist TLS-basiertes VPN.
```

OpenVPN

OpenVPN ist eine verbreitete VPN-Lösung.

Eigenschaften:

```
nutzt TLS
kann TCP oder UDP verwenden
```

flexibel konfigurierbar
oft für Remote-Access und Site-to-Site nutzbar
benötigt meist Clientsoftware

Merksatz:

OpenVPN ist flexibel und TLS-basiert.

WireGuard

WireGuard ist ein modernes VPN-Protokoll.

Eigenschaften:

schlank
schnell
vergleichsweise einfache Konfiguration
nutzt moderne Kryptografie
arbeitet meist über UDP

Wichtig:

Sicherheit hängt trotzdem von richtiger Schlüsselverwaltung,
Routen
Firewall-Regeln
und Zugriffskonzept ab.

Merksatz:

WireGuard ist modernes,
schlankes VPN über UDP.

L2TP/IPsec

L2TP steht für:

Layer 2 Tunneling Protocol

L2TP selbst verschlüsselt nicht stark genug, deshalb wird es häufig mit IPsec kombiniert.

Merksatz:

```
L2TP wird für Sicherheit typischerweise mit IPsec kombiniert.
```

Split Tunneling

Split Tunneling bedeutet:

```
Nur bestimmter Verkehr geht durch den VPN-Tunnel.
```

Anderer Verkehr, zum Beispiel normales Internet, geht direkt über den lokalen Anschluss.

Beispiel:

```
Zugriff auf Firmennetz:
durch VPN

YouTube oder private Webseiten:
direkt über lokalen Internetanschluss
```

Merksatz:

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

Full Tunnel

Full Tunnel bedeutet:

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

Auch Internetzugriffe gehen zuerst ins Firmennetz und von dort weiter ins Internet.

Vorteile:

```
zentrale Kontrolle
zentrale Filterung
```

einheitliche Sicherheitsrichtlinien

Nachteile:

mehr Last auf VPN und Internetanschluss der Firma
höhere Latenz
mehr Bandbreitenbedarf

Merksatz:

Full Tunnel leitet den gesamten Clientverkehr durch VPN.

Split Tunnel und Full Tunnel vergleichen

Merkmal	Split Tunnel	Full Tunnel
Internetverkehr	direkt lokal	durch Firma
Last auf VPN	geringer	höher
zentrale Kontrolle	geringer	höher
Latenz	oft niedriger	oft höher
Sicherheitspolitik	schwieriger einheitlich	zentraler steuerbar

Merksatz:

Split Tunnel spart Last.
Full Tunnel bietet mehr zentrale Kontrolle.

VPN-Routing

Damit ein VPN funktioniert, müssen passende Routen vorhanden sein.

Der Client muss wissen:

Welche Netze sind über VPN erreichbar?

Beispiele:

```
192.168.10.0/24 über VPN
10.10.0.0/16 über VPN
nur bestimmte Server über VPN
```

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

Merksatz:

```
VPN braucht passende Routen.
```

VPN-DNS

VPN-Benutzer müssen oft interne Namen auflösen können.

Beispiele:

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

Dafür kann der VPN-Client interne DNS-Server bekommen.

Typische Fehler:

```
VPN verbunden,
aber interne Namen lösen nicht auf.
```

Merksatz:

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

Split DNS bei VPN

Split DNS bedeutet:

bestimmte Namen werden über interne DNS-Server aufgelöst,
andere Namen über normale DNS-Server.

Beispiel:

firma.local
→ interner DNS über VPN

öffentliche Webseiten
→ normaler DNS

Merksatz:

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

VPN-Adresspool

Ein VPN-Adresspool ist der IP-Adressbereich, aus dem VPN-Clients eine Adresse bekommen.

Beispiel:

VPN-Clients:
10.8.0.0/24

Wichtig:

Der VPN-Adressbereich darf nicht mit bestehenden Netzen kollidieren.

Problem:

Wenn das Heimnetz des Benutzers denselben Bereich nutzt,
kann Routing fehlschlagen.

Merksatz:

VPN-Adresspool muss eindeutig und konfliktfrei sein.

Adresskonflikt bei VPN

Ein häufiger Fehler:

```
Heimnetz des Benutzers:
192.168.1.0/24

Firmennetz:
192.168.1.0/24
```

Dann weiß der Client nicht eindeutig, ob 192.168.1.50 lokal oder über VPN erreichbar ist.

Folge:

```
interne Server sind nicht erreichbar.
```

Merksatz:

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

Firewall-Regeln für VPN

VPN-Zugriff muss durch Firewall-Regeln gesteuert werden.

Nicht gut:

```
VPN → LAN any erlauben
```

Besser:

```
VPN-Gruppe Support → bestimmte Server TCP 3389
VPN-Gruppe Admin → Managementnetz SSH/RDP
VPN-Gruppe Mitarbeiter → Intranet HTTPS
VPN-Gruppe Dienstleister → nur Wartungssystem
```

Merksatz:

```
VPN-Zugriff nach Rolle und Bedarf begrenzen.
```

VPN und Least Privilege

Auch beim VPN gilt:

```
nur notwendige Rechte erlauben.
```

Ein VPN-Benutzer sollte nicht automatisch Zugriff auf das gesamte interne Netz erhalten.

Warum?

```
kompromittierter VPN-Client
gestohlene Zugangsdaten
Malware auf Heimgerät
externe Dienstleister
zu breite Angriffsfläche
```

Merksatz:

```
VPN ist Zugang,
aber kein Freifahrtschein.
```

VPN und MFA

VPN-Zugänge sollten nach Möglichkeit mit MFA geschützt werden.

Warum?

```
Passwörter können gestohlen werden.
Phishing kann Zugangsdaten abgreifen.
Passwort-Wiederverwendung ist häufig.
VPN-Zugang ist ein direkter Einstieg ins Netz.
```

MFA erhöht die Sicherheit deutlich.

Merksatz:

VPN ohne MFA ist deutlich riskanter.

VPN und Zertifikate

VPNs können Zertifikate nutzen für:

Serverauthentifizierung
Clientauthentifizierung
Gerätezulassung
starke Identitätsprüfung

Vorteil:

nicht nur Passwort,
sondern zusätzlich kryptografischer Nachweis.

Wichtig:

Zertifikate müssen verwaltet,
erneuert
und bei Verlust widerrufen werden.

Merksatz:

Zertifikate erhöhen VPN-Sicherheit,
brauchen aber gutes Management.

VPN und Gerätesicherheit

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

Deshalb ist wichtig:

aktuelles Betriebssystem
aktuelle Schutzsoftware
Festplattenverschlüsselung
Bildschirmsperre

sichere Konfiguration
kein kompromittiertes Gerät
Gerätezertifikat oder Geräteprüfung
Patchstand prüfen

Merksatz:

Unsicheres Endgerät plus VPN ist ein Risiko.

VPN und öffentliche WLANs

VPN kann in öffentlichen WLANs schützen, weil der Verkehr im Tunnel verschlüsselt wird.

Aber:

VPN schützt nicht vor allem.

Weiterhin wichtig:

HTTPS prüfen
Phishing vermeiden
Gerät aktuell halten
keine fremden Zertifikate akzeptieren
keine Warnungen ignorieren

Merksatz:

VPN hilft im öffentlichen WLAN,
ersetzt aber kein sicheres Verhalten.

VPN und Performance

VPN kann die Leistung beeinflussen.

Mögliche Ursachen:

Verschlüsselungsaufwand
längerer Weg

```
zentrale Internetleitung
Full Tunnel
schwacher VPN-Gateway
schlechte Clientverbindung
MTU-Probleme
Paketverlust
hohe Latenz
```

Merksatz:

```
VPN kann sicher sein,
aber Geschwindigkeit und Latenz beeinflussen.
```

VPN und MTU

VPN fügt zusätzliche Header hinzu.

Dadurch kann die effektive Nutzlast kleiner werden.

MTU-Probleme zeigen sich oft so:

```
kleine Pakete funktionieren
große Übertragungen hängen
Webseiten laden teilweise
VPN-Verbindung instabil
RDP oder SSH bricht sporadisch ab
```

Merksatz:

```
Bei VPN-Problemen mit großen Daten an MTU denken.
```

VPN und Logging

VPN-Logs sind wichtig für Sicherheit und Fehlersuche.

Sie zeigen:

wer sich verbunden hat
wann Verbindung aufgebaut wurde
von welcher IP
mit welchem Gerät
ob MFA erfolgreich war
welche VPN-IP vergeben wurde
warum Verbindung getrennt wurde
ob Fehler auftraten

Merksatz:

VPN-Zugriffe müssen nachvollziehbar sein.

VPN und Monitoring

VPN-Infrastruktur sollte überwacht werden.

Wichtige Werte:

Anzahl aktiver Verbindungen
CPU-Auslastung
RAM
Bandbreite
Tunnelstatus
Fehlversuche
Zertifikatsablauf
Latenz
Paketverlust
Authentifizierungsfehler

Merksatz:

VPN ist kritische Infrastruktur und muss überwacht werden.

Typische VPN-Fehler

Häufige Fehler:

- VPN baut nicht auf
- Anmeldung schlägt fehl
- MFA funktioniert nicht
- Zertifikat ungültig
- Client bekommt keine VPN-IP
- Route fehlt
- DNS fehlt
- interne Dienste nicht erreichbar
- nur manche Netze erreichbar
- Adresskonflikt mit Heimnetz
- Firewall blockiert
- Split Tunnel falsch
- Full Tunnel überlastet
- MTU-Problem
- Verbindung bricht ab

Merksatz:

VPN-Fehler können Authentifizierung,
Routing,
DNS,
Firewall
oder MTU betreffen.

Fehlerbild: VPN verbindet nicht

Mögliche Ursachen:

- falscher Servername
- Internetverbindung gestört
- VPN-Gateway nicht erreichbar
- falscher Port blockiert
- Benutzername oder Passwort falsch
- MFA schlägt fehl
- Zertifikat ungültig
- Clientversion inkompatibel
- Konto gesperrt
- Lizenz oder Berechtigung fehlt

Merksatz:

```
Wenn VPN nicht verbindet,
zuerst Erreichbarkeit,
Anmeldung
und Zertifikate prüfen.
```

Fehlerbild: VPN verbunden, aber kein interner Zugriff

Mögliche Ursachen:

```
- Route fehlt
- DNS fehlt
- Firewall-Regel fehlt
- Benutzergruppe nicht berechtigt
- falscher VPN-Adresspool
- Adresskonflikt mit Heimnetz
- Split Tunnel falsch
- Zielsystem-Firewall blockiert
- Rückweg fehlt
```

Merksatz:

```
VPN verbunden heißt nicht automatisch:
interne Ressourcen erreichbar.
```

Fehlerbild: Interne Namen gehen nicht

Mögliche Ursachen:

```
- interner DNS wird nicht verteilt
- Split DNS falsch
- DNS-Suffix fehlt
- DNS-Anfragen gehen lokal statt durch VPN
- interne Zone fehlt
- Firewall blockiert DNS
- falscher DNS-Server antwortet
```

Merksatz:

Bei VPN-Namensproblemen DNS und Split DNS prüfen.

Fehlerbild: Nur manche internen Netze erreichbar

Mögliche Ursachen:

- Route für bestimmtes Netz fehlt
- Firewall-Regel fehlt
- Benutzergruppe darf nur bestimmte Netze
- Rückroute fehlt
- Zielnetz überschneidet sich mit lokalem Netz
- ACL blockiert

Merksatz:

Teilweise Erreichbarkeit deutet oft auf Routing oder Berechtigung hin.

Fehlerbild: VPN langsam

Mögliche Ursachen:

- Full Tunnel überlastet
- hohe Latenz
- schwache Internetleitung
- VPN-Gateway ausgelastet
- Paketverlust
- MTU-Problem
- WLAN instabil
- Verschlüsselungsleistung begrenzt
- zentraler Proxy langsam

Merksatz:

VPN-Langsamkeit mit Latenz,
Paketverlust,

MTU
und Auslastung prüfen.

Fehlerbild: VPN bricht ab

Mögliche Ursachen:

- instabile Internetverbindung
- WLAN-Roaming
- NAT-Timeout
- Firewall-Timeout
- Mobilfunkwechsel
- Energiesparmodus
- Clientproblem
- Zertifikat oder Token läuft ab
- Gateway überlastet
- MTU-Problem

Merksatz:

VPN-Abbrüche brauchen Zeitbezug,
Logs
und Verbindungsmessung.

VPN und Extranet unterscheiden

Ein Extranet kann über VPN bereitgestellt werden, muss aber nicht.

Beispiele:

Extranet über Webportal:
Partner meldet sich im Browser an.

Extranet über VPN:
Partner bekommt VPN-Zugang zu bestimmten Systemen.

Wichtig:

```
Extranet ist das Zugriffskonzept.
VPN ist eine mögliche technische Umsetzung.
```

Merksatz:

```
Extranet beschreibt Zielgruppe und Zugriff.
VPN beschreibt den Tunnel.
```

Extranet-Sicherheit

Extranet-Zugänge brauchen klare Begrenzung.

Wichtig:

```
- eigene Benutzerkonten
- MFA
- Rollen und Rechte
- Protokollierung
- Vertrags- und Zweckbindung
- zeitliche Begrenzung
- Zugriff nur auf benötigte Daten
- keine gemeinsamen Konten
- regelmäßige Prüfung
- Sperrung nach Projektende
```

Merksatz:

```
Externe Zugänge müssen besonders sauber kontrolliert werden.
```

Partnerzugriff

Partnerzugriff sollte nicht ungefiltert ins interne Netz führen.

Besser:

```
Partnerportal
API-Gateway
Reverse Proxy
```

dedizierte Extranet-Zone
VPN mit begrenzten Regeln
Bastion Host
getrennte Benutzerrollen

Merksatz:

Partner nur auf das zugreifen lassen,
was sie wirklich benötigen.

Intranet über VPN

Im Homeoffice greifen Benutzer oft per VPN auf das Intranet zu.

Beispiel:

Benutzer verbindet VPN.
Danach öffnet er internes Wiki.
DNS löst internen Namen auf.
Firewall erlaubt VPN → Intranet HTTPS.
Webserver prüft Anmeldung.

Merksatz:

Intranet-Zugriff über VPN braucht Tunnel,
DNS,
Firewall
und Berechtigung.

Intranet über Zero Trust

Moderne Umgebungen nutzen teilweise Zero-Trust-Zugriffe statt klassischem Voll-VPN.

Grundidee:

Benutzer bekommt nicht Zugriff auf das ganze Netz,
sondern nur auf einzelne Anwendungen.

Prüfung:

```
Identität
Gerät
Standort
Risiko
MFA
Anwendung
Richtlinie
```

Merksatz:

```
Zero Trust ersetzt oft breiten Netzwerkzugriff durch gezielten Anwendungszugriff.
```

VPN und Zero Trust vergleichen

Merkmal	klassisches VPN	Zero-Trust-Zugriff
Zugriffsebene	oft Netzwerkzugriff	meist Anwendungszugriff
Risiko	breiter Zugriff möglich	stärker begrenzter Zugriff
Prüfung	häufig beim Verbindungsaufbau	kontinuierlicher und kontextbezogener
Nutzung	interne Netze	einzelne Anwendungen
Vorteil	bewährt und flexibel	feiner steuerbar

Merksatz:

```
VPN verbindet oft Netze.
Zero Trust gibt gezielt Anwendungen frei.
```

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 der Unterschied zwischen Remote-Access-VPN und Site-to-Site-VPN?
```

- Was ist ein VPN-Gateway?
- Was ist Split Tunneling?
- Was ist Full Tunnel?
- Warum braucht VPN Routing?
- Warum ist DNS bei VPN wichtig?
- Warum können gleiche IP-Netze bei VPN Probleme verursachen?
- Warum sollte VPN-Zugriff nicht automatisch das ganze LAN erlauben?
- Warum ist MFA bei VPN sinnvoll?
- Was ist ein Intranet?
- Was ist ein Extranet?
- Was ist der Unterschied zwischen Intranet, Extranet und Internet?
- Warum ist ein Extranet besonders zu schützen?

Typische Prüfungsfallen

VPN bedeutet Virtual Private Network.

VPN ist ein Tunnel,
nicht automatisch ein komplettes Sicherheitskonzept.

VPN schützt den Transportweg.

VPN ersetzt keine Firewall-Regeln.

VPN ersetzt keine Berechtigungen.

Remote-Access-VPN verbindet einzelne Benutzer.

Site-to-Site-VPN verbindet Standorte oder Netze.

Split Tunnel leitet nur ausgewählten Verkehr durch VPN.

Full Tunnel leitet gesamten Verkehr durch VPN.

VPN braucht passende Routen.

VPN braucht oft interne DNS-Einstellungen.

VPN verbunden heißt nicht:

Zugriff auf alles erlaubt.

Gleiche IP-Netze auf beiden Seiten erzeugen Routingprobleme.

MFA erhöht VPN-Sicherheit.

Externe Dienstleister nur begrenzt berechtigen.

Intranet ist intern.

Extranet ist kontrolliert für externe Berechtigte.

Internet ist öffentlich.

Extranet ist nicht automatisch VPN.

VPN kann durch MTU-Probleme langsam oder instabil wirken.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
VPN	Virtual Private Network
VPN-Tunnel	geschützte logische Verbindung
Tunneling	Einpacken von Daten in eine Tunnelverbindung
Remote-Access-VPN	VPN für einzelne Benutzer
Site-to-Site-VPN	VPN zwischen Netzwerken
VPN-Gateway	Gegenstelle für VPN-Verbindungen
VPN-Client	Software oder Gerät des Benutzers
IPsec	VPN-Technik auf IP-Ebene
IKE	Schlüsselaushandlung bei IPsec
TLS-VPN	VPN auf Basis von TLS
OpenVPN	verbreitete TLS-basierte VPN-Lösung
WireGuard	modernes schlankes VPN-Protokoll
Split Tunnel	nur ausgewählter Verkehr durch VPN
Full Tunnel	gesamter Verkehr durch VPN
VPN-Adresspool	IP-Bereich für VPN-Clients

Begriff	Kurze Erklärung
Split DNS	getrennte DNS-Auflösung je nach Ziel
Intranet	internes Netzwerk oder internes Portal
Extranet	kontrollierter Zugriff für externe Berechtigte
MFA	Multi-Faktor-Authentifizierung
Least Privilege	nur notwendige Rechte
Zero Trust	kein automatisches Vertrauen

IHK-sichere Kurzformulierung

Ein VPN, also Virtual Private Network, stellt über ein unsicheres oder fremdes Netz einen geschützten Tunnel bereit. Es wird genutzt, um einzelne Benutzer per Remote-Access-VPN oder ganze Standorte per Site-to-Site-VPN sicher mit internen Ressourcen zu verbinden. Für den VPN-Betrieb sind Authentifizierung, Verschlüsselung, Routing, DNS, Firewall-Regeln und Berechtigungen wichtig. Split Tunneling leitet nur ausgewählten Verkehr durch das VPN, während Full Tunnel den gesamten Clientverkehr durch den Tunnel führt. Ein Intranet ist ein internes Netzwerk oder internes Portal einer Organisation. Ein Extranet stellt ausgewählten externen Partnern kontrollierten Zugriff auf bestimmte Ressourcen bereit. VPN-Zugriff sollte durch MFA, Rollen, Firewall-Regeln und Least Privilege abgesichert werden.

Merksätze

```
Intranet = intern.

Extranet = kontrolliert extern erweitert.

Internet = öffentlich.

VPN = Virtual Private Network.

VPN baut einen verschlüsselten Tunnel.

VPN schützt den Transportweg.

VPN ersetzt keine Rechteprüfung.

VPN ersetzt keine Firewall-Regeln.

Remote-Access-VPN verbindet Benutzer.
```

Site-to-Site-VPN verbindet Netze.

VPN-Gateway ist der Zugangspunkt.

VPN-Client baut den Tunnel auf.

IPsec schützt IP-Kommunikation.

IKE handelt Schlüssel aus.

TLS-VPN nutzt TLS.

OpenVPN ist flexibel.

WireGuard ist schlank und modern.

Split Tunnel leitet nur ausgewählten Verkehr.

Full Tunnel leitet alles durch VPN.

VPN braucht passende Routen.

VPN braucht oft internes DNS.

Split DNS hilft bei internen Namen.

VPN-Adresspool darf sich nicht überschneiden.

Gleiche Netze verursachen Routingprobleme.

VPN-Zugriff nach Rolle begrenzen.

MFA für VPN ist wichtig.

Unsichere Endgeräte sind trotz VPN riskant.

VPN kann durch MTU-Probleme instabil werden.

VPN verbunden heißt nicht:

alles erreichbar.

Extranet ist Zugriffskonzept,

VPN ist Tunneltechnik.

Zero Trust gibt gezielter Zugriff auf Anwendungen.