Name: _____ Datum: _____ Punkte: _____

Unternehmens-VPN

Umsetzung von Zero-Trust-Netzwerkzugriff, dedizierten Gateway-Knoten und zentralen Administrationskontrollen für Unternehmen.

LERNÜBERSICHT ZU VPN-NETZWERKEN IM UNTERNEHMEN

LERNENDE
STUDIERENDENSTATUS
Lernpfad Netzwerkverteidigung

SICHER
VERBINDUNGSSTATUS
Abschirmung von Datenpaketen

AKTIV
SCHUTZ VOR LECKS
Schutz vor DNS- und IPv6-Leaks

Willkommen! Dieses Aktivitätspaket führt Sie durch VPN-Netzwerke für Unternehmen. Sie lernen Zero-Trust-Architekturen, dedizierte Gateways mit statischer IP, Administratorkonsolen, Bereitstellung und Site-to-Site-IPsec-Tunnel kennen.

KONTROLLPUNKTE DES ARBEITSBLATTS

- [ ] **Teil 1-4: VPN- und Netzwerksicherheitskonfigurationen beherrschen.**
- [ ] **Teil 5-7: Kreuzworträtsel und Suchsel lösen.**
- [ ] **Teil 8-9: Fallstudien und Chiffre-Aufgabe lösen.**
- [ ] **Teil 10: Seiten mit grundlegenden und fortgeschrittenen häufigen Fragen durchgehen.**
- [ ] **Teil 11: 10 interessante Fakten aus der Praxis entdecken.**
- [ ] **Bonus: Herausforderung Schnell denken.**

Leitfaden „Beste VPNs“ von VPN.com öffnen

URL: https://www.vpn.com/de/vpn/bestes-vpn-unternehmen/enterprise/

Ihr Lernfahrplan: VPN-Netzwerke für Unternehmen

- Rahmenwerke für Zero Trust Network Access (ZTNA) umsetzen.
- Konfigurieren Sie dedizierte Gateway-IP-Adressen der Server für Whitelist-Filter.
- Zentrale Unternehmens-Verwaltungsoberflächen und Listen der Nutzerlizenzen verwalten.
- Prüfen Sie Netzwerkzugriffsprotokolle und Verbindungsverläufe der Nutzer.
- Konfigurieren Sie Regeln für Single Sign-On (SSO) und Multi-Faktor-Authentifizierung.
- Site-to-Site-IPsec-Tunnel zwischen Zweigstellen einrichten.

ANLEITUNG ZU VPN-NETZWERKEN IM UNTERNEHMEN

Beantworten Sie die Auswahlaufgaben und Richtig/Falsch-Fragen, vervollständigen Sie die Lückensätze mithilfe der Wortliste, ordnen Sie die Definitionen zu und lösen Sie das Kreuzworträtsel und das Suchsel. Wenden Sie Ihr Wissen in folgenden Bereichen an: Zero Trust und Site-to-Site-IPsec. Zum Schluss folgt die Bonusaufgabe Schnell denken.

ZERO-TRUST-ARCHITEKTUREN UND DEDIZIERTE GATEWAYS (EINFÜHRUNG)

Unternehmens-VPNs schützen Unternehmenswerte durch den Umstieg auf Zero Trust Network Access (ZTNA) und das Whitelisting dedizierter statischer IP-Gateways. IT-Manager nutzen zentrale Verwaltungskonsolen, um Site-to-Site-IPsec-Tunnel und Single-Sign-On-Verbindungen (SSO) zu steuern.

LESEN SIE JEDEN KONTROLLPUNKT SORGFÄLTIG UND WÄHLEN ODER SCHREIBEN SIE DIE RICHTIGE ANTWORT.

Kontrollpunkt 1: Auswahlaufgaben

1 **1. Welches Sicherheitsmodell löst herkömmliche Unternehmens-VPNs ab?**

- A) Zero Trust
- B) Multi-Hop
- C) Peer-to-Peer
- D) Einzelnes Gateway

2 **2. Welche Funktion ist erforderlich, um den Datenbankzugriff auf Unternehmensserver zu beschränken?**

- A) Dedizierte IP
- B) Dynamisches Routing
- C) Split Tunnel
- D) DNS-Proxy

3 **3. Welches Protokoll ist der Standard für Site-to-Site-Tunnel in Unternehmen?**

- A) IPsec
- B) PPTP
- C) SOCKS5
- D) SSL v3

4 **4. Mit welchem zentralen Tool können Administratoren Mitarbeiterlizenzen verwalten?**

- A) Admin-Konsole
- B) Registrierungsschlüssel
- C) Router-Firmware
- D) Systemprotokoll

5 **5. Welcher Authentifizierungsstandard ermöglicht die Anmeldung über Okta oder Microsoft Entra ID?**

- A) Single Sign-On
- B) Gemeinsames Geheimnis
- C) EPP-Authentifizierung
- D) WEP-Schlüssel

Kontrollpunkt 2: Richtig oder falsch

6 Frage 6

6. Zero Trust Network Access gewährt Zugang zum Netzwerk erst, nachdem die Vertrauenswürdigkeit des Geräts fortlaufend überprüft wurde.

○ Richtig ○ Falsch

7 Frage 7

7. Dedizierte IP-Gateways leiten den Datenverkehr der Mitarbeitenden zusammen mit dem zufälliger öffentlicher Privatnutzer.

○ Richtig ○ Falsch

8 Frage 8

8. Zentrale Admin-Konsolen ermöglichen es IT-Managern, die Lizenzplätze einzelner Mitarbeiter sofort zu entziehen.

○ Richtig ○ Falsch

9 Frage 9

9. IPsec ist ein schlankes Protokoll, das keine Site-to-Site-Netzwerktunnel unterstützt.

○ Richtig ○ Falsch

10 Frage 10

10. Single Sign-On ermöglicht eine sichere Authentifizierung von Mitarbeitern über die Identitätsanbieter des Unternehmens.

○ Richtig ○ Falsch

Kontrollpunkt 3: Schlüsselbegriffe einsetzen

Lesen Sie jeden der folgenden Sätze und füllen Sie die Lücke mit dem richtigen Begriff aus der Wortliste.

1. Moderne Sicherheitsarchitekturen ersetzen veraltete Tunnel durch Zugriff nach dem Prinzip _____ .

2. Um den Datenbankzugriff einzuschränken, konfigurieren Unternehmen eine _____ als Gateway-Adresse.

3. Zweigstellen werden über Site-to-Site-Tunnel mit _____ sicher verbunden.

4. IT-Administratoren vergeben Benutzerlizenzen für Mitarbeitende in der zentralen _____ .

5. Durch die Okta-Integration können sich Mitarbeitende per unternehmensweitem _____ authentifizieren.

6. Zum Schutz der Anmeldungen schreiben Unternehmensportale die _____ - Authentifizierung vor.

WORTSCHATZ-WORTBANK

ADMIN-KONSOLE BEREITSTELLUNG DEDIZIERTE IP GATEWAY IPSEC MULTIFAKTOR SINGLE SIGN-ON ZERO TRUST

Schreiben Sie Ihre Antworten hier:

1.
2.
3.
4.
5.
6.

Kontrollpunkt 4: Zuordnung von Schlüsselbegriffen

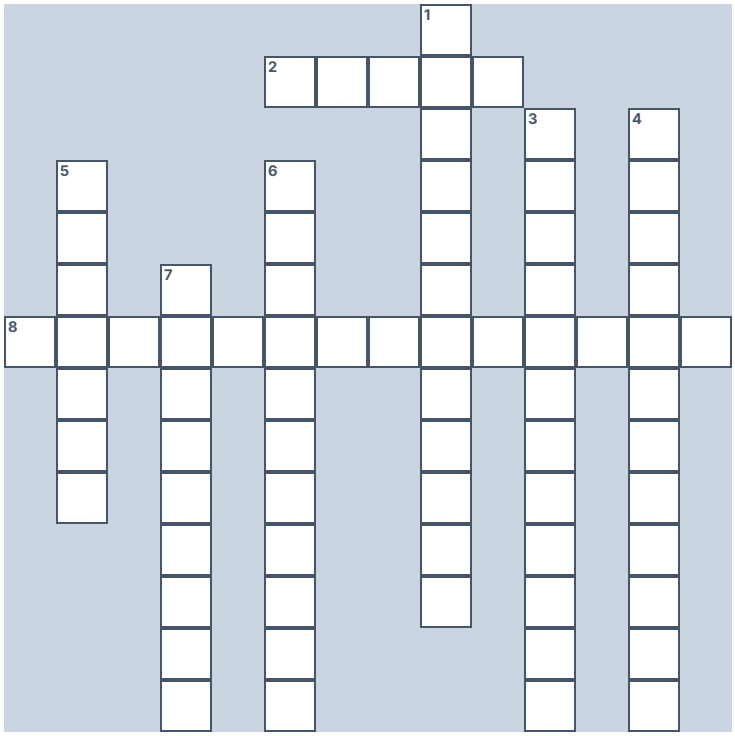
DEFINITIONEN ZUORDNEN

Ordnen Sie jeden Fachbegriff links der richtigen Definition rechts zu, indem Sie den passenden Buchstaben (A–H) in das ausfüllbare Eingabefeld schreiben.

☐	1. ZERO TRUST	A	Zuteilung von VPN-Zugangslizenzen an Mitarbeitende.
☐	2. DEDIZIERTE IP	B	Identitätsverknüpfung mit Okta und Entra ID.
☐	3. IPSEC	C	Anmeldesicherheit, die zusätzliche Token erfordert.
☐	4. ADMIN-KONSOLE	D	Statische Gateway-Adresse auf der Whitelist.
☐	5. SINGLE SIGN-ON	E	Standard für Site-to-Site-Tunnel.
☐	6. MEHRFAKTOR	F	Routing-Knoten am Netzwerkeingang.
☐	7. GATEWAY	G	Zentrales Portal für Lizenzplätze von IT-Managern.
☐	8. BEREITSTELLUNG	H	Rahmenwerk zur kontinuierlichen Überprüfung von Vertrauen.

Kontrollpunkt 5: Kreuzworträtsel

Lösen Sie das Kreuzworträtsel, indem Sie Buchstaben in die aktiven weißen Felder eingeben. Die Zahlen entsprechen den Hinweisen unten.



WAAGERECHT

2. Standard für Site-to-Site-Tunnel (5)

8. Zuteilung von VPN-Zugangslizenzen an Mitarbeitende (14)

SENKRECHT

1. Statische Gateway-Adresse für Whitelists (12)

3. Identitätsanbindung an Okta und Entra ID (12)

4. Zentrales Portal, in dem die IT Lizenzplätze verwaltet (12)

5. Netzwerkknoten am Zugangspunkt, der den Verkehr weiterleitet (7)

6. Anmeldeschutz, der zusätzliche Token erfordert (11)

7. Rahmenwerk zur fortlaufenden Überprüfung von Vertrauen (9)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

Nutzer von Screenreadern und Tastatur können die Kreuzworträtsel-Antworten direkt in die Textfelder unten eingeben.

WAAGERECHT

2 waagerecht: Standard für Site-to-Site-Tunnel (5 Buchstaben):

8 waagerecht: Zuteilung von VPN-Zugangslizenzen an Mitarbeitende (14 Buchstaben):

SENKRECHT

1 senkrecht: Statische Gateway-Adresse für Whitelists (12 Buchstaben):

3 senkrecht: Identitätsanbindung an Okta und Entra ID (12 Buchstaben):

4 senkrecht: Zentrales Portal, in dem die IT Lizenzplätze verwaltet (12 Buchstaben):

5 senkrecht: Netzwerkknoten am Zugangspunkt, der den Verkehr weiterleitet (7 Buchstaben):

6 senkrecht: Anmeldeschutz, der zusätzliche Token erfordert (11 Buchstaben):

7 senkrecht: Rahmenwerk zur fortlaufenden Überprüfung von Vertrauen (9 Buchstaben):

Kontrollpunkt 6: Suchsel

Finden Sie die 8 wichtigen Fachbegriffe, die im Gitter unten versteckt sind. Die Wörter können waagerecht, senkrecht oder diagonal verlaufen.

P Y J K V J Y W Y P J I Z I J
I N A E I A S A J F W E K Z K
E E K Q M U L T I F A K T O R
T N J A F O K N D N C D H I B
R A P R L P W T I Y F Y S G X
E W H F R T N U K R D T S L P
I L M S H K P H Y P L W U N Y
Z Q N O N G I S E L G N I S Q
I B A L P M B L I F I N Y B Z
D Z Y B N V X M C C E S P I F
E B E R E I T S T E L L U N G
D P W Z E R O T R U S T Q Q X
H E A D M I N K O N S O L E Y
C W L F G H Z W C O R J X X R
K Z Y A W E T A G A N R Z R M

WORTSCHATZ-WORTLISTE

ZEROTRUST DEDIZIERTEIP IPSEC ADMINKONSOLE SINGLESIGNON
MULTIFAKTOR GATEWAY BEREITSTELLUNG

Kontrollpunkt 6, Alternative: Barrierefreie Begriffszuordnung

Ordnen Sie jeden der 8 Fachbegriffe aus dem Suchrätsel der richtigen Definition zu, indem Sie den Buchstaben (A–H) in die Lücke schreiben.

FACHBEGRIFFE

- **A. ZEROTRUST**
- **B. DEDIZIERTEIP**
- **C. IPSEC**
- **D. ADMINKONSOLE**
- **E. SINGLESIGNON**
- **F. MULTIFAKTOR**
- **G. GATEWAY**
- **H. BEREITSTELLUNG**

DEFINITIONEN UND ZUORDNUNGSFELDER

1. Statische Gateway-Adresse für Whitelists.
2. Netzwerkknoten am Zugangspunkt, der den Verkehr weiterleitet.
3. Zuteilung von VPN-Zugangslizenzen an Mitarbeitende.
4. Anmeldeschutz, der zusätzliche Token erfordert.
5. Standard für Site-to-Site-Tunnel.
6. Rahmenwerk zur fortlaufenden Überprüfung von Vertrauen.
7. Identitätsanbindung an Okta und Entra ID.
8. Zentrales Portal, in dem die IT Lizenzplätze verwaltet.

Kontrollpunkt 7: Buchstabensalat

Bringen Sie die Buchstaben unten in die richtige Reihenfolge, um zentrale Begriffe aus diesem Arbeitsblatt aufzudecken. Schreiben Sie Ihre Antworten in die vorgesehenen Eingabefelder.

1. RTOEZUSTR
2. ICESP
3. SIISOGNENLNG
4. YAWEAGT
5. EEREPDZTIDII
6. ENSOKLNADOMI
7. KIMUARTOLFT
8. ETUTELEGBSRNLI

Bonusaufgabe: Schnell denken

3 ANTWORTEN PRO KATEGORIE. WER DIE LISTE ZUERST VOLLSTÄNDIG AUSFÜLLT, GEWINNT.

1	Werkzeuge, die ein Unternehmen jeden Tag nutzt			
2	Dinge, die ein VPN verbergen kann			
3	Rollen in einer IT-Abteilung			
4	Wörter, die Zero Trust beschreiben			
5	Möglichkeiten, sich sicher anzumelden			
6	Gründe, Mitarbeitenden ein VPN zu geben			
7	Dinge, die nach einem Sicherheitsvorfall zu tun sind			
8	Gründe, auf Reisen ein VPN zu nutzen			
9	Regeln für sicheres Arbeiten im Homeoffice			
10	Daten, die ein Unternehmen schützen muss			
11	Dinge, die eine Videokonferenz stören können			
12	Geräte, die ein VPN nutzen können			
13	Büroprogramme, die Sie kennen			
14	Orte, von denen aus Mitarbeitende arbeiten			
15	Geräte, die Mitarbeitende haben könnten			

Kontrollpunkt 8: Fallstudien zu VPN und Netzwerken

Wenden Sie die erlernten Konzepte an, um die folgenden praxisnahen Szenarien zu lösen.

FALLSTUDIE 1: MIGRATION ZU ZERO TRUST



Szenario: Ein Unternehmen möchte seine lokalen Server absichern, indem es Konformitätszertifikate der Geräte, den Firewall-Status und den Standort der Nutzer laufend überprüft, statt jedem innerhalb des Netzwerks zu vertrauen.

Diskussionsfrage: Welches Konzept sollte die IT-Sicherheitsleitung einführen, um dies zu erreichen?

FALLSTUDIE 2: GATEWAY-BESCHRÄNKUNG



Szenario: Ein Unternehmen hostet private Finanzdatenbanken in der Cloud. Es möchte jeglichen öffentlichen Internetzugriff auf die Verwaltungsoberflächen sperren und Anmeldungen nur von verifizierten Firmengeräten zulassen.

Diskussionsfrage: Welche Netzwerkkonfiguration sollte der Datenbankadministrator in der Cloud-Firewall einrichten?

Kontrollpunkt 9: Entschlüsselung der Chiffre

Eine Netzwerktechnikerin oder ein Netzwerktechniker sichert Routing-Kanäle und Client-Tunnel. Entschlüsseln Sie mithilfe des Buchstaben-Zahlen-Schlüssels unten die Nachricht, indem Sie die passenden Buchstaben in die Lücken schreiben.

SCHLÜSSEL FÜR DIE BUCHSTABEN-ZAHLEN-VERSCHLÜSSELUNG

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

26	5	18	15		20	18	21	19	20		16	18	21	5	6	20	
10	5	4	5	19		7	5	18	1	5	20		9	13			
					14	5	20	26	23	5	18	11					

Entschlüsselte Nachricht:

TIPP: JEDE ZAHL STEHT FÜR DIE POSITION DIESES BUCHSTABENS IM ALPHABET (Z. B. 1 = A, 2 = B, 26 = Z).

Kontrollpunkt 10: Grundlegende häufige Fragen zu VPN (Teil A)

Sehen Sie sich die häufigsten Fragen und Antworten zu virtuellen privaten Netzwerken (VPNs) und Tunneling an.

Q1: Was ist ein Unternehmens-VPN?

Ein sicherer Netzwerktunnel für Unternehmen, über den Mitarbeitende aus der Ferne mit zentraler Verwaltung auf Firmennetzwerke zugreifen können.

Q2: Wie unterscheidet sich Zero Trust von herkömmlichen VPNs?

Herkömmliche VPNs vertrauen jedem innerhalb des Tunnels, während Zero Trust jede Geräte- und Benutzerverbindung fortlaufend überprüft.

Q3: Was ist eine Dedicated IP bei Business-VPNs?

Eine statische IP-Adresse, die ausschließlich für Ihr Unternehmen reserviert ist, sodass Sie sie für den sicheren Zugriff auf Cloud-Datenbanken auf eine Whitelist setzen können.

Q4: Warum ist SSO für Business-VPNs wichtig?

Single Sign-On ermöglicht es Mitarbeitern, sich mit ihren Unternehmens-Zugangsdaten (etwa über Okta oder Microsoft Entra ID) sicher anzumelden.

Q5: Was ist ein Site-to-Site-VPN?

Ein Tunnel, der zwei physische Standorte (etwa eine Filiale und die Zentrale) mithilfe von IPsec über das öffentliche Internet verbindet.

Kontrollpunkt 10: Grundlegende häufige Fragen zu VPN (Teil B)

Sehen Sie sich die häufigsten Fragen und Antworten zu virtuellen privaten Netzwerken (VPNs) und Tunneling an.

Q6: Welche Funktion hat eine Administrationskonsole?

Ein Dashboard, mit dem IT-Administratoren Mitarbeiterplätze hinzufügen oder entfernen, Gateways zuweisen und aktive Verbindungen überwachen.

Q7: Wie sichert MFA Business-VPNs ab?

Indem ein zweiter Code (etwa ein Token aus einer Authenticator-App) verlangt wird, um unbefugten Zugang mit kompromittierten Passwörtern zu verhindern.

Q8: Kann ich den Verbindungsverlauf von Mitarbeitern prüfen?

Ja, Unternehmens-VPNs protokollieren Verbindungszeitpunkte, Verbindungsdauer und zugewiesene IP-Adressen für Compliance-Prüfungen.

Q9: Was ist ZTNA?

Zero Trust Network Access, ein Sicherheitsmodell, das nur Zugriff auf bestimmte Anwendungen statt auf das gesamte Netzwerk gewährt.

Q10: Welche Rolle spielen Gateway-Knoten?

Sie dienen als sichere Zugangspunkte für entfernten Datenverkehr und leiten Daten direkt an private Unternehmensserver weiter.

Kontrollpunkt 10: Fortgeschrittene häufige Fragen zu VPN (Teil C)

Erkunden Sie fortgeschrittene technische Aspekte von VPN-Tunnelprotokollen, der Integration mobiler Clients und des Einsatzes in Unternehmen.

Q1: Wie schützt IPsec die Site-to-Site-Kommunikation von Unternehmen?

IPsec verschlüsselt den Datenverkehr auf der Netzwerkschicht mit Encapsulating Security Payload (ESP), um Vertraulichkeit und Integrität der Daten zu gewährleisten.

Q2: Warum versagt die herkömmliche perimeterbasierte Sicherheit bei Remote-Belegschaften?

Weil Mitarbeitende von mehreren Standorten und Geräten aus auf Daten zugreifen, wodurch ein einzelner Netzwerk-Firewall-Perimeter überholt ist.

Q3: Wie setzen IT-Manager die automatisierte Bereitstellung um?

Durch Abbilden von SCIM-Protokollen zwischen Identitätsanbietern (Okta) und der VPN-Verwaltungskonsole, um Benutzerverzeichnisse zu synchronisieren.

Q4: Welchen Vorteil bietet Split-Tunneling in Unternehmensumgebungen?

Es leitet lokalen SaaS-Verkehr (etwa Microsoft 365) außerhalb des VPN-Tunnels und schont so die Bandbreite des Unternehmens-Gateways für private Datenbanken.

Q5: Wie überprüfen Device Posture Checks die Sicherheit von Endgeräten?

Der VPN-Client überprüft das Gerät vor dem Verbinden, um sicherzustellen, dass die Firewall aktiv ist, der Virenschutz läuft und die Betriebssystem-Patches aktuell sind.

Kontrollpunkt 10: Fortgeschrittene häufige Fragen zu VPN (Teil D)

Erkunden Sie fortgeschrittene technische Aspekte von VPN-Tunnelprotokollen, der Integration mobiler Clients und des Einsatzes in Unternehmen.

Q6: Welche Rolle spielt NAT-Traversal bei Business-VPN-Setups?

NAT-T kapselt IPsec-Pakete in UDP, damit sie Heimrouter und Firewalls ohne Verbindungsabbrüche passieren können.

Q7: Wie verhindern Unternehmen Bandbreitenengpässe am Gateway?

Durch Bereitstellen mehrerer regionaler Gateway-Knoten und Verteilen des eingehenden Nutzerverkehrs auf diese mittels Load Balancern.

Q8: Warum werden statische IP-Whitelists dynamischen vorgezogen?

Statische Whitelists verhindern, dass nicht autorisierte externe IPs einen Verbindungs-Handshake versuchen, und verkleinern so die Angriffsfläche erheblich.

Q9: Welche Rolle spielt die zertifikatsbasierte Authentifizierung in Unternehmens-VPNs?

Es prüft eindeutige digitale Zertifikate auf vom Unternehmen verwalteten Geräten und blockiert nicht verwaltete private Computer.

Q10: Wie verringert ZTNA das Risiko seitlicher Bewegungen im Netzwerk?

Durch Beschränken von Benutzersitzungen auf bestimmte autorisierte Ressourcen, sodass Hacker sich nicht durch das Netzwerk bewegen können, wenn ein Knoten kompromittiert wird.

Teil 11: 10 Fakten und Einblicke zu VPNs aus der Praxis

Lernen Sie reale Fakten zu VPN-Verschlüsselungsgeschwindigkeiten, Protokoll-Audits, mobiler Konnektivität und Remote-Arbeit in Unternehmen kennen.

1. VPN-EINBLICK

Zero-Trust-Architekturen überprüfen fortlaufend den Sicherheitsstatus jedes Geräts, das eine Netzwerkverbindung herstellen will.

2. VPN-EINBLICK

Mit dedizierten IP-Gateways können Unternehmen Cloud-Datenbanken abschotten, indem sie statische Adressen auf eine Whitelist setzen.

3. VPN-EINBLICK

IPsec ist das branchenübliche Standardprotokoll für die Einrichtung sicherer Site-to-Site-Tunnel zwischen Büronetzwerken.

4. VPN-EINBLICK

Mit Admin-Konsolen können IT-Abteilungen VPN-Zugänge für Mitarbeitende bereitstellen, verwalten und prüfen.

5. VPN-EINBLICK

Single Sign-On verbindet den VPN-Zugang mit Identitätsanbietern von Unternehmen wie Okta und Entra ID.

6. VPN-EINBLICK

Mehr-Faktor-Authentifizierung blockiert unbefugte Verbindungsversuche, die von gestohlenen Passwörtern ausgehen.

7. VPN-EINBLICK

Split Tunneling optimiert die Bandbreite des Unternehmens, indem öffentlicher SaaS-Verkehr vom verschlüsselten Tunnel ausgenommen wird.

8. VPN-EINBLICK

Prüfungen des Gerätezustands überprüfen lokale Sicherheitseinstellungen, bevor Zugriff auf Unternehmensserver gewährt wird.

9. VPN-EINBLICK

Die SCIM-Verzeichnissynchronisierung automatisiert die Zugriffskontrolle beim Ein- und Austritt von Mitarbeitenden.

10. VPN-EINBLICK

Zero Trust Network Access beschränkt den Zugriff der Nutzer auf bestimmte autorisierte Anwendungen und verhindert so laterale Bewegungen im Netzwerk.

Technische Referenzen und Quellen

Der Lernleitfaden und die interaktiven Rätsel wurden aus globalen technischen Standards, Spezifikationen und Regulierungsrahmen zusammengestellt.

WISSENSCHAFTLICHE UND FACHLICHE QUELLEN

[1] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.
https://www.vpn.com/vpn/best-vpn-for-business/

[2] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.
https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.
https://nordlayer.com/

Lösungsschlüssel: Kontrollpunkt 1 – Auswahlaufgaben

1 **Zero Trust** ZTNA-MODELL **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

Zero-Trust-Modelle überprüfen vor dem Zugang zum Netzwerk fortlaufend die Konformität von Geräten. Quelle: NIST Zero Trust.

2 **Dedizierte IP** STATISCHE IP **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

Mit dedizierten IP-Adressen können Gateways per Whitelist öffentlichen Datenverkehr blockieren. Quelle: Dedicated IP Guide.

3 **IPsec-Standard** IPSEC-TUNNEL **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

IPsec ist das Standardprotokoll für Site-to-Site-Tunnel zwischen Zweigstellen. Quelle: IPsec Tunneling.

4 **IT-Zuweisung** ADMIN-KONSOLE **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

Zentrale Admin-Dashboards ermöglichen es IT-Managern, Lizenzplätze zuzuweisen. Quelle: CISA Guidelines.

5 **Frage 5** **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

Welcher Authentifizierungsstandard ermöglicht die Anmeldung über Okta oder Microsoft Entra ID? → Single Sign-On

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 **Zero Trust** ZTNA-PRÜFUNGEN — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Zero-Trust-Modelle überprüfen vor dem Zugang zum Netzwerk fortlaufend die Konformität von Geräten. Quelle: NIST Zero Trust.

7 **Frage 7** — **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

Dedizierte IPs sind für ein einzelnes Unternehmen reserviert, sodass dessen Datenverkehr nicht mit dem anderer Nutzer vermischt wird.

8 **IT-Zuweisung** IT-ADMIN-PLATZ — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Zentrale Admin-Dashboards ermöglichen es IT-Managern, Lizenzplätze zuzuweisen. Quelle: CISA Guidelines.

9 **IPsec-Standard** SITE-TO-SITE — **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

IPsec ist das Standardprotokoll für Site-to-Site-Tunnel zwischen Zweigstellen. Quelle: IPsec Tunneling.

10 **Okta-SSO-Verbindung** SSO-ANMELDUNG — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Single Sign-On verbindet VPN-Anmeldungen mit Unternehmensverzeichnissen wie Okta. Quelle: Okta SSO.

Vokabelschlüssel und Bewertungsraster

Bewertungsraster für Lehrkräfte: Vergeben Sie 1 Punkt für jede richtige Zuordnung (insgesamt 8 Punkte) und jeden Kontextbegriff (insgesamt 6 Punkte).

KONTROLLPUNKT 4: LÖSUNG BEGRIFFSZUORDNUNG

H 1. ZERO TRUST	D 2. DEDIZIERTE IP	E 3. IPSEC	G 4. ADMIN-KONSOLE
B 5. SINGLE SIGN-ON	C 6. MEHRFAKTOR	F 7. GATEWAY	A 8. BEREITSTELLUNG

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

1 ZERO TRUST	2 DEDIZIERTE IP	3 IPSEC	4 ADMIN-KONSOLE
5 SINGLE SIGN-ON	6 MULTIFAKTOR		

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

1 B – DEDIZIERTEIP	2 G – GATEWAY	3 H – BEREITSTELLUNG	4 F – MULTIFAKTOR
5 C – IPSEC	6 A – ZEROTRUST	7 E – SINGLESIGNON	8 D – ADMINKONSOLE

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden ZERO TRUST, DEDIZIERTE IP und IPSEC in eigenen Worten erklären und jeweils ein Beispiel nennen können.

Fallstudien:
Bitten Sie die Lernenden, ihre Empfehlungen mit Fakten aus dem Arbeitsblatt statt mit Vermutungen zu begründen.

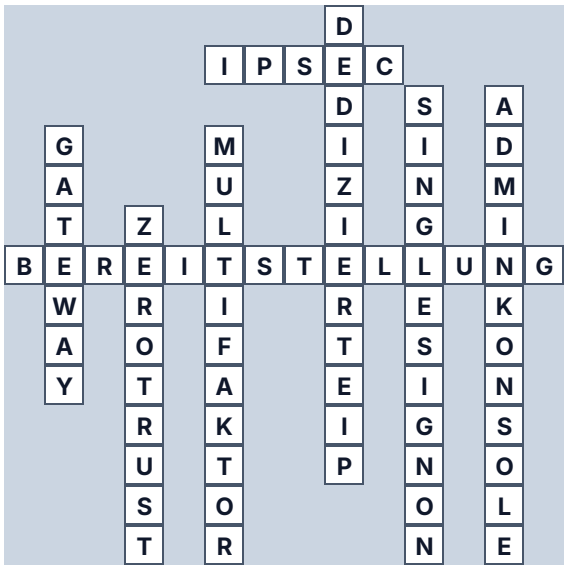
Quellenbewertung:
Lassen Sie die Lernenden mindestens eine Aussage anhand der Quellen des Arbeitsblatts prüfen und besprechen Sie, warum sich Zahlen, Preise und Regeln mit der Zeit ändern können.

Rätsellösungen und Hinweise für Lehrkräfte

LÖSUNG DES SUCHSELS

P	Y	J	K	V	J	Y	W	Y	P	J	I	Z	I	J
I	N	A	E	I	A	S	A	J	F	W	E	K	Z	K
E	E	K	Q	M	U	L	T	I	F	A	K	T	O	R
T	N	J	A	F	O	K	N	D	N	C	D	H	I	B
R	A	P	R	L	P	W	T	I	Y	F	Y	S	G	X
E	W	H	F	R	T	N	U	K	R	D	T	S	L	P
I	L	M	S	H	K	P	H	Y	P	L	W	U	N	Y
Z	Q	N	O	N	G	I	S	E	L	G	N	I	S	Q
I	B	A	L	P	M	B	L	I	F	I	N	Y	B	Z
D	Z	Y	B	N	V	X	M	C	C	E	S	P	I	F
E	B	E	R	E	I	T	S	T	E	L	L	U	N	G
D	P	W	Z	E	R	O	T	R	U	S	T	Q	Q	X
H	E	A	D	M	I	N	K	O	N	S	O	L	E	Y
C	W	L	F	G	H	Z	W	C	O	R	J	X	X	R
K	Z	Y	A	W	E	T	A	G	A	N	R	Z	R	M

KREUZWORTRÄTSEL-LÖSUNG



LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

2 waagerecht: IPSEC Standard für Site-to-Site-Tunnel (5 Buchstaben)

8 waagerecht: BEREITSTELLUNG Zuteilung von VPN-Zugangslizenzen an Mitarbeitende (14 Buchstaben)

SENKRECHT

1 senkrecht: DEDIZIERTEIP Statische Gateway-Adresse für Whitelists (12 Buchstaben)

3 senkrecht: SINGLESIGNON Identitätsanbindung an Okta und Entra ID (12 Buchstaben)

4 senkrecht: ADMINKONSOLE Zentrales Portal, in dem die IT Lizenzplätze verwaltet (12 Buchstaben)

5 senkrecht: GATEWAY Netzwerkknoten am Zugangspunkt, der den Verkehr weiterleitet (7 Buchstaben)

6 senkrecht: MULTIFAKTOR Anmeldeschutz, der zusätzliche Token erfordert (11 Buchstaben)

7 senkrecht: ZEROTRUST Rahmenwerk zur fortlaufenden Überprüfung von Vertrauen (9 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

Lösungsschlüssel für die Wort-Entwirr-Aufgabe und die Geheime Chiffre-Aufgabe.

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1.	RTOEZUSTR	ZEROTRUST	5.	EEREPDZTIDII	DEDIZIERTEIP
2.	ICESP	IPSEC	6.	ENSOKLNADOMI	ADMINKONSOLE
3.	SIISOGNENLNG	SINGLESIGNON	7.	KIMUARTOLFT	MULTIFAKTOR
4.	YAWEAGT	GATEWAY	8.	ETUTELEGBSRNLI	BEREITSTELLUNG

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"ZERO TRUST PRUEFT JEDES GERAET IM NETZWERK"

Lösungsschlüssel zu den Fallstudien

A Fallstudie 1: Migration zu Zero Trust

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Ein Unternehmen möchte seine lokalen Server absichern, indem es Konformitätszertifikate der Geräte, den Firewall-Status und den Standort der Benutzer laufend überprüft, statt jedem innerhalb des Netzwerks zu vertrauen.
- Empfohlene Strategie und Lösung: Die Leitung sollte auf ein Zero-Trust-Network-Access-Modell (ZTNA) umstellen, das kontinuierliche, kontextbasierte Sicherheitsprüfungen durchsetzt.

B Fallstudie 2: Gateway-Beschränkung

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Ein Unternehmen hostet private Finanzdatenbanken in der Cloud. Es möchte jeden Zugriff aus dem öffentlichen Internet auf die Admin-Panels sperren und Anmeldungen nur von verifizierten Unternehmensgeräten zulassen.
- Empfohlene Strategie und Lösung: Der Administrator sollte im Unternehmens-VPN ein Gateway mit dedizierter IP konfigurieren und diese statische Adresse in der Firewall der Cloud-Datenbank auf die Positivliste setzen.