Name: _____ Datum: _____ Punkte: _____

Fernzugriffs-VPN

Absicherung von Endgeräten der Remote-Belegschaft, Multi-Faktor-Authentifizierung und Konfiguration von IPsec-Tunneln.

REMOTE-ACCESS-VPNS – LERNÜBERSICHT

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 den Fernzugriff. Sie lernen Client-to-Site-Tunnel, Anmeldungen mit mehreren Faktoren, Statusprüfungen von Endgeräten, Bandbreitenbegrenzungen und Sicherheitsaudits per Syslog 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/fernzugriff/

Ihr Lernfahrplan: VPN für den Fernzugriff

- Endgeräte von Remote-Mitarbeitern absichern, die auf lokale Netzwerkknoten zugreifen.
- Konfigurieren Sie Richtlinien zur Multi-Faktor-Authentifizierung für Remote-Anmeldungen.
- Client-to-Site-Konfigurationen mit IPsec und OpenVPN einrichten.
- Prüfen Sie Fernverbindungsprotokolle auf Verstöße gegen die Zugriffskontrolle.
- Vor der Freigabe von Netzwerkverbindungen Prüfungen des Gerätezustands durchführen.
- Serverdurchsatz optimieren, um Bandbreitenengpässe bei der Telearbeit zu verhindern.

ANLEITUNG ZU REMOTE-ACCESS-VPNS

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: Gerätezustandsprüfungen und Mehrfaktor-Anmeldungen. Zum Schluss folgt die Bonusaufgabe Schnell denken.

CLIENT-TO-SITE-TUNNEL UND ENDGERÄTE-COMPLIANCE (EINFÜHRUNG)

Fernzugriffs-VPNs bauen sichere Client-to-Site-Tunnel für Mitarbeitende außerhalb des Standorts auf. Um diese Verbindungen abzusichern, müssen Anmeldungen mit Multi-Faktor-Authentifizierung (MFA) durchgesetzt, die Konformität der Endgeräte geprüft und Protokolle über zentrale Syslog-Collector ausgewertet werden.

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

Kontrollpunkt 1: Auswahlaufgaben

1. Welchen Authentifizierungsstandard sollten Portale für VPN-Fernzugriff vorschreiben?

- A) Mehrstufig
- B) Einzelner Faktor
- C) Unverschlüsselt
- D) Lokaler Gast

2. Welches Protokoll ist der Standard für die Absicherung von Client-to-Site-Verbindungen im Homeoffice?

- A) OpenVPN
- B) SOCKS5
- C) PPTP
- D) FTP

3. Welche Prüfung stellt fest, ob ein Laptop im Fernzugriff sauber ist, bevor er sich verbindet?

- A) Statusprüfung des Geräts
- B) Geschwindigkeitstest
- C) Ping-Test
- D) Speicheranzahl

4. Wo werden die Verbindungsprotokolle von Remote-Mitarbeitenden für Sicherheitsaudits gespeichert?

- A) Syslog-Server
- B) Registrierungsschlüssel
- C) Client-Speicher
- D) Webbrowser

5. Welches Problem entsteht, wenn die Zahl der Remote-Mitarbeitenden die Bandbreitenkapazität des Gateways übersteigt?

- A) Bandbreitendrosselung
- B) DNS-Leck
- C) Handshake-Durchlass
- D) Offenlegung der IP

Kontrollpunkt 2: Richtig oder falsch

6 Frage 6

6. Mehr-Faktor-Authentifizierung fügt ein zweites Prüf-Token hinzu, um Remote-Anmeldungen abzusichern.

○ Richtig ○ Falsch

7 Frage 7

7. Statusprüfungen erlauben entfernten Geräten mit deaktivierter Firewall den Zugriff auf private Server.

○ Richtig ○ Falsch

8 Frage 8

8. Protokolle von Fernzugriffs-VPNs sind unverzichtbar, um unbefugtes Eindringen in das Unternehmensnetzwerk nachzuverfolgen.

○ Richtig ○ Falsch

9 Frage 9

9. OpenVPN und IPsec sind veraltete Protokolle, die die Nutzdaten entfernter Clients nicht verschlüsseln.

○ Richtig ○ Falsch

10 Frage 10

10. Ein Bandbreitenengpass am Gateway entsteht, wenn der Remote-Datenverkehr die Kapazität der Netzwerkkarte übersteigt.

○ 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. Zum Schutz von Unternehmensportalen müssen Fernanmeldungen eine _____ - Authentifizierung erfordern.

2. Remote-Clients verschlüsseln die Nutzdaten im Tunnel mit Standardprotokollen wie _____ .

3. Bevor Geräte eine Netzwerkverbindung erhalten, muss ihr _____ eine Sicherheitsprüfung bestehen.

4. Prüfbare Zugriffsprotokolle werden fortlaufend an einen zentralen _____ -Server übertragen.

5. Starker Datenverkehr während der Geschäftszeiten kann am Gateway zu Engpässen bei der _____ führen.

6. Virtuelle Adaptertreiber übernehmen unter Windows und macOS das Client-to-Site- _____ .

WORTSCHATZ-WORTBANK

BANDBREITE FIREWALL GERÄTESTATUS MULTIFAKTOR OPENVPN SYSLOG TUNNELING VERSCHLÜSSELUNG

Schreiben Sie Ihre Antworten hier:

1. **2.**

3. **4.**

5. **6.**

Kontrollpunkt 4: Zuordnung von Schlüsselbegriffen

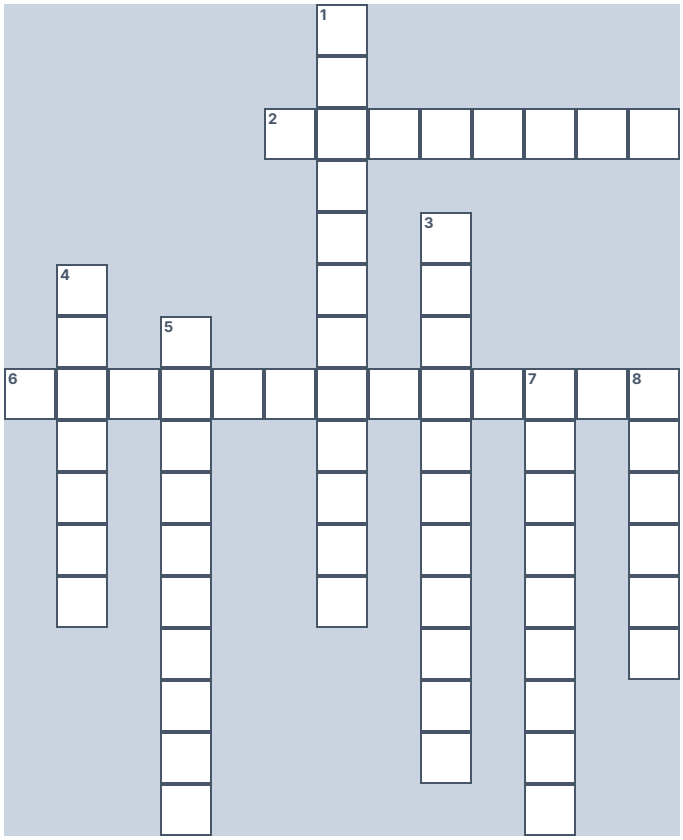
DEFINITIONEN ZUORDNEN

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

☐	1. MEHRFAKTOR	A	Kapselung von Daten in einem sicheren Pfad.
☐	2. OPENVPN	B	Zentraler Sammelpunkt für Sicherheitsprotokolle.
☐	3. SICHERHEITSSTATUS	C	Grenze für das Datenvolumen im Netzwerk.
☐	4. SYSLOG	D	Standardprotokoll für Client-to-Site-Verbindungen.
☐	5. BANDBREITE	E	Prüfung des Zustands entfernter Geräte.
☐	6. VERSCHLÜSSELUNG	F	Regeln des Systems zur Filterung des Datenverkehrs.
☐	7. TUNNELING	G	Kryptografisches Verwürfeln von Paketen.
☐	8. FIREWALL	H	Anmeldesicherheit, die zusätzliche Token erfordert.

Kontrollpunkt 5: Kreuzworträtsel

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



WAAGERECHT

2. Regelsystem zur Filterung des Datenverkehrs (8)

6. Prüfung des Sicherheitszustands entfernter Geräte (13)

SENKRECHT

1. Kryptografisches Verschlüsseln von Datenpaketen (12)

3. Anmeldeschutz, der zusätzliche Token erfordert (11)

4. Standardprotokoll für Client-to-Site-Verbindungen (7)

5. Kapazitätsgrenze für Netzwerkdaten (10)

7. Kapseln von Daten in einem sicheren Pfad (9)

8. Zentrale Sammelstelle für Sicherheitsprotokolle (6)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

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

WAAGERECHT

2 waagerecht: Regelsystem zur Filterung des Datenverkehrs (8 Buchstaben):

6 waagerecht: Prüfung des Sicherheitszustands entfernter Geräte (13 Buchstaben):

SENKRECHT

1 senkrecht: Kryptografisches Verschlüsseln von Datenpaketen (12 Buchstaben):

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

4 senkrecht: Standardprotokoll für Client-to-Site-Verbindungen (7 Buchstaben):

5 senkrecht: Kapazitätsgrenze für Netzwerkdaten (10 Buchstaben):

7 senkrecht: Kapseln von Daten in einem sicheren Pfad (9 Buchstaben):

8 senkrecht: Zentrale Sammelstelle für Sicherheitsprotokolle (6 Buchstaben):

Kontrollpunkt 6: Suchsel

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

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

WORTSCHATZ-WORTLISTE

MULTIFAKTOR OPENVPN GERAETESTATUS SYSLOG BANDBREITE
CHIFFRIERUNG TUNNELING FIREWALL

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. MULTIFAKTOR**
- **B. OPENVPN**
- **C. GERAETESTATUS**
- **D. SYSLOG**
- **E. BANDBREITE**
- **F. CHIFFRIERUNG**
- **G. TUNNELING**
- **H. FIREWALL**

DEFINITIONEN UND ZUORDNUNGSFELDER

1. Zentrale Sammelstelle für Sicherheitsprotokolle.
2. Regelsystem zur Filterung des Datenverkehrs.
3. Kapseln von Daten in einem sicheren Pfad.
4. Kryptografisches Verschlüsseln von Datenpaketen.
5. Standardprotokoll für Client-to-Site-Verbindungen.
6. Kapazitätsgrenze für Netzwerkdaten.
7. Prüfung des Sicherheitszustands entfernter Geräte.
8. Anmeldeschutz, der zusätzliche Token erfordert.

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. IAOUFKMTLRT
2. UEETRGTEST ASA
3. BRTEABEDIN
4. EGNNILTUN
5. VNNEOPP
6. OLSSGY
7. ERFCHIGUNIR F
8. EIWLFLAR

Bonusaufgabe: Schnell denken

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

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

Kontrollpunkt 8: Fallstudien zu VPN und Netzwerken

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

FALLSTUDIE 1: DURCHSETZUNG VON MFA

👮

Szenario: Eine Business-Analystin versucht, sich bei der Arbeit aus der Ferne an der Firmendatenbank anzumelden. Sie gibt den richtigen Benutzernamen und das richtige Passwort ein, doch das VPN-Portal sperrt den Zugriff und verlangt einen Code von einem physischen Token.

Diskussionsfrage: Welche Sicherheitsrichtlinie erzwingt diesen doppelten Prüfschritt?

FALLSTUDIE 2: EINHALTUNG DES SICHERHEITSSTATUS

👮

Szenario: Ein externer Auftragnehmer verbindet seinen privaten Laptop mit dem Firmennetzwerk. Der VPN-Client trennt die Verbindung sofort und teilt mit, dass die Virendefinitionen veraltet sind.

Diskussionsfrage: Welche spezielle Prüfung am VPN-Gateway hat diesen Verbindungsversuch blockiert?

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

6	5	18	14	26	21	7	18	9	6	6	22	16	14

19	3	8	21	5	20	26	20	22	5	18	20	5	9	12	20	5

5	14	4	7	5	18	1	5	20	5

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 VPN für den Fernzugriff?

Eine sichere Verbindungsmethode, mit der sich Mitarbeitende außerhalb des Büros direkt mit privaten Unternehmensservern verbinden können.

Q2: Warum unterscheidet sich Client-to-Site von Site-to-Site?

Client-to-Site verbindet einzelne Benutzergeräte, während Site-to-Site ganze physische Bürostandorte verbindet.

Q3: Was ist ein Device Posture Check?

Eine Prüfung des Sicherheitsstatus eines entfernten Geräts (Antivirus, Patchstand des Betriebssystems), bevor Zugriff gewährt wird.

Q4: Warum wird OpenVPN für den Fernzugriff verwendet?

Wegen seines starken Sicherheitsprotokolls, seiner plattformübergreifenden Kompatibilität und der Fähigkeit, einzelne Verbindungen zu verarbeiten.

Q5: Wie schützt MFA den Fernzugriff?

Es fügt ein zweites Verifizierungs-Token hinzu und verhindert so den Zugriff, selbst wenn Passwörter von Mitarbeitenden geleakt oder gestohlen werden.

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: Was ist ein Syslog-Server?

Ein zentrales Protokollarchiv, das Verbindungsereignisse, Anmeldungen und Systemwarnungen für Compliance-Audits speichert.

Q7: Was verursacht Bandbreitenengpässe?

Wenn der gesamte Bandbreitenbedarf der Remote-Mitarbeitenden die Internetgeschwindigkeit des Unternehmens-Gateways übersteigt.

Q8: Kann ich meinen Heimcomputer mit einem Firmen-VPN verbinden?

Nur wenn das Gerät die Prüfungen des Sicherheitsstatus im Unternehmen besteht und von IT-Administratoren freigegeben ist.

Q9: Was ist Netzwerkkapselung?

Das Verpacken von Datenpaketen während der Übertragung in verschlüsselte Protokoll-Header, um die Übertragung abzusichern.

Q10: Wie optimiert Split Tunneling den Fernzugriff?

So können Mitarbeitende für normales Surfen ihren lokalen ISP nutzen, während arbeitsbezogene Dateien über das VPN laufen.

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 verbessert zertifikatsbasierte Authentifizierung den Fernzugriff?

Es bindet Verbindungsberechtigungen an vorinstallierte lokale digitale Zertifikate und blockiert nicht verwaltete oder nicht autorisierte Geräte.

Q2: Welches Sicherheitsrisiko birgt Split Tunneling bei der Fernarbeit?

Es entsteht eine mögliche Brücke, über die ein kompromittiertes lokales Gerät externe Bedrohungen in das private Netzwerk leiten kann.

Q3: Wie prüfen Posture Checks die Registry-Einstellungen?

Der VPN-Client führt lokale Skripte aus, die Registrierungspfade abfragen, um zu prüfen, ob die Sicherheitssoftware des Unternehmens aktiv läuft.

Q4: Warum verwenden Syslogs standardmäßig den UDP-Port 514?

Um Protokolle schnell und mit minimalem Overhead zu übertragen, wobei sichere Setups heute eine TLS-Kapselung über TCP vorschreiben.

Q5: Wie beheben Unternehmen Bandbreitenengpässe am Gateway?

Durch Einsatz von Load Balancern und Verteilen des Fernzugriffsverkehrs auf regionale Serverknoten.

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 Funktion haben virtuelle TAP/TUN-Adapter auf Remote-Clients?

Sie fungieren als virtuelle Netzwerkkarten und leiten den TCP/IP-Datenverkehr auf Geräteebene direkt in den verschlüsselten VPN-Tunnel.

Q7: Wie unterstützt IKEv2 MOBIKE die Mobilität von Remote-Belegschaften?

Es aktualisiert die Bindungen der IP-Adressen dynamisch, sodass das VPN aktiv bleibt, während der Nutzer zwischen WLAN und Mobilfunkdaten wechselt.

Q8: Was ist der Unterschied zwischen Split- und Full-Tunnel-Routing?

Beim Full-Tunnel-Routing wird der gesamte Internetverkehr des Geräts durch das VPN geleitet, beim Split-Routing nur der Verkehr zu Ziel-IPs des Unternehmens.

Q9: Wie gehen NAT-Geräte mit entfernten VPN-Verbindungen um?

Durch Zuordnen lokaler Portbereiche zu öffentlichen Gateway-IP-Adressen, um zurückkehrende verschlüsselte Datenpakete weiterzuleiten.

Q10: Welche Compliance-Standards schreiben eine Prüfung des Fernzugriffs vor?

Standards wie HIPAA, SOC 2 und PCI DSS verlangen die Protokollierung und Überwachung aller Fernzugriffssitzungen.

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

Fernzugriffs-VPNs bauen sichere Client-to-Site-Tunnel für Beschäftigte außerhalb des Standorts auf.

2. VPN-EINBLICK

Mehr-Faktor-Authentifizierung ist laut Compliance-Vorschriften erforderlich, um Remote-Portale von Unternehmen zu schützen.

3. VPN-EINBLICK

Statusprüfungen kontrollieren die lokalen Sicherheitseinstellungen des Clients, bevor Zugriff auf das private Netzwerk gewährt wird.

4. VPN-EINBLICK

Syslog-Server sammeln Verbindungsprotokolle, um unbefugte Zugriffsversuche zu prüfen und zu erkennen.

5. VPN-EINBLICK

Bandbreitenengpässe am Gateway treten auf, wenn der gesamte Remote-Datenverkehr die Internetkapazität des Servers übersteigt.

6. VPN-EINBLICK

Virtuelle Netzwerkadapter kapseln Netzwerkanfragen des Betriebssystems in sichere Protokolle.

7. VPN-EINBLICK

Die Unterstützung von MOBIKE ermöglicht es Remote-Clients, das Netzwerk zu wechseln, ohne dass der VPN-Tunnel abbricht.

8. VPN-EINBLICK

Full-Tunnel-Routing sichert den gesamten Internetverkehr der Mitarbeitenden, erhöht aber die Last am Unternehmens-Gateway.

9. VPN-EINBLICK

Bei der Zertifikatsauthentifizierung ist die Berechtigung für VPN-Verbindungen direkt an vom Unternehmen verwaltete Hardware gebunden.

10. VPN-EINBLICK

Rahmenwerke wie SOC 2 und PCI DSS erwarten die Protokollierung und Überwachung von Fernzugriffssitzungen.

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/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).

https://www.rfc-editor.org/rfc/rfc4555

Lösungsschlüssel: Kontrollpunkt 1 – Auswahlaufgaben

1 Anmeldetoken MFA-SICHERHEIT — Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Mehr-Faktor-Authentifizierung erzwingt bei Anmeldungen eine zweite Überprüfung. Quelle: MFA Implementation.

2 OpenVPN-Tunnel CLIENT-TO-SITE — Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

OpenVPN ist ein Standardprotokoll zur Absicherung von Client-to-Site-Tunneln. Quelle: OpenVPN Client.

3 Prüfungen des Sicherheitsstatus GERÄTEPRÜFUNG — Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Statusprüfungen untersuchen Endgeräte auf aktive Firewalls und Antivirenprogramme. Quelle: Posture Compliance.

4 Log-Aggregator SYSLOG-SERVER — Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Syslog-Server sammeln Protokolle von Sicherheitsereignissen, um Zugriffsverstöße zu überwachen. Quelle: Syslog Standard.

5 Kartenüberlauf GATEWAY-ENGPASS — Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Ein Bandbreitenengpass am Gateway tritt auf, wenn der Nutzerverkehr die Grenzen des Servers übersteigt. Quelle: Capacity Planning.

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 **Anmeldetoken** MFA-PRÜFUNGEN — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Mehr-Faktor-Authentifizierung erzwingt bei Anmeldungen eine zweite Überprüfung. Quelle: MFA Implementation.

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

HINWEIS FÜR LEHRKRÄFTE

Statusprüfungen (Posture Checks) sperren Geräte, deren Firewall oder Virenschutz ausgeschaltet ist, sodass solchen Geräten der Zugang verweigert wird.

8 **Log-Aggregator** SYSLOG-SERVER — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Syslog-Server sammeln Protokolle von Sicherheitsereignissen, um Zugriffsverstöße zu überwachen. Quelle: Syslog Standard.

9 **Frage 9** — **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

OpenVPN und IPsec sind aktuelle Protokolle, die den Datenverkehr von Remote-Clients sehr wohl verschlüsseln.

10 **Kartenüberlauf** GATEWAY-ENGPASS — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Ein Bandbreitenengpass am Gateway tritt auf, wenn der Nutzerverkehr die Grenzen des Servers übersteigt. Quelle: Capacity Planning.

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. MEHRFAKTOR	D 2. OPENVPN	E 3. SICHERHEITSSTATUS	B 4. SYSLOG
C 5. BANDBREITE	G 6. VERSCHLÜSSELUNG	A 7. TUNNELING	F 8. FIREWALL

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

1 MULTIFAKTOR	2 OPENVPN	3 GERÄTESTATUS	4 SYSLOG
5 BANDBREITE	6 TUNNELING		

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

1 D – SYSLOG	2 H – FIREWALL	3 G – TUNNELING	4 F – CHIFFRIERUNG
5 B – OPENVPN	6 E – BANDBREITE	7 C – GERAETESTATUS	8 A – MULTIFAKTOR

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden MEHRFAKTOR, OPENVPN und SICHERHEITSSTATUS 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.

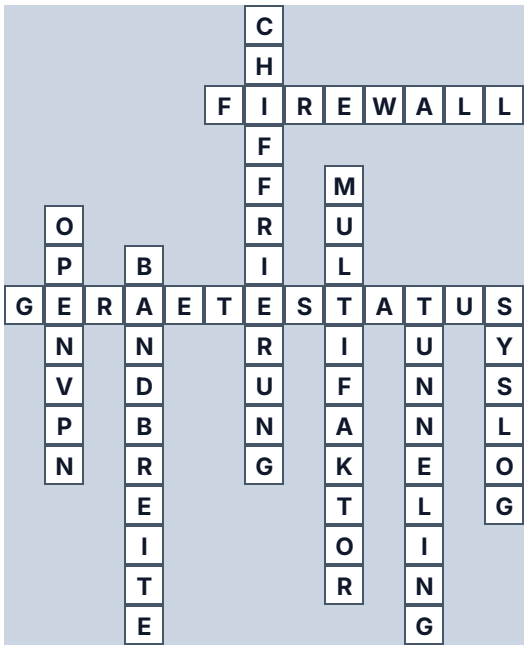
Quellenbewertung:
Lassen Sie die Lernenden mindestens eine Aussage anhand der Quellen des Arbeitsblatts prüfen und besprechen Sie, warum sich Zahlen, Preise und Regeln mit der Zeit ändern können.

Rätsellösungen und Hinweise für Lehrkräfte

LÖSUNG DES SUCHSELS

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

KREUZWORTRÄTSEL-LÖSUNG



LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

2 waagerecht: FIREWALL Regelsystem zur Filterung des Datenverkehrs (8 Buchstaben)

6 waagerecht: GERAETESTATUS Prüfung des Sicherheitszustands entfernter Geräte (13 Buchstaben)

SENKRECHT

1 senkrecht: CHIFFRIERUNG Kryptografisches Verschlüsseln von Datenpaketen (12 Buchstaben)

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

4 senkrecht: OPENVPN Standardprotokoll für Client-to-Site-Verbindungen (7 Buchstaben)

5 senkrecht: BANDBREITE Kapazitätsgrenze für Netzwerkdaten (10 Buchstaben)

7 senkrecht: TUNNELING Kapseln von Daten in einem sicheren Pfad (9 Buchstaben)

8 senkrecht: SYSLOG Zentrale Sammelstelle für Sicherheitsprotokolle (6 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

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

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. IAOUFKMTLRT — **MULTIFAKTOR**
2. UEETRGTESTASA — **GERAETESTATUS**
3. BRTEABEDIN — **BANDBREITE**
4. EGNNILTUN — **TUNNELING**
5. VNNEOPP — **OPENVPN**
6. OLSSGY — **SYSLOG**
7. ERFCHIGUNIRF — **CHIFFRIERUNG**
8. EIWLFLAR — **FIREWALL**

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"FERNZUGRIFF VPN SCHUETZT VERTEILTE ENDGERAETE"

Lösungsschlüssel zu den Fallstudien

A Fallstudie 1: Durchsetzung von MFA

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Ein Business-Analyst versucht, sich im Homeoffice bei der Unternehmensdatenbank anzumelden. Er gibt Benutzernamen und Passwort korrekt ein, doch das VPN-Portal sperrt den Zugriff und verlangt einen Code von einem physischen Token.
- Empfohlene Strategie und Lösung: Das VPN-Portal des Unternehmens setzt eine strenge Richtlinie zur Multi-Faktor-Authentifizierung (MFA) durch, um Remote-Anmeldungen abzusichern.

B Fallstudie 2: Einhaltung des Sicherheitsstatus

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Ein externer Auftragnehmer verbindet seinen privaten Laptop mit dem entfernten Unternehmensnetzwerk. Der VPN-Client trennt die Verbindung sofort und meldet, dass die Signaturen seines Antivirenprogramms veraltet sind.
- Empfohlene Strategie und Lösung: Das Gateway für den Fernzugriff hat eine Statusprüfung des Endgeräts durchgeführt und das Gerät wegen veralteter Sicherheitskonfigurationen blockiert.