Jméno: _____ Datum: _____ Body: _____

Podniková VPN

Zavádění síťového přístupu Zero Trust, dedikovaných uzlů bran a centralizovaných firemních administrátorských kontrol.

PODNIKOVÉ VPN SÍTĚ – PŘEHLED UČIVA

STUDENT
STUDENTSKÝ STATUS
Dráha obránce sítě

ZABEZPEČENÝ
STAV PŘIPOJENÍ
Stínění datových paketů

AKTIVNÍ
OCHRANA PROTI ÚNIKŮM
Ochrana proti únikům DNS a IPv6

Vítejte! Tento balíček aktivit vás provede podnikovými sítěmi VPN. Prozkoumáte architektury Zero Trust, dedikované statické IP brány, administrátorské konzole, provisioning a site-to-site tunely IPsec.

KONTROLNÍ BODY PRACOVNÍHO LISTU

- [ ] **Část 1-4: Zvládněte konfigurace VPN a zabezpečení sítě.**
- [ ] **Část 5-7: Vyřešte křížovku a osmisměrku.**
- [ ] **Část 8-9: Vyřešte případové studie a šifrovací výzvu.**
- [ ] **Část 10: Projděte si stránky se základními i pokročilými FAQ.**
- [ ] **Část 11: Prozkoumejte 10 zajímavých faktů z praxe.**
- [ ] **Bonus: výzva Mysli rychle.**

Otevřete průvodce nejlepšími VPN od VPN.com

URL: https://www.vpn.com/cs/vpn/nejlepsi-vpn-pro-firmy/enterprise/

Váš studijní plán: podniková síť VPN

- Zavést rámce Zero Trust Network Access (ZTNA).
- Nakonfigurujte IP adresy bran dedikovaných serverů pro whitelistové filtry.
- Spravujte centralizované firemní administrátorské panely a seznamy uživatelských licencí.
- Proveďte audit logů přístupu k síti a historie připojení uživatelů.
- Nakonfigurujte jednotné přihlášení (SSO) a pravidla vícefaktorové autentizace.
- Nastavte site-to-site tunely IPsec mezi pobočkami.

PODNIKOVÉ VPN SÍTĚ – POKYNY K PRŮVODCI

Odpovězte na otázky s výběrem odpovědí a otázky pravda/nepravda, doplňte věty s vynechanými slovy pomocí banky slov, přiřaďte definice a vyřešte křížovku a osmisměrku. Uplatněte své znalosti na Zero Trust a site-to-site IPsec. Zakončete bonusovou aktivitou Mysli rychle.

ARCHITEKTURY ZERO TRUST A DEDIKOVANÉ BRÁNY (ÚVOD)

Podnikové VPN zabezpečují firemní aktiva přechodem na rámce Zero Trust Network Access (ZTNA) a whitelistováním dedikovaných statických IP bran. IT manažeři využívají centralizované administrátorské konzole k orchestraci site-to-site IPsec tunelů a propojení jednotného přihlášení (SSO).

PŘEČTĚTE SI POZORNĚ KAŽDÝ KONTROLNÍ BOD A VYBERTE NEBO NAPIŠTE SPRÁVNOU ODPOVĚĎ.

Kontrolní bod 1: Výzva s výběrem odpovědí

1. **1. Jaký bezpečnostní model nahrazuje starší podnikové VPN?**
   - A) Zero Trust
   - B) Multi-hop
   - C) Peer-to-peer
   - D) Jediná brána

2. **2. Jaká funkce je potřebná k omezení přístupu k databázi na firemní servery?**
   - A) Vyhrazená IP
   - B) Dynamické směrování
   - C) Rozdělený tunel
   - D) DNS proxy

3. **3. Jaký protokol je standardem pro firemní site-to-site tunely?**
   - A) IPsec
   - B) PPTP
   - C) SOCKS5
   - D) SSL v3

4. **4. Jaký centrální nástroj umožňuje administrátorům spravovat místa zaměstnanců?**
   - A) Administrátorská konzole
   - B) Klíč registru
   - C) Firmware routeru
   - D) Systémový log

5. **5. Jaký autentizační standard umožňuje přihlášení přes Okta nebo Microsoft Entra ID?**
   - A) Single Sign-On
   - B) Sdílené tajemství
   - C) Autentizace EPP
   - D) Klíč WEP

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. Zero Trust Network Access uděluje vstup do sítě až po ověření průběžné důvěryhodnosti zařízení.

○ Pravda ○ Nepravda

7 Otázka 7

7. Brány s dedikovanou IP směrují provoz zaměstnanců společně s náhodnými veřejnými spotřebiteli.

○ Pravda ○ Nepravda

8 Otázka 8

8. Centralizované administrátorské konzole umožňují IT manažerům okamžitě odebrat licence jednotlivým zaměstnancům.

○ Pravda ○ Nepravda

9 Otázka 9

9. IPsec je odlehčený protokol, který nepodporuje síťové tunely site-to-site.

○ Pravda ○ Nepravda

10 Otázka 10

10. Single Sign-On umožňuje bezpečnou autentizaci zaměstnanců pomocí firemních poskytovatelů identity.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

Přečtěte si každou větu níže a doplňte do vynechaného místa správný termín ze slovní banky.

1. Moderní bezpečnostní architektury nahrazují starší tunely přístupem zvaným _____ .
2. K omezení přístupu k databázi slouží brána, které je přidělena _____ .
3. Pobočky se bezpečně propojují site-to-site tunely postavenými na protokolu _____ .
4. Uživatelské licence zaměstnanců přidělují IT administrátoři v centrálním rozhraní zvaném _____ .
5. Integrace se službou Okta umožňuje zaměstnancům přihlášení metodou _____ .
6. Podnikové portály chrání přihlášení tím, že vyžadují ověřování, které je _____ .

ZÁSOBNÍK SLOV

ADMINISTRÁTORSKÁ KONZOLE BRÁNA IPSEC PŘIDĚLOVÁNÍ SINGLE SIGN-ON
VÍCEFAKTOROVÉ VYHRAZENÁ IP ADRESA ZERO TRUST

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování klíčových pojmů

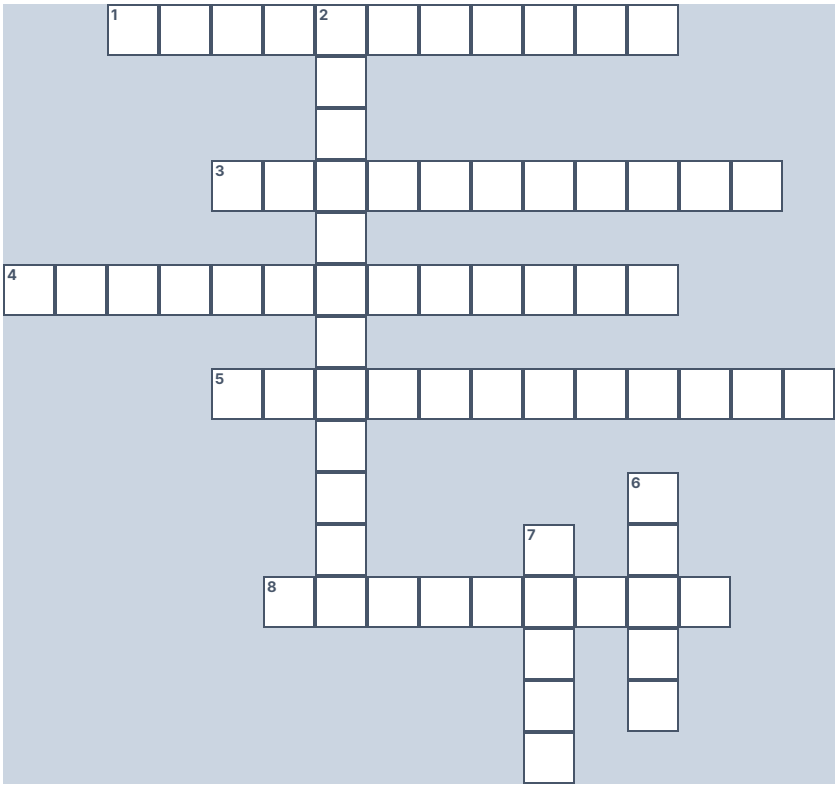
PŘIŘAZOVÁNÍ DEFINIC

Přiřaďte každý slovníčkový pojem vlevo k jeho správné definici vpravo zapsáním odpovídajícího písmene (A–H) do vyplnitelného pole.

☐	1. ZERO TRUST	A	Přidělování licencí VPN přístupu zaměstnancům.
☐	2. VYHRAZENÁ IP ADRESA	B	Propojení identity Okta a Entra ID.
☐	3. IPSEC	C	Zabezpečení přihlášení vyžadující dodatečné tokeny.
☐	4. ADMINISTRÁTORSKÁ KONZOLE	D	Statická adresa brány na whitelistu.
☐	5. SINGLE SIGN-ON	E	Standard site-to-site tunelů.
☐	6. VÍCEFAKTOROVÉ	F	Vstupní směrovací uzel sítě.
☐	7. VPN BRÁNA	G	Centrální portál IT manažera pro správu seatů.
☐	8. ZŘÍDIT	H	Rámec nepřetržitého ověřování důvěry.

Kontrolní bod 5: Křížovka

Vyřešte křížovku zapisováním písmen do aktivních bílých políček. Čísla odpovídají nápovědám níže.



VODOROVNÉ NÁPOVĚDY

1. Statická adresa brány pro povolené seznamy (11)

3. Přidělování licencí VPN přístupu zaměstnancům (11)

4. Zabezpečení přihlášení vyžadující další tokeny (13)

5. Propojení identity přes Okta a Entra ID (12)

8. Rámec průběžného ověřování důvěry (9)

SVISLÉ NÁPOVĚDY

2. Centrální portál IT správce pro správu licencí (12)

6. Standard pro site-to-site tunely (5)

7. Směrovací uzel na vstupu do sítě (5)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

Uživatelé čteček obrazovky a klávesnice mohou odpovědi křížovky zapisovat přímo do textových polí níže.

VODOROVNÉ NÁPOVĚDY

1 vodorovně: Statická adresa brány pro povolené seznamy (11 písmen):

3 vodorovně: Přidělování licencí VPN přístupu zaměstnancům (11 písmen):

4 vodorovně: Zabezpečení přihlášení vyžadující další tokeny (13 písmen):

5 vodorovně: Propojení identity přes Okta a Entra ID (12 písmen):

8 vodorovně: Rámec průběžného ověřování důvěry (9 písmen):

SVISLÉ NÁPOVĚDY

2 svisle: Centrální portál IT správce pro správu licencí (12 písmen):

6 svisle: Standard pro site-to-site tunely (5 písmen):

7 svisle: Směrovací uzel na vstupu do sítě (5 písmen):

Kontrolní bod 6: Hledání skrytých slov

Najděte 8 klíčových pojmů skrytých v mřížce níže. Slova mohou být vodorovně, svisle nebo úhlopříčně.

E K Ť Š V Ř Z E H E Š C A M R

L P I Á N E Z A R H Y V C I Ž

O N K V B R Á N A Š Ú Á P Š X

Z J N N G H Ň H S Ě L S Ť M S

N X H B Ú É Ý Ó Z X E T G Ť Y

O A Q Ú O O Z P H C R Ť H Q Ů

K U P Ú U K A E P Ň L Á O Ů Ě

N F R Ř X T S U R T O R E Z Ý

I J J Ů J Z W Y Q J I Ž I Í Ň

M Í N Á V O L Ě D I Ř P A E H

D V Í C E F A K T O R O V É Á

A T A J É W E K Ž K Ď L Ř Ň J

A Ě S I N G L E S I G N O N P

K O Č Ň C D G I B Á P S M Q V

U I Ý Ě Z Š F Y W H É S U Ó Ú

SEZNAM SLOV

ZEROTRUST VYHRAZENÁIP IPSEC ADMINKONZOLE SINGLESIGNON VÍCEFAKTOROVÉ BRÁNA PŘIDĚLOVÁNÍ

Kontrolní bod 6, alternativa: Přístupné přiřazování slovíček

Přiřaďte každý z 8 slovníčkových pojmů z osmisměrky k jeho správné definici zapsáním písmene (A–H) do prázdného pole.

POJMY SLOVNÍ ZÁSOBY
A. ZEROTRUST
B. VYHRAZENÁIP
C. IPSEC
D. ADMINKONZOLE
E. SINGLESIGNON
F. VÍCEFAKTOROVÉ
G. BRÁNA
H. PŘIDĚLOVÁNÍ

DEFINICE A POLE K PŘIŘAZENÍ
[ ] 1. Statická adresa brány pro povolené seznamy.
[ ] 2. Směrovací uzel na vstupu do sítě.
[ ] 3. Přidělování licencí VPN přístupu zaměstnancům.
[ ] 4. Zabezpečení přihlášení vyžadující další tokeny.
[ ] 5. Standard pro site-to-site tunely.
[ ] 6. Rámec průběžného ověřování důvěry.
[ ] 7. Propojení identity přes Okta a Entra ID.
[ ] 8. Centrální portál IT správce pro správu licencí.

Kontrolní bod 7: Výzva s přeházenými slovy

Přeuspořádejte písmena níže a odhalte klíčové pojmy a termíny z tohoto pracovního listu. Odpovědi pište do připravených polí.

1. RTOEZUSTR
2. ICESP
3. SIISOGNENLNG
4. ÁANBR
5. ÁYNEHPAZVIR
6. ENZOKLNADOMI
7. ROTAVÍOFÉVCKE
8. ÁOÍLIPĚŘNVD

Bonusová aktivita: Mysli rychle

3 ODPOVĚDI V KAŽDÉ KATEGORII. VYHRÁVÁ, KDO PRVNÍ VYPLNÍ CELÝ SEZNAM.

1	Nástroje, které firma používá každý den			
2	Věci, které VPN dokáže skrýt			
3	Role v IT oddělení			
4	Slova, která popisují Zero Trust			
5	Způsoby bezpečného přihlašování			
6	Důvody, proč dát zaměstnancům VPN			
7	Co udělat po bezpečnostním incidentu			
8	Důvody, proč používat VPN na cestách			
9	Pravidla bezpečné práce na dálku			
10	Data, která musí firma chránit			
11	Věci, které mohou narušit videoschůzku			
12	Zařízení, která mohou používat VPN			
13	Kancelářské programy, které znáte			
14	Místa, odkud zaměstnanci pracují			
15	Zařízení, která zaměstnanec může mít			

Kontrolní bod 8: Případové studie VPN a sítí

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: MIGRACE NA ZERO TRUST



Scénář: Podnik chce zabezpečit své lokální servery tím, že bude u zařízení průběžně ověřovat certifikáty shody, stav firewallu a polohu uživatele, místo aby důvěřoval komukoli uvnitř sítě.

Otázka k diskusi: Jaký rámec má ředitel IT bezpečnosti zavést, aby toho dosáhl?

PŘÍPADOVÁ STUDIE 2: OMEZENÍ BRÁNY



Scénář: Společnost hostuje soukromé finanční databáze v cloudu. Chce zablokovat veškerý veřejný přístup z internetu k administračním panelům a povolit přihlášení pouze z ověřených firemních koncových bodů.

Otázka k diskusi: Jakou síťovou konfiguraci má databázový administrátor nastavit na cloudovém firewallu?

Kontrolní bod 9: Dešifrování šifry

Síťový inženýr zabezpečuje směrovací kanály a klientské tunely. Pomocí níže uvedeného klíče písmeno–číslo dešifrujte zprávu zapsáním odpovídajících písmen do prázdných polí.

ŠIFROVACÍ KLÍČ PÍSMENO–ČÍSLO

A=1 Á=2 B=3 C=4 Č=5 D=6 Ď=7 E=8 É=9 Ě=10 F=11 G=12 H=13 I=14
Í=15 J=16 K=17 L=18 M=19 N=20 Ň=21 O=22 Ó=23 P=24 Q=25 R=26 Ř=27 S=28
Š=29 T=30 Ť=31 U=32 Ú=33 Ů=34 V=35 W=36 X=37 Y=38 Ý=39 Z=40 Ž=41

40	8	26	22		30	26	32	28	30		22	35	10	27	32	16	8

17	1	41	6	9		40	1	27	15	40	8	20	15		35		28	15	30	14

Dešifrovaná zpráva:

TIP: KAŽDÉ ČÍSLO PŘEDSTAVUJE POZICI DANÉHO PÍSMENE V ABECEDĚ (NAPŘ. 1 = A, 2 = B, 41 = Ž).

Kontrolní bod 10: Základní časté otázky k VPN (část A)

Projděte si nejčastější otázky a odpovědi o virtuálních privátních sítích (VPN) a tunelování.

Q1: Co je podniková VPN?

Zabezpečený síťový tunel určený pro firmy, který vzdáleným pracovníkům umožňuje přístup k firemním sítím s centralizovanou správou.

Q2: Čím se Zero Trust liší od tradičních VPN?

Tradiční VPN důvěřují každému uvnitř tunelu, zatímco Zero Trust nepřetržitě ověřuje každé zařízení a každé připojení uživatele.

Q3: Co je dedikovaná IP ve firemních VPN?

Statická IP adresa vyhrazená výhradně pro vaši firmu, kterou můžete přidat na povolený seznam pro bezpečný přístup ke cloudové databázi.

Q4: Proč je SSO důležité pro firemní VPN?

Single Sign-On umožňuje zaměstnancům bezpečně se přihlašovat pomocí firemních přihlašovacích údajů (např. Okta nebo Microsoft Entra ID).

Q5: Co je site-to-site VPN?

Tunel spojující dvě fyzické kanceláře (například pobočku a centrálu) přes veřejný internet pomocí IPsec.

Kontrolní bod 10: Základní časté otázky k VPN (část B)

Projděte si nejčastější otázky a odpovědi o virtuálních privátních sítích (VPN) a tunelování.

Q6: Jaká je funkce administrátorské konzole?

Řídicí panel pro IT administrátory umožňující přidávat nebo odebírat zaměstnanecká místa, přiřazovat brány a sledovat aktivní připojení.

Q7: Jak MFA zabezpečuje firemní VPN?

Vyžadováním sekundárního kódu (např. tokenu z ověřovací aplikace), aby se zabránilo neoprávněnému vstupu při kompromitovaných heslech.

Q8: Mohu auditovat historii připojení zaměstnanců?

Ano, podnikové VPN logují časové značky připojení, dobu trvání a přidělené IP pro účely auditu shody.

Q9: Co je ZTNA?

Zero Trust Network Access, bezpečnostní model, který uděluje přístup pouze ke konkrétním aplikacím, nikoli k celé síti.

Q10: Jaká je role vstupních uzlů (gateway)?

Slouží jako zabezpečené vstupní body pro vzdálený provoz a směrují data přímo na privátní firemní servery.

Kontrolní bod 10: Pokročilé časté otázky k VPN (část C)

Prozkoumejte pokročilé technické aspekty VPN tunelovacích protokolů, integrací mobilních klientů a podnikového nasazení.

Q1: Jak IPsec chrání korporátní komunikaci site-to-site?

IPsec šifruje provoz na síťové vrstvě pomocí Encapsulating Security Payload (ESP) k zajištění důvěrnosti a integrity dat.

Q2: Proč starší perimetrické zabezpečení u vzdálených týmů selhává?

Protože zaměstnanci přistupují k datům z více míst a zařízení, čímž se jediný perimetr síťového firewallu stává zastaralým.

Q3: Jak IT manažeři zavádějí automatizované zřizování účtů?

Mapováním protokolů SCIM mezi poskytovateli identit (Okta) a administrátorskou konzolí VPN k synchronizaci uživatelských adresářů.

Q4: Jaký je přínos split tunnelingu ve firemním prostředí?

Směruje místní SaaS provoz (jako Microsoft 365) mimo VPN tunel a šetří šířku pásma firemní brány pro privátní databáze.

Q5: Jak kontroly stavu zařízení ověřují zabezpečení koncových bodů?

VPN klient před připojením prohledá zařízení a ověří, že je aktivní firewall, běží antivirus a systém má aktuální záplaty.

Kontrolní bod 10: Pokročilé časté otázky k VPN (část D)

Prozkoumejte pokročilé technické aspekty VPN tunelovacích protokolů, integrací mobilních klientů a podnikového nasazení.

Q6: Jaká je role NAT traversal ve firemních VPN?

NAT-T zapouzdřuje pakety IPsec do UDP, aby prošly domácími routery a firewally bez výpadků připojení.

Q7: Jak firmy předcházejí škrcení šířky pásma na bráně?

Nasazením více regionálních uzlů bran a rozkládáním příchozího uživatelského provozu mezi ně pomocí load balancerů.

Q8: Proč se statické whitelisty IP upřednostňují před dynamickými?

Statické whitelisty brání neautorizovaným externím IP v pokusech o handshake připojení, čímž dramaticky zmenšují útočnou plochu.

Q9: Jaká je role certifikátového ověřování v podnikových VPN?

Ověřuje jedinečné digitální certifikáty nainstalované na firemně spravovaných zařízeních a blokuje nespravované osobní počítače.

Q10: Jak ZTNA snižuje riziko laterálního pohybu?

Izolací uživatelských relací na konkrétní autorizované zdroje, což hackerům brání v pohybu po síti při průniku do jednoho uzlu.

Část 11: 10 faktů a poznatků o VPN z praxe

Projděte si fakta z praxe o rychlostech VPN šifrování, auditech protokolů, mobilní konektivitě a podnikové práci na dálku.

1. VPN POSTŘEH

Architektury Zero Trust průběžně ověřují stav zabezpečení každého zařízení, které se pokouší o síťové připojení.

2. VPN POSTŘEH

Brány s dedikovanou IP umožňují firmám uzamknout cloudové databáze whitelistováním statických adres.

3. VPN POSTŘEH

IPsec je průmyslový standardní protokol pro konfiguraci zabezpečených tunelů site-to-site mezi kancelářskými sítěmi.

4. VPN POSTŘEH

Administrátorské konzole umožňují IT oddělením zřizovat, spravovat a auditovat přístupová místa zaměstnanců k VPN.

5. VPN POSTŘEH

Single Sign-On integruje přístup k VPN s firemními poskytovateli identity, jako jsou Okta a Entra ID.

6. VPN POSTŘEH

Vícefaktorové ověřování blokuje neoprávněné pokusy o připojení pocházející z ukradených hesel.

7. POSTŘEH K VPN

Split tunneling optimalizuje firemní šířku pásma vyloučením veřejného SaaS provozu ze šifrovaného tunelu.

8. POSTŘEH K VPN

Kontroly stavu zařízení ověřují místní bezpečnostní nastavení před udělením přístupu k firemním serverům.

9. POSTŘEH K VPN

Synchronizace adresáře SCIM automatizuje řízení přístupů při nástupu a odchodu zaměstnanců.

10. VPN POSTŘEH

Zero Trust Network Access omezuje přístup uživatelů na konkrétní povolené aplikace, čímž brání laterálnímu pohybu po síti.

Technické reference a zdroje

Studijní příručka a interaktivní hádanky jsou sestaveny z globálních technických standardů, specifikací a regulačních rámců.

AKADEMICKÉ A OBOROVÉ REFERENCE

[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/

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 **Zero Trust** ZTNA MODEL — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Modely Zero Trust průběžně ověřují shodu zařízení před vstupem do sítě.

2 **Dedikovaná IP** STATICKÁ IP — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Dedikované IP adresy umožňují whitelistovacím branám blokovat veřejný provoz.

3 **Standard IPsec** TUNEL IPSEC — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

IPsec je standardní protokol používaný pro tunely site-to-site mezi pobočkami.

4 **Přidělení IT** ADMINISTRÁTORSKÁ KONZOLE — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Centralizované administrátorské řídicí panely umožňují IT manažerům přidělovat licence (seaty).

5 **Otázka 5** — Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

Jaký autentizační standard umožňuje přihlášení přes Okta nebo Microsoft Entra ID? → Single Sign-On

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Zero Trust** ZTNA CHECKS — Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

Modely Zero Trust průběžně ověřují shodu zařízení před vstupem do sítě.

7 **Otázka 7** — Správná odpověď: Nepravda

POZNÁMKA PRO VYUČUJÍCÍ

Dedikované IP jsou vyhrazeny jedné firmě, takže se její provoz nemíchá s ostatními uživateli.

8 **Přidělení IT** ADMINISTRÁTORSKÉ MÍSTO IT — Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

Centralizované administrátorské řídicí panely umožňují IT manažerům přidělovat licence (seaty).

9 **Standard IPsec** SITE-TO-SITE — Správná odpověď: Nepravda

POZNÁMKA PRO VYUČUJÍCÍ

IPsec je standardní protokol používaný pro tunely site-to-site mezi pobočkami.

10 **Odkaz Okta SSO** PŘIHLÁŠENÍ SSO — Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

Single Sign-On integruje přihlašování k VPN s firemními adresáři, jako je Okta.

Klíče slovní zásoby a hodnoticí rubrika

Hodnoticí rubrika pro vyučující: Udělte 1 bod za každé správné přiřazení (celkem 8 bodů) a kontextový termín (celkem 6 bodů).

KONTROLNÍ BOD 4: KLÍČ K PŘIŘAZOVÁNÍ POJMŮ

H 1. ZERO TRUST	D 2. VYHRAZENÁ IP ADRESA	E 3. IPSEC	G 4. ADMINISTRÁTORSKÁ KONZOLE
B 5. SINGLE SIGN-ON	C 6. VÍCEFAKTOROVÉ	F 7. VPN BRÁNA	A 8. ZŘÍDIT

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 ZERO TRUST	2 VYHRAZENÁ IP ADRESA	3 IPSEC	4 ADMINISTRÁTORSKÁ KONZOLE
5 SINGLE SIGN-ON	6 VÍCEFAKTOROVÉ		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 B – VYHRAZENÁIP	2 G – BRÁNA	3 H – PŘIDĚLOVÁNÍ	4 F – VÍCEFAKTOROVÉ
5 C – IPSEC	6 A – ZEROTRUST	7 E – SINGLESIGNON	8 D – ADMINKONZOLE

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy ZERO TRUST, VYHRAZENÁ IP ADRESA a IPSEC a ke každému uvést příklad.

Případové studie:
Požádejte studenty, aby svá doporučení zdůvodnili fakty z pracovního listu, nikoli domněnkami.

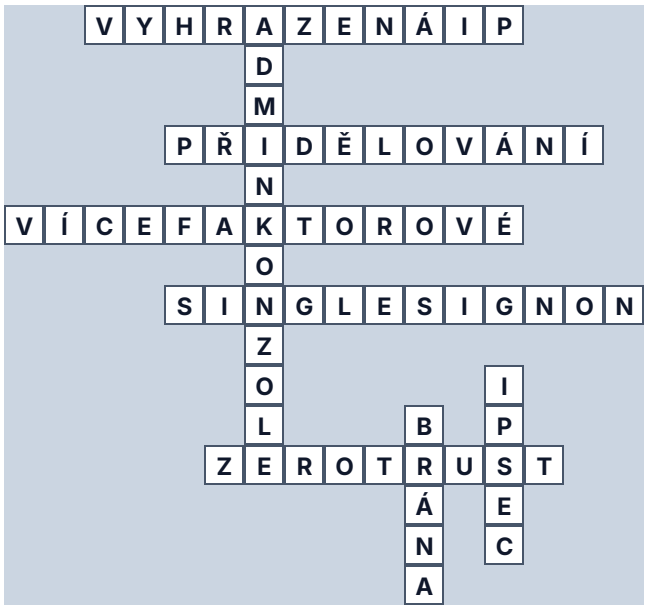
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

E	K	Ť	Š	V	Ř	Z	E	H	E	Š	C	A	M	R
L	P	I	Á	N	E	Z	A	R	H	Y	V	C	I	Ž
O	N	K	V	B	R	Á	N	A	Š	Ú	Á	P	Š	X
Z	J	N	N	G	H	Ň	H	S	Ě	L	S	Ť	M	S
N	X	H	B	Ú	É	Ý	Ó	Z	X	E	T	G	Ť	Y
O	A	Q	Ú	O	O	Z	P	H	C	R	Ť	H	Q	Ů
K	U	P	Ú	U	K	A	E	P	Ň	L	Á	O	Ů	Ě
N	F	R	Ř	X	T	S	U	R	T	O	R	E	Z	Ý
I	J	J	Ů	J	Z	W	Y	Q	J	I	Ž	I	Í	Ň
M	Í	N	Á	V	O	L	Ě	D	I	Ř	P	A	E	H
D	V	Í	C	E	F	A	K	T	O	R	O	V	É	Á
A	T	A	J	É	W	E	K	Ž	K	Ď	L	Ř	Ň	J
A	Ě	S	I	N	G	L	E	S	I	G	N	O	N	P
K	O	Č	Ň	C	D	G	I	B	Á	P	S	M	Q	V
U	I	Ý	Ě	Z	Š	F	Y	W	H	É	S	U	Ó	Ú

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

1 vodorovně: VYHRAZENÁIP Statická adresa brány pro povolené seznamy (11 písmen)

3 vodorovně: PŘIDĚLOVÁNÍ Přidělování licencí VPN přístupu zaměstnancům (11 písmen)

4 vodorovně: VÍCEFAKTOROVÉ Zabezpečení přihlášení vyžadující další tokeny (13 písmen)

5 vodorovně: SINGLESIGNON Propojení identity přes Okta a Entra ID (12 písmen)

8 vodorovně: ZEROTRUST Rámec průběžného ověřování důvěry (9 písmen)

SVISLÉ NÁPOVĚDY

2 svisle: ADMINKONZOLE Centrální portál IT správce pro správu licencí (12 písmen)

6 svisle: IPSEC Standard pro site-to-site tunely (5 písmen)

7 svisle: BRÁNA Směrovací uzel na vstupu do sítě (5 písmen)

Klíč řešení přesmyček a šifry

Klíč k hodnocení aktivity s přesmyčkami slovní zásoby a výzvy Tajná šifra.

KLÍČ K PŘESMYČKÁM

1.	RTOEZUSTR	ZEROTRUST	5.	ÁYNEHPAZVIR	VYHRAZENÁIP
2.	ICESP	IPSEC	6.	ENZOKLNADOMI	ADMINKONZOLE
3.	SIISOGNENLNG	SINGLESIGNON	7.	ROTAVÍOFÉVCKE	VÍCEFAKTOROVÉ
4.	ÁANBR	BRÁNA	8.	ÁOÍLIPĚŘNVD	PŘIDĚLOVÁNÍ

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"ZERO TRUST OVĚŘUJE KAŽDÉ ZAŘÍZENÍ V SÍTI"

Klíč k případovým studiím

A Případová studie 1: Migrace na Zero Trust

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Podnik chce zabezpečit své lokální servery průběžným ověřováním certifikátů souladu zařízení, stavu firewallu a polohy uživatele, místo aby důvěřoval komukoli uvnitř sítě.
- Doporučená strategie a řešení: Ředitel by měl přejít na model Zero Trust Network Access (ZTNA), který vynucuje průběžné kontextové bezpečnostní kontroly.

B Případová studie 2: Omezení brány

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Firma hostuje soukromé finanční databáze v cloudu. Chce zablokovat veškerý veřejný přístup z internetu k administračním panelům a povolit přihlášení jen z ověřených firemních koncových zařízení.
- Doporučená strategie a řešení: Správce by měl na podnikové VPN nastavit bránu s dedikovanou IP a tuto statickou adresu povolit na firewallu cloudové databáze.