Jméno: _____ Datum: _____ Body: _____

Nejlepší VPN pro firmy

Praktická recenze zabezpečení, škálovatelnosti a centrální správy firemní VPN.

PŘEHLED UČIVA NEJLEPŠÍ VPN PRO FIRMY

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 firemními VPN a sítěmi pro vzdálený přístup. Prozkoumáte architektury Zero Trust, site-to-site tunely IPsec, rámce SASE, vícefaktorová přihlášení a kontroly zabezpečení koncových bodů.

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/

Váš studijní plán: firemní VPN

- Určete nejlepší poskytovatele firemních VPN a jejich funkce zaměřené na týmy.
- Analyzujte rozdíly mezi soukromím spotřebitelských VPN a firemními administrativními kontrolami.
- Rozlište VPN pro vzdálený přístup a firemní tunely site-to-site.

POKYNY K PRŮVODCI FIREMNÍ VPN

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 podniková nastavení vzdáleného přístupu. Zakončete bonusovou aktivitou Mysli rychle.

PODNIKOVÝ VZDÁLENÝ PŘÍSTUP A SECURE EDGE (ÚVOD)

Zabezpečení firemního vzdáleného přístupu vyžaduje přechod od tradičních perimetrických modelů VPN k architekturám Zero Trust. Vynucování silné vícefaktorové autentizace (MFA) a rámců Secure Access Service Edge (SASE) chrání citlivá aktiva před kompromitovanými koncovými body.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1. **1. Jaký typ firemní VPN propojuje celé kancelářské sítě mezi sebou?**
   - A. Site-to-Site VPN
   - B. VPN pro vzdálený přístup
   - C. Spotřebitelská VPN
   - D. Smart DNS

2. **2. Která volba je zvýrazněna jako celkově nejlepší pro firemní týmy?**
   - A. NordLayer
   - B. Surfshark
   - C. Proton VPN
   - D. Private Internet Access

3. **3. Čemu předchází vyhrazená statická IP adresa u firemních týmů?**
   - A. Zařazení IP adresy na černou listinu
   - B. Rychlost routeru klesá
   - C. Komprese dat
   - D. Aktualizace klienta

4. **4. Který poskytovatel je zvýrazněn jako nejlepší pro dedikovanou infrastrukturu?**
   - A. Proton VPN
   - B. NordLayer
   - C. Surfshark
   - D. Private Internet Access

5. **5. Jaká funkce poskytuje centralizovaný administrátorský panel pro správu uživatelů?**
   - A. Administrátorské kontroly
   - B. Přesměrování portů
   - C. Emulace routeru
   - D. Split tunneling

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. VPN pro vzdálený přístup umožňují jednotlivým zaměstnancům připojit se odkudkoli.

○ Pravda ○ Nepravda

7 Otázka 7

7. Spotřebitelské VPN chrání celou organizaci pod jedním administrátorským panelem.

○ Pravda ○ Nepravda

8 Otázka 8

8. Dedikované IP adresy oddělují firemní provoz od veřejného.

○ Pravda ○ Nepravda

9 Otázka 9

9. Private Internet Access je zvýrazněna jako nejlepší pro velké podniky.

○ Pravda ○ Nepravda

10 Otázka 10

10. SASE integruje směrování WAN s bezpečnostními frameworky poskytovanými z cloudu.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. Nejlépe hodnoceným poskytovatelem pro firemní týmy je celkově _____ .
2. K propojení více firemních poboček slouží tunel typu _____ .
3. Aby adresa týmu neskončila na černé listině, nasazuje se _____ .
4. Oprávnění zařízení spravují administrátoři v centrálním rozhraní zvaném _____ .
5. Možnost dynamicky přidávat licence pro rostoucí týmy se nazývá _____ .
6. Splnění regulačních a auditních standardů pro data se označuje jako _____ .

ZÁSOBNÍK SLOV

BRÁNA DASHBOARD NORDLAYER SITE-TO-SITE SMĚROVÁNÍ
SOULAD S PŘEDPISY STATICKÁ IP ADRESA ŠKÁLOVATELNOST

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování klíčových pojmů

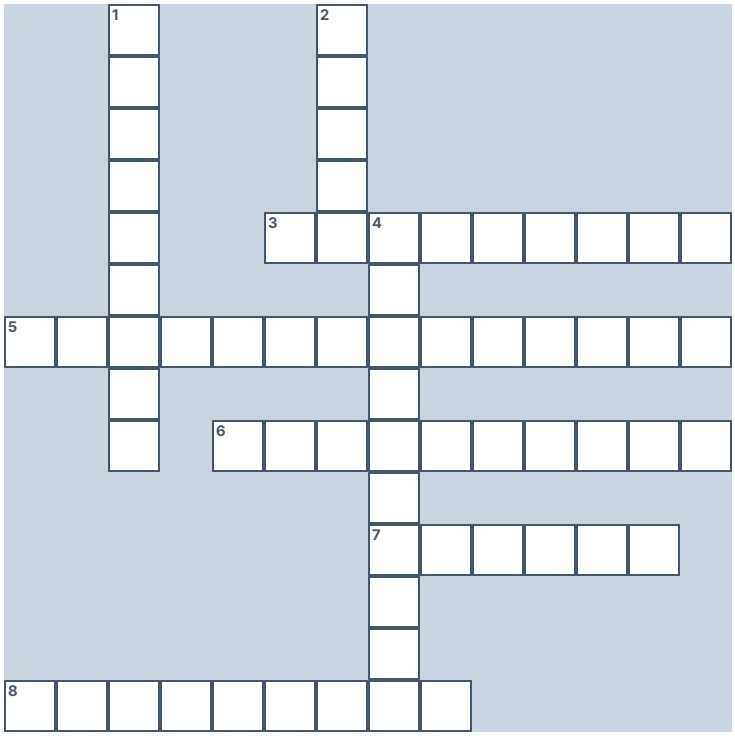
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. NORDLAYER	A	Dynamický růst týmu s více licencemi.
☐	2. SITE-TO-SITE	B	Nejlepší celková volba pro firmy.
☐	3. STATICKÁ IP ADRESA	C	Řízení provozu split tunnelingem.
☐	4. DASHBOARD	D	Regulatorní audit – standardní audit.
☐	5. ŠKÁLOVATELNOST	E	Vzdálený vstupní uzel pro ověřování.
☐	6. SOULAD S PŘEDPISY	F	Dedikovaná adresa mimo černé listiny.
☐	7. SMĚROVÁNÍ	G	Propojovací tunel kancelářských sítí.
☐	8. VPN BRÁNA	H	Centrální administrátorská řídicí konzole.

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

3. Centrální administrátorská ovládací konzole (9)

5. Dynamický růst týmů s více licencemi (14)

6. Vyhrazená adresa mimo černé listiny (10)

7. Standard regulatorních auditů (6)

8. Celkově nejlepší volba pro firmy (9)

SVISLÉ NÁPOVĚDY

1. Řízení provozu pomocí split tunnelingu (9)

2. Vstupní uzel pro ověřené vzdálené připojení (5)

4. Tunel propojující firemní pobočkové sítě (10)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

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

VODOROVNÉ NÁPOVĚDY

3 vodorovně: Centrální administrátorská ovládací konzole (9 písmen):

5 vodorovně: Dynamický růst týmů s více licencemi (14 písmen):

6 vodorovně: Vyhrazená adresa mimo černé listiny (10 písmen):

7 vodorovně: Standard regulatorních auditů (6 písmen):

8 vodorovně: Celkově nejlepší volba pro firmy (9 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Řízení provozu pomocí split tunnelingu (9 písmen):

2 svisle: Vstupní uzel pro ověřené vzdálené připojení (5 písmen):

4 svisle: Tunel propojující firemní pobočkové sítě (10 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

I D Š Ž T É Ř S Ů E A Á Ř P O

Q R U Y R J S T U Š N Č Ň Ý B

E A Ě Š X W Í A A S O Ž Ý Ý L

T O A F S I N T S J R N M Ť P

I B N G O R Ř I G Ž D Á Ó Ů Ě

S H Á Ú U C Ý C Š Ý L B G M Ž

O S R F L S J K Ó Q A O X C N

T A B Ž A M Z Á Ě Ý Y P W Ú L

E D Ů Q D Ě B I Ó V E Ť N F Ů

T Č Ý Ú K R S P Á X R Ž Y N Š

I Š K Á L O V A T E L N O S T

S R X H P V D Á Č J Ř V W X L

Í H U H Ě Á B E I K Ť Š V Ř Z

E H E Š C N A M R C Ž N K V Š

Ú Á Š X J Í N N G H Ň H S Ě L

SEZNAM SLOV

NORDLAYER SITETOSITE STATICKÁIP DASHBOARD ŠKÁLOVATELNOST
SOULAD SMĚROVÁNÍ BRÁNA

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. NORDLAYER
B. SITETOSITE
C. STATICKÁIP
D. DASHBOARD
E. ŠKÁLOVATELNOST
F. SOULAD
G. SMĚROVÁNÍ
H. BRÁNA

DEFINICE A POLE K PŘIŘAZENÍ
☐ 1. Řízení provozu pomocí split tunnelingu.
☐ 2. Centrální administrátorská ovládací konzole.
☐ 3. Vstupní uzel pro ověřené vzdálené připojení.
☐ 4. Vyhrazená adresa mimo černé listiny.
☐ 5. Standard regulatorních auditů.
☐ 6. Tunel propojující firemní pobočkové sítě.
☐ 7. Celkově nejlepší volba pro firmy.
☐ 8. Dynamický růst týmů s více licencemi.

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. **ALDONYERR**
2. **ITSTIPKÁCA**
3. **ŠEKSTTLNÁA OVOL**
4. **OÍNRÁVSMĚ**
5. **IOEIESTSTT**
6. **RHAAODBDS**
7. **ASLDUO**
8. **ABÁNR**

Bonusová aktivita: Mysli rychle

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

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

Kontrolní bod 8: Případové studie VPN a sítí

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: BLACKLISTING SDÍLENÉ VEŘEJNÉ IP



Scénář: Obchodní tým přistupuje k firemním databázím přes spotřebitelskou VPN, ale je zablokován, protože sdílenou výstupní IP zařadily systémy proti podvodům na černou listinu.

Otázka k diskusi: Navrhněte konfiguraci firemní infrastruktury VPN, která toto zablokování vyřeší.

PŘÍPADOVÁ STUDIE 2: PROPOJENÍ FIREMNÍCH POBOČEK



Scénář: Podniková společnost s kancelářemi v Mnichově a Bostonu potřebuje bezpečně sdílet místní souborové servery bez směrování provozu přes veřejný web.

Otázka k diskusi: Vyberte vhodnou topologii firemní VPN.

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

19	22	6	8	18	38		40	8	26	22		30	26	32	28	30
4	13	26	2	20	15		19	22	6	8	26	20	15			
11	14	26	8	19	20	15		28	15	30	10					

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 firemní VPN?

Zabezpečené síťové připojení umožňující vzdáleným pracovníkům a pobočkám bezpečný přístup k privátním firemním datům.

Q2: Jak se liší spotřebitelské a firemní VPN?

Spotřebitelské VPN skrývají osobní prohlížení; firemní VPN chrání firemní systémy pomocí centrálních administrátorských konzolí.

Q3: Co je Site-to-Site VPN?

Tunel, který vzájemně propojuje celé fyzické kancelářské sítě přes web.

Q4: Co je Remote Access VPN?

Tunel umožňující jednotlivým vzdáleným zaměstnancům bezpečné připojení k firemní síti.

Q5: Jaký je přínos dedikované statické IP?

Udržuje firemní provoz oddělený od veřejných fondů a předchází blacklistingu sdílených IP.

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

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

Q6: Který poskytovatel je nejlepší pro malé firmy?

Private Internet Access (PIA), známá cenovou dostupností pro malé týmy a jednoduchostí nastavení.

Q7: Která firemní VPN je celkově hodnocena jako #1?

NordLayer, ohodnocený VPN.com 92/100 za funkce a nástroje pro správu.

Q8: Co je týmová škálovatelnost u VPN?

Možnost dynamicky přidávat uživatelská místa, licence a brány s růstem firmy.

Q9: Proč je centrální správa klíčová?

Umožňuje administrátorům vynucovat bezpečnostní zásady a rušit přístup zaměstnanců v jediném panelu.

Q10: Co je SASE?

Secure Access Service Edge, který slučuje směrování WAN s bezpečnostními službami dodávanými z cloudu.

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 rozdělené tunelování zabezpečuje týmy?

Udržuje privátní SaaS provoz uvnitř zabezpečeného tunelu a veřejný webový přístup směruje lokálně.

Q2: Co Proton VPN nabízí firmám?

Infrastruktura dedikovaných serverů, hodnocení 88/100 od VPN.com (se sídlem ve Švýcarsku).

Q3: Jaké standardy souladu vyžadují VPN?

PCI DSS vyžaduje silné šifrování přes veřejné sítě; HIPAA a GDPR je očekávají jako ochranné opatření.

Q4: Lze firemní VPN provozovat na routerech?

Ano, konfigurace VPN tunelů na routerech chrání všechna kancelářská zařízení automaticky.

Q5: Co je vícefaktorové ověřování?

Vyžadování více údajů (jako čipových karet nebo SMS kódů) k ověření přihlášení.

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

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

Q6: Proč se sdílené IP adresy dostávají na černé listiny?

Protože je sdílejí tisíce uživatelů, z nichž někteří mohou provádět škodlivé činy.

Q7: Jak brána ověřuje uživatele?

Ověřováním klientských certifikátů, hesel a vícefaktorových kódů proti aktivním adresářům.

Q8: Co Surfshark nabízí týmům?

Nejlepší volba VPN.com pro bezpečnostní balíčky, hodnocení 84/100, se servery pouze v RAM.

Q9: Jak se auditují připojení k firemní VPN?

Kontrolou logů připojení, metrik využití dat a historie přihlášení v administrátorské konzoli.

Q10: Co je řízení přístupu Zero Trust?

Paradigma, kdy jsou všechna zařízení považována za nedůvěryhodná a každá relace vyžaduje ověření.

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

Firemní VPN šifruje provoz a chrání podnikové systémy před odposlechem ve veřejné síti.

2. VPN POSTŘEH

Site-to-Site VPN bezpečně propojují celé pobočkové sítě, aniž by vystavovaly lokální hostitele.

3. VPN POSTŘEH

Spotřebitelské VPN maskují osobní prohlížení, zatímco firemní VPN chrání brány podnikových prostředků.

4. VPN POSTŘEH

VPN.com hodnotí NordLayer 92/100, jako svou nejlepší celkovou firemní VPN.

5. VPN POSTŘEH

VPN.com hodnotí Proton VPN 88/100 a označuje jej za nejlepší pro dedikovanou infrastrukturu.

6. VPN POSTŘEH

VPN.com hodnotí Private Internet Access 76/100 a řadí jej jako nejlepší pro malé firemní týmy.

7. POSTŘEH K VPN

Centrální administrátorské řídicí panely umožňují bezpečnostním pracovníkům spravovat uživatelská oprávnění a pravidla přístupu.

8. POSTŘEH K VPN

Dedikované statické IP adresy brání tomu, aby týmy blokovaly antifraud systémy kvůli sdíleným IP.

9. POSTŘEH K VPN

GDPR uvádí šifrování jako vhodné opatření k ochraně osobních údajů.

10. VPN POSTŘEH

Architektury Zero Trust ověřují všechny vzdálené koncové body bez ohledu na polohu nebo přihlašovací údaje.

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 **Topologie tunelu** SITE-TO-SITE — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Site-to-Site VPN bezpečně propojují celé vzdálené pobočky mezi sebou.

2 **Otázka 2** — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

VPN.com hodnotí NordLayer 92/100 a řadí ho jako celkově nejlepší pro firemní týmy.

3 **Whitelisting IP adres** DEDIKOVANÁ IP — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Dedikované statické IP brání tomu, aby se týmy ocitly zablokované kvůli černým listinám sdílených IP.

4 **Otázka 4** — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

VPN.com hodnotí Proton VPN 88/100 a označuje ho za nejlepší pro dedikovanou infrastrukturu.

5 **Centrální konzole** ADMINISTRÁTORSKÉ KONTROLY — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Centralizované panely umožňují bezpečnostním pracovníkům spravovat uživatelská oprávnění a seaty.

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Vzdálená připojení** VZDÁLENÝ PŘÍSTUP — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

VPN pro vzdálený přístup umožňují jednotlivým vzdáleným pracovníkům připojit se k privátním serverům.

7 **Podnikové tunely** SPOTŘEBITELSKÉ LIMITY — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Spotřebitelské VPN postrádají centralizované administrátorské řízení a nejsou vhodné pro organizační audity.

8 **Izolace brány** DEDIKOVANÝ TUNEL — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Dedikované IP izolují firemní provoz od veřejného šumu a chrání tak databáze.

9 **Otázka 9** — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

VPN.com řadí PIA (76/100) jako nejlepší pro malé firmy, ne pro velké podniky.

10 **Bezpečnostní fúze** STANDARD SASE — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

SASE spojuje podnikové směrování WAN se zero-trust zabezpečením poskytovaným z cloudu.

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

B 1. NORDLAYER	G 2. SITE-TO-SITE	F 3. STATICKÁ IP ADRESA	H 4. DASHBOARD
A 5. ŠKÁLOVATELNOST	D 6. SOULAD S PŘEDPISY	C 7. SMĚROVÁNÍ	E 8. VPN BRÁNA

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 NORDLAYER	2 SITE-TO-SITE	3 STATICKÁ IP ADRESA	4 DASHBOARD
5 ŠKÁLOVATELNOST	6 SOULAD S PŘEDPISY		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 G – SMĚROVÁNÍ	2 D – DASHBOARD	3 H – BRÁNA	4 C – STATICKÁIP
5 F – SOULAD	6 B – SITETOSITE	7 A – NORDLAYER	8 E – ŠKÁLOVATELNOST

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy NORDLAYER, SITE-TO-SITE a STATICKÁ IP ADRESA a ke každému uvést příklad.

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

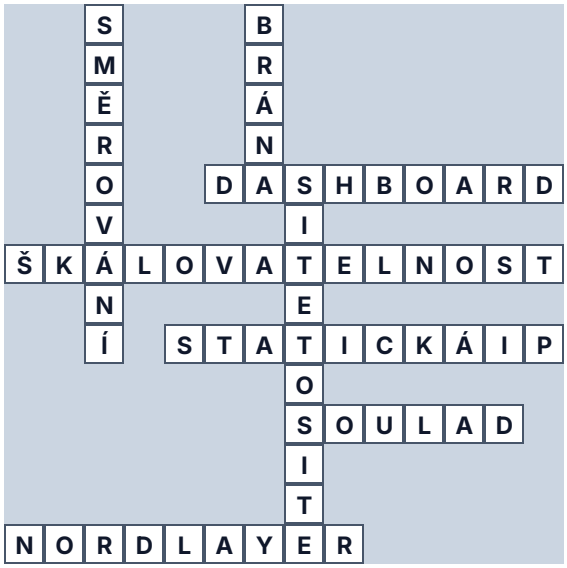
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

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

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

3 vodorovně: DASHBOARD Centrální administrátorská ovládací konzole (9 písmen)

5 vodorovně: ŠKÁLOVATELNOST Dynamický růst týmů s více licencemi (14 písmen)

6 vodorovně: STATICKÁIP Vyhrazená adresa mimo černé listiny (10 písmen)

7 vodorovně: SOULAD Standard regulatorních auditů (6 písmen)

8 vodorovně: NORDLAYER Celkově nejlepší volba pro firmy (9 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: SMĚROVÁNÍ Řízení provozu pomocí split tunnelingu (9 písmen)

2 svisle: BRÁNA Vstupní uzel pro ověřené vzdálené připojení (5 písmen)

4 svisle: SITETOSITE Tunel propojující firemní pobočkové sítě (10 písmen)

Klíč řešení přesmyček a šifry

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

KLÍČ K PŘESMYČKÁM

1. ALDONYERR — NORDLAYER
2. ITSTIPKÁCA — STATICKÁIP
3. ŠEKSTTLNÁAOVOL — ŠKÁLOVATELNOST
4. OÍNRÁVSMĚ — SMĚROVÁNÍ
5. IOEIESTSTT — SITETOSITE
6. RHAAODBDS — DASHBOARD
7. ASLDUO — SOULAD
8. ABÁNR — BRÁNA

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"MODELY ZERO TRUST CHRÁNÍ MODERNÍ FIREMNÍ SÍTĚ"

Klíč k případovým studiím

A Případová studie 1: Blacklisting sdílené veřejné IP

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Obchodní tým přistupuje k firemním databázím přes spotřebitelskou VPN, ale je odříznut, protože sdílená výstupní IP byla zablokována antifraudovými systémy.
- Doporučená strategie a řešení: Nasaďte dedikované firemní servery se statickou IP adresou, aby se firemní provoz oddělil od veřejných poolů.

B Případová studie 2: Propojení firemních poboček

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Podnik s kancelářemi v Mnichově a Bostonu potřebuje bezpečně sdílet lokální souborové servery bez směrování provozu přes veřejné webové prostory.
- Doporučená strategie a řešení: Nakonfigurujte Site-to-Site VPN tunel, který obě lokální kancelářské sítě bezpečně propojí přes internet.