Jméno: _____ Datum: _____ Body: _____

Průvodce nejbezpečnější VPN

Technická analýza návrhu vysoce bezpečných VPN, RAM-only servery s volatilní pamětí, přístupové zabezpečení Zero Trust, privátní šifrované obrany proti únikům DNS a auditované konfigurace WireGuard.

PRŮVODCE NEJBEZPEČNĚJŠÍ VPN – 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 technickými standardy vysoce bezpečných VPN. Prozkoumáte serverový hardware jen s RAM, přístupové zabezpečení Zero Trust, soukromé šifrované resolvery DNS a auditované konfigurace WireGuard.

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/nejbezpecnejsi-vpn/

Váš studijní plán: nejbezpečnější VPN

- Analyzujte technickou architekturu a šifrovací standardy průvodce nejbezpečnější VPN.
- Nakonfigurujte nastavení klienta tak, aby bránilo únikům IP, DNS a WebRTC provozu.
- Porovnejte proprietární tunelovací protokoly se standardními implementacemi.

PRŮVODCE NEJBEZPEČNĚJŠÍ VPN – POKYNY

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 serverový hardware RAM-Only a systémy Zero Trust. Zakončete bonusovou aktivitou Mysli rychle.

RAM-ONLY INFRASTRUKTURY A SÍTĚ ZERO TRUST (ÚVOD)

Skutečně bezpečná VPN se opírá o rámec zero trust, servery pouze v RAM, které brání tomu, aby zabavení disků odhalilo logy, privátní šifrované resolvery DNS a auditované protokoly jako WireGuard. Tyto kombinované kontroly brání cenná digitální aktiva před hrozbami odposlechu.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1. **1. Jaká architektura je zásadní pro zajištění nejvyšší bezpečnosti moderních VPN serverů?**
   - A) Serverová infrastruktura pouze v RAM
   - B) Diskové úložiště
   - C) Dynamické směrování DNS
   - D) Povolení přesměrování portů

2. **2. Jaký protokol je široce doporučován pro nejbezpečnější a nejmodernější konfigurace VPN?**
   - A) WireGuard
   - B) PPTP
   - C) L2TP/IPSec
   - D) SSTP

3. **3. Jaký bezpečnostní rámec vyžaduje nepřetržité ověřování každého připojení bez výjimky?**
   - A) Architektura Zero Trust
   - B) Perimetrové firewally
   - C) Dynamické směrování
   - D) Sdílené tajné klíče

4. **4. Jaká je primární role ochrany proti únikům DNS ve VPN klientovi?**
   - A) Směrovat všechny požadavky DNS přes privátní šifrované resolvery
   - B) Obfuskovat IP pakety
   - C) Místní kešování dotazů DNS
   - D) Zakázat jmenné servery

5. **5. Jak vícehopové směrování (Multi-Hop) zvyšuje celkové zabezpečení VPN tunelu?**
   - A) Směruje data přes dva samostatné servery za sebou
   - B) Zvyšuje rychlost komprese
   - C) Šifruje data slabými šiframi
   - D) Obchází firewally

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. RAM-Only servery ukládají soubory logů do dočasné paměti, která se při restartu vymaže.

○ Pravda ○ Nepravda

7 Otázka 7

7. WireGuard používá moderní kryptografické algoritmy, které jsou méně náchylné k rychlostním úzkým hrdlům.

○ Pravda ○ Nepravda

8 Otázka 8

8. Kill switch VPN funguje tak, že blokuje veškerý síťový provoz, pokud tunel vypadne.

○ Pravda ○ Nepravda

9 Otázka 9

9. Nezávislé audity třetích stran jsou pro ověření bezpečnostních závazků irelevantní.

○ Pravda ○ Nepravda

10 Otázka 10

10. Modely Zero Trust předpokládají, že všechna interní síťová připojení jsou ve výchozím stavu bezpečná.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. Administrátoři vynucují bezpečnost nasazením přísného rámce _____ .
2. Směrování paketů přes více vstupních bodů umožňuje zabezpečená konfigurace _____ .
3. Únikům dat z ukradených disků brání návrh označovaný jako _____ .
4. Únosy překladu jmen ze strany ISP zmírňuje nativní _____ .
5. K blokování provozu při výpadku připojení slouží mechanismus zvaný _____ .
6. K minimalizaci ukládaných logů zvolte poskytovatele, který provozuje plně _____ .

ZÁSOBNÍK SLOV

AUDITOVANÝ SYSTÉM | KILL SWITCH | MULTI-HOP | OCHRANA DNS | PROTOKOL | RAM-ONLY SERVER | ŠIFROVÁNÍ | ZERO TRUST

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování pojmů VPN a sítí

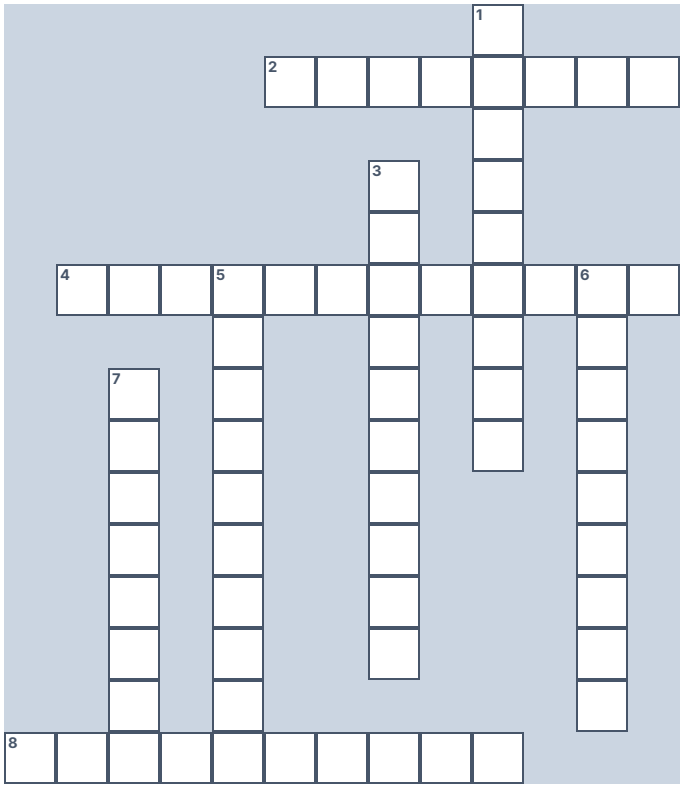
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. Zero Trust	A	Nezávisle prověřené nastavení potvrzující, že nejsou ukládány žádné logy.
☐	2. Multi-Hop	B	Kryptografické zamíchání datového obsahu k zabezpečení přenosu.
☐	3. RAM-Only server	C	Bezpečnostní rámec vyžadující nepřetržitou autentizaci všech uživatelů.
☐	4. Ochrana DNS	D	Soubor technických pravidel určujících, jak jsou data balena a odesílána.
☐	5. Kill Switch	E	Kaskádové VPN směrování, které řetězí dva serverové uzly za sebou.
☐	6. Auditovaný systém	F	Serverová architektura využívající volatilní paměť k ukládání datových payloadů.
☐	7. Šifrování	G	Vynucování soukromých dotazů DNS k ochraně vyhledávání na jmenných serverech.
☐	8. Protokol	H	Pojistný mechanismus, který blokuje provoz, pokud VPN selže.

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

2. Kaskádové VPN směrování řetězící dva serverové uzly za sebou (8)

4. Bezpečnostní rámec vyžadující nepřetržité ověřování všech uživatelů (12)

8. Pojistný mechanismus blokující provoz při výpadku VPN (10)

SVISLÉ NÁPOVĚDY

1. Kryptografické šifrování datových zátěží pro zabezpečení přenosu (9)

3. Nezávisle prověřené nastavení potvrzující, že se neukládají žádné logy (10)

5. Vynucení soukromých DNS dotazů k ochraně vyhledávání jmenných serverů (10)

6. Serverová architektura využívající volatilní paměť k ukládání datových zátěží (9)

7. Soubor technických pravidel určujících, jak jsou data balena a odesílána (8)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

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

VODOROVNÉ NÁPOVĚDY

2 vodorovně: Kaskádové VPN směrování řetězící dva serverové uzly za sebou (8 písmen):

4 vodorovně: Bezpečnostní rámec vyžadující nepřetržité ověřování všech uživatelů (12 písmen):

8 vodorovně: Pojistný mechanismus blokující provoz při výpadku VPN (10 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Kryptografické šifrování datových zátěží pro zabezpečení přenosu (9 písmen):

3 svisle: Nezávisle prověřené nastavení potvrzující, že se neukládají žádné logy (10 písmen):

5 svisle: Vynucení soukromých DNS dotazů k ochraně vyhledávání jmenných serverů (10 písmen):

6 svisle: Serverová architektura využívající volatilní paměť k ukládání datových zátěží (9 písmen):

7 svisle: Soubor technických pravidel určujících, jak jsou data balena a odesílána (8 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

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

SEZNAM SLOV

NULOVÁDŮVĚRA
MULTIHOP AUDITOVANÝ
RAMSERVER ŠIFROVÁNÍ
OCHRANADNS PROTOKOL
KILLSWITCH

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. NULOVÁDŮVĚRA**
- **B. MULTIHOP**
- **C. RAMSERVER**
- **D. OCHRANADNS**
- **E. KILLSWITCH**
- **F. AUDITOVANÝ**
- **G. ŠIFROVÁNÍ**
- **H. PROTOKOL**

DEFINICE A POLE K PŘIŘAZENÍ

_____ 1. Pojistný mechanismus blokující provoz při výpadku VPN.

_____ 2. Vynucení soukromých DNS dotazů k ochraně vyhledávání jmenných serverů.

_____ 3. Kaskádové VPN směrování řetězící dva serverové uzly za sebou.

_____ 4. Soubor technických pravidel určujících, jak jsou data balena a odesílána.

_____ 5. Kryptografické šifrování datových zátěží pro zabezpečení přenosu.

_____ 6. Serverová architektura využívající volatilní paměť k ukládání datových zátěží.

_____ 7. Nezávisle prověřené nastavení potvrzující, že se neukládají žádné logy.

_____ 8. Bezpečnostní rámec vyžadující nepřetržité ověřování všech uživatelů.

Kontrolní bod 7: Výzva s přeházenými slovy

Přeuspořádejte písmena níže a odhalte klíčové pojmy a termíny virtuální privátní sítě (VPN). Odpovědi pište do připravených polí.

1. V Á Ů V U D Ě N R L A O
2. R R E S A R V E M
3. K W C I I S H L T L
4. O Í N R Á V Š I F
5. I H U P T M O L
6. N A R A D O C N S H
7. U I A V O A N Ý T D
8. T R O L P O K O

Bonusová aktivita: Mysli rychle

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

1	Zámky nebo klíče, které používáte každý den			
2	Věci, které VPN dokáže skrýt			
3	Věci, díky kterým je VPN bezpečná			
4	Mýty o VPN			
5	Důvody, proč používat VPN na cestách			
6	Bezpečná místa ve skutečném světě			
7	Slova, která znamenají „chráněný“			
8	Sliby, které dává dobrý poskytovatel VPN			
9	Slova související se soukromím			
10	Typy auditů nebo kontrol			
11	Slova z tohoto pracovního listu, která si chcete zapamatovat			
12	Věci, které chce hacker ukrást			
13	Způsoby, jak poznat falešnou Wi-Fi síť			
14	Místa, kde byste použili VPN			
15	Věci, které vidí váš poskytovatel internetu			

Kontrolní bod 8: Případové studie VPN a sítí

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: ZODOLNĚNÍ PODNIKOVÉ INFRASTRUKTURY



Scénář: Firemní banka přepracovává topologii svého vzdáleného přístupu. Vyžaduje architekturu zero trust propojující všechna klientská zařízení se zabezpečenými servery.

Otázka k diskusi: Jaký je hlavní přínos mikrosegmentace sítě v rámci modelu VPN Zero Trust?

PŘÍPADOVÁ STUDIE 2: OCHRANY SERVERŮ POUZE V RAM



Scénář: Na bezpečnost zaměřený poskytovatel VPN upgraduje své servery, aby zabránil tomu, že fyzické zabavení serveru odhalí historii uživatelských logů.

Otázka k diskusi: Vysvětlete, jak hardwarové konfigurace pouze s RAM brání forenzní extrakci dat při fyzickém zabavení serverů.

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

3 8 40 24 8 5 20 9 35 24 20 4 13 26 2 20 15

4 8 20 20 2 6 14 12 14 30 2 18 20 15

1 17 30 14 35 1

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 dělá VPN 'nejbezpečnější'?

Kombinace Zero Trust, serverů pouze v RAM a auditovaných protokolů.

Q2: Co jsou servery pouze v RAM?

Servery běžící ve volatilní paměti, navržené tak, aby na disk neukládaly žádné logy.

Q3: Co je Zero Trust VPN?

Rámec, který průběžně ověřuje každý požadavek na přístup a každé připojení.

Q4: Proč je WireGuard považován za bezpečný?

Má malou, snadno auditovatelnou kódovou základnu a používá moderní šifry.

Q5: Jak bezpečné VPN zabraňují únikům DNS?

Směrováním všech dotazů přes privátní, šifrované DNS resolvery.

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

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

Q6: Vyžaduje bezpečná VPN audity?

Ano, nezávislé audity ověřují tvrzení o zero-logs i bezpečnost kódu.

Q7: Jaká je role kill switche?

Okamžitě zastaví síťový provoz, pokud VPN připojení spadne.

Q8: Jaké šifrování se používá v bezpečných VPN?

AES-256 a ChaCha20 jsou průmyslové standardy šifrování.

Q9: Je Multi-Hop směrování bezpečné?

Ano, řetězí dva nebo více serverů, aby zabránila analýze provozu.

Q10: Jak pomáhá offshorová jurisdikce?

Může omezit, které zákony se uplatní, ale neposkytuje žádnou absolutní imunitu.

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 servery pouze v RAM předcházejí rizikům zabavení dat?

Protože běží v RAM, vytažení ze zásuvky smaže data držená v paměti.

Q2: Jak Zero Trust nahrazuje standardní perimetrovou bezpečnost?

Považuje každého klienta za nepřátelského a vyžaduje průběžnou autentizaci.

Q3: Proč se kód WireGuard snáze audituje?

Jeho linuxový kód má méně než 4,000 řádků, výrazně méně než typické VPN stacky. [4]

Q4: Jak DNSSEC chrání DNS dotazy?

Podepisuje DNS záznamy, takže resolvery dokážou odhalit padělané nebo pozměněné odpovědi.

Q5: Jak Multi-Hop komplikuje korelaci provozu?

Oddělením příchozích a odchozích IP adres mezi různé hostingové poskytovatele.

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 jsou jurisdikce Five Eyes pro VPN rizikové?

Členské státy sdílejí zpravodajské informace a mohou pomocí právních příkazů požadovat data uživatelů.

Q7: Jak je kill switch implementován na úrovni jádra?

Používá systémová pravidla firewallu (jako iptables nebo WFP) k blokování odchozího provozu.

Q8: Co je forward secrecy při VPN handshake?

Generuje jedinečné klíče relace, takže minulé relace nelze dešifrovat.

Q9: Jak bezpečné VPN zmírňují úniky WebRTC?

Blokováním požadavků WebRTC nebo jejich směrováním skrz tunel.

Q10: Jak nezávislé audity zajišťují dodržování ochrany soukromí?

Auditoři provádějí penetrační testování a kontrolují konfigurace serverů.

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

RAM-only servery načítají operační systém do paměti při startu, takže po restartu nezůstává na disku nic.

2. VPN POSTŘEH

WireGuard používá framework Noise s Curve25519, ChaCha20, Poly1305, BLAKE2s a HKDF. [3]

3. VPN POSTŘEH

Zero Trust uděluje přístup podle jednotlivých zdrojů a nedává žádnou implicitní důvěru na základě umístění v síti (NIST SP 800-207). [1]

4. VPN POSTŘEH

Zpravodajská aliance Five Eyes zahrnuje USA, Spojené království, Kanadu, Austrálii a Nový Zéland.

5. VPN POSTŘEH

K únikům WebRTC dochází, když prohlížeče odhalí skutečnou veřejnou IP adresu klienta prostřednictvím dotazů STUN.

6. VPN POSTŘEH

Dokonalé dopředné utajení (PFS) zajišťuje, že kompromitace dlouhodobého klíče neodhalí minulé klíče relací. [3]

7. POSTŘEH K VPN

Cure53, bezpečnostní firma se sídlem v Berlíně, zveřejnila audity několika poskytovatelů VPN.

8. POSTŘEH K VPN

K únikům DNS dochází, když dotazy DNS obcházejí tunel VPN a míří na jmenné servery místního ISP.

9. POSTŘEH K VPN

Volatilní čipy RAM vyžadují k udržení dat stálé napájení a při vypnutí svůj obsah ztrácejí.

10. VPN POSTŘEH

Podnikové systémy Zero Trust vynucují kontroly stavu zařízení před povolením připojení k zabezpečeným zdrojům. [1]

Technické reference a zdroje

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

AKADEMICKÉ A OBOROVÉ REFERENCE

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

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[3] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[6] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 **RAM-Only server** RAM-ONLY **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

RAM-Only servery neukládají na disk žádné logy a data při restartu vymažou.

2 **Otázka 2** **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

WireGuard spojuje malou, auditovatelnou kódovou základnu s moderními šiframi.

3 **Model Zero Trust** ZERO TRUST **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Modely Zero Trust průběžně ověřují shodu zařízení před udělením přístupu.

4 **Ochrana DNS** OCHRANA DNS **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Ochrana proti únikům DNS směruje vyhledávací dotazy přes soukromé resolvery.

5 **Tunely Multi-Hop** MULTI-HOP **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Směrování Multi-Hop řetězí dva samostatné serverové uzly za sebou.

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **RAM-Only server** RAM-ONLY

Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

Hardware RAM-Only serverů nezapisuje žádná data na disk a při restartu se vše vymaže.

7 **Rychlost WireGuard** WIREGUARD

Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

WireGuard používá moderní kryptografii, která se vyhýbá úzkým hrdlům zpracování.

8 **Kill Switch** POJISTNÝ VYPÍNAČ

Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

Kill switch blokuje veškerý provoz, pokud spojení VPN vypadne.

9 **Audity třetích stran** AUDITY JSOU ZÁSADNÍ

Správná odpověď: Nepravda

POZNÁMKA PRO VYUČUJÍCÍ

Audity třetích stran jsou nezbytné k ověření firemních tvrzení o soukromí.

10 **Otázka 10**

Správná odpověď: Nepravda

POZNÁMKA PRO VYUČUJÍCÍ

Zero Trust nepřiznává žádnou implicitní důvěru na základě umístění v síti. [1]

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

C 1. Zero Trust	E 2. Multi-Hop	F 3. RAM-Only server	G 4. Ochrana DNS
H 5. Kill Switch	A 6. Auditovaný systém	B 7. Šifrování	D 8. Protokol

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 ZERO TRUST	2 MULTI-HOP	3 RAM-ONLY SERVER	4 OCHRANA DNS
5 KILL SWITCH	6 AUDITOVANÝ SYSTÉM		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 E – KILLSWITCH	2 D – OCHRANADNS	3 B – MULTIHOP	4 H – PROTOKOL
5 G – ŠIFROVÁNÍ	6 C – RAMSERVER	7 F – AUDITOVANÝ	8 A – NULOVÁDŮVĚRA

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy Zero Trust, Multi-Hop a RAM-Only server 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	Í	L	Š	Ž	T	É	A	Ř	Ů	E	A	Á	Ř	P
O	N	O	Q	U	Y	R	U	J	S	R	U	Š	Č	Ň
S	Á	K	Ý	B	Ě	Š	D	X	W	A	Í	A	S	Ž
N	V	O	Ý	Ý	L	F	I	I	N	M	S	J	N	M
D	O	T	Ť	P	G	R	T	Ř	G	S	Ž	Á	K	Ó
A	R	O	Ů	Ě	Ú	C	O	Ý	Š	E	Ý	B	I	G
N	F	R	M	Ž	F	J	V	Ó	Q	R	O	X	L	C
A	I	P	N	Ž	Z	Ě	A	Ý	P	V	W	Ú	L	L
R	Š	Ů	Q	B	Ó	V	N	Ť	N	E	F	Ů	S	Č
H	Ý	Ú	K	S	Á	X	Ý	Ž	Y	R	N	Š	W	R
C	N	U	L	O	V	Á	D	Ů	V	Ě	R	A	I	X
O	H	P	D	Á	Č	J	Ř	V	W	X	L	Í	T	H
U	H	M	U	L	T	I	H	O	P	Ě	B	E	C	I
K	Ť	Š	V	Ř	Z	E	H	E	Š	C	A	M	H	R
C	Ž	N	K	V	Š	Ú	Á	Š	X	J	N	N	G	H

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

2 vodorovně: MULTIHOP Kaskádové VPN směrování řetězící dva serverové uzly za sebou (8 písmen)

4 vodorovně: NULOVÁDŮVĚRA Bezpečnostní rámec vyžadující nepřetržité ověřování všech uživatelů (12 písmen)

8 vodorovně: KILLSWITCH Pojistný mechanismus blokující provoz při výpadku VPN (10 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: ŠIFROVÁNÍ Kryptografické šifrování datových zátěží pro zabezpečení přenosu (9 písmen)

3 svisle: AUDITOVANÝ Nezávisle prověřené nastavení potvrzující, že se neukládají žádné logy (10 písmen)

5 svisle: OCHRANADNS Vynucení soukromých DNS dotazů k ochraně vyhledávání jmenných serverů (10 písmen)

6 svisle: RAMSERVER Serverová architektura využívající volatilní paměť k ukládání datových zátěží (9 písmen)

7 svisle: PROTOKOL Soubor technických pravidel určujících, jak jsou data balena a odesílána (8 písmen)

Klíč řešení přesmyček a šifry

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

KLÍČ K PŘESMYČKÁM

1. VÁŮVUDĚNRLAO — NULOVÁDŮVĚRA
2. RRESARVEM — RAMSERVER
3. KWCIISHLTL — KILLSWITCH
4. OÍNRÁVŠIF — ŠIFROVÁNÍ
5. IHUPTMOL — MULTIHOP
6. NARADOCNSH — OCHRANADNS
7. UIAVOANÝTD — AUDITOVANÝ
8. TROLPOKO — PROTOKOL

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"BEZPEČNÉ VPN CHRÁNÍ CENNÁ DIGITÁLNÍ AKTIVA"

Klíč k případovým studiím

A PŘÍPADOVÁ STUDIE 1: ZODOLNĚNÍ PODNIKOVÉ INFRASTRUKTURY

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Korporátní banka přepracovává topologii vzdáleného přístupu. Vyžaduje architekturu zero trust propojující všechna klientská zařízení se zabezpečenými servery.
- Doporučená strategie a řešení: Pokyny k hodnocení: Vysvětlete, že mikrosegmentace omezuje přístup ke konkrétním zdrojům a brání laterálnímu pohybu hrozby, pokud je zařízení kompromitováno.

B PŘÍPADOVÁ STUDIE 2: OCHRANY SERVERŮ POUZE V RAM

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Poskytovatel VPN zaměřený na bezpečnost modernizuje své servery, aby fyzické zabavení serveru nemohlo odhalit historie uživatelských logů.
- Doporučená strategie a řešení: Pokyny k hodnocení: Popište, že RAM-Only servery nemají fyzické diskové úložiště. Výpadek napájení automaticky vymaže všechna dočasná data ve volatilní paměti.