Jméno: _____ **Datum:** _____ **Body:** _____

Zabezpečení Surfshark

Zkoumání bezpečnostních funkcí Surfsharku včetně blokování reklam CleanWeb, dynamického směrování MultiHop, SDN architektury Nexus, serverové flotily pouze s RAM a režimu Camouflage.

ZABEZPEČENÍ SURFSHARK – 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 bezpečnostní architekturou Surfsharku. Prozkoumáte hardware serverů běžících pouze v RAM, dynamickou rotaci IP v SDN Nexus, blokátory reklam CleanWeb a směrování MultiHop.

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/surfshark/bezpecnost/

Váš studijní plán: zabezpečení Surfshark

- Analyzujte technickou architekturu a konfigurační pravidla zabezpečení Surfshark.
- Nakonfigurujte nastavení klienta tak, aby bránilo únikům IP, DNS a WebRTC provozu.
- Porovnejte vlastní ceny, zkušební verze a výkonnostní funkce se standardními modely.

POKYNY K BEZPEČNOSTNÍMU PRŮVODCI SURFSHARK

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 RAM-only infrastrukturu, Nexus SDN a CleanWeb. Zakončete bonusovou aktivitou Mysli rychle.

FLOTILA RAM-ONLY SERVERŮ, NEXUS SDN A ARCHITEKTURA CLEANWEB (ÚVOD)

Surfshark chrání soukromí uživatelů flotilou serverů běžících výhradně v RAM, softwarově definovanou sítí Nexus s IP Rotatorem, blokováním reklam CleanWeb a šifrovacími cestami Dynamic MultiHop.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1. **1. Jak se jmenuje integrovaný blokátor reklam a malwaru od Surfshark?**
   - A) AdGuard
   - B) CleanWeb
   - C) ThreatShield
   - D) NetBlocker

2. **2. Jakou hardwarovou architekturu používá Surfshark na všech serverech?**
   - A) Pevné disky
   - B) 100% RAM-Only
   - C) Optické úložiště
   - D) Magnetická páska

3. **3. Jaká funkce směruje provoz přes dva různé VPN servery?**
   - A) Bypasser
   - B) MultiHop (Double VPN)
   - C) Síť Nexus
   - D) Statická IP

4. **4. Jaká obfuskační funkce maskuje VPN provoz jako běžná webová data?**
   - A) Kill Switch
   - B) Režim Camouflage
   - C) CleanWeb 2.0
   - D) Split Tunnel

5. **5. Jaká je funkce nástroje Surfshark Bypasser?**
   - A) Speed Booster
   - B) Rozdělené tunelování
   - C) Správce hesel
   - D) DNS resolver

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. RAM-only servery vymažou všechna provozní data okamžitě po restartu serveru.

○ Pravda ○ Nepravda

7 Otázka 7

7. Režim Camouflage brání poskytovatelům internetu zjistit, že používáte VPN.

○ Pravda ○ Nepravda

8 Otázka 8

8. CleanWeb 2.0 pracuje v rozšířeních prohlížeče a blokuje vyskakovací okna souhlasu s cookies.

○ Pravda ○ Nepravda

9 Otázka 9

9. Surfshark uchovává dočasné časové značky připojení a protokoly využití šířky pásma.

○ Pravda ○ Nepravda

10 Otázka 10

10. Síť Nexus pravidelně střídá IP adresy uživatelů bez odpojení.

○ Pravda ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. Otravné reklamy, sledovací skripty a phishingové odkazy blokují filtry funkce _____ .

2. Aktivita uživatelů nezanechává forenzní stopu, protože provoz obsluhují _____ .

3. Směrování dat přes dva samostatné šifrované serverové skoky zajišťují tunely typu _____ .

4. Ke skrytí používání VPN před poskytovatelem internetu aktivují uživatelé režim _____ .

5. Výjimky, díky nimž bankovní aplikace obcházejí VPN tunel, spravuje nastavení _____ .

6. SDN architekturou nové generace, která propojuje serverovou flotilu, je systém _____ .

ZÁSOBNÍK SLOV

BYPASSER CAMOUFLAGE CLEANWEB KILL SWITCH MULTI-HOP NEXUS RAM-ONLY ROTUJÍCÍ IP

Sem napište své odpovědi:

1. 2.

3. 4.

5. 6.

Kontrolní bod 4: Přiřazování pojmů VPN a sítí

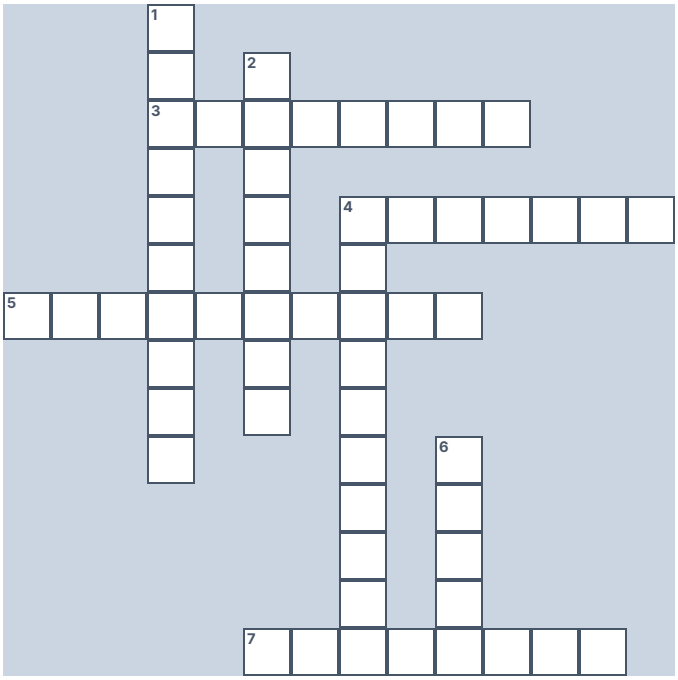
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. CLEANWEB	A	Automatická bezpečnostní funkce blokující síťový provoz, když VPN vypadne.
☐	2. RAM-ONLY	B	Funkce split tunnelingu umožňující vybraným aplikacím obejít VPN.
☐	3. MULTI-HOP	C	Pokročilý filtr blokující reklamy, malware a lišty souhlasu s cookies.
☐	4. CAMOUFLAGE	D	Serverový hardware s volatilní pamětí, který při každém vypnutí a zapnutí vymaže všechna data.
☐	5. BYPASSER	E	Funkce, která pravidelně mění vaši externí IP adresu bez přerušení tunelů.
☐	6. KILL SWITCH	F	Obfuskační technologie, která skrývá signatury VPN, aby napodobila běžný provoz HTTPS.
☐	7. NEXUS	G	Funkce dvojité VPN šifrující provoz přes dva odlišné serverové uzly.
☐	8. ROTUJÍCÍ IP ADRESA	H	Proprietární softwarově definovaná síť propojující všechny servery do jednotné sítě mesh.

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

3. Funkce dvojité VPN šifrující provoz přes dva odlišné serverové uzly (8)

4. Serverový hardware s volatilní pamětí mazající všechna data při každém restartu (7)

5. Automatická bezpečnostní funkce blokující síťový provoz při výpadku VPN (10)

7. Funkce split tunelingu umožňující vybraným aplikacím obejít VPN (8)

SVISLÉ NÁPOVĚDY

1. Obfuskační technologie skrývající znaky VPN, aby provoz vypadal jako běžné HTTPS (10)

2. Pokročilý filtr blokující reklamy, malware a cookie lišty souhlasu (8)

4. Funkce pravidelně měnící vaši vnější IP adresu bez přerušení tunelů (10)

6. Proprietární softwarově definovaná síť spojující všechny servery do jednotné 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

3 vodorovně: Funkce dvojité VPN šifrující provoz přes dva odlišné serverové uzly (8 písmen):

4 vodorovně: Serverový hardware s volatilní pamětí mazající všechna data při každém restartu (7 písmen):

5 vodorovně: Automatická bezpečnostní funkce blokující síťový provoz při výpadku VPN (10 písmen):

7 vodorovně: Funkce split tunelingu umožňující vybraným aplikacím obejít VPN (8 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Obfuskační technologie skrývající znaky VPN, aby provoz vypadal jako běžné HTTPS (10 písmen):

2 svisle: Pokročilý filtr blokující reklamy, malware a cookie lišty souhlasu (8 písmen):

4 svisle: Funkce pravidelně měnící vaši vnější IP adresu bez přerušení tunelů (10 písmen):

6 svisle: Proprietární softwarově definovaná síť spojující všechny servery do jednotné sítě (5 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

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

SEZNAM SLOV

CLEANWEB RAMONLY MULTIHOP NEXUS CAMOUFLAGE ROTUJÍCÍIP BYPASSER 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. CLEANWEB**
- **B. RAMONLY**
- **C. MULTIHOP**
- **D. CAMOUFLAGE**
- **E. BYPASSER**
- **F. KILLSWITCH**
- **G. NEXUS**
- **H. ROTUJÍCÍIP**

DEFINICE A POLE K PŘIŘAZENÍ

1. Obfuskační technologie skrývající znaky VPN, aby provoz vypadal jako běžné HTTPS.
2. Automatická bezpečnostní funkce blokující síťový provoz při výpadku VPN.
3. Pokročilý filtr blokující reklamy, malware a cookie lišty souhlasu.
4. Funkce split tunelingu umožňující vybraným aplikacím obejít VPN.
5. Serverový hardware s volatilní pamětí mazající všechna data při každém restartu.
6. Funkce pravidelně měnící vaši vnější IP adresu bez přerušení tunelů.
7. Funkce dvojité VPN šifrující provoz přes dva odlišné serverové uzly.
8. Proprietární softwarově definovaná síť spojující všechny servery do jednotné sítě.

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. **EANCWLBE** _____
2. **TMPUOHIL** _____
3. **AYBSSREP** _____
4. **XSUNE** _____
5. **NYOMRLA** _____
6. **GUOLACAFEM** _____
7. **ILKIWTCHSL** _____
8. **IUÍPRJOCÍT** _____

Bonusová aktivita: Mysli rychle

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

1	Bezpečnostní funkce v Surfshark			
2	Známky toho, že je vaše VPN připojení pomalé			
3	VPN protokoly, které znáte			
4	Věci, které šifrování chrání			
5	Hrozby na veřejné Wi-Fi			
6	Země známé přísnými zákony na ochranu soukromí			
7	Způsoby, jak vytvořit silné heslo			
8	Zařízení, na která byste nainstalovali Surfshark			
9	Otázky pro zákaznickou podporu Surfshark			
10	Nastavení, která zapnete pro extra bezpečnost			
11	Věci, které Surfshark dokáže skrýt před vaší sítí			
12	Typy úniků u VPN			
13	Data, která by VPN nikdy neměla ukládat			
14	Slova, která popisují dobrou VPN aplikaci			
15	Věci, které může audit prověřit			

Kontrolní bod 8: Případové studie VPN a sítí

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: OBCHÁZENÍ FILTRŮ V KAMPUSU A NA PRACOVIŠTI



Scénář: Student zjistí, že univerzitní kampusová Wi-Fi blokuje všechny standardní porty OpenVPN a WireGuard.

Otázka k diskusi: Která funkce Surfsharku umožňuje studentovi připojit se, aniž by ho odhalili správci sítě?

PŘÍPADOVÁ STUDIE 2: VYSOCE RIZIKOVÉ NOVINÁŘSKÉ VYŠETŘOVÁNÍ



Scénář: Investigativní novinář potřebuje při průzkumu citlivých firemních záznamů zvýšenou ochranu před sledováním.

Otázka k diskusi: Jak Dynamic MultiHop poskytuje lepší soukromí ve srovnání se směrováním přes jeden server?

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

26	22	30	32	16	15	4	15	14	24	20	8	37	32	28

40	18	8	24	29	32	16	8	28	22	32	17	26	22	19	15

32	41	14	35	1	30	8	18	34

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 Surfshark CleanWeb?

CleanWeb je integrovaná bezpečnostní funkce, která blokuje reklamy, trackery, malware a phishingové weby.

Q2: Co jsou servery pouze v RAM?

RAM-only servery běží na volatilní paměti, což znamená, že data v paměti se při každém restartu serverů vymažou.

Q3: Co je Surfshark MultiHop?

MultiHop (Double VPN) směruje a šifruje vaše internetové připojení přes dvě různé serverové lokality.

Q4: Jak funguje Camouflage Mode?

Režim Camouflage obfuskuje VPN provoz, takže váš ISP nepozná, že používáte VPN.

Q5: Co je funkce Bypasser?

Bypasser je nástroj Surfsharku pro rozdělené tunelování, který umožňuje konkrétním aplikacím nebo webům obejít VPN.

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

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

Q6: Má Surfshark kill switch?

Ano, Kill Switch vás odpojí od internetu, pokud VPN nečekaně vypadne.

Q7: Jaký šifrovací standard používá Surfshark?

Surfshark používá AES-256-GCM a ChaCha20, plus AEGIS-256X2 na svém novém protokolu Dausos.

Q8: Byla politika neuchovávání logů Surfsharku auditována?

Ano, Deloitte ověřil no-logs politiku Surfshark v roce 2023 a znovu v roce 2025.

Q9: Co je Surfshark Nexus?

Nexus je pokročilá SDN architektura, která propojuje všechny servery do jednotné sítě pro plynulejší směrování.

Q10: Co je funkce IP Rotator?

IP Rotator automaticky mění vaši IP adresu každých několik minut bez odpojení vaší VPN relace.

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

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

Q1: Čím se Dynamic MultiHop liší od tradiční dvojité VPN?

Dynamic MultiHop vám umožňuje libovolně kombinovat vstupní a výstupní servery po celém světě.

Q2: Funguje CleanWeb 2.0 v rozšířeních prohlížeče?

Ano, CleanWeb 2.0 blokuje videoreklamy, vyskakovací okna souhlasu s cookies a upozorňovací bannery v Chrome/Firefoxu.

Q3: Co je Alternative ID v bezpečnostním balíčku?

Alternative ID generuje jedinečné osobní pseudonymy, e-mailové adresy a masky telefonních čísel.

Q4: Jak Surfshark zabraňuje únikům DNS?

Surfshark směruje všechny doménové požadavky přes vlastní privátní DNS servery na každém uzlu.

Q5: Podporuje Surfshark na mobilu šifrování ChaCha20?

Ano, WireGuard na Androidu a iOS používá ChaCha20-Poly1305 pro vynikající mobilní efektivitu.

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

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

Q6: Co je režim NoBorders v Surfsharku?

NoBorders automaticky rozpoznává restriktivní síťová prostředí a nabízí specializované servery.

Q7: Kdo provedl bezpečnostní audity rozšíření prohlížeče Surfshark?

Nezávislá kyberbezpečnostní firma Cure53 dokončila audity rozšíření prohlížečů a serverových systémů.

Q8: Jak Surfshark chrání před úniky IPv6?

Surfshark směruje provoz IPv6 bezpečně, nebo jej bezpečně omezuje, aby zabránil jakémukoli nešifrovanému úniku.

Q9: Kde má Surfshark právní jurisdikci?

Surfshark působí podle práva Nizozemska a dodržuje přísné evropské standardy ochrany soukromí GDPR.

Q10: Podporuje Surfshark dvoufaktorové ověřování (2FA)?

Ano, a Surfshark One přidává 2FA zámek, takže nastavení funkcí můžete měnit jen vy.

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

1. Surfshark uvádí, že celá jeho síť 4,500+ serverů běží na bezdiskovém volatilním hardwaru pouze s RAM.

2. VPN POSTŘEH

2. Firma velké čtyřky Deloitte ověřila politiku no-logs Surfsharku v roce 2023 a znovu v listopadu 2025.

3. VPN POSTŘEH

3. Proprietární architektura Nexus propojuje všechny globální servery do dynamické softwarově definované sítě.

4. VPN POSTŘEH

4. Rotating IP mění vaši IP adresu přibližně každých pět minut bez přerušení VPN připojení.

5. VPN POSTŘEH

5. CleanWeb 2.0 blokuje otravná vyskakovací okna souhlasu s cookies a videoreklamy přímo v prohlížečích.

6. VPN POSTŘEH

6. Dynamický MultiHop umožňuje uživatelům vytvářet vlastní dvouserverové šifrovací cesty ve 100 zemích.

7. POSTŘEH K VPN

7. Camouflage Mode odstraňuje signatury hlaviček VPN, takže je provoz k nerozeznání od běžného provozu HTTPS.

8. POSTŘEH K VPN

8. Alternative ID generuje jednorázové pseudonymy a e-mailové masky na ochranu uživatelů před úniky z databází.

9. POSTŘEH K VPN

9. Surfshark vynucuje symetrické šifrování AES-256-GCM spolu s ChaCha20 na protokolech WireGuard.

10. VPN POSTŘEH

10. Režim NoBorders se na omezených sítích aktivuje automaticky a poskytuje odolný tunelovací přístup.

Technické reference a zdroje

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

AKADEMICKÉ A OBOROVÉ REFERENCE

[1] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 **Integrovaný blokátor obsahu** OBRANA PROTI REKLAMÁM A MALWARU — **Správná odpověď: B**

POZNÁMKA PRO VYUČUJÍCÍ

CleanWeb je integrovaný bezpečnostní filtr Surfsharku, který na úrovni sítě blokuje reklamy, sledovací domény, phishingové weby a škodlivé URL skripty.

2 **100% RAM-only infrastruktura** ARCHITEKTURA RAM — **Správná odpověď: B**

POZNÁMKA PRO VYUČUJÍCÍ

Surfshark provozuje servery běžící pouze v RAM, takže data držená v paměti serveru se při vypnutí nebo restartu vymažou.

3 **Dvojité tunelování MultiHop** MULTIHOP VPN — **Správná odpověď: B**

POZNÁMKA PRO VYUČUJÍCÍ

MultiHop (Double VPN) šifruje provoz přes dva samostatné serverové uzly v různých zemích, aby zabránil korelačním útokům na provoz.

4 **Obfuskace režimu Camouflage** OBFUSCATION — **Správná odpověď: B**

POZNÁMKA PRO VYUČUJÍCÍ

Režim Camouflage upravuje hlavičky OpenVPN paketů tak, aby maskoval VPN provoz jako běžný HTTPS provoz, a obcházel tak blokace restriktivních firewallů.

5 **Rozdělené tunelování Bypasser** ROZDĚLENÉ TUNELOVÁNÍ — **Správná odpověď: B**

POZNÁMKA PRO VYUČUJÍCÍ

Bypasser je nástroj Surfsharku pro rozdělené tunelování, který uživatelům umožňuje vybrat konkrétní aplikace nebo weby, jež se směrují přímo přes jejich běžné připojení ISP.

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Vymazání dat z volatilní paměti** ZABEZPEČENÍ SERVERŮ — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

RAM-only servery neukládají žádná data na trvalé pevné disky; restart hardwaru okamžitě vymaže celou provozní paměť.

7 **Skrytí před ISP pomocí režimu Camouflage** SKRÝVÁNÍ PROVOZU — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Režim Camouflage odstraňuje signatury protokolu OpenVPN, a brání tak ISP zjistit, že je uživatel připojen k VPN tunelu.

8 **Rozšíření prohlížeče CleanWeb 2.0** ROZŠÍŘENÍ PROHLÍŽEČE — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

CleanWeb 2.0 pracuje v rozšířeních prohlížeče a v reálném čase blokuje vyskakovací okna souhlasu s cookies, videoreklamy a škodlivé přesměrovací skripty.

9 **Nulové uchovávání logů připojení** ZÁSADY NO-LOGS — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Surfshark udržuje přísnou nezávisle auditovanou zásadu nulových logů a nezaznamenává žádné IP adresy, časové značky připojení ani protokoly šířky pásma.

10 **Dynamická rotace IP v Nexusu** SÍŤ NEXUS — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Softwarově definovaná síť Surfshark Nexus dynamicky střídá IP adresy uživatelů každých několik minut, aniž by přerušila aktivní VPN připojení.

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. CLEANWEB	D 2. RAM-ONLY	G 3. MULTI-HOP	F 4. CAMOUFLAGE
B 5. BYPASSER	A 6. KILL SWITCH	H 7. NEXUS	E 8. ROTUJÍCÍ IP ADRESA

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 CLEANWEB	2 RAM-ONLY	3 MULTI-HOP	4 CAMOUFLAGE
5 BYPASSER	6 NEXUS		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 D – CAMOUFLAGE	2 F – KILLSWITCH	3 A – CLEANWEB	4 E – BYPASSER
5 B – RAMONLY	6 H – ROTUJÍCÍIP	7 C – MULTIHOP	8 G – NEXUS

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy CLEANWEB, RAM-ONLY a MULTI-HOP a ke každému uvést příklad.

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

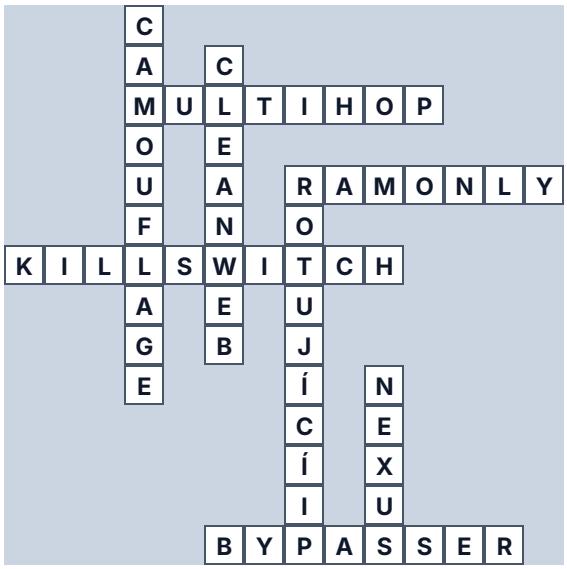
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

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

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

3 vodorovně: MULTIHOP Funkce dvojité VPN šifrující provoz přes dva odlišné serverové uzly (8 písmen)

4 vodorovně: RAMONLY Serverový hardware s volatilní pamětí mazající všechna data při každém restartu (7 písmen)

5 vodorovně: KILLSWITCH Automatická bezpečnostní funkce blokující síťový provoz při výpadku VPN (10 písmen)

7 vodorovně: BYPASSER Funkce split tunelingu umožňující vybraným aplikacím obejít VPN (8 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: CAMOUFLAGE Obfuskační technologie skrývající znaky VPN, aby provoz vypadal jako běžné HTTPS (10 písmen)

2 svisle: CLEANWEB Pokročilý filtr blokující reklamy, malware a cookie lišty souhlasu (8 písmen)

4 svisle: ROTUJÍCÍIP Funkce pravidelně měnící vaši vnější IP adresu bez přerušení tunelů (10 písmen)

6 svisle: NEXUS Proprietární softwarově definovaná síť spojující všechny servery do jednotné sítě (5 písmen)

Klíč řešení přesmyček a šifry

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

KLÍČ K PŘESMYČKÁM

1. E A N C W L B E — **CLEANWEB**
2. T M P U O H I L — **MULTIHOP**
3. A Y B S S R E P — **BYPASSER**
4. X S U N E — **NEXUS**
5. N Y O M R L A — **RAMONLY**
6. G U O L A C A F E M — **CAMOUFLAGE**
7. I L K I W T C H S L — **KILLSWITCH**
8. I U Í P R J O C Í T — **ROTUJÍCÍIP**

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"ROTUJÍCÍ IP NEXUS ZLEPŠUJE SOUKROMÍ UŽIVATELŮ"

Klíč k případovým studiím

A PŘÍPADOVÁ STUDIE 1: OBCHÁZENÍ FILTRŮ V KAMPUSU A NA PRACOVIŠTI

Řešení pro vyučující

HODNOTICÍ RUBRIKA A POKYNY K ŘEŠENÍ

- Analýza scénáře: Student zjistí, že univerzitní kampusová Wi-Fi blokuje všechny standardní porty OpenVPN a WireGuardu.
- Klíčová otázka: Která funkce Surfsharku umožňuje studentovi připojit se bez odhalení správci sítě?
- Doporučená strategie a řešení: Aktivujte Camouflage Mode (OpenVPN), který skryje metadata VPN, takže firewally vidí běžné HTTPS prohlížení.

B PŘÍPADOVÁ STUDIE 2: VYSOCE RIZIKOVÉ NOVINÁŘSKÉ VYŠETŘOVÁNÍ

Řešení pro vyučující

HODNOTICÍ RUBRIKA A POKYNY K ŘEŠENÍ

- Analýza scénáře: Investigativní novinář potřebuje zvýšenou ochranu před sledováním při zkoumání citlivých firemních záznamů.
- Klíčová otázka: Jak Dynamic MultiHop poskytuje lepší soukromí ve srovnání se směrováním přes jediný server?
- Doporučená strategie a řešení: Dynamický MultiHop směruje provoz přes vstupní a výstupní servery ve dvou zemích, takže žádný jednotlivý server nemůže uživatele odhalit.