Jméno: _____ Datum: _____ Body: _____

Proxy vs VPN Pracovní list

Porovnání proxy serverů a virtuálních privátních sítí, rozdílů v šifrování a směrování na úrovni aplikace vs. celého systému

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 základními principy virtuálních privátních sítí (VPN). Prozkoumáte, jak šifrované tunely zabezpečují vaše data, jak fungují síťové protokoly a jak rozpoznat a zmírnit úniky soukromí.

KONTROLNÍ BODY PRACOVNÍHO LISTU

- [ ] **Část 1-4: Zvládněte koncepty a protokoly VPN.**
- [ ] **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 VPN od VPN.com

URL: https://www.vpn.com/cs/vpn/

Váš studijní plán: VPN

- Porovnejte aplikační proxy se systémovým VPN šifrováním.
- Určete schopnosti SOCKS5 ve srovnání se základními HTTP proxy.
- Analyzujte, jak proxy v prohlížeči ponechávají aplikace na pozadí nechráněné.
- Pochopte, jak ISP logují nešifrovaný provoz na proxy tunelech.
- Vyberte správný nástroj směrování podle potřeb rychlosti a zabezpečení.

POKYNY K PRACOVNÍMU LISTU SROVNÁNÍ PROXY

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 porovnání proxy a VPN. Zakončete bonusovou aktivitou Mysli rychle.

PROXY VS VPN (ÚVOD)

Proxy a VPN plní odlišné funkce digitálního soukromí. Proxy server funguje jako přesměrování na aplikační vrstvě a maskuje vaši IP adresu pro konkrétní programy bez šifrování dat. VPN pracuje na úrovni sítě a zabezpečuje veškerý systémový provoz šifrováním. Volba správného nástroje závisí na vašich bezpečnostních požadavcích.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1. **1. Na které vrstvě modelu OSI pracuje standardní HTTP proxy?**
   - A. Fyzická vrstva
   - B. Síťová vrstva
   - C. Aplikační vrstva
   - D. Linková vrstva

2. **2. Jaká je klíčová protokolová výhoda SOCKS5 oproti standardním HTTP proxy?**
   - A. Vynucuje úplné šifrování obsahu
   - B. Podporuje směrování jakéhokoli provozu TCP/UDP
   - C. Je imunní vůči únikům DNS
   - D. Pracuje přímo v prostoru jádra

3. **3. Proč je VPN obecně bezpečnější než proxy server?**
   - A. Běží na rychlejším vzdáleném hardwaru
   - B. Šifruje veškerý síťový provoz v celém systému
   - C. Nevyžaduje místní směrovací tabulky
   - D. Zcela eliminuje síťovou latenci

4. **4. Jaký typ proxy přesměrovává provoz ve výchozím stavu bez jakéhokoli šifrování?**
   - A. Základní HTTP proxy
   - B. Šifrovaná HTTPS proxy
   - C. Zabezpečený klient WireGuard
   - D. Obfuskovaný VPN server

5. **5. Co se stane s provozem aplikací na pozadí při použití proxy v prohlížeči?**
   - A. Je automaticky šifrována
   - B. Je blokován proxy serverem
   - C. Prochází proxy tunelem
   - D. Obchází proxy a odhalí vaši IP

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. Proxy SOCKS5 šifruje veškerý obsah paketů procházejících serverem.

- ○ Pravda
- ○ Nepravda

7 Otázka 7

7. VPN pracuje na síťové vrstvě a zabezpečuje veškerý systémový provoz.

- ○ Pravda
- ○ Nepravda

8 Otázka 8

8. Proxy jsou obecně rychlejší než VPN, protože provádějí hloubkové šifrování paketů.

- ○ Pravda
- ○ Nepravda

9 Otázka 9

9. Konfigurace proxy vyžaduje nastavení přesměrování provozu uvnitř konkrétních aplikací.

- ○ Pravda
- ○ Nepravda

10 Otázka 10

10. Použití proxy nezabezpečí váš datový provoz před sledováním místním ISP.

- ○ Pravda
- ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. _____ aplikační vrstvy přesměrovává vybraný provoz prohlížeče, ale nechrání ostatní aplikace.

2. Robustní _____ zapouzdřuje a šifruje všechny datové pakety zařízení.

3. Protokol _____ se nachází mezi aplikační a transportní vrstvou.

4. HTTP proxy fungují na _____ vrstvě modelu OSI.

5. Standardním proxy serverům chybí _____ obsahu, takže data zůstávají zranitelná.

6. VPN nabízí _____ krytí pro všechny síťové adaptéry.

ZÁSOBNÍK SLOV

APLIKAČNÍ CELOSYSTÉMOVÉ PODPORA UDP PROXY SOCKS5 ŠIFROVÁNÍ VIDITELNOST PRO ISP VPN TUNEL

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování síťových pojmů

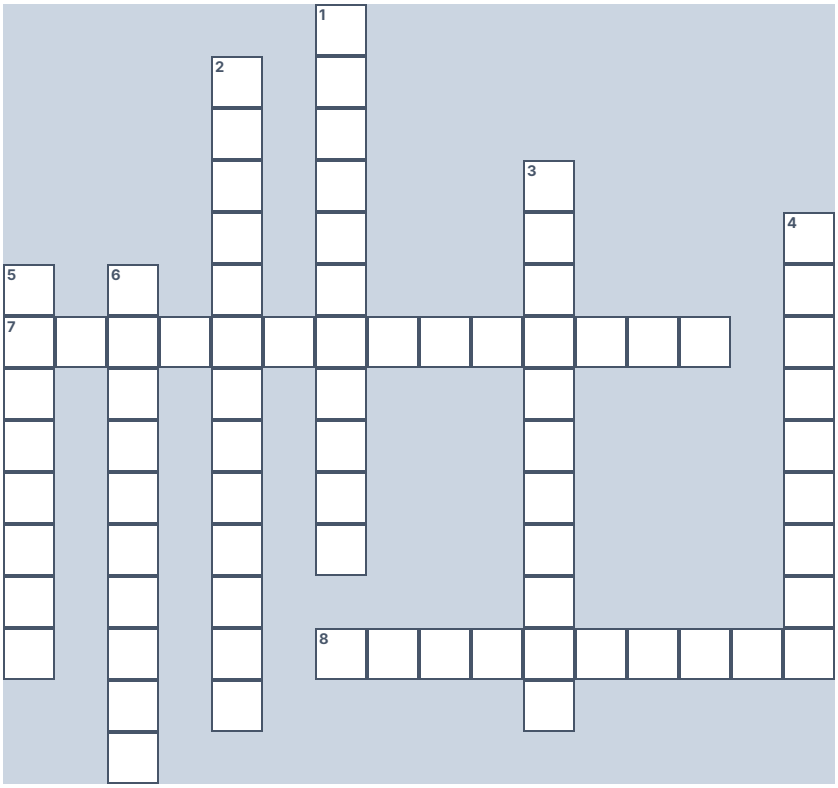
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. HTTP proxy	A	Směrování na úrovni operačního systému, které šifruje provoz všech aplikací.
☐	2. SOCKS5 proxy	B	Aplikační vrstva, kde fungují standardní webové proxy protokoly.
☐	3. VPN tunel	C	Schopnost SOCKS5 přenášet UDP i TCP, na rozdíl od obyčejných HTTP proxy.
☐	4. Celosystémové	D	Klientské rozšíření, které skrývá provoz jen uvnitř sandboxu prohlížeče.
☐	5. Vrstva OSI 7	E	Šifrování a zapouzdření obalující veškerý provoz zařízení na pozadí.
☐	6. Podpora UDP	F	Stav provozu, kdy nešifrovaná proxy data zůstávají viditelná pro ISP.
☐	7. Proxy v prohlížeči	G	Proxy aplikační vrstvy přesměrovávající konkrétní provoz webového prohlížeče.
☐	8. Viditelnost pro ISP	H	Proxy protokol mezi aplikační a transportní vrstvou, bez šifrování.

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

7. Rozšíření klienta skrývající pouze provoz uvnitř sandboxu prohlížeče (14)

8. Proxy protokol mezi aplikační a transportní vrstvou, bez šifrování (10)

SVISLÉ NÁPOVĚDY

1. Aplikační vrstva, kde fungují standardní webové proxy protokoly (11)

2. Směrování na úrovni operačního systému šifrující provoz všech aplikací (13)

3. Stav provozu, kdy nešifrovaná proxy data zůstávají viditelná poskytovatelům (11)

4. Proxy aplikační vrstvy přesměrovávající vybraný provoz webového prohlížeče (9)

5. Šifrování a zapouzdření obalující veškerý provoz zařízení na pozadí (8)

6. Schopnost SOCKS5 přenášet UDP i TCP, na rozdíl od čistých HTTP proxy (10)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

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

VODOROVNÉ NÁPOVĚDY

7 vodorovně: Rozšíření klienta skrývající pouze provoz uvnitř sandboxu prohlížeče (14 písmen):

8 vodorovně: Proxy protokol mezi aplikační a transportní vrstvou, bez šifrování (10 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Aplikační vrstva, kde fungují standardní webové proxy protokoly (11 písmen):

2 svisle: Směrování na úrovni operačního systému šifrující provoz všech aplikací (13 písmen):

3 svisle: Stav provozu, kdy nešifrovaná proxy data zůstávají viditelná poskytovatelům (11 písmen):

4 svisle: Proxy aplikační vrstvy přesměrovávající vybraný provoz webového prohlížeče (9 písmen):

5 svisle: Šifrování a zapouzdření obalující veškerý provoz zařízení na pozadí (8 písmen):

6 svisle: Schopnost SOCKS5 přenášet UDP i TCP, na rozdíl od čistých HTTP proxy (10 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

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

SEZNAM SLOV

HTTPPROXY SOCKSPROXY VPNTUNEL CELOSYSTÉMOVÉ SEDMÁVRSTVA
PODPORAUDP PROXYPROHLIZEC VIDITELNOST

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. HTTPPROXY**
- **B. SOCKSPROXY**
- **C. VPNTUNEL**
- **D. CELOSYSTÉMOVÉ**
- **E. SEDMÁVRSTVA**
- **F. PODPORAUDP**
- **G. PROXYPROHLIZEC**
- **H. VIDITELNOST**

DEFINICE A POLE K PŘIŘAZENÍ

1. Aplikační vrstva, kde fungují standardní webové proxy protokoly.
2. Schopnost SOCKS5 přenášet UDP i TCP, na rozdíl od čistých HTTP proxy.
3. Proxy aplikační vrstvy přesměrovávající vybraný provoz webového prohlížeče.
4. Rozšíření klienta skrývající pouze provoz uvnitř sandboxu prohlížeče.
5. Šifrování a zapouzdření obalující veškerý provoz zařízení na pozadí.
6. Směrování na úrovni operačního systému šifrující provoz všech aplikací.
7. Stav provozu, kdy nešifrovaná proxy data zůstávají viditelná poskytovatelům.
8. Proxy protokol mezi aplikační a transportní vrstvou, bez šifrování.

Kontrolní bod 7: Výzva s přeházenými slovy

Přeuspořádejte písmena níže a odhalte klíčové pojmy a termíny VPN. Odpovědi pište do vyplnitelných polí.

1. RPPTHOXYT
2. TVLPENUN
3. SRVSDEVAÁTM
4. RRELXHPCOZIPOY
5. OPYOKRSSXC
6. SMSYOLVÉCETÉO
7. OPPARUDPOD
8. OLTEDVTISNI

Bonusová aktivita: Mysli rychle

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

1	Rozdíly mezi proxy a VPN			
2	Věci, které bez VPN zůstávají nešifrované			
3	Způsoby, jak poznat falešnou Wi-Fi síť			
4	Věci, které dělá prostředník v každodenním životě			
5	Situace, kdy stačí proxy			
6	Zařízení, která mohou používat VPN			
7	Typy proxy, které znáte			
8	Věci, které VPN dokáže skrýt			
9	Mýty o VPN			
10	Sliby, které dává dobrý poskytovatel VPN			
11	Věci, před kterými vás VPN neochrání			
12	Slova z tohoto pracovního listu, která si chcete zapamatovat			
13	Důvody, proč používat VPN na cestách			
14	Situace, kdy chcete VPN			
15	Místa, kde byste použili VPN			

Kontrolní bod 8: Případové studie VPN

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

SARAH (STUDENTKA V KAVÁRNĚ)

👩‍💻 "Ahoj! Jsem v Coffee & Bytes na otevřené síti 'Free_Wi-Fi_No_Password'. Potřebuji se přihlásit do školního e-mailu a kamarád tvrdí, že bezplatná proxy v prohlížeči na ochranu stačí. Ochránila by proxy moje přihlášení a soubory, nebo potřebuji VPN?"

ALEX (CESTUJÍCÍ STUDENT)

👩‍💻 "Jsem v zahraničí a u biologického dokumentu hostovaného v mé domovské zemi se píše 'Toto video není ve vaší aktuální lokalitě dostupné.' Spolužák používá proxy a já mám VPN. Proč jsem blokován a který nástroj by fungoval lépe?"

Kontrolní bod 9: Dešifrování šifry

K dokončení výcviku porovnávání proxy dešifrujte tuto tajnou zprávu o bezpečném tunelování.

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

24	27	8	28	19	10	26	32	16	30	8		28	35	34	16

24	26	22	35	22	40		24	27	8	28		24	26	22	37	38

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 zájemců o používání virtuálních privátních sítí.

Q1: Co je VPN a jak funguje?

Virtuální privátní síť (VPN) šifruje vaše internetové připojení a směruje váš provoz přes zabezpečený vzdálený server. Tím maskuje vaši veřejnou IP adresu a omezuje, co mohou místní pozorovatelé sítě a váš ISP vidět o provozu vedeném tunelem VPN.

Q2: Co je proxy server?

Proxy server je prostředník, který předává požadavky mezi vaší aplikací a cílovým serverem. Web vidí IP adresu proxy místo vaší, ale přesměrován je jen provoz aplikací nastavených na použití proxy a základní proxy tento provoz nešifruje.

Q3: Zajistí mi VPN na internetu úplnou anonymitu?

Ne. VPN sice skrývá vaši IP adresu a šifruje provoz, ale stále vás lze sledovat přes cookies prohlížeče, aktivní účty (jako Google nebo Facebook), otisk prohlížeče, nebo pokud váš poskytovatel VPN loguje vaše data.

Q4: Zpomalí VPN mé internetové připojení?

Ano, mírně. Proces šifrování a fyzická vzdálenost k serveru VPN přidávají latenci a režii. Dopad se liší podle poskytovatele, protokolu, vzdálenosti serveru, zařízení a stavu sítě.

Q5: Je proxy totéž co VPN?

Ne. Proxy předává provoz jen konkrétních aplikací, obvykle bez šifrování. VPN vytváří šifrovaný tunel na síťové vrstvě, kterým prochází veškerý provoz zařízení včetně aplikací na pozadí.

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

Projděte si nejčastější otázky a odpovědi zájemců o používání virtuálních privátních sítí.

Q6: Mohu použít bezplatnou proxy?

Můžete, ale bezplatné proxy často provozují neznámí operátoři. Protože základní proxy provoz nešifruje, její provozovatel může nezašifrované stránky vidět a dokonce upravovat. Před použitím si ověřte, kdo službu provozuje.

Q7: Uchovává proxy logy?

Může. Proxy zpracovává každý požadavek, který předává, takže její provozovatel může zaznamenávat vaši IP adresu, navštěvované weby i časy. Ověřte si, kdo ji provozuje a co říkají její zásady ochrany soukromí.

Q8: Kdy stačí proxy?

Proxy může stačit pro málo rizikové úkoly, například změnu zdánlivé polohy jednoho prohlížeče. Pro bankovnictví, veřejné Wi-Fi nebo ochranu všech aplikací na zařízení je bezpečnější volbou VPN, protože šifruje veškerý provoz.

Q9: Může proxy chránit všechny aplikace v telefonu?

Ne. Nastavení proxy respektují a používají jen některé aplikace; ostatní se připojují přímo. Aplikace VPN místo toho směruje všechny aplikace telefonu přes svůj šifrovaný tunel.

Q10: Co je SOCKS5 proxy?

SOCKS5, definovaný v RFC 1928, je proxy protokol ležící mezi aplikační a transportní vrstvou. Umí přenášet TCP spojení a UDP datagramy a podporuje ověřování, ale nemá vestavěné šifrování. [1]

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

Prozkoumejte technické a strukturální aspekty virtuálních privátních sítí a zabezpečených tunelovacích protokolů.

Q1: Na kterých síťových vrstvách fungují proxy a VPN?

HTTP proxy pracuje na aplikační vrstvě (vrstva 7) a rozumí webovým požadavkům. SOCKS5 se nachází mezi aplikační a transportní vrstvou. Protokoly VPN jako IPsec nebo WireGuard pracují na síťové vrstvě, takže mohou přenášet veškerý IP provoz ze zařízení.

Q2: Zůstává HTTPS web šifrovaný přes proxy?

Ano. Když otevřete web HTTPS přes proxy, šifrování TLS běží mezi vaším prohlížečem a webem od začátku do konce, takže proxy vidí doménu, ale ne obsah stránek. Stránky s prostým HTTP zůstávají čitelné.

Q3: Co je únik WebRTC a jak mu VPN zabraňuje?

WebRTC je protokol prohlížeče, který může odhalit vaši skutečnou lokální i veřejnou IP adresu, i když je VPN aktivní. Prémiové VPN blokují nebo podvrhují požadavky WebRTC ve svých desktopových/mobilních aplikacích a rozšířeních prohlížeče.

Q4: Co je transparentní proxy a kdo ji používá?

Transparentní proxy zachytává provoz bez jakéhokoli nastavení na zařízení uživatele. Školy, firmy a ISP je používají pro ukládání do mezipaměti nebo filtrování obsahu. Uživatelé často nevědí, že je nasazena, a žádné soukromí jim neposkytuje.

Q5: Jak obfuskace obchází blokování VPN?

Obfuskace (neboli „Stealth VPN“) maskuje VPN provoz tak, aby vypadal jako běžný provoz HTTPS (port 443). To mu může pomoci projít přes hloubkovou inspekci paketů (DPI), kterou vlády nebo školní/firemní sítě používají k blokování VPN.

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

Prozkoumejte technické a strukturální aspekty virtuálních privátních sítí a zabezpečených tunelovacích protokolů.

Q6: Co je split tunneling a kdy jej mám použít?

Split Tunneling vám umožňuje zvolit, které aplikace se směrují šifrovaným tunelem VPN a které se připojují přímo k internetu. Použijte jej ke směrování citlivých bankovních aplikací přes VPN, zatímco lokální hry se připojují přímo a vyhnou se latenci přidané VPN.

Q7: Proč může proxy působit rychleji než VPN připojení?

Základní proxy vynechává šifrování a zpracovává provoz jen z jedné aplikace, takže přidává méně zpracování. VPN šifruje každý paket ze zařízení. S moderními protokoly je rozdíl často malý a proxy nabízí mnohem menší ochranu.

Q8: Poznají weby, že používám proxy nebo VPN?

Často ano. Mnoho webů kontroluje IP adresy proti seznamům známých proxy a VPN serverů a HTTP proxy mohou přidávat hlavičky jako Via nebo X-Forwarded-For. Streamovací služby běžně blokují obojí.

Q9: Co je ochrana proti únikům DNS?

Ochrana proti únikům DNS nutí vaše zařízení posílat dotazy na vyhledání webů (dotazy DNS) přes soukromé, šifrované DNS servery VPN místo serverů vašeho ISP. Tím brání vašemu ISP sledovat, které stránky navštěvujete.

Q10: Dokáže proxy zastavit škrcení ze strany poskytovatele?

Zřídka. Základní proxy provoz nešifruje, takže ISP stále vidí, o jaký typ aktivity jde. VPN typy provozu skryje, ale ani jeden nástroj nevyřeší přetížení nebo datové limity.

Část 11: 10 zajímavých faktů o VPN a poznatků z praxe

Projděte si tato velmi cenná fakta a poznatky z praxe o historii, trhu a technologii VPN.

1. STANDARD SOCKS

SOCKS Protocol Version 5 publikovala IETF jako RFC 1928 v březnu 1996 a dodnes je referenční specifikací pro SOCKS5 proxy používané prohlížeči a aplikacemi. [1]

2. VRSTVA SHIM

RFC 1928 popisuje SOCKS jako mezivrstvu mezi aplikační a transportní vrstvou, takže nedokáže předávat provoz síťové vrstvy, jako je ICMP. [1]

3. UDP RELAY

SOCKS5 přidal příkaz UDP ASSOCIATE, díky němuž proxy přenáší vedle TCP spojení i UDP datagramy, což běžné HTTP proxy neumí. [1]

4. VÝCHOZÍ PORT SOCKS

Klienti SOCKS5 se k proxy serveru ve výchozím stavu připojují na TCP portu 1080, jak definuje RFC 1928; řada proxy služeb umožňuje zvolit jiné porty. [1]

5. HTTP PROSTŘEDNÍCI

Standard HTTP (RFC 9110) definuje proxy jako agenta pro předávání zpráv zvoleného klientem, který předává požadavky směrem ke zdrojovému serveru.

6. HLOUBKOVÁ INSPEKCE PAKETŮ

Hloubková inspekce paketů (DPI) zkoumá obsah paketů a vzorce provozu; nešifrovaný provoz proxy je pro ni plně viditelný, zatímco provoz VPN odhaluje mnohem méně.

7. VPN NA SÍŤOVÉ VRSTVĚ

IPsec, popsaný v NIST SP 800-77, chrání provoz na síťové vrstvě, takže IP pakety každé aplikace lze zabezpečit bez nastavování jednotlivých aplikací. [2]

8. ROZSAH POUZE PRO PROHLÍŽEČ

Proxy nastavená v jednom prohlížeči ovlivňuje jen tento prohlížeč; e-mailoví klienti, hry a systémové aktualizace dál používají běžné připojení zařízení.

9. TOR VS. PROXY

Tor posílá provoz přes tři dobrovolnická relé (vstupní, prostřední a výstupní) a obvykle se k němu přistupuje přes lokální SOCKS proxy, což přidává vrstvy, které jedna proxy nemá.

10. KOMPROMIS RYCHLOSTI

Proxy se mohou zdát rychlejší, protože vynechávají šifrování, ale moderní VPN protokoly jako WireGuard přidávají minimální režii a přitom chrání veškerý provoz zařízení.

Technické reference a zdroje

Citované publikace, kryptografické specifikace a oficiální dokumentační standardy použité v celém tomto pracovním listu.

AKADEMICKÉ A OBOROVÉ REFERENCE

[1] IETF. (1996). RFC 1928: SOCKS Protocol Version 5.
https://datatracker.ietf.org/doc/html/rfc1928

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

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

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

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

Klíč odpovědí: Porovnání proxy serverů a virtuálních privátních sítí, rozdílů v šifrování a směrování na úrovni aplikace vs. celého systému

1 OSI vrstva proxy

PROTOKOLY

Správná odpověď: C

POZNÁMKA PRO VYUČUJÍCÍ

Standardní HTTP/HTTPS proxy fungují na aplikační vrstvě (vrstva 7) a přesměrovávají konkrétní provoz prohlížeče. Postrádají celosystémové síťové směrování.

2 Otázka 2

Správná odpověď: B

POZNÁMKA PRO VYUČUJÍCÍ

SOCKS5 přenáší provoz TCP a UDP mezi aplikační a transportní vrstvou, ale ve výchozím stavu nešifruje, zatímco HTTP proxy zpracovávají webové požadavky.

3 Systémové šifrování VPN

ZABEZPEČENÍ WI-FI

Správná odpověď: B

POZNÁMKA PRO VYUČUJÍCÍ

VPN zapouzdřuje a šifruje veškerý provoz operačního systému v celém systému, zatímco proxy přesměrovává provoz pouze pro konkrétní nakonfigurované aplikace.

4 Absence šifrování u proxy

ŘÍZENÍ SMĚROVÁNÍ

Správná odpověď: A

POZNÁMKA PRO VYUČUJÍCÍ

HTTP proxy předávají provoz prohlížeče na aplikační vrstvě bez šifrování obsahu paketů, což znamená, že váš provozovatel sítě nebo ISP může stále sledovat váš obsahový provoz.

5 Zranitelnost umožňující obejití

SOUKROMÍ

Správná odpověď: D

POZNÁMKA PRO VYUČUJÍCÍ

Proxy v prohlížeči uplatňují pravidla jen na samotný webový prohlížeč. Aplikace na pozadí, aktualizace operačního systému a e-mailoví klienti proxy obcházejí a odhalují vaši nativní IP adresu.

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Otázka 6** Správná odpověď: Nepravda

POZNÁMKA PRO VYUČUJÍCÍ

SOCKS5 přenáší provoz mezi aplikační a transportní vrstvou, ale ve výchozím stavu neprovádí žádné šifrování, takže obsah paketů zůstává při přenosu čitelný.

7 **Tunely síťové vrstvy** RYCHLOSTI Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

Díky běhu na síťové vrstvě VPN směruje a šifruje odchozí provoz z vašeho zařízení, což pomáhá chránit provoz v celém systému.

8 **Šifrovací limit proxy** RIZIKO SNIFFINGU Správná odpověď: Nepravda

POZNÁMKA PRO VYUČUJÍCÍ

Proxy mohou být někdy rychlejší, ale jen proto, že NEPROVÁDĚJÍ šifrování. Tato absence šifrování nechává data zranitelná vůči inspekci.

9 **Přesměrování na úrovni aplikací** FIREWALLY Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

Na rozdíl od celosystémových VPN vyžadují proxy servery ruční nastavení v prohlížeči nebo v polích proxy konkrétních aplikací.

10 **Riziko sledování ze strany ISP** NO-LOGS Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

Protože standardní HTTP/SOCKS5 proxy nešifrují datovou část, váš místní ISP má i nadále plný přehled o vašich online aktivitách.

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

G 1. HTTP proxy	H 2. SOCKS5 proxy	E 3. VPN tunel	A 4. Celosystémové
B 5. Vrstva OSI 7	C 6. Podpora UDP	D 7. Proxy v prohlížeči	F 8. Viditelnost pro ISP

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 PROXY	2 VPN TUNEL	3 SOCKS5	4 APLIKAČNÍ
5 ŠIFROVÁNÍ	6 CELOSYSTÉMOVÉ		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 E – SEDMÁVRSTVA	2 F – PODPORAUDP	3 A – HTTPPROXY	4 G – PROXYPROHLIZEC
5 C – VPNTUNEL	6 D – CELOSYSTÉMOVÉ	7 H – VIDITELNOST	8 B – SOCKSPROXY

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy HTTP proxy, SOCKS5 proxy a VPN tunel a ke každému uvést příklad.

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

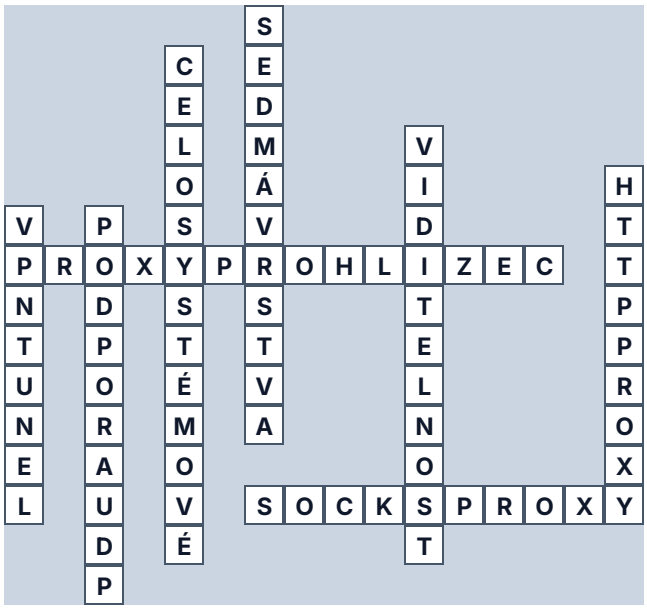
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

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

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

7 vodorovně: PROXYPROHLIZEC Rozšíření klienta skrývající pouze provoz uvnitř sandboxu prohlížeče (14 písmen)

8 vodorovně: SOCKSPROXY Proxy protokol mezi aplikační a transportní vrstvou, bez šifrování (10 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: SEDMÁVRSTVA Aplikační vrstva, kde fungují standardní webové proxy protokoly (11 písmen)

2 svisle: CELOSYSTÉMOVÉ Směrování na úrovni operačního systému šifrující provoz všech aplikací (13 písmen)

3 svisle: VIDITELNOST Stav provozu, kdy nešifrovaná proxy data zůstávají viditelná poskytovatelům (11 písmen)

4 svisle: HTTPPROXY Proxy aplikační vrstvy přesměrovávající vybraný provoz webového prohlížeče (9 písmen)

5 svisle: VPNTUNEL Šifrování a zapouzdření obalující veškerý provoz zařízení na pozadí (8 písmen)

6 svisle: PODPORAUDP Schopnost SOCKS5 přenášet UDP i TCP, na rozdíl od čistých HTTP proxy (10 písmen)

Klíč řešení přesmyček a šifry

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

KLÍČ K PŘESMYČKÁM

1. RPPTHOXYT — HTTPPROXY
2. TVLPENUN — VPNTUNEL
3. SRVSDEVAÁTM — SEDMÁVRSTVA
4. RRELXHPCOZIPOY — PROXYPROHLIZEC
5. OPYOKRSSXC — SOCKSPROXY
6. SMSYOLVÉCETÉO — CELOSYSTÉMOVÉ
7. OPPARUDPOD — PODPORAUDP
8. OLTEDVTISNI — VIDITELNOST

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"PŘESMĚRUJTE SVŮJ PROVOZ PŘES PROXY"

Klíč k případovým studiím

A Scénář A: Bezpečnost na veřejné síti

SNIFFING A ŠIFROVÁNÍ | Sarahino dilema

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Rizika: Odposlech paketů (sniffing), zachycení dat a útoky man-in-the-middle. Někdo na stejné kavárenské síti by mohl zachytit její přihlašovací údaje nebo soubor s úkolem.
- Proxy vs VPN: Základní proxy v prohlížeči její provoz nešifruje. VPN šifruje vše na zařízení, takže zachycené pakety jsou pro místní slídily nečitelné.

B Scénář B: Přístup k blokovaným zdrojům

GEOBLOKACE A IP ADRESY | Alexovo dilema

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Proč blokováno: Streamovací služba používá geoblokaci, která mapuje cestovatelovu lokální IP adresu na jeho fyzickou zemi a blokuje ji na základě územních licencí.
- Co funguje lépe: Obojí mu poskytne IP domovské země, ale proxy pokrývá jen nakonfigurovanou aplikaci, zatímco VPN navíc šifruje veškerý provoz jeho zařízení.