Jméno: _____ Datum: _____ Body: _____

Co je VPN Pracovní list

Praktická cvičení ze síťových protokolů, tunelování a bezpečnostních kontrol.

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

- Vysvětlete koncept tunelování dat a zapouzdření.
- Určete standardní konfigurace protokolů a metody šifrování.
- Analyzujte role serverů a maskování IP ve virtuálních privátních sítích.
- Pochopte, jak ISP sledují prohlížení a jak tomu VPN brání.
- Rozlište provozní hranice virtuální síťové topologie.

PRŮVODCE CO JE 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 reálné scénáře v sekci případových studií. Zakončete bonusovou aktivitou Mysli rychle.

CO JE VPN? (ÚVOD)

Virtuální privátní síť je víc než jen přepínač soukromí. Je to šifrovaný tunel, který směruje váš internetový provoz přes vzdálený server. Tím skrývá vaši IP adresu, brání vašemu ISP v sestavování záznamů o vašich online akcích a zabezpečuje vaše data ve veřejných sítích. Porozumění terminologii je zásadní pro udržení digitální bezpečnosti.

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

Kontrolní bod 1: Výzva s výběrem odpovědí

1 **1. Jaká je primární funkce virtuální privátní sítě (VPN)?**

- A. Zvýšit rychlost vykreslování internetového prohlížeče
- B. Šifrovat datové pakety a maskovat vaši veřejnou IP
- C. Ukládat databáze cookies webů lokálně
- D. Nahradit fyzický hardware počítače

2 **2. Co je síťové tunelování v kontextu VPN?**

- A. Mazání duplicitních souborů síťových logů
- B. Instalace místních úložných souborů databáze
- C. Sdílení souborů s ostatními místními počítači
- D. Zapouzdření jednoho síťového paketu do jiného zabezpečeného paketu

3 **3. Který šifrovací standard se široce používá k ochraně provozu VPN?**

- A. Zastaralé šifrování DES
- B. Moderní standard AES-256
- C. Kódování base64 v prostém textu
- D. Běžná šifra rot13

4 **4. Která součást vašeho síťového provozu je šifrována VPN?**

- A. Pouze tiskové úlohy místní sítě zařízení
- B. Fyzická trasa vedení ethernetového kabelu
- C. Celá datová část (payload) síťového paketu
- D. Pouze historie vyhledávání ve vašem prohlížeči

5 **5. Co znamená pojem 'šifrování' v sítích?**

- A. Převod čitelných dat na nečitelný šifrovaný text
- B. Mazání starých záznamů komunikace
- C. Zvyšování limitů rychlosti vaší místní šířky pásma
- D. Veřejné sdílení přístupových klíčů k databázi

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. VPN šifruje váš provoz, aby zabránila místnímu odposlechu na veřejné Wi-Fi.

- ○ Pravda
- ○ Nepravda

7 Otázka 7

7. VPN fyzicky mění hardwarovou konfiguraci vašeho routeru.

- ○ Pravda
- ○ Nepravda

8 Otázka 8

8. Tunelovací protokoly balí datové pakety do šifrované transportní vrstvy.

- ○ Pravda
- ○ Nepravda

9 Otázka 9

9. Symetrické šifrování používá stejný klíč k šifrování i dešifrování provozu.

- ○ Pravda
- ○ Nepravda

10 Otázka 10

10. Použití VPN činí vaše internetové připojení fyzicky imunním vůči výpadkům proudu.

- ○ Pravda
- ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

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

1. Pro zabezpečení provozu balí VPN vaše datové pakety do jiného protokolu, což je proces známý jako _____ .

2. Pomalé stahování při streamování může způsobovat omezená síťová _____ .

3. Streamovací služba dostupná pouze v konkrétní zemi omezuje globální uživatele pomocí _____ .

4. Sada pravidel definující šifrovací a připojovací parametry se nazývá VPN _____ .

5. Síťový provoz sleduje a nebezpečná připojení blokuje místní _____ ve vašem počítači.

6. Po připojení k VPN směruje vaše data vzdálený _____ , který skryje vaši veřejnou IP.

ZÁSOBNÍK SLOV

FIREWALL GEOBLOKACE POSKYTOVATEL PROTOKOL SERVER SOUKROMÍ ŠÍŘKA PÁSMA TUNELOVÁNÍ

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování síťových pojmů

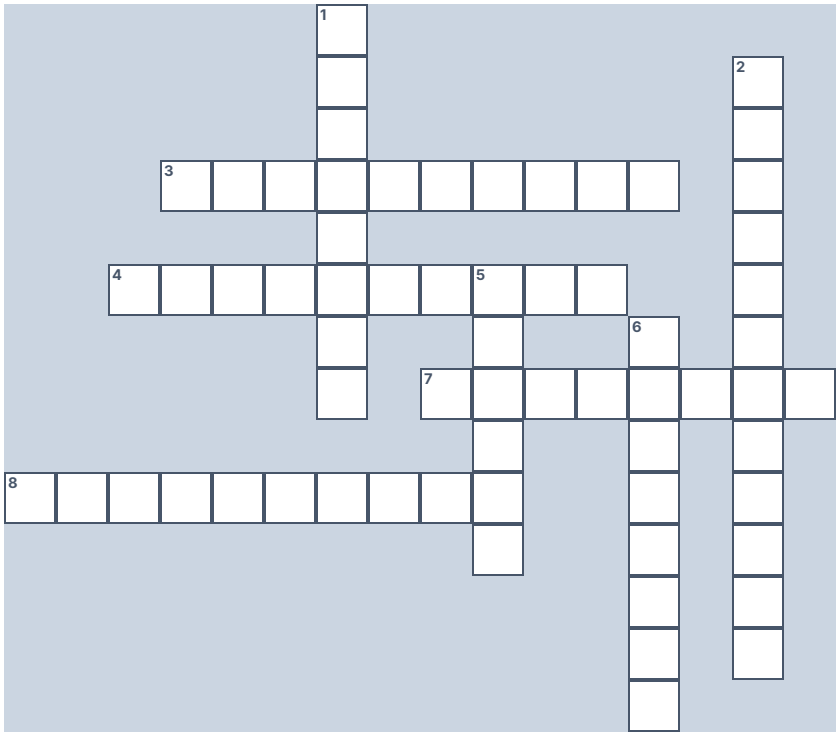
PŘIŘAZOVÁNÍ DEFINIC

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

☐	1. Tunelování	A	Vzdálený počítač, který směruje váš provoz a maskuje vaši IP.
☐	2. Protokol	B	Poskytovatel internetových služeb, který přenáší váš provoz a vidí nešifrovanou aktivitu.
☐	3. Šířka pásma	C	Omezení bránící přístupu na web na základě fyzické polohy.
☐	4. Server	D	Bezpečnostní systém, který monitoruje a blokuje neoprávněný provoz.
☐	5. Geoblokace	E	Soubor pravidel určujících, jak jsou data přenášena po síti.
☐	6. Firewall	F	Stav, kdy člověk není sledován ani veřejně monitorován.
☐	7. Soukromí	G	Maximální rychlost přenosu dat přes připojení.
☐	8. ISP	H	Zabalení datových paketů do jiného paketu pro bezpečný přenos.

Kontrolní bod 5: Křížovka

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



VODOROVNÉ NÁPOVĚDY

3. Balení datových paketů do jiného paketu pro bezpečný přenos (10)

4. Maximální rychlost přenosu dat přes připojení (10)

7. Soubor pravidel určujících, jak jsou data přenášena sítí (8)

8. Omezení bránící přístupu na web podle fyzické polohy (10)

SVISLÉ NÁPOVĚDY

1. Bezpečnostní systém, který sleduje a blokuje neoprávněný provoz (8)

2. Poskytovatel internetových služeb, který loguje váš provoz, pokud není šifrován (12)

5. Vzdálený počítač, který směruje váš provoz a maskuje vaši IP (6)

6. Stav bez sledování a veřejného dohledu (8)

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: Balení datových paketů do jiného paketu pro bezpečný přenos (10 písmen):

4 vodorovně: Maximální rychlost přenosu dat přes připojení (10 písmen):

7 vodorovně: Soubor pravidel určujících, jak jsou data přenášena sítí (8 písmen):

8 vodorovně: Omezení bránící přístupu na web podle fyzické polohy (10 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Bezpečnostní systém, který sleduje a blokuje neoprávněný provoz (8 písmen):

2 svisle: Poskytovatel internetových služeb, který loguje váš provoz, pokud není šifrován (12 písmen):

5 svisle: Vzdálený počítač, který směruje váš provoz a maskuje vaši IP (6 písmen):

6 svisle: Stav bez sledování a veřejného dohledu (8 písmen):

Kontrolní bod 6: Hledání skrytých slov

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

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

SEZNAM SLOV

TUNELOVÁNÍ PROTOKOL ŠÍŘKAPÁSMA SERVER GEOBLOKACE FIREWALL SOUKROMÍ POSKYTOVATEL

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. TUNELOVÁNÍ**
- **B. PROTOKOL**
- **C. ŠÍŘKAPÁSMA**
- **D. SERVER**
- **E. GEOBLOKACE**
- **F. FIREWALL**
- **G. SOUKROMÍ**
- **H. POSKYTOVATEL**

DEFINICE A POLE K PŘIŘAZENÍ

1. Soubor pravidel určujících, jak jsou data přenášena sítí.
2. Omezení bránící přístupu na web podle fyzické polohy.
3. Bezpečnostní systém, který sleduje a blokuje neoprávněný provoz.
4. Stav bez sledování a veřejného dohledu.
5. Poskytovatel internetových služeb, který loguje váš provoz, pokud není šifrován.
6. Balení datových paketů do jiného paketu pro bezpečný přenos.
7. Vzdálený počítač, který směruje váš provoz a maskuje vaši IP.
8. Maximální rychlost přenosu dat přes připojení.

Kontrolní bod 7: Výzva s přeházenými slovy

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

1. NVOLUTÁÍEN
2. MKŠÍAAÁSPŘ
3. GOCKELEBAO
4. KMÍORSOU
5. OKRLTPOO
6. EVSRRE
7. FLWALIER
8. VSYTOLPTOE AK

Bonusová aktivita: Mysli rychle

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

1	Věci, které může prozradit IP adresa			
2	Mýty o VPN			
3	Věci, které putují internetem			
4	Sliby, které dává dobrý poskytovatel VPN			
5	Tajemství, která byste zašifrovali			
6	Věci, před kterými vás VPN neochrání			
7	Způsoby, jak poznat falešnou Wi-Fi síť			
8	Slova související se soukromím			
9	Zařízení, která mohou používat VPN			
10	Věci, které se stanou, když stisknete „Připojit“			
11	Místa, kde byste použili VPN			
12	Důvody, proč používat VPN na cestách			
13	Věci ze skutečného života, které vypadají jako tunel			
14	Slova z tohoto pracovního listu, která si chcete zapamatovat			
15	Slova, kterými byste vysvětlili VPN dítěti			

Kontrolní bod 8: Případové studie VPN

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

SARAH (STUDENTKA V KAVÁRNĚ)

👩‍💻 "Ahoj! Sedím v Coffee & Bytes. Je tu nezabezpečená veřejná síť 'Free_Wi-Fi_No_Password'. Chci se přihlásit do školního e-mailu a nahrát úkol, ale bojím se hackerů. Jaká jsou rizika používání této sítě bez VPN a jak VPN zabezpečí moje data?"

ALEX (CESTUJÍCÍ STUDENT)

👩‍💻 "Ale ne! Cestuji kvůli projektu v zahraničí a snažím se sledovat biologický dokument hostovaný na serveru v mé domovské zemi. Web ale hlásí 'Toto video není ve vaší aktuální lokalitě dostupné.' Proč jsem blokován a jak mi VPN pomůže ho sledovat?"

Kontrolní bod 9: Dešifrování šifry

VPN šifruje váš provoz, aby jej zabezpečila. Pomocí níže uvedeného klíče písmeno–číslo dešifrujte kyberbezpečnostní 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

4	13	26	1	21	30	8		28	35	9		28	22	32	17	26	22	19	15
3	8	40	24	8	5	20	39	19		30	32	20	8	18	8	19			

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: Proč bych měl používat VPN?

VPN chrání vaše digitální soukromí, zabezpečuje připojení na veřejných Wi-Fi sítích (například v kavárnách nebo na letištích), může omezit zpomalování podle typu aktivity, když ISP nedokáže identifikovat druh šifrovaného provozu, obchází geografická omezení pro přístup ke globálnímu obsahu a pomáhá zabezpečit prostředky pro práci na dálku.

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 používání VPN legální?

Používání VPN je v mnoha zemích legální, ale některé jurisdikce služby VPN omezují, regulují nebo blokují. Uživatelé by si měli před použitím ověřit aktuální místní zákony. Podrobnosti najdete v průvodcích legálností na VPN.com.

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 VPN?

Bezplatné VPN se mohou spoléhat na reklamu, omezené funkce, analytiku používání, datové limity nebo jiné modely monetizace. Uživatelé by si měli před použitím prostudovat zásady ochrany soukromí poskytovatele, jeho vlastnictví, audity a obchodní model.

Q7: Co je politika "nulových logů"?

Zásada nulových logů popisuje, která data o aktivitě a připojení poskytovatel podle svého prohlášení neuchovává. Přesný rozsah se liší, proto by si čtenáři měli prostudovat zásady i zjištění nezávislých auditů.

Q8: Jak si vyberu nejlepší VPN?

Hledejte auditované zásady no-logs, silné protokoly (WireGuard, OpenVPN), bezpečné lokality serverů, vysoké rychlosti, servery běžící pouze v RAM, funkci kill switch a jurisdikci mimo aliance sdílející zpravodajské informace (jako 5/9/14 očí).

Q9: Mohu VPN používat na telefonu i chytré televizi?

Ano. Moderní poskytovatelé VPN nabízejí vyhrazené aplikace pro iOS, Android, macOS, Windows, Linux a chytré televize a také nastavení na routeru pro ochranu všech zařízení ve vaší domácí síti.

Q10: Co je kill switch?

Kill switch je bezpečnostní funkce, která automaticky odpojí vaše zařízení od internetu, pokud spojení VPN vypadne. Tím zabraňuje úniku vašich nešifrovaných dat nebo skutečné IP adresy.

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

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

Q1: Jaký je rozdíl mezi WireGuardem, OpenVPN a IKEv2?

WireGuard je moderní, odlehčený protokol (jen ~4,000 řádků kódu) nabízející vysoké rychlosti a rychlá připojení. OpenVPN je vysoce bezpečný, prověřený open-source protokol. IKEv2 je vynikající pro mobilní zařízení díky schopnosti rychle se znovu připojit při změně sítě. [4]

Q2: Co je dvojitá VPN neboli směrování Multi-Hop?

Multi-Hop směruje váš provoz postupně přes dva a více serverů VPN. Přidává tak druhou vrstvu šifrování a pomáhá udržet vaši skutečnou IP adresu skrytou před druhým skokem, pokud by byl jeden server kompromitován.

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 jsou RAM-only servery a proč na nich záleží?

Tradiční servery zapisují data na pevné disky, které lze zabavit nebo kompromitovat. RAM-only (bezdiskové) servery běží výhradně ve volatilní paměti (RAM). Při restartu nebo vypnutí serveru se data v paměti vymažou.

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: Jak funguje Forward Secrecy (Perfect Forward Secrecy)?

PFS zajišťuje, že pro každou jednotlivou relaci se generuje jedinečný, dočasný šifrovací klíč. I když bude privátní klíč v budoucnu kompromitován, nelze jej použít k dešifrování minulých ani budoucích relací, protože ty používaly nezávislé klíče.

Q8: Co jsou aliance 5/9/14 Eyes a proč by mě měly zajímat?

Jurisdikce může ovlivnit právní proces, kterému poskytovatel může čelit, ale praktické riziko pro soukromí závisí také na tom, jaká data poskytovatel uchovává, na jeho technické architektuře, vlastnictví, zprávách o transparentnosti a historii auditů.

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 VPN obejít škrcení internetu poskytovatelem?

Někdy. VPN může pomoci, když ISP selektivně zpomaluje identifikovatelné aktivity, ale nepřekoná přetížení, datové limity, rychlostní limity na úrovni účtu ani špatnou kvalitu sítě.

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. PRVNÍ VPN PROTOKOL

PPTP (Point-to-Point Tunneling Protocol) byl vyvinut skupinou dodavatelů včetně Microsoftu a publikován jako RFC 2637 v červenci 1999 pro podporu VPN se vzdáleným přístupem. [6]

2. TRŽNÍ OCENĚNÍ

Globální trh s VPN zažil rychlý růst, tažený rostoucími požadavky práce na dálku a poptávkou po podnikové bezpečnosti.

3. REVOLUCE WIREGUARD

WireGuard má vysoce zjednodušenou kódovou základnu navrženou pro efektivitu, takže se snáze audituje na bezpečnostní zranitelnosti než tradiční protokoly. [4]

4. PŘÍSNÉ AUDITNÍ STANDARDY

Přední poskytovatelé VPN najímají externí auditory (jako Cure53 nebo PwC) k nezávislým revizím kódu a ověření, že nelogují žádnou aktivitu uživatelů.

5. POČÁTKY ALIANCE 5 OČÍ

Aliance Five Eyes vyrostla z dohody UKUSA o signálovém zpravodajství z roku 1946 mezi USA a Spojeným královstvím, k níž se později připojily Kanada, Austrálie a Nový Zéland.

6. HLOUBKOVÁ INSPEKCE PAKETŮ

Hloubková inspekce paketů (DPI) zkoumá obsah paketů a vzorce provozu, nejen hlavičky, a některé firewally ji používají k detekci a blokování běžných VPN protokolů.

7. FIREMNÍ VYUŽITÍ

Velké procento zaměstnanců podniků po celém světě používá zabezpečené VPN k přihlašování do interních databází, což z nich činí klíčový bezpečnostní standard.

8. DECENTRALIZOVANÉ VPN

Decentralizované VPN (dVPN) rozdělují provoz přes síť uzlů provozovaných jednotlivci, čímž snižují závislost na jediném centralizovaném poskytovateli.

9. ANONYMITA TOR VS. VPN

VPN tuneluje provoz přes jediného poskytovatele, zatímco Tor (The Onion Router) posílá provoz přes tři dobrovolnická relé (vstupní, prostřední a výstupní), takže žádné jednotlivé relé nezná oba konce.

10. NÁKLADY NA ÚNIKY DAT

Zavedení modelu zabezpečeného přístupu zero-trust s VPN pomáhá organizacím chránit duševní vlastnictví a zmírnit finanční dopad úniků dat.

Technické reference a zdroje

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

AKADEMICKÉ A OBOROVÉ REFERENCE

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/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] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

Klíč odpovědí: Pracovní list Co je VPN

1 **Primární funkce** PROTOKOLY — **Správná odpověď: B**

POZNÁMKA PRO VYUČUJÍCÍ

Hlavním úkolem VPN je vytvořit šifrovaný tunel, který chrání obsah datových paketů a maskuje veřejnou IP adresu uživatele.

2 **Síťové tunelování** LATENCE — **Správná odpověď: D**

POZNÁMKA PRO VYUČUJÍCÍ

Tunelovací protokoly zapouzdřují původní datové pakety do vnějších nosných paketů pro bezpečný průchod veřejnými sítěmi.

3 **Otázka 3** — **Správná odpověď: B**

POZNÁMKA PRO VYUČUJÍCÍ

Který šifrovací standard se široce používá k ochraně provozu VPN? → Moderní standard AES-256

4 **Šifrované komponenty** ŘÍZENÍ SMĚROVÁNÍ — **Správná odpověď: C**

POZNÁMKA PRO VYUČUJÍCÍ

VPN šifruje celý datový segment IP paketů, čímž udržuje obsah přenosu důvěrný.

5 **Otázka 5** — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Šifrování používá algoritmus a klíč k přeměně prostého textu na nečitelný šifrovaný text.

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Blokování odposlechu** MASKOVÁNÍ IP

Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

Šifrované tunely zajišťují, že obsah paketů zůstane nečitelný pro aktéry zachytávající data na místních Wi-Fi sítích.

7 **Změny hardwaru** RYCHLOSTI

Správná odpověď: Nepravda

POZNÁMKA PRO VYUČUJÍCÍ

VPN jsou softwarové síťové tunely a fyzicky neupravují hardware vašeho routeru.

8 **Tunelování paketů** RIZIKO SNIFFINGU

Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

Tunelování funguje tak, že původní síťové pakety obalí transportními hlavičkami pro přenos.

9 **Symetrické klíče** FIREWALLY

Správná odpověď: Pravda

POZNÁMKA PRO VYUČUJÍCÍ

Symetrická kryptografie využívá sdílený klíč k šifrování i dešifrování síťových streamů.

10 **Odolnost proti výpadku napájení** NO-LOGS

Správná odpověď: Nepravda

POZNÁMKA PRO VYUČUJÍCÍ

VPN pouze šifruje aktivní signály připojení; nemůže zabránit výpadkům služby způsobeným místními výpadky proudu.

Klíče slovní zásoby a hodnoticí rubrika

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

KONTROLNÍ BOD 4: KLÍČ K PŘIŘAZOVÁNÍ POJMŮ

H 1. Tunelování	E 2. Protokol	G 3. Šířka pásma	A 4. Server
C 5. Geoblokace	D 6. Firewall	F 7. Soukromí	B 8. ISP

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 TUNELOVÁNÍ	2 ŠÍŘKA PÁSMA	3 GEOBLOKACE	4 PROTOKOL
5 FIREWALL	6 SERVER		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 B – PROTOKOL	2 E – GEOBLOKACE	3 F – FIREWALL	4 G – SOUKROMÍ
5 H – POSKYTOVATEL	6 A – TUNELOVÁNÍ	7 D – SERVER	8 C – ŠÍŘKAPÁSMA

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy Tunelování, Protokol a Šířka pásma a ke každému uvést příklad.

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

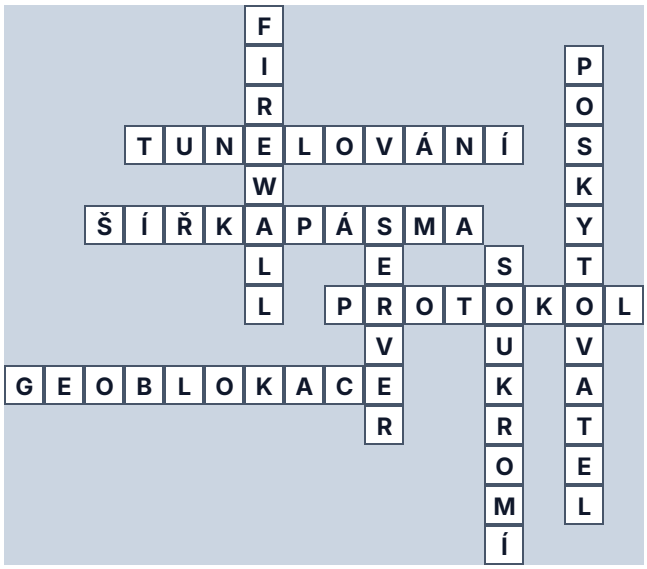
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

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

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

3 vodorovně: TUNELOVÁNÍ Balení datových paketů do jiného paketu pro bezpečný přenos (10 písmen)

4 vodorovně: ŠÍŘKAPÁSMA Maximální rychlost přenosu dat přes připojení (10 písmen)

7 vodorovně: PROTOKOL Soubor pravidel určujících, jak jsou data přenášena sítí (8 písmen)

8 vodorovně: GEOBLOKACE Omezení bránící přístupu na web podle fyzické polohy (10 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: FIREWALL Bezpečnostní systém, který sleduje a blokuje neoprávněný provoz (8 písmen)

2 svisle: POSKYTOVATEL Poskytovatel internetových služeb, který loguje váš provoz, pokud není šifrován (12 písmen)

5 svisle: SERVER Vzdálený počítač, který směruje váš provoz a maskuje vaši IP (6 písmen)

6 svisle: SOUKROMÍ Stav bez sledování a veřejného dohledu (8 písmen)

Klíč řešení přesmyček a šifry

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

KLÍČ K PŘESMYČKÁM

1. NVOLUTÁÍEN — TUNELOVÁNÍ
2. MKŠÍAAÁSPŘ — ŠÍŘKAPÁSMA
3. GOCKELEBAO — GEOBLOKACE
4. KMÍORSOU — SOUKROMÍ
5. OKRLTPOO — PROTOKOL
6. EVSRRE — SERVER
7. FLWALIER — FIREWALL
8. VSYTOLPTOEAK — POSKYTOVATEL

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"CHRAŇTE SVÉ SOUKROMÍ BEZPEČNÝM TUNELEM"

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.
- Ochrana VPN: Šifruje obsah síťových paketů, takže zachycený tunelový provoz je pro pasivní odposlech v místní síti nečitelný, je-li VPN správně nakonfigurována.

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.
- Jak VPN pomáhá: Maskuje jeho skutečnou polohu směrováním provozu přes server v jeho domovské zemi. Web vidí IP adresu domovské země a umožní přístup.