Namn: _____ Datum: _____ Poäng: _____

WireGuard mot OpenVPN Arbetsblad

Jämförelse av protokollen WireGuard och OpenVPN, kodbasernas storlek, hastighet och kryptografiska standarder

LÄRANDEÖVERSIKT OM VPN

ELEV
STUDENTSTATUS
Nätverksförsvararspåret

SÄKER
ANSLUTNINGSSTATUS
Skydda datapaket

AKTIV
LÄCKSKYDD
Skydd mot DNS- och IPv6-läckor

Välkommen! Det här aktivitetshäftet guidar dig genom grundläggande principer för virtuella privata nätverk (VPN). Du utforskar hur krypterade tunnlar skyddar dina data, hur nätverksprotokoll fungerar och hur du identifierar och åtgärdar integritetsläckor.

KONTROLLPUNKTER I ARBETSBLADET

- [ ] **Del 1-4: Behärska VPN-begrepp och protokoll.**
- [ ] **Del 5-7: Lös korsord och ordsökare.**
- [ ] **Del 8-9: Lös fallstudier och chifferutmaning.**
- [ ] **Del 10: Gå igenom sidorna med grundläggande och avancerade vanliga frågor.**
- [ ] **Del 11: Utforska 10 intressanta fakta från verkligheten.**
- [ ] **Bonus: utmaningen Tänk snabbt.**

Öppna VPN.com:s VPN-guide

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

Din inlärningsplan för VPN

- Jämför kodbasens komplexitet och granskningshastighet för protokoll.
- Analysera prestandavinsterna av att köra i kärnutrymmet.
- Jämför OpenSSL-chiffer med WireGuards moderna kryptografi.
- Ställ in publika och privata nyckelpar för peer-handskakningar.
- Dirigera VPN-trafik genom brandväggsportar för TCP och UDP.

INSTRUKTIONER FÖR ARBETSBLADET OM PROTOKOLLJÄMFÖRELSE

Besvara flervalsfrågorna och sant/falskt-frågorna, fyll i luckorna med hjälp av ordbanken, matcha definitioner och lös korsordet och ordletarpusslet. Tillämpa dina kunskaper om granskning av moderna protokoll. Avsluta med bonusaktiviteten Tänk snabbt.

WIREGUARD MOT OPENVPN (INTRODUKTION)

Valet av VPN-protokoll kräver en avvägning mellan hastighet och konfigurationsmöjligheter. OpenVPN har varit standarden i decennier och erbjuder flexibla TCP/UDP-inställningar. WireGuard är en modern ersättare som körs direkt i kärnutrymmet med bara 4 000 rader kod. Att förstå skillnaderna mellan protokoll är avgörande för att optimera dina säkra nätverk.

LÄS VARJE KONTROLLPUNKT NOGGRANT OCH VÄLJ ELLER SKRIV DET RÄTTA SVARET.

Kontrollpunkt 1: Utmaning med flerval

1. **1. Hur stor är ungefär kodbasen i protokollet WireGuard?**
   - A. Ungefär 70 000 rader
   - B. Över 100 000 rader
   - C. Färre än 1 000 rader
   - D. Cirka 4 000 rader

2. **2. I vilken del av operativsystemet körs WireGuard?**
   - A. Användarutrymme
   - B. Kärnrymd
   - C. Applikationsutrymme
   - D. Virtuellt utrymme

3. **3. Vilket kryptografiskt bibliotek förlitar sig OpenVPN främst på?**
   - A. ChaCha20-Poly1305
   - B. Kryptografibiblioteket OpenSSL
   - C. Ramverket Noise protocol
   - D. Klartextkodning med DES

4. **4. Vad är en viktig prestandafördel med WireGuard jämfört med OpenVPN?**
   - A. Snabbare anslutningshandskakningar och lägre fördröjning
   - B. Genom att slippa behovet av offentliga IP-adresser
   - C. Inbyggt stöd för äldre uppringd anslutning
   - D. Noll batteribelastning på mobila enheter

5. **5. Hur autentiserar WireGuard anslutningar mellan peers?**
   - A. Genom att byta vanliga användarlösenord
   - B. Genom att verifiera domänregistreringens certifikat
   - C. Genom att använda statiska offentliga och privata nyckelpar
   - D. Genom att kontrollera maskinvarans serienummer

Kontrollpunkt 2: Utmaning med sant eller falskt

6 Fråga 6

6. WireGuards kompakta kodbas gör det betydligt enklare att granska.

- ( ) Sant
- ( ) Falskt

7 Fråga 7

7. OpenVPN är i allmänhet snabbare än WireGuard eftersom det körs i kärnutrymmet.

- ( ) Sant
- ( ) Falskt

8 Fråga 8

8. OpenVPN är mycket konfigurerbart och stöder både UDP och TCP.

- ( ) Sant
- ( ) Falskt

9 Fråga 9

9. WireGuard använder modern kryptografi som ChaCha20 för snabb paketkryptering.

- ( ) Sant
- ( ) Falskt

10 Fråga 10

10. WireGuard kräver komplexa uppsättningar med certifikatutfärdare för att autentisera.

- ( ) Sant
- ( ) Falskt

Kontrollpunkt 3: Infoga nyckelbegrepp

Läs varje mening nedan och fyll i luckan med rätt term från ordbanken.

1. Det moderna protokollet _____ körs direkt i operativsystemets kärna.
2. Det äldre protokollet _____ förlitar sig på kryptobiblioteket OpenSSL.
3. Att köra kod i _____ minskar overhead vid kontextbyten.
4. OpenVPN körs i _____ och dirigerar paket via virtuella gränssnitt.
5. WireGuard använder offentliga och privata _____ för att identifiera anslutningens parter.
6. En liten kodbas förbättrar programvarans säkerhetsmässiga _____ .

ORDBANK

ANVÄNDARLÄGE GRANSKNINGSBARHET KÄRNLÄGE NYCKELPAR OPENSSL
OPENVPN TCP OCH UDP WIREGUARD

Skriv dina svar här:

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

Kontrollpunkt 4: Matchning av nätverksbegrepp

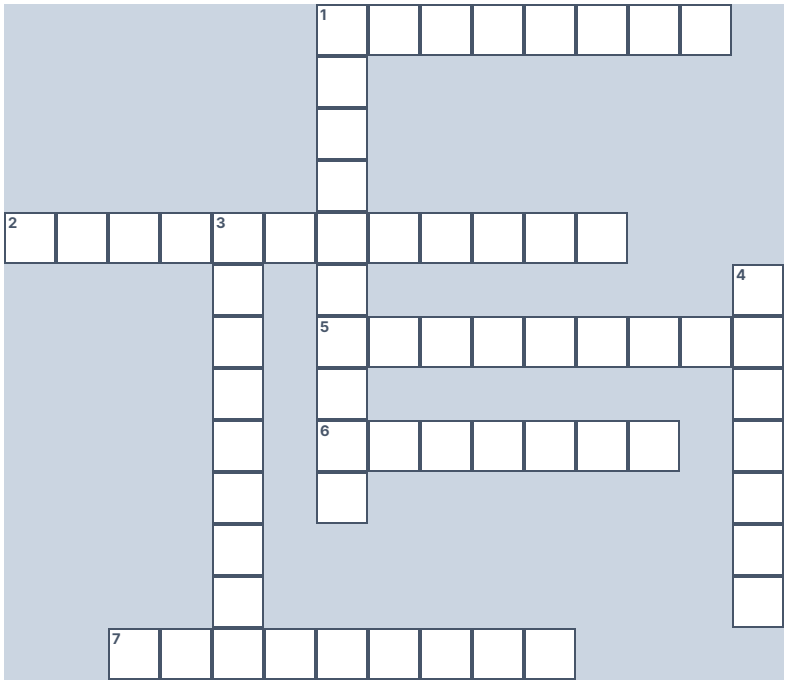
MATCHNING AV DEFINITIONER

Para ihop varje begrepp till vänster med rätt definition till höger genom att skriva motsvarande bokstav (A–H) i det ifyllbara fältet.

☐	1. WireGuard	A	Kområde där OpenVPN körs, vilket skapar belastning vid kontextbyten.
☐	2. OpenVPN	B	Den kompakta storleken på WireGuards kodbas, vilket gör den mycket lättare att granska.
☐	3. Kärnutrymme	C	Kryptografiskt bibliotek som OpenVPN förlitar sig på för chifferalgoritmer.
☐	4. Användarutrymme	D	Transportprotokoll som OpenVPN stöder; WireGuard själv körs bara över UDP.
☐	5. 4,000 rader	E	Det område i operativsystemet där WireGuard körs för att uppnå hastighet.
☐	6. OpenSSL	F	Asymmetriska nycklar som WireGuard använder för att verifiera peer-anslutningar.
☐	7. Nyckelpar	G	Modernt VPN-protokoll utformat för hög hastighet och enkel kodgranskning.
☐	8. TCP/UDP	H	Robust äldre protokoll med en stor, komplex konfigurationskodbas.

Kontrollpunkt 5: Korsord

Lös korsordet genom att skriva bokstäver i de aktiva vita rutorna. Siffrorna motsvarar ledtrådarna nedan.



VÅGRÄTT

1. Det område i operativsystemet där WireGuard körs för att uppnå hastighet (8)

2. Det körningsområde där OpenVPN körs, vilket skapar overhead vid kontextbyten (12)

5. Transportprotokoll som OpenVPN stöder; WireGuard körs själv bara över UDP (9)

6. Robust äldre protokoll med en stor och komplex konfigurationskodbas (7)

7. Modernt VPN-protokoll som är utformat för hög hastighet och enkel kodgranskning (9)

LODRÄTT

1. WireGuards kompakta kodbas, som gör den mycket enklare att granska (10)

3. Asymmetriska nycklar som WireGuard använder för att verifiera anslutningens parter (9)

4. Kryptografiskt bibliotek som OpenVPN förlitar sig på för chifferalgoritmer (7)

Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

Användare av skärmläsare och tangentbord kan skriva korsordssvaren direkt i textfälten nedan.

VÅGRÄTT

1 vågrätt: Det område i operativsystemet där WireGuard körs för att uppnå hastighet (8 bokstäver):

2 vågrätt: Det körningsområde där OpenVPN körs, vilket skapar overhead vid kontextbyten (12 bokstäver):

5 vågrätt: Transportprotokoll som OpenVPN stöder; WireGuard körs själv bara över UDP (9 bokstäver):

6 vågrätt: Robust äldre protokoll med en stor och komplex konfigurationskodbas (7 bokstäver):

7 vågrätt: Modernt VPN-protokoll som är utformat för hög hastighet och enkel kodgranskning (9 bokstäver):

LODRÄTT

1 lodrätt: WireGuards kompakta kodbas, som gör den mycket enklare att granska (10 bokstäver):

3 lodrätt: Asymmetriska nycklar som WireGuard använder för att verifiera anslutningens parter (9 bokstäver):

4 lodrätt: Kryptografiskt bibliotek som OpenVPN förlitar sig på för chifferalgoritmer (7 bokstäver):

Kontrollpunkt 6: Dolt ordsök

Hitta de 8 viktiga ordförrådstermerna som är gömda i rutnätet nedan. Orden kan vara vågräta, lodräta eller diagonala.

O P E N V P N N V Ä X C Ö Y G
L E I Ö D O E Y S Z T R C W B
D G A Ö P E M C A E C Q E F H
O Ä J D T S N K F J P U Ö U G
K L S Y F A A E S Q O O R W W
T N Å S L T W L U D C O Ä I B
K R G U Z Z K P A T H Ö Ä R Ä
A Ä M H J O T A L N U N V E Q
P K I S S H Ö R A Q D X G G X
M C Ä T Ä B I N Ö H P K P U R
O A N V Ä N D A R L Ä G E A P
K Z C N Ö Ä G Å Q Y X M X R R
B P O P E N S S L Y V N H D X
D Ä X L T B Z Ö Å N T S Å J Q
E A D L S Y Z Z M K I W I G B

ORDLISTA

WIREGUARD, OPENVPN, KÄRNLÄGE, ANVÄNDARLÄGE, KOMPAKTKOD, OPENSSL, NYCKELPAR, TCPOCHUDP

Kontrollpunkt 6, alternativ: Tillgänglig matchning av ordförråd

Para ihop var och en av de 8 begreppen från ordsökningen med rätt definition genom att skriva bokstaven (A–H) på den tomma raden.

ORDLISTA

- **A. WIREGUARD**
- **B. OPENVPN**
- **C. KÄRNLÄGE**
- **D. ANVÄNDARLÄGE**
- **E. KOMPAKTKOD**
- **F. OPENSSL**
- **G. NYCKELPAR**
- **H. TCPOCHUDP**

DEFINITIONER OCH MATCHNINGSFÄLT

_____ 1. Kryptografiskt bibliotek som OpenVPN förlitar sig på för chifferalgoritmer.

_____ 2. Det område i operativsystemet där WireGuard körs för att uppnå hastighet.

_____ 3. Robust äldre protokoll med en stor och komplex konfigurationskodbas.

_____ 4. Asymmetriska nycklar som WireGuard använder för att verifiera anslutningens parter.

_____ 5. Transportprotokoll som OpenVPN stöder; WireGuard körs själv bara över UDP.

_____ 6. WireGuards kompakta kodbas, som gör den mycket enklare att granska.

_____ 7. Modernt VPN-protokoll som är utformat för hög hastighet och enkel kodgranskning.

_____ 8. Det körningsområde där OpenVPN körs, vilket skapar overhead vid kontextbyten.

Kontrollpunkt 7: Utmaning med blandade ord

Avkoda bokstäverna nedan för att avslöja viktiga VPN-begrepp och termer. Skriv dina svar i de ifyllbara rutorna.

1. UGEIWARDR
2. NKEÄGÄLR
3. KKOTOADPKM
4. ERAKPLNYC
5. VNNEOPP
6. ENLÄDGRANAVÄ
7. OSSLPNE
8. PCDTOCHUP

Bonusaktivitet: Tänk snabbt

3 SVAR PER KATEGORI. DEN SOM FÖRST FYLLER I LISTAN VINNER.

1	Skäl till att välja WireGuard			
2	Löften som en bra VPN-leverantör ger			
3	Skäl till att välja OpenVPN			
4	Skäl till att använda ett VPN under resor			
5	Saker som din internetleverantör kan se			
6	Sätt att upptäcka ett falskt wifi-nätverk			
7	Myter om VPN			
8	Platser där du skulle använda ett VPN			
9	Snabba saker i vardagen			
10	Saker som ett VPN inte kan skydda dig från			
11	Saker som gör kod lättare att granska			
12	Saker som ett VPN kan dölja			
13	Skillnader mellan WireGuard och OpenVPN			
14	Ord som hör ihop med integritet			
15	Krypteringsnamn du känner till			

Kontrollpunkt 8: Fallstudier om VPN

Tillämpa de begrepp du har lärt dig för att lösa de verkliga scenarierna nedan.

SARAH (STUDENT PÅ KAFÉ)

👷 "Hej! Jag sitter på kafé-Wi-Fi och min VPN-app låter mig välja WireGuard eller OpenVPN. Mina videosamtal bryts hela tiden när jag går mellan kaféets nätverk och min mobils hotspot. Vilket protokoll ska jag välja, och varför skulle det klara bytet bättre?"

ALEX (RESANDE STUDENT)

👷 "Jag är utomlands på ett hotellnätverk som verkar blockera det mesta av VPN-trafiken. WireGuard ansluter inte alls, men jag måste nå skolans resurser hemma. Vad är det som troligen blockeras, och hur kan OpenVPN hjälpa mig att ta mig igenom?"

Kontrollpunkt 9: Knäck chiffret

För att slutföra din träning i protokollgranskning ska du dekryptera det här dolda meddelandet om körning i kärnutrymmet.

KRYPTERINGSNYCKEL FÖR BOKSTAV TILL SIFFRA

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26 Å=27 Ä=28 Ö=29

21 16 16 7 18 1 4 5 18 1 4 9 14

15 16 5 14 22 16 14 13 5 4 5 14

19 14 1 2 2 1 18 5 20 21 14 14 5 12

Avkodat meddelande:

TIPS: VARJE SIFFRA MOTSVARAR BOKSTAVENS PLATS I ALFABETET (T.EX. 1 = A, 2 = B, 29 = Ö).

Kontrollpunkt 10: Grundläggande vanliga frågor om VPN (Del A)

Gå igenom de vanligaste frågorna och svaren som presumtiva kunder har om att använda virtuella privata nätverk.

Q1: Vad är ett VPN och hur fungerar det?

Ett virtuellt privat nätverk (VPN) krypterar din internetanslutning och dirigerar din trafik via en säker fjärrserver. Det döljer din publika IP-adress och begränsar vad lokala nätverksobservatörer och din internetleverantör kan se av trafik som dirigeras genom VPN-tunneln.

Q2: Varför spelar protokoll roll?

Protokollet avgör hur din VPN-tjänst bygger sin tunnel, vilken kryptografi som skyddar dina data och hur snabbt den ansluter och återansluter. WireGuard och OpenVPN är de två protokoll med öppen källkod som de flesta VPN-appar erbjuder, och de gör olika avvägningar mellan enkelhet, hastighet och konfigurerbarhet.

Q3: Är någon av dem mer privat än den andra?

Inget av protokollen gör dig anonym. Båda krypterar tunneltrafiken med starka chiffer; din integritet beror främst på vad VPN-leverantören loggar och hur den hanterar nycklar, konton och servrar.

Q4: Gör ett VPN min internethastighet långsammare?

Ja, något. Krypteringsprocessen och det fysiska avståndet till VPN-servern ger ökad latens och extra belastning. Påverkan varierar med leverantör, protokoll, serveravstånd, enhet och nätverksförhållanden.

Q5: Är båda öppen källkod?

Ja. WireGuard och OpenVPN community edition publicerar båda sin källkod, så att oberoende forskare kan granska dem. WireGuards lilla kodbas gör en fullständig granskning betydligt snabbare.

Kontrollpunkt 10: Grundläggande vanliga frågor om VPN (Del B)

Gå igenom de vanligaste frågorna och svaren som presumtiva kunder har om att använda virtuella privata nätverk.

Q6: Vilken är snabbast?

WireGuard är vanligtvis snabbare: det körs i kärnan, använder slank ChaCha20-Poly1305-kryptering och slutför handskakningar snabbt. OpenVPN har mer overhead, men de verkliga hastigheterna beror också på serverbelastning och avstånd.

Q7: Kan båda köras över både TCP och UDP?

Nej. OpenVPN kan köras över UDP eller TCP, och TCP-läget hjälper i nätverk som blockerar UDP. WireGuard skickar sina paket bara över UDP, så det kan misslyckas i nätverk som bara tillåter TCP. [4]

Q8: Hur väljer jag det bästa VPN:et?

Leta efter granskade no-logs-policyer, starka protokoll (WireGuard, OpenVPN), säkra serverplatser, hög hastighet, servrar som bara använder RAM, en kill switch-funktion och en jurisdiktion utanför underrättelsedelande allianser (som 5/9/14 Eyes).

Q9: Kan jag använda WireGuard och OpenVPN på min mobil?

Ja. WireGuard fungerar på flera plattformar, med appar för Windows, macOS, Linux, iOS och Android, och det finns OpenVPN-klienter för samma system. De flesta VPN-appar låter dig välja någotdera. [1]

Q10: Varför är WireGuard så litet?

WireGuard stöder en fast uppsättning moderna chiffer i stället för många alternativ. Dess Linux-implementation behöver under 4 000 kodrader, vilket gör det enklare att granska än större VPN-kodbaser. [3]

Kontrollpunkt 10: Avancerade vanliga frågor om VPN (Del C)

Utforska tekniska och strukturella aspekter av virtuella privata nätverk och säkra tunnelprotokoll.

Q1: Vad är skillnaden mellan WireGuard, OpenVPN och IKEv2?

WireGuard är ett modernt, lättviktigt protokoll (bara cirka 4 000 kodrader) med hög hastighet och snabba anslutningstider. OpenVPN är ett mycket säkert, beprövat protokoll med öppen källkod. IKEv2 är utmärkt för mobila enheter tack vare att det snabbt kan återansluta när man byter nätverk.

Q2: Vilka chiffer använder WireGuard?

WireGuard använder ChaCha20 med Poly1305 för kryptering, Curve25519 för nyckelutbyte, BLAKE2s för hashning och ramverket Noise för handskakningen. Det finns ingen chifferförhandling, så användare kan inte välja ett svagt alternativ. [2]

Q3: Vilka chiffer och bibliotek kan OpenVPN använda?

OpenVPN är nära integrerat med biblioteket OpenSSL och använder TLS för att utbyta nycklar. Administratörer kan välja chiffer för datakanalen, till exempel AES-256-GCM, vilket ger flexibilitet men också utrymme för svaga inställningar. [4]

Q4: Hur autentiserar varje protokoll sina parter?

WireGuard-peers identifierar varandra med statiska publika nycklar, ungefär som när man utbyter SSH-nycklar, och varje nyckel kopplas till tillåtna tunnel-IP-adresser. OpenVPN förlitar sig oftast på en certifikatutfärdare med X.509-certifikat, ofta kombinerat med användarnamn och lösenord.

Q5: Hur kringgår obfuskering VPN-blockeringar?

Obfuskering (eller "stealth-VPN") förklär VPN-trafik så att den ser ut som vanlig HTTPS-trafik (port 443). Det kan hjälpa den att ta sig förbi djup paketinspektion (DPI) som regeringar eller skol- och kontorsnätverk använder för att blockera VPN.

Kontrollpunkt 10: Avancerade vanliga frågor om VPN (Del D)

Utforska tekniska och strukturella aspekter av virtuella privata nätverk och säkra tunnelprotokoll.

Q6: Vad händer när jag byter från Wi-Fi till mobilnät?

WireGuard är anslutningslöst: det skickar paket från den nya adressen och tunneln fortsätter efter en snabb handskakning. OpenVPN behåller sessionstillstånd, så ett nätverksbyte kan kräva en återanslutning som tar lite längre tid.

Q7: Hur fungerar Forward Secrecy (Perfect Forward Secrecy)?

PFS ser till att en unik, tillfällig krypteringsnyckel genereras för varje enskild session. Även om en privat nyckel skulle kompromitteras i framtiden kan den inte användas för att dekryptera tidigare eller framtida sessioner, eftersom de använde oberoende nycklar.

Q8: Är OpenVPN fortfarande ett bra val om WireGuard är snabbare?

Ja. OpenVPN är beprövat och vida spritt, körs över TCP när UDP är blockerat och stöder certifikatbaserade företagslösningar. Många leverantörer erbjuder båda protokollen så att användare kan byta om det ena är blockerat eller långsamt.

Q9: Vilka portar använder de?

OpenVPN:s standardport är 1194, men den kan flyttas till vilken UDP- eller TCP-port som helst, inklusive 443. WireGuard lyssnar på en UDP-port som anges i konfigurationen; 51820 är den port som används i dess officiella exempel.

Q10: Vilket protokoll är lättare att konfigurera för hand?

WireGuard är vanligtvis enklare: skapa ett nyckelpar, utbyt publika nycklar och ange tillåtna IP-adresser. OpenVPN kräver certifikat, en CA och fler alternativ, även om .ovpn-profiler samlar dem i en enda fil.

Del 11: 10 intressanta fakta om VPN och insikter från verkligheten

Gå igenom dessa mycket värdefulla, verkliga fakta och insikter om VPN-teknikens historia, marknad och teknik.

1. FÖRSTA VPN-PROTOKOLLET

PPTP (Point-to-Point Tunneling Protocol) utvecklades av en leverantörsgrupp som bland annat omfattade Microsoft och publicerades som RFC 2637 i juli 1999 för att stödja VPN för fjärråtkomst. [6]

2. TVÅ TRANSPORTER

OpenVPN kan bära sin tunnel över UDP eller TCP, och i TLS-läge delar dess kontroll- och datakanaler en enda port. [4]

3. WIREGUARD-REVOLUTIONEN

WireGuard har en mycket strömlinjeformad kodbas som är utformad för effektivitet, vilket gör det lättare att granska för säkerhetsbrister än traditionella protokoll. [3]

4. MODERN KRYPTOGRAFI

WireGuard kombinerar ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 och HKDF i ramverket Noise, utan chifferval som användare kan välja fel på. [2]

5. OPENSSL I OPENVPN

OpenVPN är nära integrerat med biblioteket OpenSSL och hämtar många av sina kryptografiska funktioner därifrån, bland annat TLS som används för att utbyta nycklar. [4]

6. DJUP PAKETINSPEKTION

Djup paketinspektion (DPI) undersöker paketens innehåll och trafikmönster, inte bara huvuden, och vissa brandväggar använder den för att upptäcka och blockera vanliga VPN-protokoll.

7. SSH-LIKNANDE NYCKLAR

WireGuard-anslutningar upprättas genom att enkla publika nycklar utbyts, ungefär som SSH-nycklar, utan behov av någon certifikatutfärdare. [1]

8. PLATTFORMSOBEROENDE

WireGuard släpptes först för Linux-kärnan och finns nu för Windows, macOS, BSD, iOS och Android, så samma protokoll fungerar på de flesta enheter. [1]

9. FRAMÅTSEKRETESS

WireGuard upprepar sin Noise_IK-handskakning med några minuters mellanrum för att rotera de symmetriska sessionsnycklarna, vilket ger perfekt framåtsekretess även om en långlivad nyckel senare läcker. [2]

10. TUN/TAP-GRÄNSSNITT

OpenVPN är utformat för att fungera med det virtuella nätverksgränssnittet TUN/TAP, som finns på de flesta plattformar och bär tunnelns paket. [4]

Tekniska referenser och källor

Citerade publikationer, kryptografiska specifikationer och officiella dokumentstandarder som används i detta arbetsblad.

VETENSKAPLIGA OCH BRANSCHRELATERADE REFERENSER

[1] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.

https://www.wireguard.com/

[2] WireGuard. (n.d.). Protocol & Cryptography.

https://www.wireguard.com/protocol/

[3] 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/

[4] OpenVPN. (n.d.). OpenVPN 2.6 Manual.

https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[5] WireGuard. (n.d.). Quick Start.

https://www.wireguard.com/quickstart/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).

https://datatracker.ietf.org/doc/html/rfc2637

Facit: Jämförelse av protokollen WireGuard och OpenVPN, kodstorlek, hastighet och kryptografiska standarder

1 **WireGuards kodstorlek** PROTOKOLL — Rätt svar: D

ANTECKNING FÖR LÄRAREN

WireGuard är extremt kompakt och består av cirka 4 000 kodrader. Det håller angreppsytan liten och gör granskning enklare. Källa: WireGuard Project.

2 **Hastighet i kärnutrymmet** LATENS — Rätt svar: B

ANTECKNING FÖR LÄRAREN

Genom att köras direkt i kärnrymden undviker WireGuard kontextbyten, vilket möjliggör hög genomströmning. Källa: WireGuard Project.

3 **Fråga 3** — Rätt svar: B

ANTECKNING FÖR LÄRAREN

OpenVPN är tätt integrerat med OpenSSL, som tillhandahåller chiffer som AES-GCM och gör det mycket konfigurerbart men mer komplext.

4 **Protokollets prestanda** ROUTNINGSKONTROLLER — Rätt svar: A

ANTECKNING FÖR LÄRAREN

WireGuard upprättar handskakningar på millisekunder och reagerar omedelbart på nätverksbyten (t.ex. från Wi-Fi till mobilnät). Källa: Microsoft Native Gateway, Apple Support.

5 **Asymmetrisk kryptografi** INTEGRITET — Rätt svar: C

ANTECKNING FÖR LÄRAREN

WireGuard använder Cryptokey Routing, som kopplar publika nycklar till tillåtna tunnel-IP-adresser, liknande SSH-konfigurationer. Källa: WireGuard Project.

Facit: Kontrollpunkt 2 – Sant eller falskt

6 Fråga 6

Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

WireGuards Linux-implementation är under 4 000 rader, så säkerhetsteam kan granska den mycket snabbare än betydligt större VPN-kodbaser som OpenVPN.

7 Latens i användarutrymmet HASTIGHETER

Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

OpenVPN körs i användarutrymmet och skickar paket fram och tillbaka från kärnans virtuella gränssnitt, vilket ger overhead från kontextbyten (om inte kärnavlastning som OpenVPN DCO används). Källa: DD-WRT custom firmware.

8 OpenVPN-konfiguration RISK FÖR SNIFFNING

Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

OpenVPN kan köras över TCP (för tillförlitlighet och för att ta sig förbi brandväggar) eller UDP (för hastighet), vilket gör det kompatibelt med komplexa företagsbrandväggar. Källa: IETF Cryptographic Protocols.

9 Modern kryptografi BRANDVÄGGAR

Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

WireGuard avvisar äldre chiffer till förmån för moderna, säkra primitiver som ChaCha20 och Poly1305, som körs snabbt på mobila processorer. Källa: WireGuard Project.

10 Förenklade nyckelpar INGA LOGGAR

Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

WireGuard använder inte certifikat eller komplexa CA-hierarkier. Det bygger på enkla par av publika och privata nycklar som utbyts mellan peers. Källa: WireGuard Project.

Facit för ordförråd och bedömningsmall

Bedömningsmatris för läraren: Ge 1 poäng för varje korrekt matchning (totalt 8 poäng) och kontextbegrepp (totalt 6 poäng).

KONTROLLPUNKT 4: FACIT – MATCHNING AV BEGREPP

G 1. WireGuard	H 2. OpenVPN	E 3. Kärnutrymme	A 4. Användarutrymme
B 5. 4,000 rader	C 6. OpenSSL	F 7. Nyckelpar	D 8. TCP/UDP

KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

1 WIREGUARD	2 OPENVPN	3 KÄRNLÄGE	4 ANVÄNDARLÄGE
5 NYCKELPAR	6 GRANSKNINGSBARHET		

KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

1 F – OPENSSL	2 C – KÄRNLÄGE	3 B – OPENVPN	4 G – NYCKELPAR
5 H – TCPOCHUDP	6 E – KOMPAKTKOD	7 A – WIREGUARD	8 D – ANVÄNDARLÄGE

DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

Nyckelbegrepp:
Kontrollera att eleverna kan förklara WireGuard, OpenVPN och Kärnutrymme med egna ord och ge ett exempel på varje.

Fallstudier:
Be eleverna att stödja sina rekommendationer med fakta från arbetsbladet, inte med antaganden.

Källkritik:
Be eleverna att kontrollera minst ett påstående i arbetsbladets källor och diskutera varför siffror, priser och regler kan ändras över tid.

Facit till pussel och anteckningar för läraren

LÖSNING PÅ ORDSÖKET

O	P	E	N	V	P	N	N	V	Ä	X	C	Ö	Y	G
L	E	I	Ö	D	O	E	Y	S	Z	T	R	C	W	B
D	G	A	Ö	P	E	M	C	A	E	C	Q	E	F	H
O	Ä	J	D	T	S	N	K	F	J	P	U	Ö	U	G
K	L	S	Y	F	A	A	E	S	Q	O	O	R	W	W
T	N	Å	S	L	T	W	L	U	D	C	O	Ä	I	B
K	R	G	U	Z	Z	K	P	A	T	H	Ö	Ä	R	Ä
A	Ä	M	H	J	O	T	A	L	N	U	N	V	E	Q
P	K	I	S	S	H	Ö	R	A	Q	D	X	G	G	X
M	C	Ä	T	Ä	B	I	N	Ö	H	P	K	P	U	R
O	A	N	V	Ä	N	D	A	R	L	Ä	G	E	A	P
K	Z	C	N	Ö	Ä	G	Å	Q	Y	X	M	X	R	R
B	P	O	P	E	N	S	S	L	Y	V	N	H	D	X
D	Ä	X	L	T	B	Z	Ö	Å	N	T	S	Å	J	Q
E	A	D	L	S	Y	Z	Z	M	K	I	W	I	G	B

LÖSNING PÅ KORSORDET

						K	Ä	R	N	L	Ä	G	E	
						O								
						M								
						P								
A	N	V	Ä	N	D	A	R	L	Ä	G	E			
				Y		K								O
				C		T	C	P	O	C	H	U	D	P
				K		K								E
				E		O	P	E	N	V	P	N		N
				L		D								S
				P										S
				A										L
			W	I	R	E	G	U	A	R	D			

LÄRARHANDLEDNING MED LÖSNINGAR TILL KORSORDET

VÅGRÄTT

1 vågrätt: KÄRNLÄGE Det område i operativsystemet där WireGuard körs för att uppnå hastighet (8 bokstäver)

2 vågrätt: ANVÄNDARLÄGE Det körningsområde där OpenVPN körs, vilket skapar overhead vid kontextbyten (12 bokstäver)

5 vågrätt: TCPOCHUDP Transportprotokoll som OpenVPN stöder; WireGuard körs själv bara över UDP (9 bokstäver)

6 vågrätt: OPENVPN Robust äldre protokoll med en stor och komplex konfigurationskodbas (7 bokstäver)

7 vågrätt: WIREGUARD Modernt VPN-protokoll som är utformat för hög hastighet och enkel kodgranskning (9 bokstäver)

LODRÄTT

1 lodrätt: KOMPAKTKOD WireGuards kompakta kodbas, som gör den mycket enklare att granska (10 bokstäver)

3 lodrätt: NYCKELPAR Asymmetriska nycklar som WireGuard använder för att verifiera anslutningens parter (9 bokstäver)

4 lodrätt: OPENSSL Kryptografiskt bibliotek som OpenVPN förlitar sig på för chifferalgoritmer (7 bokstäver)

Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

FACIT FÖR ORDBLANDNING

1. UGEIWARDR — **WIREGUARD**
2. NKEÄGÄLR — **KÄRNLÄGE**
3. KKOTOADPKM — **KOMPAKTKOD**
4. ERAKPLNYC — **NYCKELPAR**
5. VNNEOPP — **OPENVPN**
6. ENLÄDGRANAVÄ — **ANVÄNDARLÄGE**
7. OSSLPNE — **OPENSSL**
8. PCDTOCHUP — **TCPOCHUDP**

NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

"UPPGRADERA DIN OPENVPN MED EN SNABBARE TUNNEL"

Facit till fallstudierna

A Scenario A: Välja ett protokoll

SNIFFNING OCH KRYPTERING | Sarahs dilemma

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Rekommendation: WireGuard. Dess lätta, anslutningslösa design gör att tunneln snabbt återhämtar sig när hennes nätverk ändras, och ChaCha20-Poly1305 håller krypteringen snabb.
- Säkerhet: Båda protokollen krypterar hennes trafik på kafeets wifi, så båda skyddar hennes inloggningar när de är korrekt konfigurerade; valet påverkar främst hastighet och stabilitet.

B Scenario B: Ta sig förbi VPN-blockeringar

GEOBLOCKERING OCH IP-ADRESSER | Alex dilemma

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Varför blockerad: WireGuard använder bara UDP, och hotellets brandvägg blockerar sannolikt UDP eller känner igen WireGuard-paket genom filtrering eller djup paketinspektion.
- Så hjälper OpenVPN: Det kan köras över TCP, inklusive port 443 som används av HTTPS, vilken hotellbrandväggar sällan blockerar helt eftersom webbsurfning är beroende av den.