Emri: _____ Data: _____ Pikët: _____

VPN për qasje në distancë

Sigurimi i pikave fundore të fuqisë punëtore në distancë, autentikimi me shumë faktorë dhe konfigurimet e tuneleve IPsec.

PËRMBLEDHJE MËSIMORE PËR VPN-TË PËR AKSES NË DISTANCË

NXËNËSI

STATUSI I STUDENTIT

Rruga e mbrojtësit të rrjetit

I SIGURT

STATUSI I LIDHJES

Mbrojtja e paketave të të dhënave

AKTIV

MBROJTJE NGA RRJEDHJET

Mbrojtje nga rrjedhjet e DNS dhe IPv6

Mirë se vjen! Kjo paketë aktivitetesh të udhëheq përmes rrjeteve VPN për qasje në distancë. Do të eksplorosh tunelet klient-në-site, hyrjet me shumë faktorë, kontrollet e qëndrimit të pikave fundore, kufijtë e gjerësisë së brezit dhe auditimin e sigurisë me syslog.

PIKAT E KONTROLLIT TË FLETËS SË PUNËS

- [ ] **Pjesët 1-4: Zotëro konfigurimet e VPN-së dhe të sigurisë së rrjetit.**
- [ ] **Pjesët 5-7: Zgjidh fjalëkryqe dhe enigma me kërkim fjalësh.**
- [ ] **Pjesët 8-9: Zgjidh studime rasti dhe sfidën e kodit.**
- [ ] **Pjesa 10: Shqyrto faqet e pyetjeve të shpeshta bazë dhe të avancuara.**
- [ ] **Pjesa 11: Eksploro 10 fakte interesante nga bota reale.**
- [ ] **Bonus: sfida Mendo shpejt.**

Hap Udhëzuesin VPN.com për VPN-të më të mira

URL: https://www.vpn.com/sq/vpn/vpn-me-i-mire-per-biznese/akses-ne-distance/

Udhërrëfyesi yt mësimor për VPN-në e qasjes në distancë

- Pika fundore të sigurta të fuqisë punëtore në distancë që qasen te nyjet e rrjetit lokal.
- Konfiguro politikat e autentikimit me shumë faktorë për hyrjet në distancë.
- Konfiguro konfigurime IPsec dhe OpenVPN klient-te-site.
- Audito logjet e lidhjeve në distancë për shkelje të kontrollit të qasjes.
- Zbato kontrolle të gjendjes së pajisjes përpara dhënies së lidhjeve në rrjet.
- Optimizo xhiron e serverit për të parandaluar ngecjen e gjerësisë së brezit për punën në distancë.

UDHËZIME PËR VPN-TË PËR AKSES NË DISTANCË

Përgjigju pyetjeve me zgjedhje të shumëfishtë dhe pyetjeve E vërtetë/E gabuar, plotëso fjalitë me vende bosh duke përdorur bankën e fjalëve, përputh përkufizimet dhe zgjidh fjalëkryqin dhe enigmën e kërkimit të fjalëve. Zbato njohuritë e tua për kontrollet e qëndrimit (posture checks) dhe hyrjet me shumë faktorë. Përfundo me aktivitetin bonus Mendo shpejt.

TUNELET KLIENT-NË-SITE DHE PËRPUTHSHMËRIA E PIKAVE TË FUNDIT (HYRJE)

VPN-të për qasje në distancë krijojnë tunele të sigurt klient-në-sajt për punonjësit jashtë ambienteve. Sigurimi i këtyre lidhjeve kërkon zbatimin e hyrjeve me vërtetim shumëfaktorësh (MFA), kryerjen e kontrolleve të pajtueshmërisë së qëndrimit të pikës fundore dhe auditimin e regjistrave përmes mbledhësve qendrorë syslog.

LEXO ÇDO PIKË KONTROLLI ME KUJDES DHE ZGJIDH OSE SHKRUAJ PËRGJIGJEN E SAKTË.

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1 **1. Cilin standard autentikimi duhet të kërkojnë portalet VPN të aksesit në distancë?**

- A) Shumëfaktorëshe
- B) Një faktor
- C) I paenkriptuar
- D) Mysafir lokal

2 **2. Cili protokoll është standardi për sigurimin e lidhjeve client-to-site të punës në distancë?**

- A) OpenVPN
- B) SOCKS5
- C) PPTP
- D) FTP

3 **3. Cila kontroll verifikon nëse një laptop në distancë është i pastër para lidhjes?**

- A) Kontrolli i gjendjes së pajisjes
- B) Test shpejtësie
- C) Test ping
- D) Numri i memories

4 **4. Ku ruhen regjistrat e lidhjeve të punonjësve në distancë për auditimin e sigurisë?**

- A) Server Syslog
- B) Çelës regjistri
- C) Memoria e klientit
- D) Shfletues uebi

5 **5. Çfarë problemi shfaqet kur numri i punonjësve në distancë e tejkalon kapacitetin e gjerësisë së brezit të gateway-t?**

- A) Ngushtim i gjerësisë së brezit
- B) Rrjedhje DNS
- C) Kalim i handshake-ut
- D) Ekspozimi i IP-së

Pika e kontrollit 2: Sfida: E vërtetë ose e gabuar

6 Pyetja 6

6. Autentikimi me shumë faktorë shton një token dytësor vërtetimi për të siguruar hyrjet në distancë.

E vërtetë E gabuar

7 Pyetja 7

7. Kontrollet e qëndrimit lejojnë pajisjet në distancë me firewall të çaktivizuar të hyjnë në serverët privatë.

E vërtetë E gabuar

8 Pyetja 8

8. Regjistrat e VPN-së për qasje në distancë janë thelbësorë për gjurmimin e hyrjes së paautorizuar në rrjetin e korporatës.

E vërtetë E gabuar

9 Pyetja 9

9. OpenVPN dhe IPsec janë protokolle të vjetruara që nuk arrijnë të enkriptojnë të dhënat e klientëve në distancë.

E vërtetë E gabuar

10 Pyetja 10

10. Ngjeshja e gjerësisë së brezit të gateway-t ndodh kur trafiku në distancë e tejkalon kapacitetin e kartës së lidhjes.

E vërtetë E gabuar

Pika e kontrollit 3: Futja e termave kryesorë

Lexo secilën fjali më poshtë dhe plotëso vendin bosh me termin e saktë nga Banka e Fjalëve.

1. Për të mbrojtur portalet e korporatës, hyrjet në distancë duhet të kërkojnë autentikim _____ .

2. Klientët në distancë enkriptojnë ngarkesat e tunelit të të dhënave me protokolle standarde _____ .

3. Para se të marrin lidhje me rrjetin, pajisjet duhet të kalojnë kontrollin e: _____ .

4. Regjistrat e hyrjeve të audituara i dërgohen vazhdimisht një serveri qendror _____ .

5. Trafiku i madh gjatë orarit të punës mund të çojë në mbingarkesë të portës hyrëse për shkak të: _____ .

6. Drejtuesit e përshtatësit virtual trajtojnë, nën Windows dhe macOS, procesin e: _____ nga klienti te sajti.

BANKA E FJALËVE TË LEKSIKUT

ENKRIPTIM FIREWALL GJERËSI BANDE MULTIFAKTORIAL OPENVPN
POSTURË SIGURIE SYSLOG TUNELIM

Shkruaj përgjigjet e tua këtu:

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

Pika e kontrollit 4: Përputhja e koncepteve kryesore

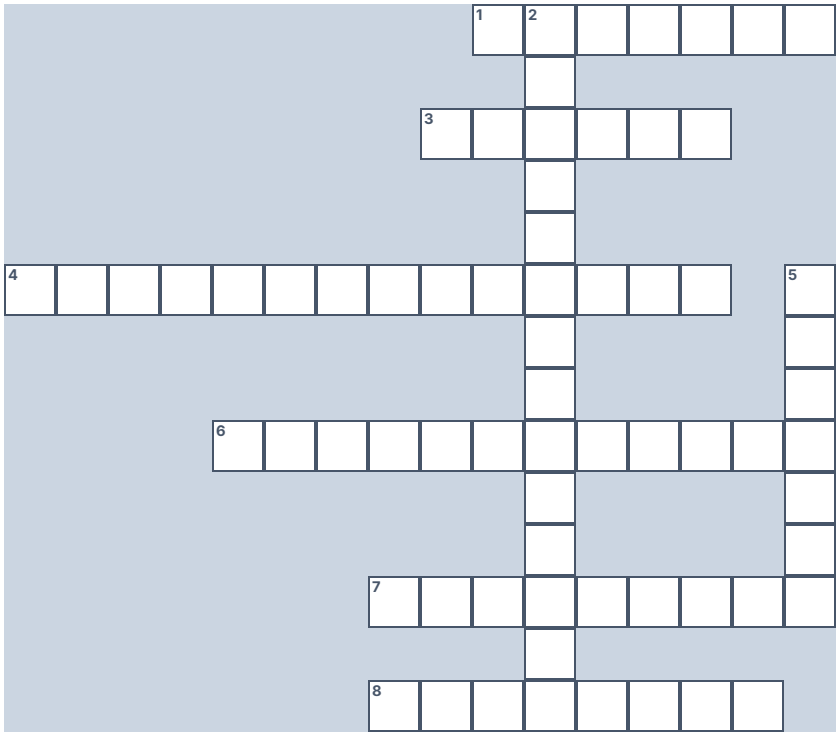
PËRPUTHJA E PËRKUFIZIMEVE

Përputh çdo term fjalori në të majtë me përkufizimin e tij të saktë në të djathtë, duke shkruar shkronjën përkatëse (A-H) në kutinë e plotësueshme.

☐	1. ME SHUMË FAKTORË	A	Enkapsulimi i të dhënave në një shteg të sigurt.
☐	2. OPENVPN	B	Mbledhësi qendror i regjistrave të sigurisë.
☐	3. QËNDRIM	C	Kufiri i kapacitetit të të dhënave të rrjetit.
☐	4. SYSLOG	D	Protokoll standard klient-te-site.
☐	5. GJERËSIA E BANDËS	E	Validimi i shëndetit të pajisjes në distancë.
☐	6. ENKRIPTIM	F	Rregullat e sistemit të filtrimit të trafikut.
☐	7. TUNELIMI	G	Përzierja kriptografike e paketave.
☐	8. FIREWALL	H	Siguri e hyrjes që kërkon token-ë shtesë.

Pika e kontrollit 5: Fjalëkryq

Zgjidhe fjalëkryqin duke shkruar shkronja në kutitë e bardha aktive. Numrat korrespondojnë me indiciet më poshtë.



HORIZONTALISHT

1. Protokoll standard nga klienti te sajti (7)

3. Mbledhës qendror i regjistrave të sigurisë (6)

4. Siguri e hyrjes që kërkon shenja shtesë (14)

6. Kufiri i kapacitetit të të dhënave të rrjetit (12)

7. Përzierja kriptografike e paketave (9)

8. Rregullat e sistemit të filtrimit të trafikut (8)

VERTIKALISHT

2. Vlerësimi i gjendjes së pajisjes në distancë (14)

5. Mbështjellja e të dhënave në një rrugë të sigurt (7)

Pika e kontrollit 5, alternativa: Çelësa të aksesueshëm të fjalëkryqit

Përdoruesit e lexuesve të ekranit dhe të tastierës mund t'i shkruajnë përgjigjet e fjalëkryqit drejtpërdrejt në fushat e tekstit më poshtë.

HORIZONTALISHT

1 horizontalisht: Protokoll standard nga klienti te sajti (7 shkronja):

3 horizontalisht: Mbledhës qendror i regjistrave të sigurisë (6 shkronja):

4 horizontalisht: Siguri e hyrjes që kërkon shenja shtesë (14 shkronja):

6 horizontalisht: Kufiri i kapacitetit të të dhënave të rrjetit (12 shkronja):

7 horizontalisht: Përzierja kriptografike e paketave (9 shkronja):

8 horizontalisht: Rregullat e sistemit të filtrimit të trafikut (8 shkronja):

VERTIKALISHT

2 vertikalisht: Vlerësimi i gjendjes së pajisjes në distancë (14 shkronja):

5 vertikalisht: Mbështjellja e të dhënave në një rrugë të sigurt (7 shkronja):

Pika e kontrollit 6: Kërkimi i fjalës së fshehur

Gjej 8 termat kyç të fjalorit të fshehur në rrjetën më poshtë. Fjalët mund të jenë horizontale, vertikale ose diagonale.

P O S T U R Ë S I G U R I E T

I Q B M I T P I R K N E V S O

Z Y K Q P X G N Ç A Ç I Y P P

U V V J H G S G Ë B E S E G J

S Q U P Z D G E Q C L N A J O

C Z K I U Q T A R O V V I K K

F F L G P Ë J S G P J Q V F B

T E Y M Y V R F N S X A O T M

M M Z N G O S G N T T N T S I

I A D N L L A W E R I F L J A

L M U L T I F A K T O R I A L

E M U Ë Ë O P X Y I I T I Y V

N X G J E R Ë S I B A N D E N

U I G Z H H L A E G A R A I E

T V D I Z I D J P L I A E N I

LISTA E FJALËVE TË LEKSIKUT

MULTIFAKTORIAL OPENVPN POSTURËSIGURIE SYSLOG GJERËSIBANDE

ENKRIPTIM TUNELIM FIREWALL

Pika e kontrollit 6, alternativa: Përputhja e aksesueshme e fjalorit

Përputh secilin nga 8 termat e fjalorit nga Kërkimi i fjalëve me përkufizimin e saktë të tij, duke shkruar shkronjën (A-H) në vendin bosh.

TERMA LEKSIKORË

A. MULTIFAKTORIAL

B. OPENVPN

C. POSTURËSIGURIE

D. SYSLOG

E. GJERËSIBANDE

F. ENKRIPTIM

G. TUNELIM

H. FIREWALL

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

1. Mbledhës qendror i regjistrave të sigurisë.
2. Rregullat e sistemit të filtrimit të trafikut.
3. Mbështjellja e të dhënave në një rrugë të sigurt.
4. Përzierja kriptografike e paketave.
5. Protokoll standard nga klienti te sajti.
6. Kufiri i kapacitetit të të dhënave të rrjetit.
7. Vlerësimi i gjendjes së pajisjes në distancë.
8. Siguri e hyrjes që kërkon shenja shtesë.

Pika e kontrollit 7: Sfida e fjalëve të përzier

Rirenditi shkronjat më poshtë për të zbuluar konceptet dhe termat kryesorë të ndërmjetësimit të domeneve. Shkruaji përgjigjet në kutitë e dhëna.

1. RFKOALUTIMALIT
2. UORSËIPRSEGUIT
3. GJBIDAESEËNR
4. MULEITN
5. VNNEOPP
6. OLSSGY
7. PEIMTRNIK
8. EIWLFLAR

Aktivitet bonus: Mendo shpejt

3 PËRGJIGJE PËR ÇDO KATEGORI. FITON KUSH E PLOTËSON I PARI LISTËN.

1	Mite për VPN-të			
2	Fjalë që përshkruajnë Zero Trust			
3	Programe zyre që njeh			
4	Rregulla për punë të sigurt në distancë			
5	Gjëra që mund të shohë ofruesi yt i internetit			
6	Shërbime VPN që njeh			
7	Vende nga ku punojnë punonjësit			
8	Mjete që përdor çdo ditë një kompani			
9	Role në një departament IT			
10	Pajisje që mund të ketë një punonjës			
11	Të dhëna që një kompani duhet t'i mbrojë			
12	Gjëra që bëhen pas një shkelje sigurie			
13	Gjëra që mund ta prishin një takim me video			
14	Mënyra për t'u identifikuar në mënyrë të sigurt			
15	Arsye për t'u dhënë punonjësve një VPN			

Pika e kontrollit 8: Studime rasti për VPN-në dhe rrjetin

Zbato konceptet që ke mësuar për të zgjidhur skenarët reale më poshtë.

STUDIMI I RASTIT 1: ZBATIMI I MFA



Skenari: Një analist biznesi përpiqet të hyjë në bazën e të dhënave të kompanisë ndërsa punon në distancë. Ai fut emrin e përdoruesit dhe fjalëkalimin e saktë, por portali i VPN-së e bllokon qasjen dhe kërkon një kod nga një token fizik.

Pyetje për diskutim: Cila politikë sigurie po e zbaton këtë hap të verifikimit të dyfishtë?

STUDIMI I RASTIT 2: PËRPUTHSHMËRIA E GJENDJES SË PAJISJES (POSTURE)



Skenari: Një kontraktor e lidh laptopin e tij personal me rrjetin e largët të kompanisë. Klienti i VPN-së e ndërpret menjëherë lidhjen dhe e njofton përdoruesin se përkufizimet e antivirusit të tij janë të vjetruara.

Pyetje për diskutim: Cilin kontroll të specializuar të portës së VPN-së e bllokoi këtë përpjekje lidhjeje?

Pika e kontrollit 9: Deshifrimi i kodit

Një inxhinier rrjeti siguron kanalet e drejtimit dhe tunelet e klientëve. Përdor çelësin shkronjë-numër më poshtë për të deshifruar mesazhin duke shkruar shkronjat përkatëse në hapësirat e zbrazëta.

ÇELËSI I ENKRIPTIMIT SHKRONJË-NË-NUMËR

A=1 B=2 C=3 Ç=4 D=5 E=6 Ë=7 F=8 G=9

H=10 I=11 J=12 K=13 L=14 M=15 N=16 O=17 P=18

Q=19 R=20 S=21 T=22 U=23 V=24 X=25 Y=26 Z=27

24	18	16		16	7		5	11	21	22	1	16	3	7		15	2	20	17	16
						18	1	12	11	21	12	6	22		6					
				16	5	7	20	15	1	20	20	12	6	21						

Mesazhi i deshifruar:

KËSHILLË: ÇDO NUMËR PËRFAQËSON POZICIONIN E ASAJ SHKRONJE NË ALFABET (P.SH. 1 = A, 2 = B, 27 = Z).

Pika e kontrollit 10: Pyetje të shpeshta bazë për VPN-në (Pjesa A)

Rishiko pyetjet dhe përgjigjet më të zakonshme për Rrjetet Private Virtuale (VPN) dhe tunelimin.

Q1: Çfarë është VPN-ja e qasjes në distancë?

Një metodë e sigurt lidhjeje që u mundëson punonjësve që punojnë jashtë zyrës të lidhen drejtpërdrejt me serverët privatë korporativë.

Q2: Pse është client-to-site ndryshe nga site-to-site?

Klient-në-site lidh pajisjet individuale të përdoruesve, ndërsa site-to-site lidh vendndodhje të tëra fizike zyrash.

Q3: Çfarë është një kontroll i qëndrimit të pajisjes (device posture check)?

Një skanim që kontrollon statusin e sigurisë të një pajisjeje të largët (antivirus, niveli i patch-eve të OS) para se të japë qasje.

Q4: Pse përdoret OpenVPN për aksesin në distancë?

Për shkak të protokollit të tij të fortë të sigurisë, përputhshmërisë ndërplatformë dhe aftësisë për të trajtuar lidhje individuale.

Q5: Si e mbron MFA aksesin në distancë?

Shton një token dytësor verifikimi, duke parandaluar qasjen edhe nëse fjalëkalimet e punonjësve rrjedhin ose vidhen.

Pika e kontrollit 10: Pyetje të shpeshta bazë për VPN-në (Pjesa B)

Rishiko pyetjet dhe përgjigjet më të zakonshme për Rrjetet Private Virtuale (VPN) dhe tunelimin.

Q6: Çfarë është një server syslog?

Një depo e centralizuar regjistrash që ruan ngjarjet e lidhjes, hyrjet dhe alarmet e sistemit për auditime përputhshmërie.

Q7: Çfarë shkakton mbytjen e gjerësisë së brezit?

Kur kërkesat e përgjithshme të gjerësisë së brezit të punonjësve në distancë e tejkalojnë kufirin e shpejtësisë së internetit të gateway-t të kompanisë.

Q8: A mund ta lidh kompjuterin tim të shtëpisë me një VPN të punës?

Vetëm nëse pajisja kalon auditimet e kontrollit të qëndrimit (posture check) të korporatës dhe autorizohet nga administratorët e IT-së.

Q9: Çfarë është enkapsulimi i rrjetit?

Mbështjellja e paketave të të dhënave gjatë tranzitit brenda kokave të enkriptuara të protokollit për të siguruar transmetimin.

Q10: Si e optimizon split tunneling qasjen në distancë?

U lejon punonjësve të përdorin ISP-në e tyre lokale për shfletimin standard, ndërsa i rrugëzon skedarët e lidhur me punën përmes VPN-së.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për VPN-në (Pjesa C)

Eksploro aspektet e avancuara teknike të protokolleve të tunelimit të VPN-ve, integrimeve të klientëve mobil dhe zbatimit në ndërmarrje.

Q1: Si e përmirëson vërtetimi i bazuar në certifikata qasjen në distancë?

Lidh lejet e lidhjes me certifikata dixhitale lokale të para-instaluara, duke bllokuar pajisjet e pamenaxhuara ose të paautorizuara.

Q2: Cili është rreziku i sigurisë i split tunneling për punën në distancë?

Krijon një urë të mundshme ku një pajisje lokale e kompromentuar mund t'i rrugëzojë kërcënimet e jashtme në rrjetin privat.

Q3: Si i inspektojnë kontrollet e qëndrimit (posture checks) cilësimet e regjistrit?

Klienti i VPN-së ekzekuton skripta lokale që kërkojnë shtigje të regjistrit për të verifikuar nëse softueri i sigurisë i korporatës është aktiv.

Q4: Pse përdorin syslog-et si parazgjedhje portën UDP 514?

Për të transmetuar regjistrat shpejt me ngarkesë minimale, megjithëse konfigurimet e sigurta tani kërkojnë mbështjellje TLS mbi TCP.

Q5: Si i zgjidhin kompanitë ngushticat e gjerësisë së brezit në portë (gateway)?

Duke zbatuar balancues ngarkese dhe duke shpërndarë trafikun në distancë nëpër nyjet rajonale të serverit.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për VPN-në (Pjesa D)

Eksploro aspektet e avancuara teknike të protokolleve të tunelimit të VPN-ve, integrimeve të klientëve mobil dhe zbatimit në ndërmarrje.

Q6: Cili është funksioni i adapterëve virtualë TAP/TUN në klientët në distancë?

Veprojnë si karta virtuale rrjeti, duke rrugëzuar trafikun TCP/IP të nivelit të pajisjes drejtpërdrejt në tunelin e enkriptuar të VPN-së.

Q7: Si e mbështet IKEv2 MOBIKE lëvizshmërinë e fuqisë punëtore në distancë?

Përditëson në mënyrë dinamike lidhjet e adresave IP, duke e mbajtur VPN-në aktive ndërsa përdoruesi lëviz midis Wi-Fi dhe të dhënave celulare.

Q8: Cili është ndryshimi mes ruterimit split dhe atij me tunel të plotë?

Rrugëzimi i plotë i detyron të gjithë trafikun e internetit të pajisjes përmes VPN-së, ndërsa rrugëzimi i ndarë dërgon vetëm IP-të e destinacioneve të korporatës.

Q9: Si i trajtojnë pajisjet NAT lidhjet VPN në distancë?

Duke hartuar diapazonet e porteve lokale te adresat IP publike të portës për të rrugëzuar paketat e kthyera të të dhënave të enkriptuara.

Q10: Cilat standarde pajtueshmërie kërkojnë auditimin e qasjes në distancë?

Standarde si HIPAA, SOC 2 dhe PCI DSS kërkojnë regjistrimin dhe monitorimin e të gjitha seancave të lidhjes në distancë.

Pjesa 11: 10 fakte dhe njohuri nga bota reale për VPN-të

Rishiko fakte reale për shpejtësitë e enkriptimit të VPN-së, auditimet e protokolleve, lidhjen mobile dhe punën në distancë të ndërmarrjeve.

1. PERSPEKTIVË PËR VPN-NË

VPN-të për qasje në distancë krijojnë tunele të sigurt klient-në-sajt për punëtorët jashtë ambienteve.

2. PERSPEKTIVË PËR VPN-NË

Autentikimi me shumë faktorë kërkohet nga rregullat e përputhshmërisë për të mbrojtur portalet e biznesit në distancë.

3. PERSPEKTIVË PËR VPN-NË

Kontrollet e qëndrimit verifikojnë cilësimet lokale të sigurisë së klientit përpara se të jepet qasja në rrjetin privat.

4. PERSPEKTIVË PËR VPN-NË

Serverët Syslog grumbullojnë regjistrat e lidhjeve për të audituar dhe zbuluar përpjekjet e paautorizuara për qasje.

5. PERSPEKTIVË PËR VPN-NË

Ngjeshjet e gjerësisë së brezit të gateway-t ndodhin kur kërkesat e përgjithshme të trafikut në distancë e tejkalojnë kufijtë e internetit të serverit.

6. PERSPEKTIVË PËR VPN-NË

Përshtatësit virtualë të rrjetit i përmbledhin kërkesat e rrjetit të sistemit operativ brenda protokolleve të sigurta.

7. NJOHURI PËR VPN-NË

Mbështetja për MOBIKE u lejon klientëve në distancë të ndërrojnë rrjete pa ndërprerë tunelin VPN.

8. NJOHURI PËR VPN-NË

Rrugëzimi me tunel të plotë siguron të gjithë trafikun e internetit të punonjësve, por rrit ngarkesën e gateway-t të korporatës.

9. NJOHURI PËR VPN-NË

Autentikimi me certifikatë e lidh autorizimin e lidhjes VPN drejtpërdrejt me harduerin e menaxhuar nga kompania.

10. PERSPEKTIVË PËR VPN-NË

Kornizat si SOC 2 dhe PCI DSS presin regjistrimin dhe monitorimin e sesioneve të qasjes në distancë.

Referenca teknike dhe burime

Udhëzuesi i studimit dhe enigmat interaktive janë përpiluar nga standardet teknike globale, specifikimet dhe kuadrot rregullatore.

REFERENCA AKADEMIKE DHE TË INDUSTRISË

[1] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.
https://www.vpn.com/vpn/best-vpn-for-business/

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

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.
https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.
https://nordlayer.com/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).
https://www.rfc-editor.org/rfc/rfc4555

Çelësi i përgjigjeve: Pika e kontrollit 1 - Zgjedhje e shumëfishtë

1 **Token-ët e hyrjes** SIGURIA MFA **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Autentikimi me shumë faktorë e zbaton verifikimin dytësor për hyrjet. Citim: MFA Implementation.

2 **Tuneli OpenVPN** KLIENT-NË-SITE **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

OpenVPN është një protokoll standard për sigurimin e tuneleve nga klienti te sajti. Citim: OpenVPN Client.

3 **Auditime të qëndrimit** KONTROLLI I PAJISJES **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Kontrollet e qëndrimit skanojnë pikat fundore për firewall-e dhe mjete antivirus aktive. Citim: Posture Compliance.

4 **Grumbullues regjistrash** SERVERI SYSLOG **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Serverët Syslog mbledhin regjistrat e ngjarjeve të sigurisë për të monitoruar shkeljet e qasjes. Burimi: Syslog Standard.

5 **Tejmbushja e kartës** NGJESHJA E GATEWAY-T **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Ngjeshja e gjerësisë së brezit të gateway-t ndodh kur trafiku i përdoruesve i tejkalon kufijtë e serverit. Citim: Capacity Planning.

Çelësi i përgjigjeve: Pika e kontrollit 2 - E vërtetë ose e gabuar

6 **Token-ët e hyrjes** KONTROLLET MFA — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Autentikimi me shumë faktorë e zbaton verifikimin dytësor për hyrjet. Citim: MFA Implementation.

7 **Pyetja 7** — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

Kontrollet e qëndrimit (posture checks) i bllokojnë pajisjet që kanë firewall-in ose antivirusin të fikur, ndaj ato pajisje refuzohen.

8 **Grumbullues regjistrash** SERVERI SYSLOG — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Serverët Syslog mbledhin regjistrat e ngjarjeve të sigurisë për të monitoruar shkeljet e qasjes. Burimi: Syslog Standard.

9 **Pyetja 9** — **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

OpenVPN dhe IPsec janë protokolle aktuale që e enkriptojnë trafikun e klientëve në distancë.

10 **Tejmbushja e kartës** NGJESHJA E GATEWAY-T — **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Ngjeshja e gjerësisë së brezit të gateway-t ndodh kur trafiku i përdoruesve i tejkalon kufijtë e serverit. Citim: Capacity Planning.

Çelësat e fjalorit dhe rubrika e vlerësimit

Rubrika e vlerësimit për mësuesin: Jep 1 pikë për çdo përputhje të saktë (8 pikë gjithsej) dhe term konteksti (6 pikë gjithsej).

PIKA E KONTROLLIT 4: ÇELËSI – PËRPUTHJA E KONCEPTEVE

H 1. ME SHUMË FAKTORË	D 2. OPENVPN	E 3. QËNDRIM	B 4. SYSLOG
C 5. GJERËSIA E BANDËS	G 6. ENKRIPTIM	A 7. TUNELIMI	F 8. FIREWALL

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 MULTIFAKTORIAL	2 OPENVPN	3 POSTURË SIGURIE	4 SYSLOG
5 GJERËSI BANDE	6 TUNELIM		

PIKA E KONTROLLIT 6, ALTERNATIVA: ÇELËSI – PËRPUTHJA E FJALËVE

1 D – SYSLOG	2 H – FIREWALL	3 G – TUNELIM	4 F – ENKRIPTIM
5 B – OPENVPN	6 E – GJERËSIBANDE	7 C – POSTURËSIGURIE	8 A – MULTIFAKTORIAL

SHËNIME PËR DISKUTIM PËR MËSUESIT

Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë ME SHUMË FAKTORË, OPENVPN dhe QËNDRIM me fjalët e tyre dhe të japin një shembull për secilin.

Studimet e rastit:
Kërkoju nxënësve t'i mbështesin rekomandimet me fakte nga fleta, jo me supozime.

Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË

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

ZGJIDHJA E FJALËKRYQIT

						O	P	E	N	V	P	N		
							O							
				S	Y	S	L	O	G					
							T							
							U							
M	U	L	T	I	F	A	K	T	O	R	I	A	L	T
							Ë							U
							S							N
			G	J	E	R	Ë	S	I	B	A	N	D	E
							G							L
							U							I
					E	N	K	R	I	P	T	I	M	
							I							
					F	I	R	E	W	A	L	L		

UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

1 horizontalisht: OPENVPN Protokoll standard nga klienti te sajti (7 shkronja)

3 horizontalisht: SYSLOG Mbledhës qendror i regjistrave të sigurisë (6 shkronja)

4 horizontalisht: MULTIFAKTORIAL Siguri e hyrjes që kërkon shenja shtesë (14 shkronja)

6 horizontalisht: GJERËSIBANDE Kufiri i kapacitetit të të dhënave të rrjetit (12 shkronja)

7 horizontalisht: ENKRIPTIM Përzierja kriptografike e paketave (9 shkronja)

8 horizontalisht: FIREWALL Rregullat e sistemit të filtrimit të trafikut (8 shkronja)

VERTIKALISHT

2 vertikalisht: POSTURËSIGURIE Vlerësimi i gjendjes së pajisjes në distancë (14 shkronja)

5 vertikalisht: TUNELIM Mbështjellja e të dhënave në një rrugë të sigurt (7 shkronja)

Çelësi i fjalëve të përzierura dhe i zgjidhjes së kodit

Çelësi i vlerësimit për aktivitetin e rirenditjes së fjalorit dhe për Sfidën e Kodit të Fshehtë.

ÇELËSI I RIRENDITJES SË FJALËVE

1.	RFKOALUTIMALIT	MULTIFAKTORIAL	5.	VNNEOPP	OPENVPN
2.	UORSËIPRSEGUIT	POSTURËSIGURIE	6.	OLSSGY	SYSLOG
3.	GJBIDAESEËNR	GJERËSIBANDE	7.	PEIMTRNIK	ENKRIPTIM
4.	MULEITN	TUNELIM	8.	EIWLFLAR	FIREWALL

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"VPN NË DISTANCË MBRON PAJISJET E NDËRMARRJES"

Çelësi i studimeve të rastit

A Studimi i rastit 1: Zbatimi i MFA

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një analist biznesi përpiqet të hyjë në bazën e të dhënave të korporatës ndërsa punon në distancë. Ai fut emrin e saktë të përdoruesit dhe fjalëkalimin, por portali VPN e bllokon qasjen dhe kërkon një kod fizik tokeni.
- Strategjia dhe zgjidhja e rekomanduar: Portali VPN i korporatës zbaton një politikë të rreptë Vërtetimi Shumëfaktorësh (MFA) për të siguruar hyrjet në distancë.

B Studimi i rastit 2: Përputhshmëria e gjendjes së pajisjes (posture)

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një kontraktues lidh laptopin e tij personal me rrjetin e korporatës në distancë. Klienti VPN e shkëput menjëherë lidhjen, duke njoftuar përdoruesin se përkufizimet e antivirusit të tij janë të vjetruara.
- Strategjia dhe zgjidhja e rekomanduar: Gateway-i i qasjes në distancë kreu një kontroll të qëndrimit të pikës fundore dhe e bllokoi pajisjen për shkak të konfigurimeve të sigurisë së vjetruara.