Emri: _____ Data: _____ Pikët: _____

VPN për ndërmarrje

Zbatimi i qasjes në rrjet Zero Trust, i nyjeve të dedikuara gateway dhe i kontrolleve të centralizuara administrative të korporatës.

PËRMBLEDHJE MËSIMORE PËR RRJETET VPN TË NDËRMARRJEVE

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 të ndërmarrjeve. Do të eksplorosh arkitekturat Zero Trust, portat statike IP të dedikuara, konsolat e administratorit, ofrimin e llogarive dhe tunelet IPsec site-to-site.

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/ndermarrje/

Udhërrëfyesi yt mësimor për rrjetin VPN të ndërmarrjes

- Zbato kornizat Zero Trust Network Access (ZTNA).
- Konfiguro adresat IP të gateway-t të serverit të dedikuar për filtrat e listës së bardhë.
- Menaxho panelet qendrore të administrimit korporativ dhe listat e vendeve të përdoruesve.
- Audito logjet e qasjes në rrjet dhe historikun e lidhjeve të përdoruesve.
- Konfiguro rregullat e Single Sign-On (SSO) dhe të autentikimit me shumë faktorë.
- Konfiguro tunele IPsec site-to-site nga dega në degë.

UDHËZIME PËR RRJETET VPN TË NDËRMARRJEVE

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 Zero Trust dhe IPsec site-to-site. Përfundo me aktivitetin bonus Mendo shpejt.

ARKITEKTURAT ZERO TRUST DHE PORTAT E DEDIKUARA (HYRJE)

VPN-të e ndërmarrjeve i sigurojnë pasuritë e korporatës duke kaluar te kornizat Zero Trust Network Access (ZTNA) dhe duke vendosur në listë të bardhë portat hyrëse statike IP të dedikuara. Menaxherët IT përdorin konsola administrimi të centralizuara për të orkestruar tunele IPsec nga site në site dhe lidhje me kyçje të vetme (SSO).

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

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1 **1. Cili model sigurie po zëvendëson VPN-të e vjetra të ndërmarrjeve?**

- A) Zero Trust
- B) Multi-hop
- C) Peer-to-peer
- D) Gateway i vetëm

2 **2. Cila veçori nevojitet për të kufizuar aksesin në bazën e të dhënave vetëm te serverët e kompanisë?**

- A) IP e dedikuar
- B) Rrugëzim dinamik
- C) Tunel i ndarë
- D) Proxy DNS

3 **3. Cili protokoll është standardi për tunelet e kompanive nga një vend në tjetrin (site-to-site)?**

- A) IPsec
- B) PPTP
- C) SOCKS5
- D) SSL v3

4 **4. Cili mjet qendror u lejon administratorëve të menaxhojnë vendet e punonjësve?**

- A) Paneli i administratorit
- B) Çelës regjistri
- C) Firmueri i router-it
- D) Regjistri i sistemit

5 **5. Cili standard autentikimi lejon identifikimin përmes Okta ose Microsoft Entra ID?**

- A) Single Sign-On
- B) Sekret i përbashkët
- C) Autentikimi EPP
- D) Çelësi WEP

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

6 Pyetja 6

6. Zero Trust Network Access jep hyrje në rrjet vetëm pasi të verifikojë besueshmërinë e vazhdueshme të pajisjes.

○ E vërtetë ○ E gabuar

7 Pyetja 7

7. Portat e hyrjes me IP të dedikuar e drejtojnë trafikun e punonjësve së bashku me përdorues publikë konsumatorë të rastësishëm.

○ E vërtetë ○ E gabuar

8 Pyetja 8

8. Konsolat e centralizuara të administratorit u lejojnë menaxherëve të IT të revokojnë menjëherë vendet individuale të punonjësve.

○ E vërtetë ○ E gabuar

9 Pyetja 9

9. IPsec është një protokoll i lehtë që nuk mbështet tunele rrjeti site-to-site.

○ E vërtetë ○ E gabuar

10 Pyetja 10

10. Single Sign-On mundëson autentikim të sigurt të punonjësve duke përdorur ofrues identiteti korporativ.

○ 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. Arkitekturat moderne të sigurisë i zëvendësojnë tunelet e vjetra me qasje _____ .

2. Për të kufizuar qasjen në bazat e të dhënave, kompanitë konfigurojnë një adresë porte hyrëse me: _____ .

3. Zyrat e degëve lidhen në mënyrë të sigurt me tunele site-to-site _____ .

4. Administratorët e IT-së ndajnë licencat e përdoruesve të punonjësve brenda një _____ qendrore.

5. Integrimi me Okta u lejon punonjësve të autentikohen përmes sistemit të korporatës: _____ .

6. Për të mbrojtur hyrjet, portalet e ndërmarrjeve kërkojnë autentikim _____ .

BANKA E FJALËVE TË LEKSIKUT

ALOKIM HYRJE E VETME IP I DEDIKUAR IPSEC KONSOLË ADMINI MULTIFAKTORIAL PORTË HYRËSE ZERO TRUST

Shkruaj përgjigjet e tua këtu:

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

Pika e kontrollit 4: Përputhja e koncepteve kryesore

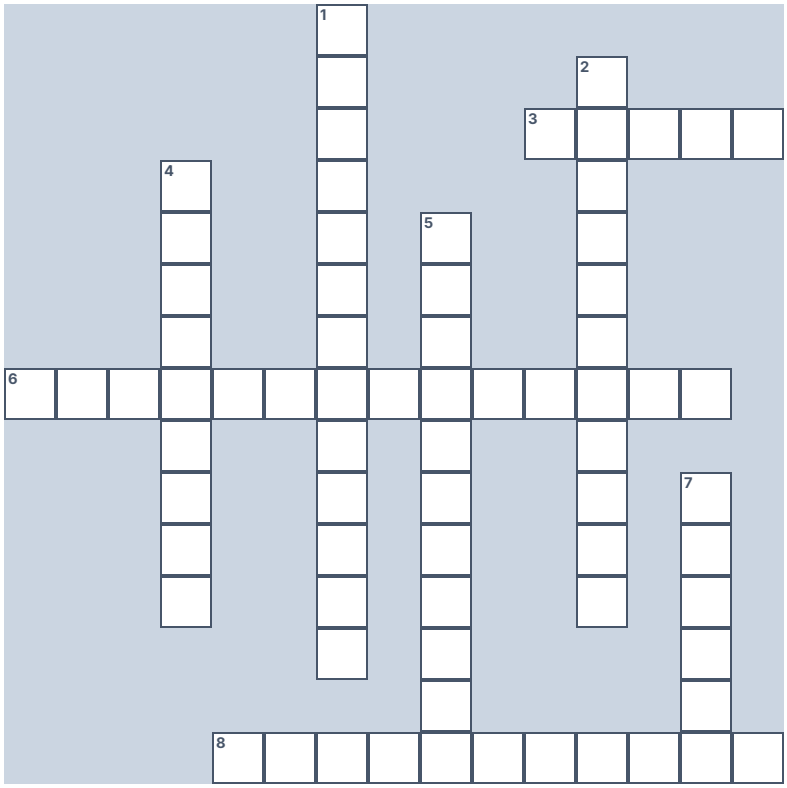
PËRPUTHJA E PËRKUFIZIMEVE

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. ZERO TRUST	A	Ndarja e licencave të qasjes VPN për punonjësit.
☐	2. IP E DEDIKUAR	B	Lidhja e identitetit Okta dhe Entra ID.
☐	3. IPSEC	C	Siguri e hyrjes që kërkon token-ë shtesë.
☐	4. PANELI I ADMINISTRATORIT	D	Adresë gateway-i në listë të bardhë statike.
☐	5. SINGLE SIGN-ON	E	Standard tuneli site-to-site.
☐	6. ME SHUMË FAKTORË	F	Nyje rutimi hyrëse e rrjetit.
☐	7. PORTË	G	Portali qendror i vendeve të menaxherit të IT.
☐	8. FURNIZIM	H	Kuadër i vazhdueshëm i verifikimit të besimit.

Pika e kontrollit 5: Fjalëkryq

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



HORIZONTALISHT

3. Standard i tunelit nga sit në sit (5)

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

8. Lidhja e identitetit me Okta dhe Entra ID (11)

VERTIKALISHT

1. Portal qendror i vendit të menaxherit të IT-së (13)

2. Adresë statike e portës hyrëse për listën e lejuar (11)

4. Kornizë e verifikimit të vazhdueshëm të besimit (9)

5. Nyja e drejtimit në hyrje të rrjetit (11)

7. Ndarja e licencave të qasjes VPN për punonjësit (6)

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

3 horizontalisht: Standard i tunelit nga sit në sit (5 shkronja):

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

8 horizontalisht: Lidhja e identitetit me Okta dhe Entra ID (11 shkronja):

VERTIKALISHT

1 vertikalisht: Portal qendror i vendit të menaxherit të IT-së (13 shkronja):

2 vertikalisht: Adresë statike e portës hyrëse për listën e lejuar (11 shkronja):

4 vertikalisht: Kornizë e verifikimit të vazhdueshëm të besimit (9 shkronja):

5 vertikalisht: Nyja e drejtimit në hyrje të rrjetit (11 shkronja):

7 vertikalisht: Ndarja e licencave të qasjes VPN për punonjësit (6 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.

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

LISTA E FJALËVE TË LEKSIKUT

ZEROTRUST IPIDEDIKUAR IPSEC KONSOLËADMINI HYRJEEVETME
MULTIFAKTORIAL PORTËHYRËSE ALOKIM

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. ZEROTRUST

B. IPIDEDIKUAR

C. IPSEC

D. KONSOLËADMINI

E. HYRJEEVETME

F. MULTIFAKTORIAL

G. PORTËHYRËSE

H. ALOKIM

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

1. Adresë statike e portës hyrëse për listën e lejuar.
2. Nyja e drejtimit në hyrje të rrjetit.
3. Ndarja e licencave të qasjes VPN për punonjësit.
4. Siguri e hyrjes që kërkon shenja shtesë.
5. Standard i tunelit nga sit në sit.
6. Kornizë e verifikimit të vazhdueshëm të besimit.
7. Lidhja e identitetit me Okta dhe Entra ID.
8. Portal qendror i vendit të menaxherit të IT-së.

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. RTOEZUSTR _____

2. ICESP _____

3. HVEERYMEETJ _____

4. YSEHRËËRPOT _____

5. UPKIIREDIAD _____

6. OMËLINNDKOAIS _____

7. RAOMTULLFIKTAI _____

8. OMAIKL _____

Aktivitet bonus: Mendo shpejt

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

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

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: MIGRIMI TE ZERO TRUST

👷

Skenari: Një ndërmarrje dëshiron t'i sigurojë serverët e saj lokalë duke verifikuar vazhdimisht certifikatat e përputhshmërisë së pajisjeve, statusin e firewall-it dhe vendndodhjen e përdoruesit, në vend që t'i besojë këdo brenda rrjetit.

Pyetje për diskutim: Cilën kornizë duhet ta zbatojë drejtori i sigurisë IT për ta arritur këtë?

STUDIMI I RASTIT 2: KUFIZIMI I GATEWAY-T

👷

Skenari: Një kompani mban në cloud baza të dhënash financiare private. Ajo dëshiron të bllokojë çdo qasje publike në internet te panelet e administrimit dhe të lejojë identifikimin vetëm nga pikat fundore të verifikuara të kompanisë.

Pyetje për diskutim: Cilin konfigurim rrjeti duhet ta vendosë administratori i bazës së të dhënave në firewall-in e cloud-it?

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

27	6	20	17		22	20	23	21	22		24	6	20	11	8	11	13	17	16
4	**5**	**17**		**18**	**1**	**12**	**11**	**21**	**12**	**6**		**22**	**7**		**14**	**11**	**5**	**10**	**23**	**20**

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 një VPN për ndërmarrje?

Një tunel i sigurt rrjeti i dizajnuar për biznese, që u lejon punonjësve në distancë të hyjnë në rrjetet korporative me menaxhim të centralizuar.

Q2: Si ndryshon Zero Trust nga VPN-të tradicionale?

VPN-të tradicionale i besojnë këdo brenda tunelit, ndërsa Zero Trust verifikon vazhdimisht çdo lidhje pajisjeje dhe përdoruesi.

Q3: Çfarë është një IP e dedikuar në VPN-të e biznesit?

Një adresë IP statike e rezervuar vetëm për biznesin tënd, që të lejon ta vendosësh në listë të bardhë për qasje të sigurt në bazat e të dhënave cloud.

Q4: Pse është i rëndësishëm SSO për VPN-të e biznesit?

Single Sign-On u lejon punonjësve të përdorin kredencialet e tyre korporative (si Okta ose Microsoft Entra ID) për të hyrë në mënyrë të sigurt.

Q5: Çfarë është një VPN site-to-site?

Një tunel që lidh dy zyra fizike (si një degë dhe selia qendrore) përmes internetit publik duke përdorur IPsec.

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: Cili është funksioni i një konsole administruese?

Një panel për administratorët IT për të shtuar ose hequr vendet e punonjësve, caktuar gateway-e dhe monitoruar lidhjet aktive.

Q7: Si i siguron MFA VPN-të e biznesit?

Duke kërkuar një kod dytësor (si një token i aplikacionit autentikues) për të parandaluar hyrjen e paautorizuar nga fjalëkalime të kompromentuara.

Q8: A mund të auditoj historikun e lidhjeve të punonjësve?

Po, VPN-të e ndërmarrjeve regjistrojnë kohët e lidhjes, kohëzgjatjen dhe IP-të e caktuara për auditim përputhshmërie.

Q9: Çfarë është ZTNA?

Zero Trust Network Access, një model sigurie që jep qasje vetëm në aplikacione specifike dhe jo në tërë rrjetin.

Q10: Cili është roli i nyjeve gateway?

Shërbejnë si pika të sigurta hyrjeje për trafikun në distancë, duke rrugëzuar të dhënat drejtpërdrejt te serverët privatë të korporatës.

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 i mbron IPsec komunikimet korporative nga sajti në sajt?

IPsec enkripton trafikun në shtresën e rrjetit duke përdorur Encapsulating Security Payload (ESP) për të siguruar konfidencialitetin dhe integritetin e të dhënave.

Q2: Pse dështon siguria e vjetër e bazuar në perimetër për fuqinë punëtore në distancë?

Sepse punonjësit i qasen të dhënave nga vendndodhje dhe pajisje të shumta, çka e bën të vjetruar perimetrin e një firewall-i të vetëm të rrjetit.

Q3: Si e zbatojnë menaxherët e IT-së ofrimin e automatizuar të akseseve (provisioning)?

Duke hartuar protokollet SCIM mes ofruesve të identitetit (Okta) dhe konsolës së administratorit të VPN-së për të sinkronizuar direktoritë e përdoruesve.

Q4: Cili është përfitimi i split tunneling në mjediset korporative?

E rrugëzon trafikun lokal SaaS (si Microsoft 365) jashtë tunelit VPN, duke ruajtur gjerësinë e brezit të gateway-t të korporatës për bazat e të dhënave private.

Q5: Si e vlerësojnë kontrollet e qëndrimit të pajisjes sigurinë e pikës fundore (endpoint)?

Klienti i VPN-së skanon pajisjen para lidhjes për të verifikuar që firewall-i është aktiv, antivirusi po funksionon dhe arnat e sistemit operativ janë të përditësuara.

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 roli i NAT traversal në konfigurimet e VPN-ve të biznesit?

NAT-T i enkapsulon paketat IPsec në UDP që të kalojnë përmes ruterave shtëpiakë dhe firewall-eve pa ndërprerje të lidhjes.

Q7: Si e parandalojnë bizneset mbytjen e gjerësisë së brezit në portë (gateway)?

Duke vendosur nyje të shumta rajonale porte dhe duke balancuar trafikun hyrës të përdoruesve nëpër to me balancues ngarkese.

Q8: Pse parapëlqehen listat e bardha me IP statike ndaj atyre dinamike?

Listat e bardha statike parandalojnë që IP-të e jashtme të paautorizuara të provojnë handshake lidhjeje, duke zvogëluar ndjeshëm sipërfaqen e sulmit.

Q9: Cili është roli i vërtetimit të bazuar në certifikata në VPN-të e ndërmarrjeve?

Validon certifikata unike dixhitale të instaluara në pajisjet e menaxhuara nga kompania, duke bllokuar kompjuterët personalë të pamenaxhuar.

Q10: Si e zvogëlon ZTNA rrezikun e lëvizjes anësore?

Duke izoluar sesionet e përdoruesve në burime të caktuara të autorizuara, duke parandaluar që hakerët të lëvizin nëpër rrjet nëse një nyje cenohet.

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

Arkitekturat Zero Trust verifikojnë vazhdimisht gjendjen e sigurisë së çdo pajisjeje që përpiqet të lidhet me rrjetin.

2. PERSPEKTIVË PËR VPN-NË

Portat e hyrjes me IP të dedikuar u lejojnë bizneseve t'i mbyllin bazat e të dhënave në cloud duke vendosur adresa statike në listë të bardhë.

3. PERSPEKTIVË PËR VPN-NË

IPsec është protokolli standard i industrisë për konfigurimin e tuneleve të sigurta të rrjetit site-to-site të zyrave.

4. PERSPEKTIVË PËR VPN-NË

Panelet e administratorit u lejojnë departamenteve IT të ndajnë, menaxhojnë dhe auditojnë vendet e qasjes VPN të punonjësve.

5. PERSPEKTIVË PËR VPN-NË

Single Sign-On integron qasjen VPN me ofrues identiteti korporativ si Okta dhe Entra ID.

6. PERSPEKTIVË PËR VPN-NË

Autentikimi me shumë faktorë bllokon tentativat e paautorizuara të lidhjes që vijnë nga çelësa fjalëkalimi të vjedhur.

7. NJOHURI PËR VPN-NË

Split tunneling optimizon brezin korporativ duke përjashtuar trafikun publik SaaS nga tuneli i enkriptuar.

8. NJOHURI PËR VPN-NË

Kontrollet e gjendjes së pajisjes verifikojnë cilësimet lokale të sigurisë përpara se të jepet qasja te serverët e korporatës.

9. NJOHURI PËR VPN-NË

Sinkronizimi i drejtorisë SCIM automatizon kontrollet e qasjes për pranimin dhe largimin e punonjësve.

10. PERSPEKTIVË PËR VPN-NË

Zero Trust Network Access ia kufizon përdoruesit qasjen në aplikacione specifike të autorizuara, duke parandaluar lëvizjen anësore në rrjet.

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/

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

1 **Zero Trust** MODELI ZTNA **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Modelet Zero Trust verifikojnë vazhdimisht përputhshmërinë e pajisjes para hyrjes në rrjet. Citim: NIST Zero Trust.

2 **IP e dedikuar** IP STATIKE **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Adresat IP të dedikuara lejojnë vendosjen e portave të hyrjes në listë të bardhë për të bllokuar trafikun publik. Citim: Dedicated IP Guide.

3 **Standardi IPsec** TUNELI IPSEC **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

IPsec është protokolli standard që përdoret për tunelet site-to-site të degëve. Citim: IPsec Tunneling.

4 **Ndarja e IT** PANELI I ADMINISTRATORIT **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Panelet e centralizuara të administratorit u lejojnë menaxherëve të IT të ndajnë licencat e vendeve. Citim: CISA Guidelines.

5 **Pyetja 5** **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Cili standard autentikimi lejon identifikimin përmes Okta ose Microsoft Entra ID? → Single Sign-On

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

6 **Zero Trust** KONTROLLE ZTNA **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Modelet Zero Trust verifikojnë vazhdimisht përputhshmërinë e pajisjes para hyrjes në rrjet. Citim: NIST Zero Trust.

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

SHËNIM PËR MËSUESIN

IP-të e dedikuara rezervohen për një biznes të vetëm, ndaj trafiku i tij nuk përzihet me përdoruesit e tjerë.

8 **Ndarja e IT** VENDI I ADMINISTRATORIT TË IT **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Panelet e centralizuara të administratorit u lejojnë menaxherëve të IT të ndajnë licencat e vendeve. Citim: CISA Guidelines.

9 **Standardi IPsec** SITE-TO-SITE **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

IPsec është protokolli standard që përdoret për tunelet site-to-site të degëve. Citim: IPsec Tunneling.

10 **Lidhja Okta SSO** HYRJE ME SSO **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Single Sign-On integron hyrjet në VPN me drejtoritë korporative si Okta. Burimi: Okta SSO.

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. ZERO TRUST	D 2. IP E DEDIKUAR	E 3. IPSEC	G 4. PANELI I ADMINISTRATORIT
B 5. SINGLE SIGN-ON	C 6. ME SHUMË FAKTORË	F 7. PORTË	A 8. FURNIZIM

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 ZERO TRUST	2 IP I DEDIKUAR	3 IPSEC	4 KONSOLË ADMINI
5 HYRJE E VETME	6 MULTIFAKTORIAL		

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

1 B – IPIDEDIKUAR	2 G – PORTËHYRËSE	3 H – ALOKIM	4 F – MULTIFAKTORIAL
5 C – IPSEC	6 A – ZEROTRUST	7 E – HYRJEEVETME	8 D – KONSOLËADMINI

SHËNIME PËR DISKUTIM PËR MËSUESIT

Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë ZERO TRUST, IP E DEDIKUAR dhe IPSEC 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.

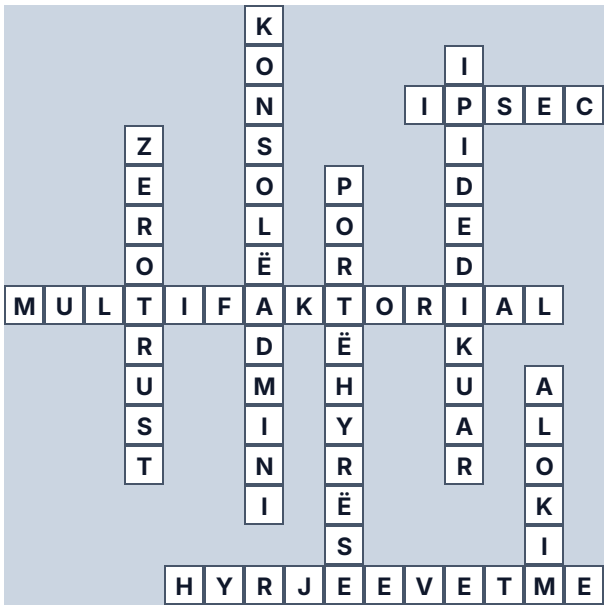
Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË

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

ZGJIDHJA E FJALËKRYQIT



UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

3 horizontalisht: IPSEC Standard i tunelit nga sit në sit (5 shkronja)

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

8 horizontalisht: HYRJEEVETME Lidhja e identitetit me Okta dhe Entra ID (11 shkronja)

VERTIKALISHT

1 vertikalisht: KONSOLËADMINI Portal qendror i vendit të menaxherit të IT-së (13 shkronja)

2 vertikalisht: IPIDEDIKUAR Adresë statike e portës hyrëse për listën e lejuar (11 shkronja)

4 vertikalisht: ZEROTRUST Kornizë e verifikimit të vazhdueshëm të besimit (9 shkronja)

5 vertikalisht: PORTËHYRËSE Nyja e drejtimit në hyrje të rrjetit (11 shkronja)

7 vertikalisht: ALOKIM Ndarja e licencave të qasjes VPN për punonjësit (6 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.	RTOEZUSTR	ZEROTRUST	5.	UPKIIREDIAD	IPIDEDIKUAR
2.	ICESP	IPSEC	6.	OMËLINNDKOAIS	KONSOLËADMINI
3.	HVEERYMEETJ	HYRJEEVETME	7.	RAOMTULLFIKTAI	MULTIFAKTORIAL
4.	YSEHRËËRPOT	PORTËHYRËSE	8.	OMAIKL	ALOKIM

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"ZERO TRUST VERIFIKON ÇDO PAJISJE TË LIDHUR"

Çelësi i studimeve të rastit

A Studimi i rastit 1: Migrimi te Zero Trust

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një ndërmarrje dëshiron t'i sigurojë serverët e saj lokalë duke verifikuar vazhdimisht certifikatat e pajtueshmërisë së pajisjeve, statusin e firewall-it dhe vendndodhjen e përdoruesit, në vend që t'i besojë këdo brenda rrjetit.
- Strategjia dhe zgjidhja e rekomanduar: Drejtori duhet të migrojë te një model Zero Trust Network Access (ZTNA), që zbaton kontrolle sigurie të vazhdueshme të bazuara në kontekst.

B Studimi i rastit 2: Kufizimi i gateway-t

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një kompani hoston baza të dhënash financiare private në cloud. Ajo dëshiron të bllokojë gjithë qasjen publike të internetit te panelet e administrimit, duke lejuar hyrjet vetëm nga pikat fundore të verifikuara të kompanisë.
- Strategjia dhe zgjidhja e rekomanduar: Administratori duhet të konfigurojë një gateway Dedicated IP në VPN-në e ndërmarrjes dhe ta vendosë këtë adresë statike në listën e lejimeve të firewall-it të bazës së të dhënave cloud.