

ארכיטקטורת רשת מאובטחת



CYBER SCHOOL



מודול זה מכסה מושגי אבטחת רשת בסיסיים, מונחים וארכיטקטורת רשתות.
המטרה היא להכיר את המרכיבים שיוצרים רשת מאובטחת היטב.

- סיכום ניהול רשתות <
- שיטות של Redundancy <
- עיצוב אבטחת רשתות <

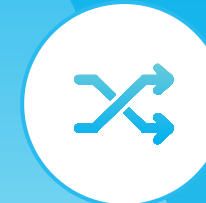


CYBER SCHOOL

מערכות אבטחת רשתות והארכיטקטורה שלהן

סיכום ניהול רשתות

התקני רשתות



התקן	תיאור
כרטיס ממשק רשת (NIC)	מאפשר אינטראקציה בין התקנים דרך הרשת.
Switch	התקן תקשורת שכבה 2 (במסגרת LAN).
נתב	התקן תקשורת שכבה 3 שמחבר בין רשתות.
חומת אש	חומרה או תוכנה שמסננת תעבורה.
התקן קצה	התקן רשת של המקור או היעד.
נקודת גישה	התקן שמספק חיבור רשת אלחוטי (WLAN).



תהליך ניתוב (Routing)



תהליך הניתוב קובע באיזה מסלול תעבור התעבורה בדרכה לרשת אחרת המחוברת גם היא לנתב.



מנתב ומעביר מנות דרך התקני שכבה 3.
החלטות לגבי ניתוב מבוססות על טבלאות ניתוב.
נתבים יכולים לשלוח מנות אל רשתות המחוברות באופן ישיר.



חלוקה לרשתות משנה



רשתות משנה עוזרות לעצב תוכנית יעילה להקצאת כתובות IP על ידי יצירת חטיבות רשת.

מפחיתות את התעבורה הכוללת על ידי חלוקת העומס על פני רשתות משנה.

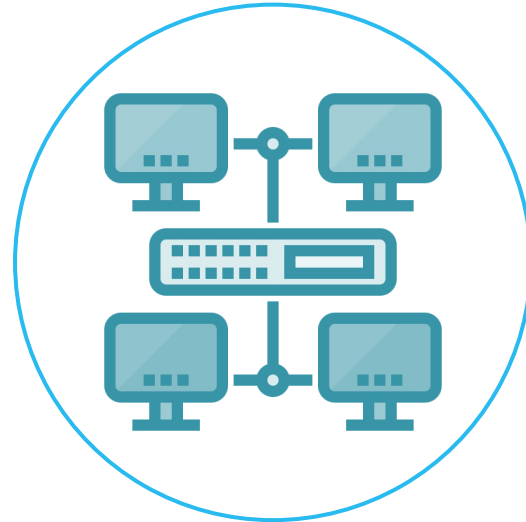
משתמשים בהן גם כאמצעי אבטחה כדי לאפשר הפצה קלה יותר של מדיניות האבטחה.



VLANs



מושגים פופולריים המוטמעים ברוב הרשתות
האדמיניסטרטיביות.
VLANs הן חטיבות רשת לוגיות, לעומת חטיבות פיזיות.
העברת נתונים בין VLANs מצריכה ניתוב שכבה 3.



רשימת בקרת גישה (Access Control List)



תכונת אבטחה מבוססת כללים המשמשת לצורך
סינון תעבורה בסיסי.
מסננת תעבורה נכנסת ותעבורה יוצאת.
חייבת להיות הצהרת "היתר" אחת לפחות בכללים
של רשימת הגישה.



שרתים



שרת יחיד יכול לשרת לקוחות רבים.
Clients בודדים יכולים לעבוד עם מספר שרתים.



התקן או שירות, המנהל משאבי רשת.

שרתים הם בדרך כלל ייעודיים, כלומר הם לא מבצעים פונקציות אחרות
מאשר אלה שאותן הם נועדו לבצע.

סוגי שרתים



שרת מסד נתונים



שרת תקשורת



שרת רשת



שרת דוא"ל



שרת יישומים



CYBER SCHOOL

מערכות אבטחת רשתות והארכיטקטורה שלהן

שיטות של יתירות (Redundancy)

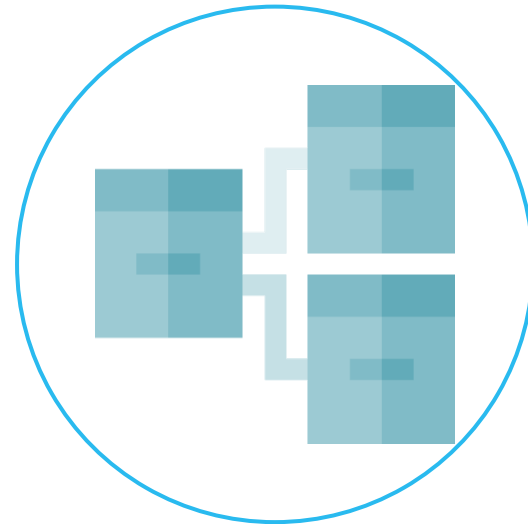
IP וירטואלי (Virtual IP)



כתובות IP שאינן מקושרות למכונה.
משפרות את היתירות על ידי כך שהן מספקות למכונה
חלופות failover.

אשכולות זמינות גבוהה

(Fail Over Cluster)

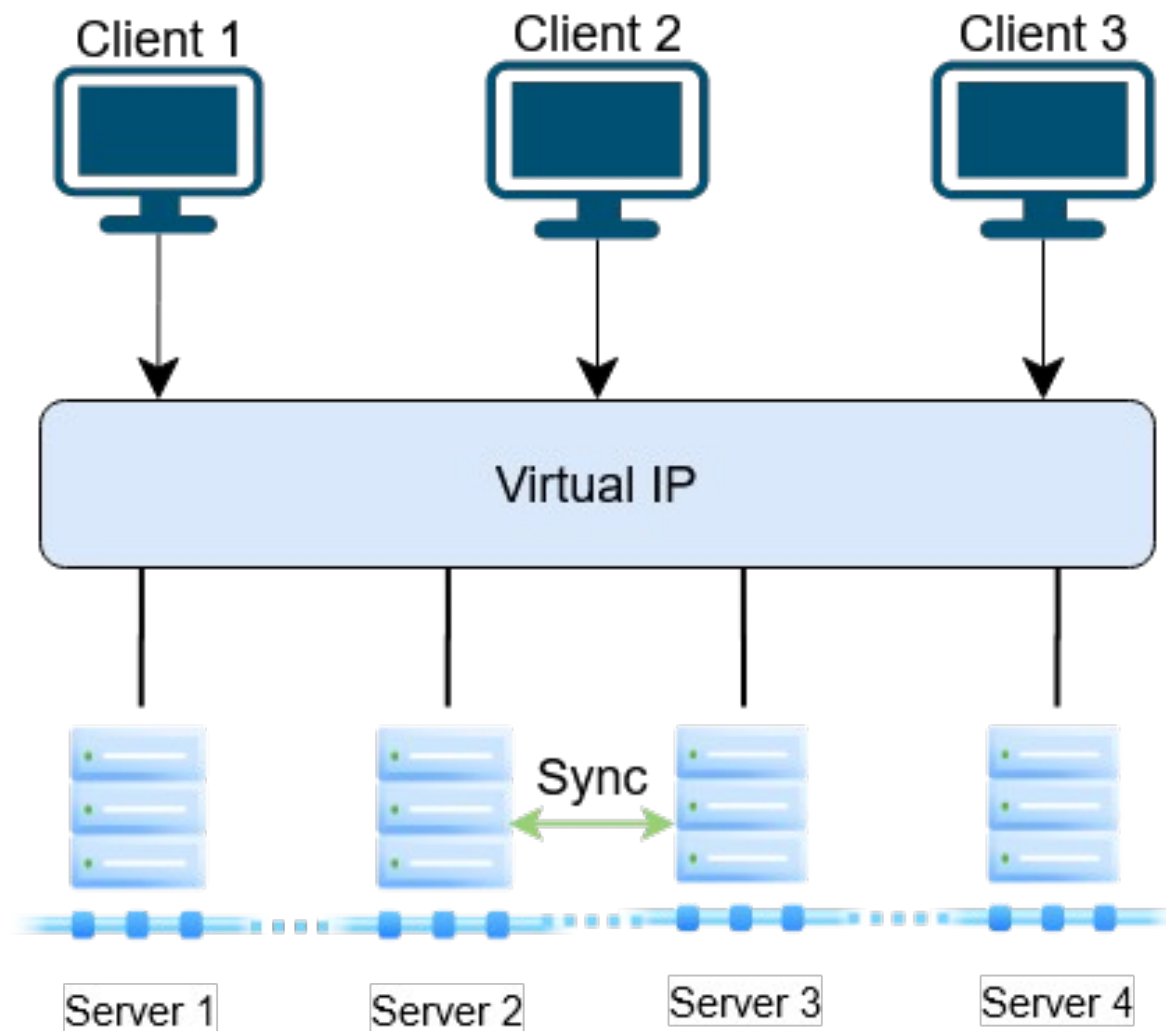
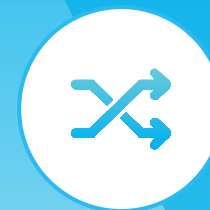


שיטה המשמשת לצורך גיבוי של רשת במקרה של כשל.
פועלת כמערכת אחת.

אם צומת אחד (שרת אשכולות) נופל, צומת אחר יתחיל להציע את שירותיו.



תרשים זרימת אשכול

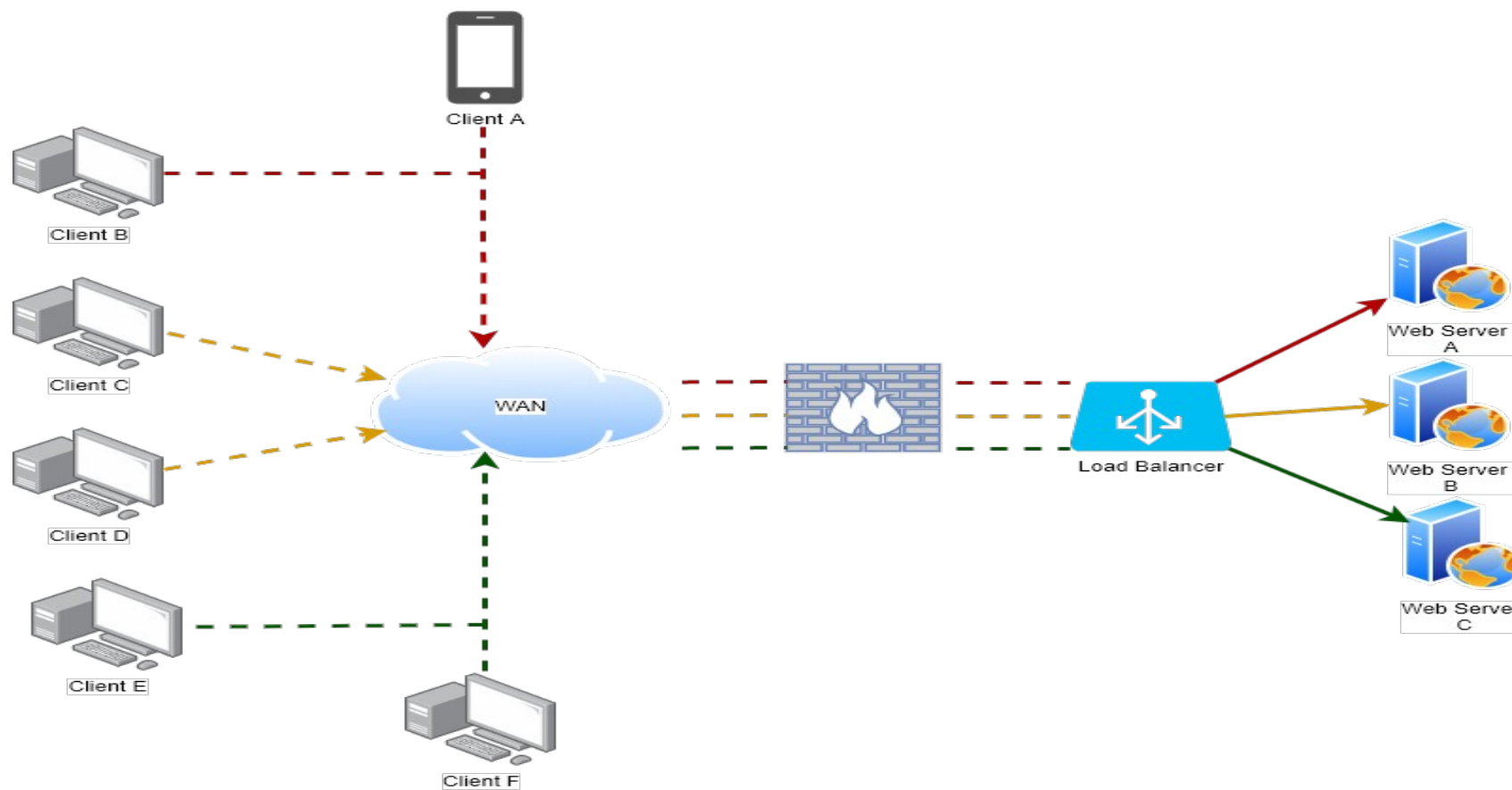
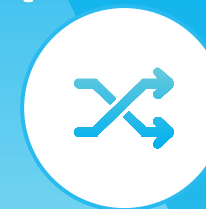




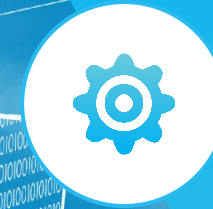
התקן שמפלג/מחלק את התעבורה על פני מספר מכשירים.
משמש ליצירת עקביות במקרה ששרת נופל.
שלא בדומה לאשכול, תהליך איזון העומס אינו מודע
לשרתים אחרים שאליהם התעבורה יכולה להיות מנותבת.



תרשים זרימת מאזן עומסים (Load Balancer)



תרגול קצר - עיצוב הרשת



10 – 5 דקות 

המשימה

למרכז נתונים גדול יש בעיית השהיית שרת. בשעות העומס השרת הראשי מתעכב. יש לפתור בעיה זו באמצעות פלטפורמת Draw.io.

השלבים

לצורך משימה זו יש להשתמש בקישור <http://draw.io>. יש ליצור ארכיטקטורת רשת חדשה עם שני שרתי רשת. יש להשתמש במאזן עומסים כדי לפתור בעיות השהייה.



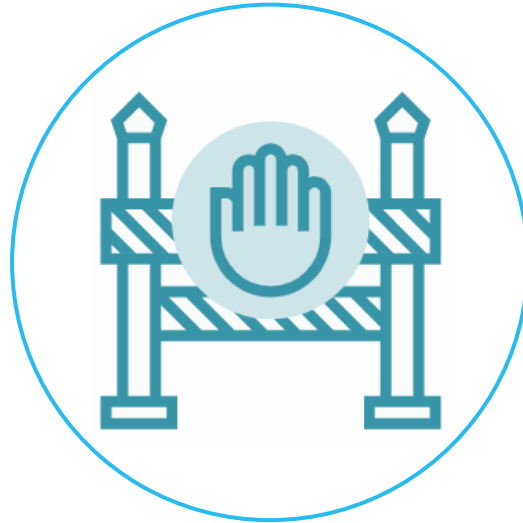
CYBER SCHOOL



CYBER SCHOOL

מערכות אבטחת רשתות והארכיטקטורה שלהן

עיצוב אבטחת רשתות

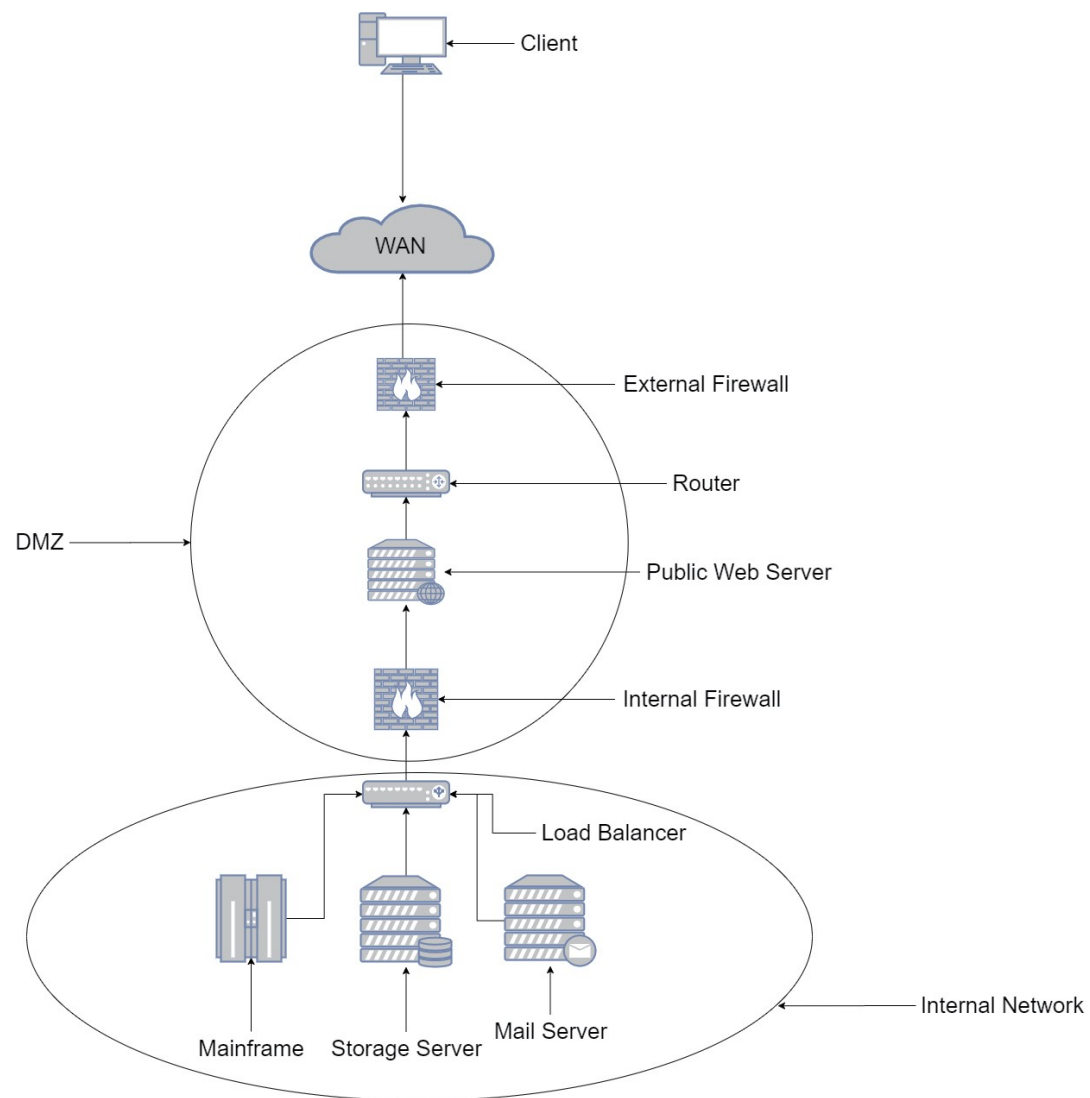
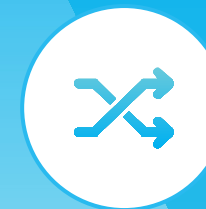


אזור מפורז הוא רשת הפונה כלפי חוץ.

מגנה על הרשת הפנימית על ידי גיבוש שכבה שכוללת רק שירותים חיצוניים.

מסדי נתונים יימצאו ב-LAN, שרתי רשת יהיו ב-DMZ ולקוחות יהיו ב-WAN.

ארכיטקטורת אזור מפורז (DMZ)



Forward Proxy Reverse Proxy-I



שרתים מתווכים (שרתי פרוקסי) פועלים בצד של הלקוח.

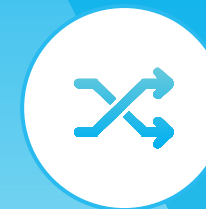
ניתן להשתמש בהם כדי לעקוף הגבלות IP, כדי לשמור על אנונימיות וכדי לסנן תעבורת רשת.



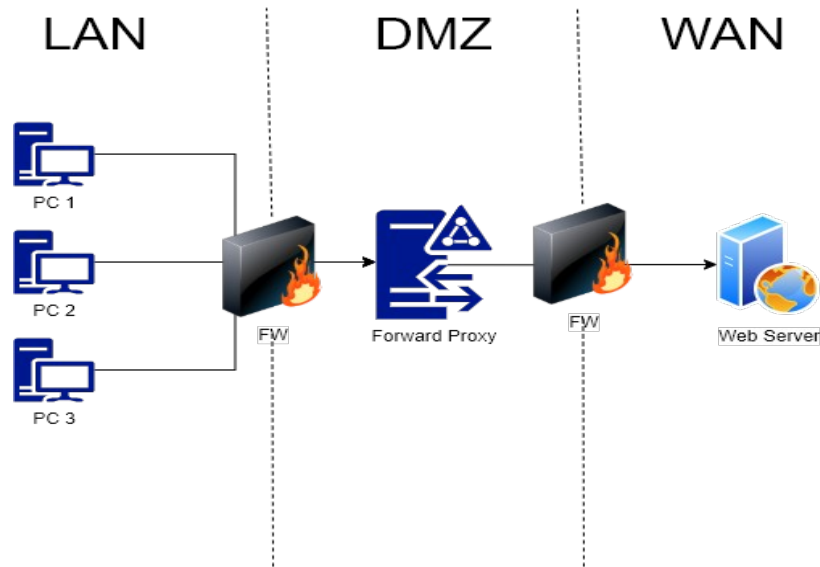
שרתים מתווכים הפוכים פועלים בצד של השרת.

ניתן להשתמש בהם כדי למזער מתקפות DDoS ובתור חומות אש ליישומי אינטרנט.

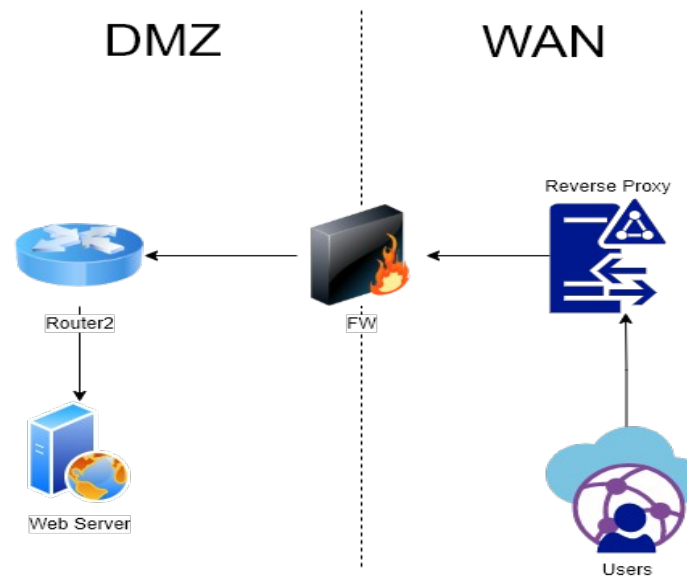




Forward Proxy



Reverse Proxy



שרת ממסר דואר (Mail Relay)



מעביר הודעות דואר אלקטרוני מהשולח אל הנמען.
יכול לשמש לצורך אנטי ספאם, הרשימה השחורה
והרשימה הלבנה.





שכבת אבטחה השולטת בתעבורה ברשת משנית
אחת או יותר.

מגבילה או מאפשרת תעבורה באמצעות שימוש
בכללים המבוססים על פורטים, פרוטוקולים,
מקורות ויעדים.



המשימה

אתם בתפקיד מנהל האבטחה והוטלה עליכם המשימה לעצב ארכיטקטורת רשת מאובטחת עבור החברה שלכם.

השלבים

יש להתחיל פרויקט רשת ב-<http://Draw.io>.
הרשת חייבת לכלול:

- שני נתבים ומתג אחד
- שתי חומות אש
- סביבת DMZ
- פילוח של ה-LAN

שרתים -

עמדות עבודה -

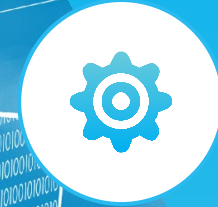
רשימת בקרת גישה (ממוקמת)

שרתים

שלושה שרתי רשת בעלי זמינות גבוהה -

מסד נתונים -

בקר דומיין -



15-20 דקות



CYBER SCHOOL



שאלות?

