סייבר ישראל
מערך הסייבר הלאומי

מסמך המלצות הגנה לנתבים ביתיים

סייבר ישראל
מערך הסייבר הלאומי

המלצות הגנה לנתב אלחוטי ביתי

אפריל 2020

תוכן עניינים

מהו נתב (Router) אלחוטי ביתי וכיצד נאבטח אותו?

הנתב הביתי משמש אותנו כשער גישה לאינטרנט. הוא מאפשר לנו לגלוש באינטרנט, להשתמש ולהתחבר למספר רב של מכשירים בו זמנית, לאפשר שיחות בטלפון הביתי, להתחבר למצלמות, התחברות לכבלים וצפייה ב VOD ועוד המון אפשרויות.

נתב (router) הוא רכיב תקשורת מחשבים הנמצא בין האינטרנט לכלל המכשירים החכמים ומייצר עבורם רשת מקומית. הנתב מאפשר לריבוי המכשירים החכמים להתחבר לרשת האינטרנט (כמו מחשבים, טלפון חכם, טאבלט, מצלמות אבטחה, מדפסות, מערכות משחק ועוד), לעשות שימוש בחיבור אינטרנט יחיד - באמצעות חיבור קווי או באמצעות גישה אלחוטית (Wi-Fi).

כיום, שכיח כי הנתב יסופק ללקוח ע"י ספקית האינטרנט (ISP), אך ניתן גם לרכוש באופן פרטי כמכשיר בודד או משולב, לשם כך חשוב לבדוק התאמתו לתשתית הספק וכן הידע הנדרש לבצע בו התאמות והגדרות אבטחה.

בטבלה הבאה נציג את המודולים השונים, כאשר כל נתב יכול להגיע כנתב בודד המתחבר לשאר המודולים בנפרד או כנתב המשולב עם מספר מודלים:

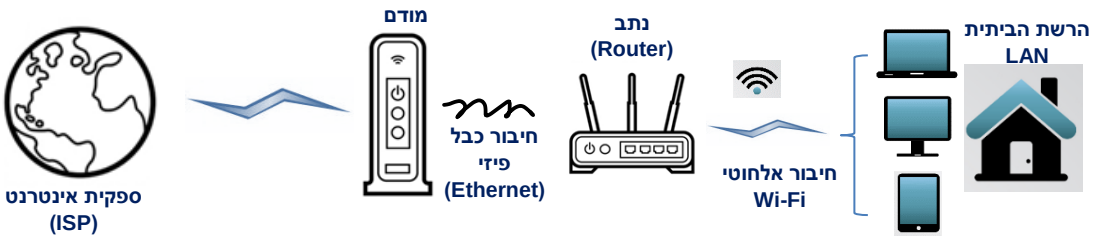
מודולים שונים			
מודם - Modem	נתב - Router	חומת אש - Fire-wall	נקודת גישה Access Point
המודם מתקשר עם ספקית האינטרנט (ISP - Internet Service Provider) לקבלת חיבור לאינטרנט. המודם יכול להיות להגיע כמוצר בודד או משולב.	הנתב מתחבר למודם באמצעות כבל פיזי[1] והמודם מתקשר עם ספקית האינטרנט לקבלת חיבור לאינטרנט. נתב קווי - מיועד למחשבים נייחים, לתשתית קווית, פריסת כבלים המאפשר גלישה מהירה ויציבה. נתב אלחוטי - יוצר רשת אלחוטית	רוב הנתבים מכילים חומת אש מובנית, כחומרה. חומת האש מגנה על הרשת בכך שהיא מאשרת או מונעת תנועה לתוך או מחוץ לרשת הביתית.	נקודת הגישה -AP משמש כתחנת ממסר אלחוטי. מתחבר לנתב המחובר למודם, ולחשמל. ה- AP אחראי לחיבור המכשירים לרשת האלחוטית, במטרה להגדיל את טווח הקליטה. מומלץ בדר"כ לבתים עם חדר ממ"ד / מפלסים.

[1] – הטכנולוגיה המאפשרת את תקשורת הנתונים ברמה הפיזית.Ethernet בפרוטוקול

	באמצעות טכנולוגית Wi-Fi, מאפשר ניידות וחיסכון בהרצת כבלים וחיבורים.		

הידעת? נתב משולב יבצע את עדכוני האבטחה לכלל המודולים המובנים בו. במכשיר שאינו משולב - חשוב לבצע עדכוני אבטחה לכל מודול בנפרד.

מרבית הנתבים מגיעים עם יכולת Wi-Fi, כאשר עלינו לבצע את ההגדרות הראשוניות והבסיסיות. ברוב המקרים, לאחר ביצוע ההגדרות על ידינו או ע"י אנשי התמיכה של הספק, נדאג לאחסן אותו בארון או פינה נסתרת ללא צורך בתשומת לב נוספת, מלבד הצורך אולי לאתחל (boot) את הנתב במקרי תקלה מסוימים.
משמע, על פי רוב לא מבוצעים עדכוני אבטחה לציוד זה (בטח לא באופן תדיר וקבוע).



תרשים א' - תהליך חיבור הנתב לאינטרנט

הנתב אינו מאחסן בתוכו את המידע האישי שלנו אולם כל תעבורת המידע שלנו עוברת דרכו. כמו כן, ישנה אפשרות לגשת אליו מרחוק דרך הממשקים שלו (בעיקר האלחוטיים), ודרכו אף לרשת המקומית שלנו. נקודות תורפה אלו מאפשרות לתוקפים לנצלן לרעה כדי לחדור למחשבים ולמידע האישי שלנו.

למה כל כך חשוב לאבטח את הנתב?

בעת התקנת נתב ביתי, הנטייה הרווחת היא להחיל את ההגדרות הבסיסיות של היצרן, המגיעות כברירת מחדל. מרבית האנשים אפילו אינם מודעים לקיומן, ולכך שבאפשרותם לבצע בהן שינוי. לחילופין, מבצעים שינוי הגדרות וסיסמאות הנתב רק לאחר תקופה מסוימת.
כיום, בעקבות התפשטות וירוס הקורונה וההשבתה החלקית של המשק, ארגונים רבים מאפשרים לעובדיהם לגלוש בחיבור מרחוק לתוך הרשת הארגונית. הגדרות לא נכונות עשויות להוביל לאבטחה לקויה ול"שער כניסה" עבור תוקפים, שיוכלו לקבל גישה לרשת הביתית של העובד/ת ומשם לדלג לרשת הארגון. לכן חשוב מאוד להגדיר את הנתב בצורה נכונה על מנת שיאפשר שימוש וגלישה בטוחים יותר.

השלכות אפשרויות מאבטחה לקויה של נתב:

- הפנייה של המשתמש לדף אינטרנט אשר המאפשר ביצוע "דיוג נתונים".
- שכנוע של המשתמש להתקין תוכנה זדונית, במסווה של תוכנה ליגיטימית.
- השתלטות על פעילות (Session) לגיטימית של משתמש וזאת באמצעות מתקפת "האדם שבתווך" (MITM)[1] , למרות שמבחינת המשתמש הוא עשוי לראות כי החיבור מאובטח ומוצפן.
- השתלטות על הנתב ושימוש בו כחלק מתקיפה למניעת שירות (DoS/DDoS) כנגד גורם צד-שלישי, דוגמת ספק האינטרנט או אתר אינטרנט.
- השגת גישה לרשת הביתית ללא אישור המשתמש, וזאת כאשר הנתב משמש כגורם מתווך (Proxy).
- ניצול משאבי הנתב או הרשת הביתית לטובת כריית מטבע קריפטוגרפי.
- ועוד

כיצד נוכל להקשיח את הגדרות הנתב הביתי?

חשוב להבהיר כי כיום יש מגוון רחב של נתבים וכי כל נתב מכיל הגדרות וממשקים שונים, אך בכולם ניתן לבצע שינויים בהגדרות ע"י קבלת גישה לממשק הניהול של הנתב. מרבית הנתבים מאפשרים לבצע שינוי הגדרות באמצעות הדפדפן, וכיום אף מתאפשרת גישה לניהול ההגדרות באמצעות אפליקציה ייעודית. לפרטים אודות הנתב שברשותכם, ניתן לפנות לספקית האינטרנט או לאתר היצרן.

לפני שמתחילים, חשוב להבין שיש צורך להחליף את סיסמת ברירת המחדל ולהגדיר בעצמך שתי סיסמאות נפרדות: סיסמה אחת עבור סיסמת משתמש המנהל

(Administrator) - משתמש זה הינו בעל הגישה להגדרות הנתב. הסיסמה השנייה הינה עבור גישה לרשת האלחוטית (ה- Wi-Fi).

הגדרות הנתב

התחברות לממשק הניהול - לכל נתב יש כתובת IP[2] המאפשרת גישה לממשק הניהול. לעיתים קרובות ניתן למצוא את הפרטים במדבקה המוצמדת בתחתית הנתב או בהוראות/מדריך למשתמש המצורף לנתב. במידה ואין ברשותכם את המידע - ניתן לפנות לאתר היצרן לקבלת מידע אודות התחברות לממשק הניהול וההגדרות.

שינוי שם משתמש וסיסמה בנתב - שכיח שיצרן מגדיר שם משתמש וסיסמה ראשוניים כברירת מחדל, המאפשרים למשתמשים גישה להגדרות המכשיר (ישנם מספר אפשרויות שכיחות לשמות משתמש וסיסמאות כברירית מחדל של היצרנים כגון שימוש בשם משתמש וסיסמה - admin). פרטים אלו זמינים בפרסומים שונים ולפיכך ידועים היטב גם לתוקפים פוטנציאלים. לכן, במהלך ההתקנה הראשונית של הנתב, יש לשנות מיד פרטים אלו. בשינוי סיסמת ברירת המחדל של היצרן, דאגו לבחור בסיסמה חזקה אך קלה לזכירה, לדוגמה סיסמה ארוכה שהיא חלק מביטוי/שיר, או סיסמה בעלת 16 תווים לפחות, בשילוב של אותיות קטנות וגדולות, סימנים מיוחדים (@#$%) ומספרים.
*הערה -במידה ושכחתם את הסיסמה שהגדרתם, ניתן לאפס את סיסמת הנתב לברירת המחדל של היצרן ע"י לחיצה על כפתור ה- Reset הנסתר, הנמצא בחלק האחורי או התחתון של הנתב. יש לקחת בחשבון שבכך כל הגדרות הנתב מתאפסות.

הקלד את כתובת IP של הנתב בדפדפן - התחבר עם שם המשתמש וסיסמת ברירת המחדל. בהגדרות בחר "שינוי סיסמת נתב" - הקלד סיסמה חדשה - לחץ על "שמור הגדרות חדשות".

שינוי שם זיהוי הרשת האלחוטית (SSID) - כל יצרן מקצה לנתב האלחוטי שם ברירת מחדל הנקרא: "מזהה ערכת שירותים" (SSID - Service Set Identifier) או "מזהה ערכת שירות מורחב" (ESSID - extended SSID). לרוב, שם הזיהוי (SSID) חשוף בפני כל מי שיסרוק את תווך התקשורת. ע"פ SSID ברירת המחדל גורם זדוני יוכל למשל לזהות באיזה ציוד נעשה שימוש ובהתאם, לאתר חולשות ידועות בציוד ולתקוף באמצעותן. לכן, בעת הגדרתו הראשונית של הנתב חשוב להחליף מיד את השם ולבחור בשם שלא יעיד על מאפייני הדגם, היצרן, שמו של בעליו או מיקומו של הנתב.

הקלד את כתובת IP של הנתב בדפדפן - התחבר עם שם משתמש וסיסמה -

[2] IP– Internet Protocol, הוא פרוטוקול תקשורת המשמש להעברת נתונים, והינו חלק מחבילת IP, או בקיצור הינה מספר חד-חד-ערכי המשמש IP הנמצאת בשימוש נרחב ברשת האינטרנט. כתובת TCP/IPהפרוטוקולים לזיהוי נקודות קצה, ברשתות תקשורת שבהן משתמשים בפרוטוקול התקשורת IP, כגון רשת האינטרנט.

בחר בהגדרות - בחר "הגדרות אלחוטיות" - הקלד את שם ה- SSID החדש - לחץ על "שמור הגדרות חדשות" והמתן לאתחול הנתב.

שינוי סיסמת רשת ה- Wi-Fi - כאמור, גם פה מוגדרת סיסמת ברירת מחדל של היצרן. יתרה מכך - לעיתים הנתב מוגדר כך שהגישה לרשת ה-Wi-Fi אינה מצריכה סיסמת כניסה כלל. במידה וניתן, חשוב מאוד לשנות לסיסמה חזקה (ארוכה ומורכבת). מומלץ לבחור סיסמה שניתן לזכור בקלות אך שלא ניתן לאתרה על ידי חיפוש באינטרנט ברשימות "הסיסמאות הנפוצות" (ובשום פנים לא לבחור מספר טלפון או ת"ז כסיסמה) - זאת כדי שניתן יהיה להעבירה לאורחים/מבקרים שיורשו לגלוש ברשת הביתית.

פעולות אבטחה נוספות

עדכוני קושחה (Firmware) - בדיוק כמו בעדכוני אבטחה של תוכנות במחשבים, חשוב מאוד לעדכן את הקושחה בנתב בעדכון האחרון שהפיץ היצרן. בעת בחירת נתב, טרם רכישתו, חשוב לבדוק באתר היצרן באם הוא מספק עדכונים לטיפול בבעיות אבטחה, מה שיבטיח מוצר איכותי ומאובטח.

בשונה ממכשיר סלולארי או מחשב בהם לרוב נקבל התרעות והוראות לביצוע עדכוני תוכנה - עבור הנתב לרוב לא נהיה מודעים לכך שקיים עדכון. אמנם נתבים מסוימים מאפשרים לבצע עדכונים אוטומטיים - באם ניתן, הפעל אופציה זו. במקרה ולא ניתן לבצע עדכונים אוטומטיים, יש לבצע עדכונים עיתיים באופן יזום - מומלץ להגדיר תזכורת אישית עיתית לבדיקה האם קיים עדכון.

הפעלת חומת אש (Firewall) - חומות אש מסייעות להגן ולשמור מפני חדירה של גורמים זדוניים לרשת ומשימוש במכשירים שלך. חומת האש צופה ומגנה מפני ניסיונות כניסה לרשת וחוסמת תקשורת עם מקורות שאינם מורשים. נתבים, מערכות ההפעלה או תוכנות אבטחה מגיעים לרוב עם חומת אש מותקנת מראש, כשכבת הגנה נוספת, על מנת למנוע מהמחשבים לבצע חיבור לא רצוי למכשירים שלנו. חשוב לוודא מולם היצרן/הספקית שה- FW אכן מופעל וכי המערכות מעודכנות בכל העדכונים.

הגדרת רשת אלחוטית נפרדת לאורחים - נתבים מסוימים מאפשרים להגדיר גישה לרשת חיצונית המופרדת מהרשת הראשית שלנו, למשל עבור אורחים אשר יוכלו להתחבר באמצעות סיסמה שונה שתוגדר מראש. הדבר ימנע מהם יכולת לגשת למכשירים השונים והמידע שנמצא ברשת המרכזית.

בהגדרות בחרו ב"רשת אורחים" (Guest Network) - סמנו את ה-Checkbox של "שידור שם ה-SSID" (להצגת שם הנתב בפני אחרים) - בחרו שם SSID אותו יוכלו לראות האורחים - בחרו אפשרויות אבטחה - שמרו את השינויים.

הגדרת מנגנון לבידול משתמשים ברשת האלחוטית (AP Isolation) - אפשרות זו מאפשרת לבודד את כל התחנות האלחוטיות המחוברות כך שהתחנות האלחוטיות לא יהיו מסוגלות להתחבר זו לזו באמצעות רשת התקשורת.

בהגדרות הנתב, בחר Client Isolation או Access point בחר enable, בצעו שמירה של ההגדרות.

הגדרת אימות והצפנה גבוהה - בהגדרת האבטחה של הרשת האלחוטית, ניתן להגדיר את רמת האבטחה של העברת המידע ע"י אימות והצפנה. טכנולוגיית הצפנה מערבלת את המידע הנשלח על גבי הרשת אלחוטית, כך שלא יהיה ניתן לפענחו בקלות. בחרו בשיטת התצורה החזקה ביותר WPA2 או WPA3. באימות הצפנת התווך יש לבחור בתקן הצפנה מתקדם - AES. יש לבחור זאת ב- 2.4GHz וכן ב -5GHz.
*יתכן ומכשירים מסוימים לא יאפשרו שימוש מלבד WEP המכיל חולשות ידועות שניתן לנצלן לרעה. במידה ואין ברירה - הוא עדיף מכלום.

חיבורי מכשירים לא ידועים - בכל שלב ניתן לבדוק בממשק הניהול של הנתב אילו התקנים מחוברים לרשת שלך. לרוב, רשימת ההתקנים מזוהה עם שם וסוג המכשיר המחובר. במידה וזיהית מכשיר לא ידוע, הסר את המכשיר, החלף את סיסמת החיבור וישם סינון באמצעות בקרת גישה למדיה (MAC Address) על הנתב. חשוב לבצע בדיקה עיתית להתקנים המחוברים. למידע נוסף כיצד ליישם חוקים אלו ניתן לפנות לאתר היצרן.

בהגדרות היכנסו ל'רשת שלי' (My Network) או ל"מכשירים מחוברים" (Attached Devices). תוצג בפניכם רשימת כלל המכשירים המחוברים לנתב.

השבתת שרות UPnP (Universal Plug and Play) - שרות זה קיים במרבית הנתבים ומאפשר להתקנים ברשת (אפליקציות או מכשירים) ליצור תקשורת דרך הנתב. למרות שתכונת UPnP מקלה על תצורת רשת ראשונית, היא עלולה להוות סכנת אבטחה משמעותית כאשר תוכנות זדוניות הנמצאות כבר בתוך הרשת יכולות להשתמש בה כדי לפתוח פתח בחומת האש בנתב ולאפשר לפולשים לחדור פנימה. ניתן להגדיר מראש מכשירים מסוימים כמו קונסולת משחקי וידאו, מצלמות או שרת מדיה על מנת לקבל תקשורת מחוץ לרשת, על אף שזה מהווה סיכון אבטחתי. אם אין צורך בשרות זה - יש להשביתו.

השבתת שירות WPS (Wi-Fi Protected Setup) - זהו מנגנון פשוט או כפתור הממוקם בחלק מהנתבים, במטרה לאפשר לגורם בעל נגישות פיזית לקבלת גישה מהירה לרשת האלחוטית. המנגנון מאפשר שיטת הזדהות פחות חזקה, אשר עלולה להוביל לקבלת גישה אלחוטית באמצעות תהליך פריצה קל יחסית. לרוב השרות מופעל כברירת מחדל, לכן מומלץ לבטלו. תהליך השבתת השרות שונה מיצרן ליצרן.

בהגדרות Wireless, בחר Wi-Fi Protected Setup (WPS), יש לבחור ב- off או Disable, ושמירה (Apply Changes\Save).

גיבוי הגדרות תצורה - יש לבצע גיבוי הגדרות תצורה לאחר התקנה ראשונית ובאופן עתי, וזאת לשם מתן יכולת שחזור מהירה במקרה של תקלה.

לאחר התחברות לנתב, בחר בתפריט Maintenance, Backup settings, בחר Backup, בחלונית שתיפתח, בחר את מיקום ותיקיה במחשב לשמירת קובץ הגיבוי.

התנתקות ממשק הניהול - בסיום השימוש בממשק הניהול של הנתב- חשוב לבצע התנתקות מסודרת (Logout) ממשק הניהול.

כיבוי הרשת האלחוטית - כיבוי הנתב או הרשת האלחוטית בהחלט ימנע כניסת תוקפים לרשת - הדבר רלבנטי בעת נסיעות או היעדרות ארוכה.

במידה והנכם חושדים כי הראוטר שלכם הותקף או נפרץ, מומלץ להחליפו.

המלצות למתקדמים:

נטרול מענה פינג (PING) - מטרתה העיקרית של פקודת פינג היא לשמש לבחינת תקינות התקשורת ברשת מחשבים בין נקודת המקור לנקודת היעד. כאשר תגובת פינג מופעלת, ביצוע סריקה מבחוץ (מהאינטרנט) במטרה לגלות את הנתב הופכת להיות קלה יותר, היא מאפשרת לנתב להגיב לפקודות שהתקבלו מהאינטרנט, ועשויה לפיכך לחשוף את הרשת לפולשים זדוניים. לכן מומלץ לבטל תכונה זו. אמנם ביטולה לא יגן מפני גילוי, אך לפחות יגביר את הקושי לגילוי.

הקשחה וסינון כתובות MAC - אפשרות זו מגבירה את רמת האבטחה ע"י הגדרת רשימה סגורה של מכשירים, המורשים להתחבר לרשת דרך הנתב. לכל רכיב תקשורת קיימת כתובת MAC ייחודית וקבועה הצרובה בכרטיס הרשת NIC (Network Interface Card). כל התקן המתחבר לרשת ה-Wi-Fi מזוהה בנתב על ידי כתובת ה-MAC שלו. לכן ניתן להגדיר לנתב מראש רשימה סגורה של כתובות MAC, אשר רק הן מורשות להתחבר לרשת ה-Wi-Fi.

טיפ - לפני הפעלת הסינון ניתן לחבר את ההתקן האלחוטי שברצוננו לחבר. לאחר החיבור, הכנס להגדרות אבטחת הנתב ופתח את רשימת הלקוח של DHCP אשר נמצאת בדר"כ בסטטוס או בחירות רשת מקומית. כל מכשיר

שמתחבר יציג את כתובת ה- MAC אשר ניתן להעתיקו ואז להדביקו באזור רשימת סינון ה- MAC.

ביטול שידור שם הרשת האלחוטית (SSID) - לטובת איתור הרשת האלחוטית, הנתב משדר את שם הרשת (SSID) אשר יכול להיות חשוף לכולם. ניתן להשבית את אפשרות שידור ה- SSID. יחד עם זאת, בעת השבתת שם הרשת, נדרש להזין באופן ידני את שם הנתב הייחודי (ה- SSID) בעת חיבור התקן חדש לרשת.

להפסקת שידור ה- SSID, בהגדרות, בחרו Enable SSID Broadcast , לחץ על שמירה.

שימוש בכתובות IP קבועות - רוב הנתבים הביתיים מוגדרים בברירת המחדל כשרתים המקצים כתובות IP דינאמיות (DHCP- Dynamic Host Configuration Protocol). שרת ה- DHCP הופך את ניהול הרשת לקל יותר, על ידי הקצאה אוטומטית של כתובות ה-IP. עם זאת, מאפשר גם למשתמשים לא מורשים לקבל כתובת IP ברשת. ביטול שרות ה-DHCP וחלוקה ידנית של כתובות ה- IP ללקוחות ברשת יקטין משמעותית את הסיכון לכניסתו של גורם עוין לרשת.

סגירת פורטים לא נחוצים - סגירת ממשקי ניהול שונים הפעילים בנתב (לדוגמה- Telnet ,RDP, SMB, SSH וכו') ואם יש צורך בניהול מרחוק, השארת פרוטוקול TR-069 בלבד פעיל.

נטרול ממשק עדכון וניהול מרחוק של הנתב - ניהול מרחוק מאפשר לכל גורם הקרוב מספיק לנתב, להציג או לשנות את הגדרות הנתב. על מנת להישמר מפני פולשים זדוניים ולמנוע אפשרות התחברות עם הנתב מרחוק באמצעות רשת התקשורת המרחבית (WAN) יש לנטרל את ממשק הניהול מרחוק, כמו גם את אפשרות העדכון מרחוק שעשויה לאפשר התחברות ופגיעה בקושחה (Firmware) של הנתב. עם ביטול הניהול עדיין ניתן לשנות הגדרות נתב באמצעות כבל רשת. כמו כן לוודא שהנתב לא ניתן לניהול באמצעות ה - WIFI.

לאחר התחברות לנתב, בחר Advanced Settings, ובשלב יש Remote Management לבחור באפשרות של Disable.

בדקו את עצמכם -צ'ק ליסט

Check List

- ✪ שינוי שם משתמש וסיסמת גישה לנתב
- ✪ שינוי SSID (שם הנתב)
- ✪ שינוי/הגדרת סיסמת Wi-Fi
- ✪ חסימת שידור SSID
- ✪ עדכוני קושחה
- ✪ הפעלת חומת אש
- ✪ הגדרת נקודת גישה נפרדת לאורחים
- ✪ הדרת מנגנון בידול משתמשים
- ✪ הגדרת אימות והצפנה גבוהה
- ✪ חיבור מכשירים לא ידועים
- ✪ השבתת UPnP
- ✪ השבתת WPS
- ✪ גיבוי הגדרות תצוגה
- ✪ התנתקות ממשק הניהול
- ✪ נטרול מענה PING
- ✪ הקשחה וסינון כתובות MAC
- ✪ ביטול שידור שם הרשת
- ✪ שימוש בכתובת IP קבועה
- ✪ סגירת פורטים לא נחוצים
- ✪ נטרול ממשק עדכון וניהול מרחוק