

# עבודה SSH - מגיש סרג'ו

## מטרת העבודה

מנהל לא מאובטח לניהול מאובטח ומוצפן. (TechNet) העברת רשות הארגון הגדרת אימות משתמשים, והגבלה, SSH-ל Telnet התהיליך כל מעבר מפרוטוקול הגישה למנהל רשות מורשים בלבד.

---

### (R1 בוצע על) SSH-חלק א': הגדרות בסיס והכנה ל

לפני הפעלת הצפנה, הוגדרה זהות לראוטר כדי שיוכל ליצור מפתחות הצפנה ייחודיים.

#### 1. הגדרת שם ודמות:

- פקודות: `hostname R1, ip domain-name raja.local`

#### 2. יצירה מפתחות הצפנה (Crypto Keys):

- עם מפתח באורך 1024 סיביות RSA בוצע שימוש באלגוריתם ◦
- פקודה: `crypto key generate rsa general-keys modulus 1024`

#### 3. הגדרת גרסת פרוטוקול:

- נבחרה גרסה 2 (המאובטחת יותר) ◦
  - פקודה: `ip ssh version 2`
- 

### חלק ב': ניהול משתמשים והרשאות

במקום סיסמה כללית לכלם, עברנו לשיטת אימות אישית ומדורגת.

#### 1. יצירה משתמש מנהל:

- עם הרשאות מלאות `raja` נוצר משתמש מקומי בשם ◦  
וsisma מוצפנת ◦
- פקודה: `username raja privilege 15 secret 456`

#### 2. אכיפת האימות בחיבורים:

- נדרש שם משתמש וסיסמה YTV-ו Console לחיבור ◦
- login local (Line). ◦

---

## חלק ג': אבטחת ערוצי הגישה (VTY Lines)

הקשחת "הדרגות" דרך מتابצע ניהול מרוחק.

### 1. Telnet סיסמת:

- SSH הוגדר שהרואוטר יקבל אך ורק תעבורת ◦
- פקודה: `transport input ssh` (line vty 0 4).

### 2. סינון כתובות (ACL):

- המאשרת רק את כתובת המנהל **PC2RAJA** נוצרה רשיימת גישה בשם ◦
  - (10.2.2.1). וחוסמת את כל השאר ◦
  - באמצעות הפקודה VTY-החלת הרשימה על ◦ `access-class PC2RAJA in`.
- 

## חלק ד': הקשחת אבטחה נוספת (Security Hardening)

ואגניבת סיסמות Brute Force הוספת שכבות הגנה למניעת התקפות

1. **אורך סיסמה מינימלי:** הוגבל ל-8 תווים (`security passwords min-length 8`).
2. **הוגדרה חסימה ל-2 דקות אם זוהה 3 ניסיונות:** (**Login Block**) מנגנון געילה כושלים בתור דקה.
3. **הצפנת סיסמות:** כל הסיסמות בקובץ ההגדירות הוצפנו (`service password-encryption`).
4. **ניתוק אוטומטי:** הוגדר ניתוק לאחר 5 דקות של חוסר פעילות (`exec-timeout 5 0`).