2017-11-27

09:42 Sunday, December 3, 2017

סיכום פעילות באתר יד ושם מתאריך 27/11/2017:

- Portnox מותקן בתצורת standalone על שרת וירטואלי

<u>הגדרות:</u>

- האזנה ב layer 2 ל VLAN המחשבים (ומדפסות) מכיוון שיש מדפסות שלא מתקשרות מחוץ למתג שלהן (מספקות מענה מקומי).
- כלל המתגים על פי מיקום פיזי. UPLINK הוגדר עבור חיבורי WIFI עם הערה מתאימה (wifi)
- ה FW וה Backbone כ IP Helpers
- Community ברירת מחדל בעל הרשאת Read
- נתוני שליחת דוא"ל
- שיטות אימות:
  - msDomain עבור כלל המחשבים השייכים לדומיין
  - msWorkgroup עבור ציוד שאינו מחובר לדומיין (לדוגמא: מחשבי מוניטור). מכיוון שהציוד הוגדר הקבוצות (workgroup) שונים, הוגדרו מספר שיטות אימות. יש להשלים הגדרת שיטות אימות עבור שאר הקבוצות בהתאם לקבוצות הקיימות בציוד.
  - OSFP למדפסות כולל את כלל המדפסות שנמצאו ברשת
  - MISC OSFP הוגדר עבור ציודים שונים שנמצאו ברשת
- קבוצות Resident:
  - Disk - נעול ל PORT עבור 2 חיבורי דיסק
  - VCENETER - נעול ל PORT
  - LearnCenter - נעול ל PORT עבור ציוד קבוע בכיתות
  - Control Building - נעול לVLAN 101 עבור ציוד בקרת מבנה
  - Security Camera - נעול לVLAN 200 עבור מצלמות אבטחה
  - Mngmnt - נעול לVLAN 2
- POLICY:
  - המערכת מוגדרת לניטור וכל גם כלל המתגים
  - הוגדרו אירועים להתרעה אך ללא שליחת דוא"ל בשלב זה

<u>להמשך:</u>

- לסיים הגדרת שיטות אימות מסוג msWorkgroup שעדיין חסרות במערכת
- להוסיף את Backbone כמתג
- להוסיף את רשת הטלפוניה

<u>בעיות לטיפול:</u>

- שליחת דוא"ל מתבצעת בצורה מסיבית עבור כל אירוע ROGUE. על פי הנראה מתבצע אימות מחודש (לא פטרול) עבור חלק מהרכיבים. יש לאסוף לוגים על מנת לאפשר חקירה וניתוח המקרה.