2018-09-06

Thursday, 6 September 2018 14:32

שלום לכולם,

להלן סיכום בנושא פעילות שהייתה בתאריך 27.08.2018 עם יהודה מתמיכה של ה-Portnox והתרכזה ב:
- מעבר על כל הנקודות הבעייתיות שהעלה הלקוח.
- בדיקת תפקוד השרתים מבחינת המשאבים והאם יש המלצות לשיפור תפקודם.
- ביצוע בדיקה מדגמית של ההגדרות במספר המערכות (מתגים / נתבים) אשר הוכנסו אל ה-Portnox לצורך ווידוי כי הם עונים לדרישות הגדרת המערכת לתפקוד מול ה-Portnox.
- מעבר שטחי על השגיאות במערכת ה-Portnox לצורך זיהוי נושאים הדורשים טיפול.

להלן הממצאים מהבדיקה:

שרתי ה-Portnox

1. בעיית הזיכרון (RAM) על שרתי ה-Portnox.
   לסירוגין מתקבלים התראות על שימוש גבוהה בזיכרון של השרתים.
   לכל שרת של ה-Portnox מוקצה 12GB ה-RAM ולסירוגין השימוש מנצל את כל משאבי המערכת.
   יהודה לא נתן המלצה לעלות את משאבי המערכת כרגע.
   המלצה:
   א. שדרוג והתקנת ה-Patch המומלצים ע"י ה-Portnox.
   בספטמבר 09.2018 אמור לצאת ה-Patch אשר מטפל בנושא של שימוש בזיכרון ע"י המערכת.
   בנוסף, קיימת גרסה ה-Stable חדשה ומומלצת (ב-SuperPharm כרגע מותקנת גרסה מיוחדת המאפשרת ביצוע איתור בעיות מורחבת).
   המלצה לשדרג לגרסה אחרונה ולתקין את ה-Patch.
   ב. במקרה והבעיה תימשך, יהיה צורך בהעברת טיפול בבעיה לפיתוח לצורך זיהוי מקור הבעיה.
2. מקום פנוי ב-HDD.
   זיהינו כי המערכת ה-Portnox מוגדרת לייצר המון רישומים כחלק מטיפוול בתקלות אשר בערך תוך חודש מנצלים את כל מקום הפנוי.
   בנוסף, המלצת היצרן הינה שיהיו 80GB פנויים עבור המערכת ה-Portnox.
   בפועל, ה-HDD הינו 60GB וה-Windows אוכל כ-22GB~.
   ל-Portnox נותר פחות מ-40GB~.
   המלצה:
   א. לעלות ה-HDD לכל שרת ל-100GB כך שלמערכת ה-Portnox יהיה כ-80GB~ המומלצים ע"י היצרן.
   ב. מומלץ להקצות דיסק נוסף נפרד עבור כתיבת הרישומים (D:\ ).
   כתיבת רישומים המורחבים אל אותו ה-Partition בה נמצאת מערכת ההפעלה (ה-Windows) וגם מערכת ה-Portnox בזמן ניצול כל המקום הפנוי גורמת לפגיעה בתפקוד השירות.
   ג. ארבעת שרתי ה-Portnox הוגדרו להסיר את ה-Backup Logs לאחר 14 יום.
   הגדרה הינה דרך ה-Regedit:
   Registry: HKEY_LOCAL_MACHINE\SOFTWARE\AccessLayers\PortNox\WatchDog\KeepLogs
   Current setting: 14 Days

תשתית ומערכות ה-SuperPharm

3. הגדרות ה-SNMP GET ב-Switches וה-Routers בהתאם להמלצות עבור אותו היצרן וגרסה עליה הם רצים.
   מערכת ה-Portnox משתמשת ב-SNMP GET לצורך משיכת מידע והפעלת העקיפה על המתגים / נתב.
   לכן, הגדרה תקינה של רכיב זה בנתבים / מתגים חיונית עבור תפקוד מערכת ה-Portnox.
   לאורך הזמן, זוהו מספר נתבים / מתגים עם הגדרות בעיתיות אשר לא אפשרו ל-Portnox לתפקד.
   ה-Portnox הוגדר לדגום את הציוד (מבצע תהליך ה-Probe) כל 360 שניות (Reprobe Interval) כדי לוודא כי הוא מצליח לשלוט על המערכת.
   באם הציוד אינו נגיש לשליטה, הוא מסומן באדום ב-GUI של ה-Portnox ונוצר ה-Alert המתאים (Switch is NOT Accessible) ולא ניתן יהיה לבצע פעילויות על הציוד ב-GUI.
   נא לשים לב!!! ה-Alert יווצר גם באם הציוד נפל ולא היה זמין בזמן ביצוע ה-Probe וחזר לאחר זמן מה.
   הגרסה החדשה תבטל את ההתראה באופן אוט' במקרה והציוד חזר.
   כל זה בדר"כ קורה לאחר החלפת ציוד תקול או פריסת ציוד חדש ללא הגדרות המתאימות.
   לדוגמא רק מתאריך 03.09.2018:
   172.29.191.28, 172.29.191.29, 11.202.0.245, 11.0.1.42, 11.0.1.57, 11.0.1.49, 11.0.1.44, 11.0.1.55, 11.0.1.39, 11.0.1.54, 11.0.1.43 וכ"ו .....
   לצורך החזרת הציוד מצב פעיל, נדרש התערבות ידנית של איש ה-Portnox. ביצוע ה-Disable וה-Enable לנתב / מתג מפעיל אותו בחזרה.
   המלצה:
   א. שדרוג והתקנת ה-Patch המומלצים ע"י ה-Portnox.
   הדבר יפתור את הבעיה של חזרה ידנית של הנתב / מתג לאחר **בעיה שהייתה בו** למצב מבוקר / מנוהל עם נתונים עדכניים ועם עקיפה פעילה.
   ב. נדרש לבנות את ההגדרות המומלצות עבור כל סוג ציוד וכל גרסה שיש בסופרפארם.
   ג. מומלץ להפעיל מערכת בקרה לניטור ודיווח תקופתי על כל הציוד הלא תואם להמלצות של ההגדרות (מומלץ לנטר עד לרמת ה-Case Sensitive).
4. הגדרות ה-SNMP TRAP ב-Switches וה-Routers בהתאם להמלצות עבור אותו היצרן וגרסה עליה הם רצים.
   ה-SNMP TRAP מאפשר לשרתי ה-Portnox לקבל מידע על שינוי בסביבה כמעט באופן מיידי ולא לחכות עד לבדיקה מחזורית הבאה לזיהוי השינוי המוגדר להתבצע כל 120 דקות (patrol interval).
   בנוסף לבעיה שההגדרות אלו חסרות או לא מוגדרות נכון, זוהו מספר התראות נוספות ב-Portnox על ה-SNMP Traps ונדרש לעבור עליהם ולטפל בכל מצב בנפרד.
   המלצה:
   א. נדרש לבנות את ההגדרות המומלצות עבור כל סוג ציוד וכל גרסה שיש בסופרפארם.
   ב. מומלץ להפעיל מערכת בקרה לניטור ודיווח תקופתי על כל הציוד הלא תואם להמלצות של ההגדרות (מומלץ לנטר עד לרמת ה-Case Sensitive).
   ג. יש לעבור על כל סוג התראה ב-Portnox על ה-SNMP Traps ולזהות מקור הבעיה.
5. הגדרות ה-VTY על ה-Routers.
   הגישה ה-VTY נדרשת עבור הנתבים לצורך ניהול מערכת אשר לא מתאפשר דרך ה-SNMP.
   המלצה:
   א. נדרש לבנות את ההגדרות המומלצות עבור כל סוג ציוד וכל גרסה שיש בסופרפארם.
   ב. מומלץ להפעיל מערכת בקרה לניטור ודיווח תקופתי על כל הציוד הלא תואם להמלצות של ההגדרות (מומלץ לנטר עד לרמת ה-Case Sensitive).
6. הגדרות ה-ACL בנתבים / מתגים.
   ארבעת שרתי ה-Portnox חייבים להיות מאופשרים לגישה ניהולית אל הנתבים / מתגים.
   אחרת, יווצר מצב אשר תוארה בסעיף 3.
   המלצה:
   א. ראה סעיף 3.
7. יכולת התחברות של החשבון ה- portnoxacct(מה-AD) אל ה-Router.
   הגישה דרך ה-VTY מתאפשרת ע"י אימות ה-AAA מול ה-RADIUS עם חשבון ה-portnoxacct.
   נדרש עבור מניעת מצב אשר תואר בסעיף 5.
   המלצה:

א. ראה סעיף 5.

8. הגדרת ה-VLANים הקיימים במתג / נתב אל ה-Portnox.
הגדרת ה-VLANים ב-Portnox מומלץ שישקף את מצב התשתית בסופרפארם.
בזמן האחרון, היו המון שינויים ב-VLANים בסופרפארם (הרשתות התפצלו לכמה ה-VLANים, נוספו ה-VLANים חדשים וכ"ו) ולכן ההגדרות ב-Portnox אינם משקפים יותר את מצב התשתית בסופרפארם.
המלצה:

א. נדרש לעבור על כל הנתבים / מתגים המוגדרים ב-Portnox ובמקרה הצורך לבצע עדכונים ב-Portnox בהתאם.

9. הגדרת ה-IP Helpers הקיימים בנתב אל ה-Portnox.
הגדרת ה-IP Helpers ב-Portnox נדרש שישקף את מצב התשתית בסופרפארם.
בזמן האחרון, היו המון שינויים ב-VLANים בסופרפארם (הרשתות התפצלו לכמה ה-VLANים, נוספו ה-VLANים חדשים וכ"ו) וכתוצאה מכך ההגדרות של ה-IP Helper אינו משקף יותר את מצב התשתית בסופרפארם.
המלצה:

ב. נדרש לעבור על כל הנתבים / מתגים המוגדרים ב-Portnox ובמקרה הצורך לבצע עדכונים ב-Portnox בהתאם.

10. אימות ציודים חדשים.
חשוב להדגיש!!! כל ציוד חדש אשר נכנס אל סביבת הסופרפארם המבוקרת ע"י ה-Portnox דורשת הגדרת חתימות ייעודיות עבור זיהוי ואימות המערכת.
נדרש לוודא כי כל הציודים אשר הוכנסו לרשת מזוהים תקין.
המלצה:

א. לעבור על הציודים אשר לא מצליחים לעבור אימות ולוודא כי הם מזוהים תקין.

11. אימות ציודים ידועים, אבל גרסאות ה-Firmware או ה-OS חדשים.
חשוב להדגיש!!! כמו עם כל ציוד חדש, קיימים גם ציודים אשר אחרי שדרוג מתחילים לתפקד בצורה שונה ולכן נדרשת בניית חתימה חדשה ב-Portnox.
נדרש לוודא כי כל הציודים אשר הוכנסו לרשת מזוהים תקין.
המלצה:

א. לעבור על הציודים אשר לא מצליחים לעבור אימות ולוודא כי הם מזוהים תקין.

12. נוהל פעולה עבור ציוד אשר לא עובר אימות.
המלצה:

א. נדרש לבנות נוהל של סופרפארם עבור ציוד אשר לא עובר אימות עבור כל סביבה מבוקרת.

13. ה-SNMP TRAP של ה-mac-notification חסרה ב-Cisco 891.
ההגדרה זו חשובה עבור שהמערכת ה-Portnox תקבל התראה בזמן שלפורט ה-VoIP חובר מחשב והוא מייד יעבור אימות.
במצב בו מחשב מחובר דרך הטלפון, ההגדרה של ה-LinkUp אינה תזהה ולא תשלח התראה על התחברות לרשת של ציוד חדש.
המלצה:

א. נדרש לבדוק מול ה-Cisco האם יש גרסה עם תכונה זו.

מערכת ה-Portnox

14. בסופרפארם הועלה מצב בו הפורט ב-Portnox עם חיבור מחשב דרך הטלפון, מציג את הטלפון המחובר אל ה-VoIP ומחשב המחובר אל ה-VLAN ה-DATA תחת אותו ה-VLAN.
בבדיקה ראינו כי ה-VLAN המוצג תחת שדה ה-vlan הוא שמוגדר כ-Access VLAN על הפורט, ה- VoIP VLAN מוצג תחת שדה ה-ip בסוגריים (אם זה לא מופיע, כל מצב ייבדק בנפרד).
המלצה:

א. נדרש הסבר למשתמשי המערכת על כל שדה ומה הוא מציג ואיך ניתן לזהות את ה-VLAN אליו מחובר הטלפון.

ב. באם תזוהה בעיה על פורט מסוים, נדרש טיפול נפרד מול תמיכה של ה-Portnox.

15. שמירת ההגדרות ה-Configuration Running ל-Configuration Startup בציוד של ה-Cisco לאחר שינוי ה-VLAN על הפורט.
אכן במצב הקיים ההגדרה תשתנה באם הנתב / מתג יעבור אתחול.
ניתן לפתור זאת ע"י הפעלת ה-Script אשר יבצע גם את ה-write (יהודה לא המליץ על כך) וקיימות מספר פתרונות נוספים למצב.
המלצה:

א. נדרש הסבר לאנשי התמיכה כי כל שינוי ה-VLAN תקף אך ורק עד לאתחול.

ב. נדרש לפתח פתרון למצב הקיים מכל האפשרויות הקיימות כך שיתאים לצרכים של הסופרפארם מתהליך.

ג. יהודה המליץ לעלות את ה-Feature Request לצורך הוספת תכונה זאת.

16. לאחר שינוי ה-VLAN ב-Juniper, ה-VLAN משתנה ב-GUI אבל אינו השתנה במתג או שכלל לא משתנה.
הבעיה מתרחשת בדר"כ בגלל תהליך ה-COMMIT שנכשל עקב שינויים ישנים אשר התבצעו במערכת ולא בוצע להם COMMIT.
אחרי ה-PROBE, הפורט שוב משתנה למצב הישן.
המלצה:

א. נדרשת בדיקה של כל מצב בנפרד (לי עדיין לא הוצג פעם אחת מצב הבעייתי).

17. מצב שקיימת התראה אדומה ב-GUI על נתב / מתג והוא אינו מנוהל / מבוקר.
ראה הסבר על המצב בסעיף 3.

18. התראות על ה-Unauthorized SNMP Trap Alerts on.
הבעיה הינה בהגדרות לא תקינות בנתב / מתג.
ראה סעיף 4 עם ההסבר.

19. ה-GUI אינו מזהה את המיקום של הציוד בהתאם לכתובת ה-IP / MAC וכ"ו.
כדי שהזיהוי יתפקד תקין, ה-Portnox חייב לקבל תמונה עדכנית למצב הרשת מציוד שהוא מוגדר לבקר.
בשביל זה, נדרש לפעול בהתאם להמלצות אשר צוינו בסעיפים: 3, 4, 8, 9.

המלצות כלליות

20. מתאמי הא"מ, מומלץ להגביל גישה ניהולית אל הנתב /מתג ע"י ה-ACL על ה-SNMP.

21. מומלץ בחום להפעיל תהליך להקשחת את הציוד ברמת הא"מ ... על חלק זוהה כי ה-HTTP/S Service פעיל ... לא ברור מה הסטטוס כי לא נבדק ...

22. בהגדרות של ה-SNMP בציוד ה-Cisco, שיוך ה-community ל-rw / ro בוצע ע"י אותיות הגדולות RW / RO.
במצב הנ"ל, לא ברור האם שיוך ל-attribute או ל-ACL ... וגם יש סיכוי כי בשדרוג הגרסה המצב ישתנה.
המלצה:

א. לשנות ההגדרה לאותיות הקטנות.

23. כמו שצוין מספר פעמים, מומלץ בחום להפעיל מערכות בקרה עבור ווידוא כי ההגדרות פרוסות בהתאם להמלצות.
ניתן גם להעביר את הדו"חות באופן אוט' אל הגורמים החיצוניים המתאימים עבור התאמת ההגדרות לסטנדרט ... או להפעיל מערכות אוטומציה לביצוע איחוד של ההגדרות.