Technologic Papers

איך לא מומלץ לנהל את ה-Firewall שלך

מאת יורי סלובודיאניוק

הקדמה

במהלך 10 שנות עבודה יום-יומית עם ה-Firewall של CheckPoint ראיתי לא מעט תקלות שונות ומשונות, בגרסאות שונות של Firewall-ים ובטופולוגיות רשת שונות - אך המכנה המשותף היה שכמעט בכל המקרים מנהלי הרשת היו חוזרים על אותן הטעויות שוב ושוב. המאמר הבא מסכם את התקלות השכיחות ביותר שנגרמות ע"י מנהלי Firewall-ים ובא לעזור למנוע תקלות כאלה.

מחיקת אובייקט שנמצא בשימוש

השגיאה הנ"ל אופיינית במיוחד לאנשי System בסביבת Windows - כאלה שמאשרים כל פעולה שמוצגת כאזהרה (Warning) ולא כשגיאה. מכל הטעויות, זאת יכולה להיות **הקטלנית ביותר** לקריירה שלכם. CheckPoint מאפשרת למחוק אובייקט שנמצא בשימוש - אך נותנת אזהרה שגם מראה איפה בדיוק האובייקט בשימוש.

ההמלצה שלי - לא למחוק אובייקטים שנמצא בשימוש **לעולם** - אלא לעבור על כל מקומות שבהם האובייקט בשימוש ולהוציא אותו משם בהפעלת היגיון כמובן ורק אחרי זה למחוק אותו.

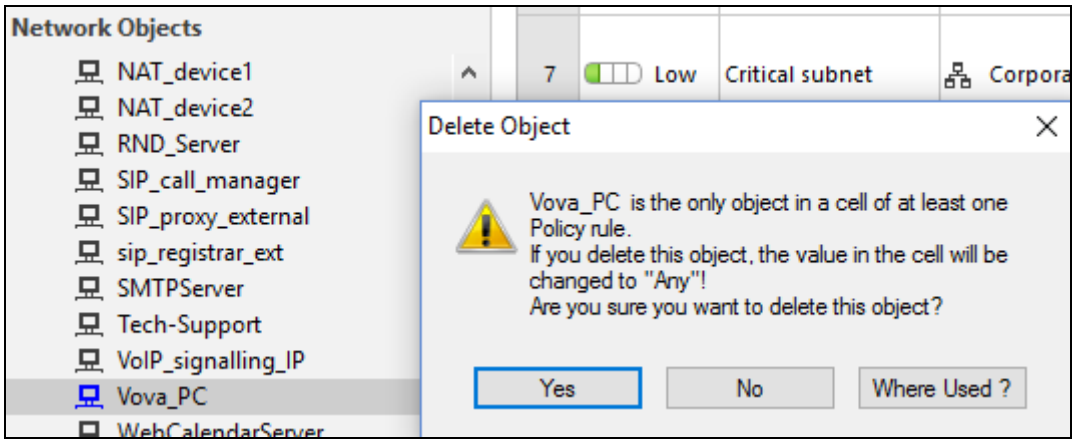
על מנת להמחיש את חשיבות העניין, אתן דוגמא מהחיים: יצא לי לטפל בלקוח שהתלונן על העובדה שכל העבודה של הארגון באינטרנט מאוד איטית ולא יציבה. אחרי כמה בדיקות נראה היה ש-Firewall שלו טוחן את הקו תמסורת של הארגון גם כאשר הרשת הפנימית מנותקת פיזית לגמרי.

אחרי חיטוטים בלוגים של ה-Firewall הסתבר שהוא נפרץ והפורצים הפכו אותו לשרת לינוקס לאחסון סרטים / תוכנות גנובות. מעבר לזה - הם השתמשו בו על מנת להריץ סורק / פורץ אוטומטי של שרתי SSH באינטרנט. מאחר וה-Firewall שומר ב-Management Log (מה שבעבר היה נקרא "Audit") שלו את כל הפעולות ניהול שבוצעו ,לא היה קשה לאתר מה קרה...

אז איך הפורצים הגיעו ל-Firewall? אחד מחוקי האבטחה שהיו בו היה החוק הבא:

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track
	Limit Access to Gateways Rule (Rule 1)							
1	Low		Vova_PC	Corporate-gw Management	Any Traffic	Any	accept	Log

כאשר Vova_PC (שם בדוי) - הוא מחשב פנימי ברשת מאחורי ה-Firewall. לאחר בירור, הסתבר שאחד ממנהלי רשת בארגון החליט "לעשות קצת ניקיון" והחליט לסדר את עץ האובייקטים. מסתבר שהוא מצא את האובייקט Vova_PC - אובייקט אשר היה שייך לאחד ממנהלי הרשת הקודמים וכבר לא עבד יותר בחברה. "יופי, צריך למחוק אותו" חשב המנהל וככה עשה. ה-Firewall-ים נתן לו אזהרה ברורה, אך הוא בחר להתעלם - ולחץ Yes. כך נראת האזהרה שהוא קיבל:



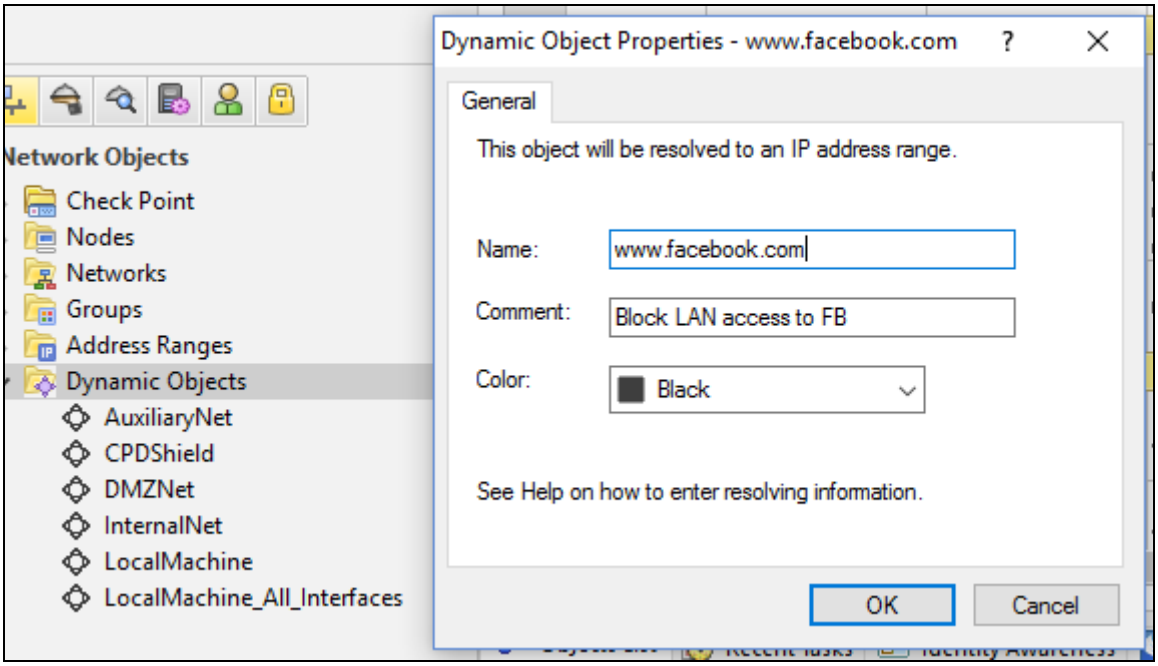
שהפך את כלל האבטחה הנ"ל ל:

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track
	Limit Access to Gateways Rule (Rule 1)							
1	Low		Any	Corporate-gw Management	Any Traffic	Any	accept	Log

או במילים אחרות - פתח גישת ניהול ל-Firewall מכל מקום בעולם. במקרה הזה - גם לא עזר שמשתמש ה-SSH עם הרשאות root היה בשם admin עם סיסמה מעולה qwe123... בפחות משעה פרצו ל-Firewall קבוצת האקרים מרומניה, העלו סקריפטי bash אוטומטיים והמשיכו משם. למזל הארגון הפורצים לא הבינו לאן הם הגיעו ולא המשיכו הלאה לרשת הפנימית, אלא פשוט ניצלו את הרכיב כשרת לינוקס להפצת Warez וסורק SSH של שרתים באינטרנט.

שימוש ב-Dynamic Object לחסימת גישה לאתרי Web

זאת גם שגיאה הרסנית ל-Firewall. חוזרת על עצמה לרב באותה סיטואציה - מנהל Firewall נדרש לחסום גישה למשאב כלשהו באינטרנט ואין לו כתובת IP קבועה (למשל: לחסום גישה ל-facebook.com או ל-youtube.com). המכשול הוא שה-Firewall של CheckPoint יודע לעשות זאת רק עם רכיב ייעודי שנקרא URL/Application filtering ודורש רישיון המתאים לכך. הרישיון כמובן עולה כסף נוסף, ומה לעשות אם אין רישיון? ממשיכים לחפש בפיירוול עד שמוצאים ב-SamartDashboard, קטגוריה שנקראת Dynamic Objects ויש באובייקטים האלה אפשרות להגדיר משאב לפי שם ולא לפי כתובת IP! נראה שזה בדיוק מה שצריכים, ועוד בחינם... בלי לחשוד מגדירים אובייקט כזה לפי דוגמה:



ומשתמשים בו בכללי אבטחה, כמו למשל פה:

מקנפגים, עושים התקנת Security Policy ו-... במקרה הגרוע אנחנו מאבדים גישה לפיירוול והארגון מאבד גישה לאינטרנט. במקרה הטוב - החיבוריות נהיה איטית להחריד עד לרמה שפשוט לא ניתן לעבוד...

אז מה בעצם קרה? עבור כל אובייקט כזה בכללי אבטחה, עבור **כל פאקטה** שיכולה להתאים לכלל הזה ה-Firewall הולך לאינטרנט ומתשאל שרתי DNS מה כתובת IP הנוכחית של אובייקט (במקרה הזה של www.facebook.com). אם יש מספיק תעבורה דרך ה-Firewall (וזה כמעט תמיד המצב) אנחנו מגיעים

לבעיה קריטית של איטיות, בגלל הבדיקה הנ"ל, ה-Firewall נכנס לעומס של 100% CPU והוא ייתקע או יקרוס. העניין שאתחול של ה-Firewall לא יעזור הרבה כי הוא יעלה בחזרה עם אותו כלל משבית...

אז מה הפתרון? אם ה-Firewall עדיין מגיב: להסיר את החוק שמשתמש באובייקט הדינמי. אך אם זה לא אפשרי ונאלצים לנתק את הרשת הפנימית אל מנת להוריד מהעומס, אין ברירה אלא להתחבר ל-Firewall עם כבל קונסול, ולהסיר את **מדיניות אבטחה כולה** עם פקודה **fw unloadlocal**, חשוב שתשימו לב: הפעולה הנ"ך תפתח גישת ניהול מכל מקום ברשת ואולי אף מחוצה לה!, לכן חשוב לעשות זאת רק לאחר ניתוק ה-Firewall מהאינטרנט ורק על מנת להסיר את הכלל הבעיתי ולהתקין את המדיניות מחדש.

ההמלצה שלי פה היא: **אל תשתמשו באובייקט דינמי**, בכלל. בכל השנים שלי עם CheckPoint אולי פעם או פעמיים נאלצתי להשתמש בהם, אז בקיצור - תשכחו שהוא קיים.

אי-בדיקת מקום פנוי בדיסק הקשיח לפני ביצוע פעולת Debugging

העניין הזה הוא אחד החביבים עליי: אם הגעתם למסכנה שחייבים להיכנס למצב Debug כדי להבין / לפתור בעיה כלשהי - דבר ראשון זה לבדוק האם אין בעיה של מקום פנוי בכונן של ה-Firewall. חוסר מקום בדיסק יכול לגרום לאין סוף תופעות מוזרות והזויות, לדוגמא:

- אי-היכולת להתקין מדיניות אבטחה
- אי-היכולת לטעון לוגים ב-SmartViewLog, או גרוע יותר - ניתן לטעון לוגים אך הם ריקים.
- לא ניתן להתחבר לשרת SmartCenter.
- לא ניתן לעדכן חוקי Application Control / AV / IPS
- ועוד ועוד...

מה שבעייתי בכל התקלות האלה הוא שלמרות שהן נובעות מחוסר מקום בדיסק זה שאף פעם לא נקבל עליהם הודעת שגיאה מתאימה. תמיד יש איזו שגיאה פנימית של CheckPoint עם מספר כלשהו ומלל שרק מטעה... במקרה הזה צריך לזכור שבסופו של דבר Firewall זה שרת לינוקס לכל דבר. כדי לבצע את התפקיד שלו הוא מוריד למשל קבצים מאתר של CheckPoint, אם זה קובץ tar הוא יאלץ לפתוח אותו בתיקיה זמנית. השרת כל הזמן פותח / מוחק / יוצר / מצפין / שולח ל-SmartCenter קבצים (ולא לשכוח בלינוקס כל דבר הוא קובץ - כולל sockets וכו'). כל פעולה כזו דורשת מקום פנוי בדיסק.

אז המלצה שלי פה - תבדקו מקום פנוי בדיסק בכל בעיה הזויה. תבדקו במיוחד את המחיצה "/" שמערכת הפעלה מותקנת בה. לפעולה תקינה מניסיוני מומלץ שיהיה שם לפחות 1GB - 0.5 פנוי.

כדי לבדוק נכנסים ב-expert mode דרך ssh ומריצים df -h:

```
smartcenterr77> expert
Enter expert password:

Warning! All configuration should be done through clish
You are in expert mode now.

[Expert@smartcenterr77:0]#
[Expert@smartcenterr77:0]# df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/vg_splat-lv_current
                      7.8G  4.6G  2.9G  62% /
/dev/hda1             289M   24M  251M   9% /boot
tmpfs                 980M     0  980M   0% /dev/shm
/dev/mapper/vg_splat-lv_log
                      3.0G  524M  2.3G  19% /var/log
[Expert@smartcenterr77:0]#
```

שימוש בסיסמאות ניהול קלות לפריצה

דבר כל כך בסיסי שבטח תשאלו - סיסמאות קלות? ועוד של Firewall? לא הגיוני שמישהו יעשה זאת... עם זאת, תתפלאו לדעת עד כמה הרבה זה קורה בשטח... בדרך כלל זה מתחיל באינטגרטור המתקין Firewall חדש / משדרג אחד הקיים ושתמיד בלחץ של עוד 3 התקנות באותו יום. וכנראה שמפני שצריך להשתמש בסיסמת ניהול גם של SSH וגם של SmartDashboard כמה וכמה פעמים בהתקנה וקנפוג ראשוני - רבים מאותם מתקינים מקלים על עצמם ובוחרים סיסמאות כגון 1q2w3e \ 123456 \ qwe123 וכו' כדי לחסוך זמן בהקלדה ואומרים לעצמם - "אין בעיה, אחרי שנסיים, אשנה את כל הסיסמאות לקשות יותר", וכמובן שוכחים לעשות זאת...

ראיתי Firewall-ים שהתקינו אותם עוד בגרסה R55 עם סיסמא קלה, ו-10 שנים לאחר מכן - שדרגו אותן מבלי לשנות סיסמא כי פחדו לאבד גישה או לגעת במשהו שעובד שנים. אז המלצה שלי פה:

- לשנות בהתקנה (CheckPoint אגב, מציעה את האופציה הזאת בתפריט ההתקנה) את שם משתמש הניהול admin למשהו אחר - אל תפחדו, לא יקרה שום דבר.
- אם המשתמש כבר קיים וחוששים למחוק אותו - תשנו סיסמא שלו למשהו מסורבל וארוך, תשמרו את הסיסמא במקום שבו אתם שומרים את הסיסמאות ואל תשתמשו ב-admin אף פעם. פשוט תצרו משתמשים נוספים לכל מנהל Firewall - אם יש לכם כמה כאלה.

לשכוח לבטל האצה בפיירוול כשמבצעים Debugging

זאת שגיאה שכיחה שקרתה גם לי לא פעם ואפילו לתמיכה של CheckPoint. כשנמצאים תחת לחץ של תקלה לא פלא ששוכחים פרטים קטנים כאלה... בעבר זה לא היה כל כך חשוב, אך היום 99% מה-Firewall-ים (גם שרתי UTM וגם Open Servers) מגיעים עם יכולת האצת חומרה, מה שנקרא "SecureXL" בתיעוד של CheckPoint. התכונה זאת מורה לרכיב להרים ל-CPU רק את החבילה הראשונה של כל Connection, ואז אם נעשה "fw monitor" נראה רק את החבילה הראשונה של החיבור (במקרה של TCP SYN) ולא נראה את ההמשך.

דבר ראשון - בימינו, כאשר עושים בכניסה ל-Firewall הקלטה עם סניפר לטובת Debugging זה לבדוק אם מופעל SecureXL ואם כן - לבטל אותו זמנית ולהחזיר אחר כך. תשימו לב: יש שתי דרכים לבטל את האופציה הנ"ל. הראשונה היא דרך תפריט ה-cpconfig - אל תעשו זאת, מפני שהיא תבטל את ההאצה באופן קבוע (פעולה שגם דורשת אתחול של ה-Firewall).

האופציה השניה היא בעזרת פקודות ב-SSH:

- ראשית - לבדוק האם אופציה זו מופעלת בכלל:

```
fwaccel stat
```

- לאחר מכן, מבטלים:

```
fwaccel off
```

- אחרי סיום ה-Debugging, מפעילים בחזרה:

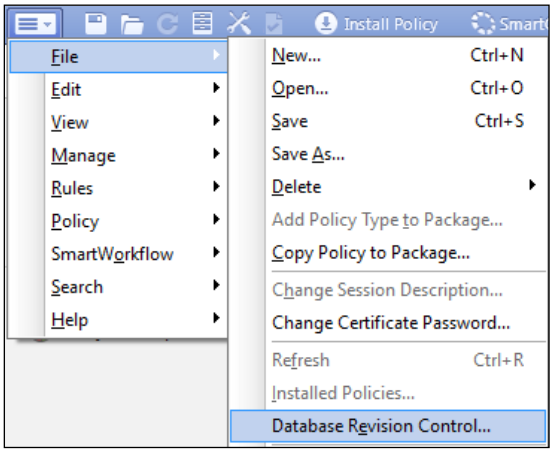
```
fwaccel on
```

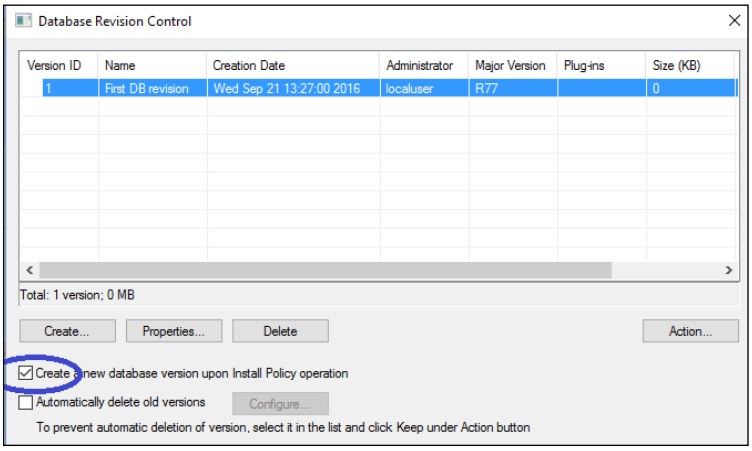
ביטול האצה כמובן יעביר את כל התקשורת ל-CPU ובך יעמיס את הפיירוול, אז תבדקו קודם שה-Firewall לא עמוס מדי לפני כן ויעמוד בהגדלת העומס או לחילופין - להפחית קודם לכן את העומס עליו.

אי-שימוש ב"ביטוח" נגד טעויות קינפוג - Database Revision Control

CheckPoint מאז ומתמיד הציעה אפשרות לשמור כגיבוי את הקונפיגורציה הנוכחית, השמירה כוללת את האובייקטים והכללים לפני התקנת מדיניות אבטחה. להפתעתי אולי רק ב-10%-15% מכלל ה-Firewall-ים שראיתי מפעילים את התכונה הזאת - וחבל. האופציה הזאת תוכל להציל את המצב אם נמחק אובייקט או חוק מורכב בטעות. עושים שינוי כלשהו שגרם לבעיות ברשת ולא בטוחים איזה שינוי בדיוק? ביצעתם מספר שינויים במקביל כאשר ה-Firewall מנוהל בו-זמנית ע"י כמה מנהלים ולא בטוחים מה בדיוק נהרס? תהליך שחזור גרסת מדיניות אבטחה דורש כמה קליקים בודדים...

הטענה היחידה הגיונית נגד גיבוי כזה היא שאם הוא מופעל להתבצע אוטומטית אז בכל התקנת מדיניות אבטחה, נוצר קובץ חדש שתופס מקום בדיסק של ה-Firewall (ב-SmartCenter ליתר דיוק), אבל גם פה אפשר לשים V על "Automatically delete old versions" וזה ימנע בזבוז מקום. אז המלצה שלי, גם לא למנהלים מתחילים - להפעיל Database Revision Control. עושים זאת כך:



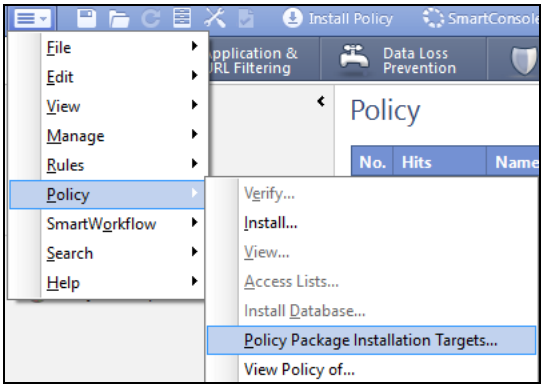


כשתרצו לשחזר קונפיגורציה - פשוט תבחרו את הגרסה מהתאריך הנדרש ותלחצו על כפתור: Action > Restore Version.

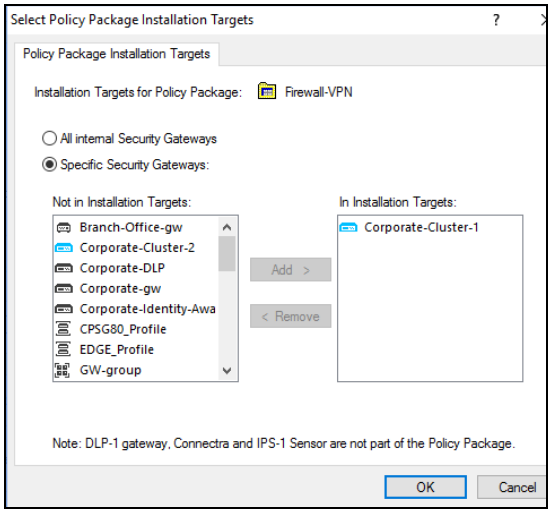
התקנת מדיניות אבטחה על Firewall הלא נכון

תקלה זו יכולה לקרות כאשר ה-SmartCenter מנהל כמה Firewall-ים במקביל או בשרת ניהול עם כמה חבילות מדיניות אבטחה עבור ה-Firewall-ים השונים שהוא מנהל. ה-SmartDashboard נפתח על מדיונית שהמשתמש הקודם סגר. לעיתים קרובות (במיוחד כשיש לחץ) קורה שפותחים SmartDashboard, מקנפגים כלל בלי לשים לב שעבדנו על מדיניות של Firewall אחר לגמרי...

CheckPoint לא מאמתת איזו מדיניות מתקינים לאיזה Firewall. ולכן, כאשר מתקינים מדיניות שמשתמשת באובייקטים וכללים לא רלוונטיים ל-Firewall, ברב רובם של המקרים הדבר יגרום להשבתה שלו ותפגע בכל התעבורה שעוברת דרכו. עם זאת - לא קשה להתאושש מתקלה שכזו - פשוט לבצע התקנה נוספת, אך הפעם עם המדיניות הנכונה. עם זאת, תמיד עדיף להמנע מבעיות מאשר לפתור אותן... CheckPoint מאפשרת לנו לקבוע מראש איזו מדיניות תותקן באיזה פיירוול. עושים את זה ככה:



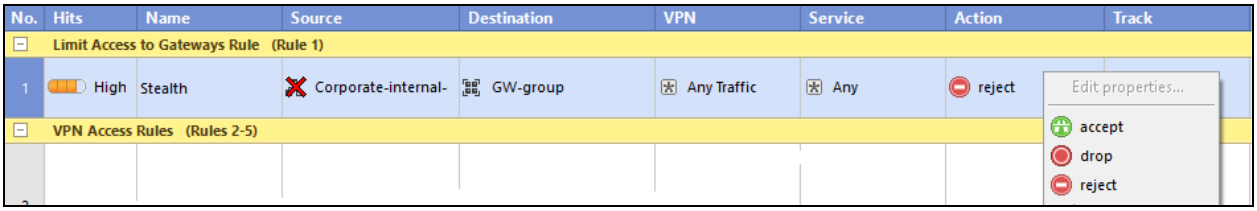
ולאחר מכן בוחרים לאיזה Firewall המדיניות הנוכחית הפתוחה ב-SmartDashboard תותקן:



כאן מדיניות שפתוחה כרגע וחלק מחבילה Firewall-VPN תותקן רק בפיירוול Corporate-Cluster-1 בעתיד בלי שתעשו בשביל זה משהו.

הפעלת כללי אבטחה עם פעולת Reject במקום Drop

קורה כשלא מבינים מהו הבדל ולכן קל להתבלבל. הדבר פשוט מאוד: Reject לא רק חוסם ניסיון תקשורת אלא גם שולח ליוזם התקשורת תגובה על כך (לדוגמה TCP RST), אופציה זו סתם מעמיסה על Firewall וגם נותנת אינדיקציה למישהו שמבצע סריקה מבחוץ שהוא אכן נחסם ע"י פיירוול.
היום אני לא מכיר שום סיבה להשתמש ב-Reject הזה...



אתחול ה-Firewall כולו כאשר צריכים לאתחל רק את ה-SmartCenter בלבד

לעיתים קרובות מנהלי רשת לא שמים לב לכך שרכיב ה-Firewall עצמו ורכיב ניהול ה-Firewall (ה-SmartCenter) הם שתי תוכנות / מערכות נפרדות, אפילו כשהן מותקנות על אותו שרת פיזי.

כשנתקלים בבעיית SmartCenter כלשהי שמחייבת אתחול (במחשבים אין כמו אתחול טוב ☺) - עושים אתחול לכל השרת, העניין אולי פותר את בעיית ה-SmartCenter אבל גם מאתחל Firewall ומשבית את כל התעבורה שעוברת דרכו... אין שום צורך בכך - תשתמשו בפקודות האלה כדי לאתחל את רכיב הניהול בלבד, מבלי לפגוע בתפקוד Firewall עצמו:

- סגירת ה-SmartCenter:

```
cpwd_admin stop -name FWM -path "$FWDIR/bin/fw" -command " fw kill fwm"
```

- הפעלתו מחדש:

```
cpwd_admin start -name FWM -path "$FWDIR/bin/fwm" -command "fwm"
```

אי-שימוש ב-NTP כמקור לשעון פיירוול

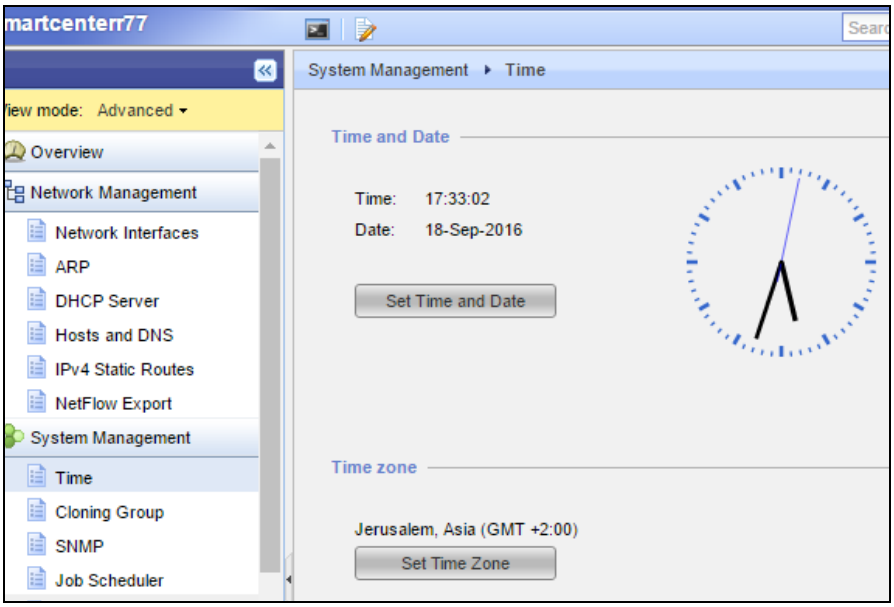
לא פעם הייתי חלק מהליך Debugging ארוך ומייגע שנבע מכך שהדברים ב-Log נראו לא הגיוניים, כל זה כדי שבסוף נבין ששעון ה-Firewall לא היה בכלל מכוון. ה-Firewall של CheckPoint יוצר לא מעט לוגים: לוגי אבטחה, לוגים של כל הרכיב הפנימיים שלו (Check Point daemons logs שסיומת שלהם elg.) והם מאוד עוזרים בעת פתרון בעיות. הלוגים שמגיעים ל-SmartCenter חתומים עם תאריך ושעה של מודול ה-Firewall שבו הם נוצרו, ואם השעון ה-Firewall לא מכוון זה פוגע באמינות הלוגים וגורם להם להטעות במקום לעזור.

מניסיון שלי - לא משנה איזה שרת, כולל השרתים היקרים והמתקדמים ביותר - השעון שלהם סוטה עם הזמן. ועם זה לא מספיק - הסטייה לא מתקיימת בצורה לינארית - מה שאומר שעם הזמן הסטייה גדלה בערך שאינו קבוע.

התוצאה מכך היא שאם אני מסתכל על לוגים של היום ורואה ששעון סוטה 10 דקות - אין לי דרך לדעת מה הייתה סטייה של שעון לפני חודש ועד כמה זמני הלוגים לא מדויקים... יש מקרים שבגלל הבעיה הזאת הלוגים פשוט לא שווים כלום.

איך מתקנים את זה? פשוט מאוד - מחברים את ה-Firewall לשרת NTP אמין (אפילו לכמה: יש תמיכה באחד ראשי ואחד משני).

אפשר לעשות את זה דרך Gaia:



או כמובן דרך ה-CLI:

```
smartcenterr77> set ntp server primary 13.13.13.1 version 2
smartcenterr77> set ntp server secondary 23.23.23.1 version 2
smartcenterr77> save config
```

אי-אימות גיבויים

העניין רלוונטי לא רק בעולם ה-Firewalling כמובן, אך עם ה-Firewall העניין קריטי במיוחד. CheckPoint מציע כמה דרכים לגבות את הקונפיגורציה של ה-Firewall: דרך Gaia, דרך CLI, לעשות זאת באופן יזום חד פעמי או באופן מתוזמן אוטומטית, הכי חשוב כמובן זה לגבות את ה-SmartCenter שמכיל את כל האובייקטים, הכללים, מסדי נתונים של ה-Firewall וכו', לגבות את המודול של ה-Firewall (ב- Distributed Installation) זה גם עניין מומלץ אך פחות קריטי מפני שהוא כולל רק את כתובות ה-IP של הממשקים.

במקרים רבים ה-SmartCenter מותקן על VmWare או תשתית וירטואליזציה מקבילה, ואז עניין הגיבוי הוא לא בעיה - פשוט לדאוג ל-Snapshots. אך, אם מבצעים את הגיבוי עם כלים של CheckPoint - אז חובה מדי פעם לנסות לשחזר Firewall מגיבוי שכזה. שוב, אני מדבר מניסיון - פנה אלינו לקוח ששרת ה-SmartCenter שלו לא עולה - שגיאה הקשורה לדיסק הקשיח. למזלו של הלקוח הוא הריץ באופן קבוע גיבוי אוטומטי מתוזמן - פעם בשבוע, אחרי סיום גיבוי ה-CheckPoint היה מעביר קובץ גיבוי לשרת ברשת דרך FTP. אגב מדובר במשרד ממשלתי מאוד גדול שלא היה חסר להם משאבים, וה-Firewall היה קריטי לעבודתו התקינה של ארגון.

הלקוח עם אינטגרטור שלו הביאו שרת חדש מאותו סוג, התקינו CheckPoint גולמי וניסו לשחזר את ה-SmartCenter מקובץ גיבוי. הם הריצו Upgrade Import וקיבלו שגיאה - הקובץ גיבוי אינו תקין, הריצו שחזור נוסף, הפעם עם קובץ גיבוי קצת ישן יותר - ושוב, אותה שגיאה. הם עברו על לפחות 20 קבצי גיבוי שהיו להם - אותו דבר, כל קבצי גיבוי יצאו פגומים! בסוף הם נאלצו להביא מישהו חיצוני ששחזר להם את הנתונים של ה-SmartCenter ישר מהדיסק הקשיח עצמו וככה ניצלו.

אז המלצה שלי - אם מריצים גיבוי בכלים של CheckPoint או עם סקריפטים משלכם, חייבים לאמת תקינותם. איך? פשוט מאוד - ע"י ביצוע שחזור.

חשוב שתבינו דבר אחד לגבי הליך הגיבוי: לא מדובר פה ב"קסם" של CheckPoint. בסופו של דבר, מה שהוא עושה זה להריץ מספר סקריפטים / תוכנות שאוספות קבצים, מאגדות אותם, מכווצת אותם לארכיון ובעזרת קליינט (למשל של FTP) מעלים לשרת שהוגדר. יש הרבה דברים שיכולים להסתבך בתהליך הזה, לדוגמא:

- לא היה מקום פנוי במחיצה המחזיקה את temp ותהלך ה-tar נכשל, מה שגרם לכך שחלק מהקבצים לא גובו.
- יכול להיות שרת ה-FTP בעיתי ופגע בשלמות הקבצים המועברים אליו.
- ועוד שלל סיבות נוספות.

סיכום

אם אתם מנהלי רשת, או חלק מצוות ה-IT ובמסגרת תפקידכם אתם מנהלים רכיב Firewall (לאו דווקא של חברת CheckPoint) אני בטוח שנתקלתם בלפחות חלק מהבעיות שהצגתי במהלך המאמר, או בבעיות דומות בעת תפעול ותחזוק ה-Firewall. חשוב מאוד להבין שמדובר בשרת לכל דבר. אם צריך אסכם בקצרה את הנקודות החשובות במאמר:

- אל תמחקו אובייקט אשר נמצא בשימוש באחד החוקים, ובכלליות - תקראו טוב טוב את השגיאות שאתם מקבלים.
- אל תשתמשו ב-Dynamic Object, ובכלליות - אל תשתמשו בפיצ'רים אם אתם לא בטוחים לחלוטין מה ההשפעה שלהם.
- חוסר במקום פנוי יכול להוביל לשלל בעיות הזויות, בכל פעם שמשהו נראה לא הגיוני - בדקו כמה מקום פנוי, ובכלליות - תדאגו תמיד שיהיה לכם לפחות 0.5 GB פנוי.
- תשתמשו בסיסמאות חזקות מאוד. אל תתעצלו. זה יכול להגמר באסון.
- בטלו את פונקציית ההאצה לפני ביצוע כל פעות Debugging הקשורה לרשת.
- בצעו גיבוי לקונפיגורציה של ה-Firewall באופן אוטומטי ופעם בכמה זמן - בדקו שאכן ניתן לבצע שחזור ממנה.
- הפעילו שרת NTP, יחסוך לכם כאב ראש לא קטן במידה ותכנסו ל-Debugg Session.

וזהו, תודה שקראתם את המאמר, אני מקווה מאוד שהפקתם תועלת ממנו. אשמח לתגובות / הערות / שאלות בקשר למאמר:

yuri@yurisk.info

יורי סלובודיאניוק,

FCNSP ,CCSE+ ,CCNP Security

LINKEDIN | BLOG