מסמך הגנה

CISCO

מתגים ונתבים

תאריך: מאי 2018

משרד ראש הממשלה
מערך הסייבר הלאומי

תוכן העניינים

תוכן העניינים 2
מבוא 3
מטרת המסמך 3
קהל היעד 3
הנחיות כלליות לשימוש במסמך 3
רקע 4
פעולות טרם יישום הקשחה ברכיב 6
רשימת המלצות הגנה למתגים ונתבים תוצרת Cisco 6
Management Plane 6
Secure Shell- SSH 6
CDP - Cisco Discovery Protocol 8
LLDP - Link Layer Discovery Protocol 8
DHCP snooping 8
Control Plane 10
DTP - Dynamic Trunk Protocol 10
VTP - Vlan Trunking Protocol 11
Data Plane 12
Native vlan 12
Port Security 13
Secure Mac Address 14
802.1x 15

מבוא

מטרת המסמך

חוברת זו נועדה לתת רקע והמלצות עיקריות לעבודה מאובטחת עם מתגים ונתבים של חברת Cisco, במטרה למנוע פגיעה בציוד התקשורת בארגון, ו/או ניצול של ציוד התקשורת לתקיפה של הרשת הארגונית והמידע העובר על גביה.

קהל היעד

החוברת נועדה לשימושם של אנשי אבטחת מידע בעלי ניסיון בציוד תקשורת רלוונטי של חברת Cisco, וכן לאנשי תשתיות תקשורת בעלי רקע באבטחת מידע.

הנחיות כלליות לשימוש במסמך

מומלץ להקפיד ולבחון כל שינוי והגדרה בסביבת בדיקות טרם הטמעה בסביבת הייצור.

יש לקרוא את המסמך בשלמותו טרם ביצוע שינויים. השמטת שלבים עלולה להוביל לתשתית תקשורת לא יציבה.

מומלץ לבצע גיבוי מלא לרכיב ולייצא את קובץ הגיבוי מהרכיב לאחסון חיצוני, טרם יישום ההמלצות. במידה שקיימת סביבת בדיקות, מומלץ לבדוק את תקינות הגיבוי טרם ביצוע שינויים כלשהם.

יש להקפיד ולבחון באתר היצרן את תאימות הרכיב הספציפי אותו רוצים לאבטח לגרסאות מערכות הפעלה עדכניות יותר. במידת האפשר מומלץ לשדרג מערכת ההפעלה ברכיב לגרסה המתקדמת ביותר הנתמכת על ידו.

במידת האפשר, מומלץ לבצע שדרוג רכיבי זיכרון (הגדלת נפח הזיכרון למקסימום האפשרי) עבור נתבים ומתגים ישנים, לשם הטמעת גרסה עדכנית של מערכת ההפעלה.

רקע

חברת Cisco הינה אחת מיצרניות ציוד התקשורת הגדולות בעולם, מוצריה פרושים בארגונים וחברות בכל רחבי העולם.

מגוון המוצרים, הן חומרה והן תוכנה שמציעה החברה, כמו גם הפופולריות שלהם בקרב ארגונים וחברות מכל המגזרים, הופכים את מוצרי החברה ליעד מועדף לתקיפות סייבר. השגת שליטה בציוד התקשורת של הארגון מאפשרת לתוקף וקטור תקיפה מצוין הן כלפי תעבורת התקשורת בארגון, לדוגמה MITM (Man In The Middle), הקלטת תעבורה וכד', והן כלפי שרתים ומערכות נוספות.

אחיזה כזו של תוקף בציוד תקשורת, קשה יותר לגילוי מתקיפה רגילה על מערכות קצה ושרתים, משום שציוד תקשורת אינו מאפשר הפעלת מערכות הגנה וזיהוי רגילות כגון AV, HOST BASED IDS או EDR.

חברת Cisco מפיצה עדכוני אבטחה למוצריה בתדירות גבוהה, ומפעילה צוות מחקר אבטחת מידע גדול ומקצועי. ב- 2014 עמדה החברה במרכזה של סערה תקשורתית כאשר הדלפה של אדוארד סנודן חשפה את יכולות ההאזנה והתקיפה של ה- NSA, שהושגו בחלקן תוך ניצול 'דלתות אחוריות' שהוטמעו במוצרי החברה.

ב- 2016 הדליפה קבוצת "ShadowBrokers" מספר כלים, שפעלו תוך ניצול חולשות Zero Days במספר מוצרי תקשורת ומערכות הגנה של החברה.

לציוד התקשורת של Cisco מספר מערכות הפעלה ייעודיות (IOS, IOS XE, IOS XR, NX-OS), כאשר הנפוצה והמוכרת ביותר מתוכן היא IOS. מערכת ההפעלה IOS XE הינה פלטפורמה מודרנית המבוססת על מערכת הפעלה לינוקס, מערכת IOS XR מיועדת לשימוש אצל ספקיות של תשתיות תקשורת (Service Providers), ומערכת NX-OS מיועדת לשימוש הכולל שינויים רבים הניתנים לתכנות באמצעות ממשקי API, ב- DATA CENTERS מבוססי תשתית וירטואלית.

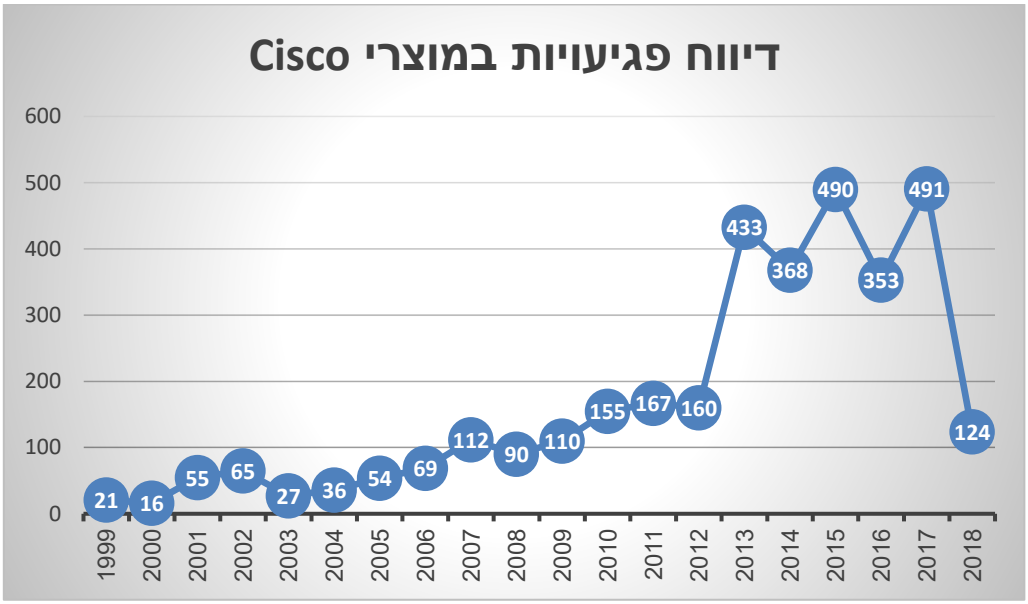
חשוב שארגונים המפעילים ציוד תקשורת מכל סוג שהוא, יעקבו אחר עדכוני האבטחה אשר מופצים ללקוחות. חלקם מיועדים לטיפול בפגיעויות קריטיות במערכת ההפעלה. כאשר מופץ עדכון מסוג זה מומלץ לבוחנו בסביבת בדיקות, ולאחר מכן להתקינו ברשת הייצור בהקדם האפשרי.

לדוגמה, בפברואר 2017 דיווחה היצרנית על תכונה בציוד תקשורת מתוצרתה אשר עלולה להיות מנוצלת לרעה. התכונה, הנקראת פרוטוקול Smart Install (SMI), מאפשרת הגדרה מרחוק של הציוד ללא הליך הזדהות. גורמים זדוניים עלולים לעשות שימוש בתכונה זו לצורך השגת גישה וביצוע שינויים בהגדרות הציוד. היצרנית מקפידה בדרך כלל להתייחס לכל דיווח על פגיעות במערכותיה, ולהוציא עדכון אבטחה רלוונטי במידה ונדרש, או להנחות את לקוחותיה לסגירת פער האבטחה באמצעות המלצות טכניות (Workarounds).

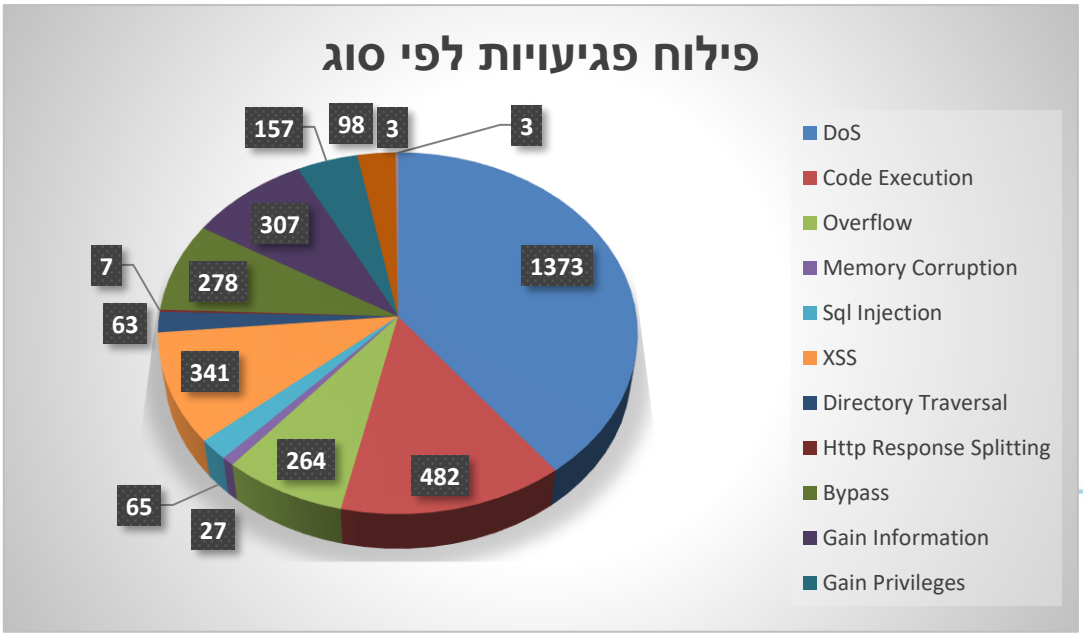
התרשים הבא מתייחס לכלל הפגיעויות שפורסמו לגבי מוצרי החברה.[1] ניתן לראות עלייה מתמדת בכמות הפגיעויות, כאשר ישנה קפיצה משמעותית החל משנת 2012. יש לציין כי לחברה כאלפיים

[1] הנתונים מעודכנים למאי 2018.

מוצרים שונים, אך כרבע מהפגיעויות מתייחסות ל- IOS.



התרשים הבא מציג פילוח לקטגוריות של הפגיעויות השונות אשר דווחו במהלך השנים. ניתן לראות כי כ-1400 פגיעויות בעלות יכולת למניעת שירות וכ-480 פגיעויות המאפשרות הרצת קוד.



פעולות טרם יישום הקשחה ברכיב

טרם יישום ההמלצות:

- מומלץ לבדוק בלוג של הרכיב אם קיימות שגיאות זיכרון וכד'.
- מומלץ לבצע בדיקת תקינות לקובץ הגיבוי האחרון בסביבת הבדיקות.
- מומלץ לבצע בדיקת תקינות ושיחזור IOS בסביבת הבדיקות.

רשימת המלצות הגנה למתגים ונתבים תוצרת Cisco

נחלק את הטיפול בציוד התקשורת לשלושה מישורים שונים.

Management Plane

עוסק במישור ממשקי הניהול של הציוד עצמו, כגון ממשקי SSH, SNMP, הגדרת סיסמאות וכד'.

Secure Shell - SSH

SSH הינו פרוטוקול המאפשר השתלטות על התקן מרוחק וביצוע פעולות לאחר תהליך של הזדהות. פרוטוקול זה מאפשר תקשורת מאובטחת ומוצפנת בין שני התקנים/מחשבים. SSH פועל מעל TCP והפורט הסטנדרטי הינו 22.

ישנם 4 שלבים שיש לבצע על מנת לאפשר SSH על מתג או נתב של סיסקו:

1. יש להגדיר תחילה שם לרכיב

```
(config)# hostname <name>
```

הגדרת תחום DNS

```
(config)# ip domain name <name>
```

2. יצירת מפתחות עבור SSH

```
(config)# crypto key generate rsa usage-keys modulus <size>
(config)# ip ssh time-out 60
(config)# ip ssh authentication-retries 3
(config)# ip ssh version 2
```

הקשחת התחברות עבור SSH

(config)# line vty **0 4**

transport input ssh

3. יש לבטל על המתג או הנתב את אפשרות הגישה ב-http

(config)# no ip http server

4. חשוב להצפין את כל הסיסמאות שהוגדרו ב- running config. מבצעים זאת באמצעות הפקודה

(config)# service password-encryption

נתבים - בעת הגדרת HSRP/VRRP, יש להגדיר מפתחות הזדהות עבור קבוצת הנתבים על מנת שגורם עוין לא ינסה להציג את עצמו כאחד הנתבים בקבוצה

(config)# interface type number

(config)# ip address ip-address mask (secondary)

(config)# standby (group-number) priority priority

(config)# standby (group-number) preempt (delay {minimum | reload | sync} seconds)

(config)**#** standby (group-number) authentication md**5** key-chain key-chain-name

(config)**#** standby (group-number) ip (ip-address (secondary))

CDP - Cisco Discovery Protocol

CDP הוא פרוטוקול קנייני של Cisco. הפרוטוקול פועל ב- L2 (רמת הרשת המקומית) ומשמש לאיסוף מידע על ציוד cisco המקושר זה לזה. הפרוטוקול אוסף מידע כגון שם הציוד, סוג הציוד, פלטפורמה, native vlan, גרסה, כתובת IP ועוד. המידע נשמר בטבלה ייעודית שניתן לראות באמצעות הפקודה #show cdp neighbors

הודעות CDP נשלחות כל 60 שניות לכתובת multicast אליה מאזינים כל רכיבי התקשורת. פרוטוקול זה פועל כברירת מחדל על ציוד תקשורת של Cisco.

סכנות

תוקף בעל גישה לרשת יכול לנצל מידע זה, העובר בגלוי, לניתוח מבנה הרשת, סוג הציוד המותקן בה, ופגיעויות אפשריות, ובכך להשיג ידע שינוצל לתקיפת הרשת.

בנוסף תוקף יכול לבצע מתקפת CDP Spoofing. במתקפה זו התוקף שולח לכתובת ה- multicast המשותפת לרכיבים ברשת, אלפי הודעות CDP בשניה ובכך ממש מתקפת מניעת שירות נגד הציוד.

ההמלצה היא לבטל גלובלית את הפרוטוקול על ציוד Cisco .

הפקודה בה נשתמש :

```
(Config)# no cdp run
```

LLDP - Link Layer Discovery Protocol

פרוטוקול זיהוי ואיסוף מידע, בדומה ל-CDP. פרוטוקול זה אינו שייך ל-cisco ומשתמשים בו גם שאר היצרנים.

הפרוטוקול בעייתי לשימוש מאותן סיבות המצוינות לעיל לגבי פרוטוקול CDP, ולכן מומלץ לנטרלו.

הפקודה בה נשתמש:

```
(config)# no lldp run
```

DHCP snooping

פרוטוקול dynamic host configuration protocol - DHCP הינו פרוטוקול שימושי מאוד המקצה באופן אוטומטי כתובות IP למחשבים ברשת מקומית. שרת DHCP ייתן לתחנה הפונה אליו, בנוסף לכתובת ה- IP, נתונים כמו Network Mask, Default Gateway ועוד, כך שהמחשב יוכל לתקשר ברשת.

נציג 2 התקפות DHCP שכיחות:

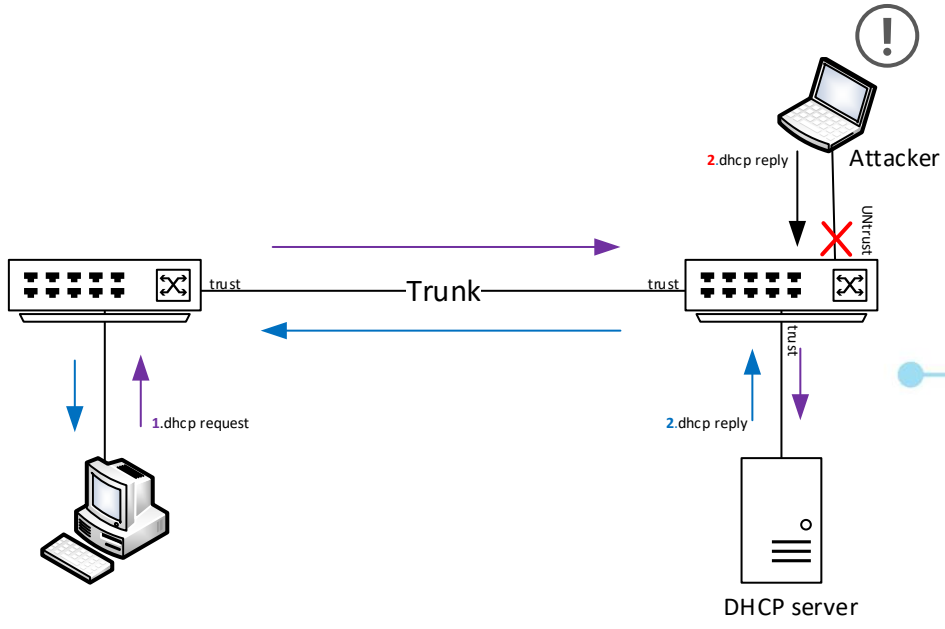
- DHCP starving - בתקיפה מסוג זה התוקף מייצר כמות בקשות גדולה להקצאת כתובות משרת ה- DHCP. התקיפה גורמת לניצול מהיר של מאגר הכתובות הזמינות, ואי-יכולת להקצות כתובות IP לפונים לגיטימיים, כלומר - מתקפת מניעת שירות.

אחד הפתרונות למתקפה זו הוא port security עליו יוסבר בהמשך.

- DHCP Snooping - בתקיפה מסוג זה התוקף מגדיר שרת DHCP משלו כדי שמשתמשים לגיטימיים יפנו אליו, במטרה לקבל מהם את נתוני התחנה לצורך תקיפת המשך.

על מנת שנוכל להגן על הרשת והמשתמשים מפני מתקפת DHCP snooping, אנו נגדיר מאילו פורטים אנחנו יכולים לקבל תשובות משרת ה- DHCP לגבי נתוני הרשת של התחנה, פורטים אלו יוגדרו כ-Trust.

בדרך כלל כל הפורטים לכיוון תחנות הקצה יוגדרו כ- Untrust כך שלא יוכלו להתקבל מהם תשובות DHCP, ופורטים לכיוון שרת ה-DHCP הארגוני יוגדרו כ-Trust על מנת לאפשר מעבר תקין של תשובות ה-DHCP.



1. נאפשר את השימוש במנגנון ההגנה מפני dhcp snooping באופן גלובלי על המתג.
2. נגדיר על אילו vlans יפעל dhcp snooping , אותם vlans עליהם אנו רוצים להגן. נגדיר את ה-vlans שהתחנות המשויכות אליהן מוגדרות לקבל כתובת משרת ה-DHCP. ברירת המחדל היא שdhcp snooping- לא פועל על אף vlan.
3. נוודא כי שרת ה-dhcp האמיתי מחובר לפורט במצב trust.

(config)# ip dhcp snooping

(config)# ip dhcp snooping vlan vlan-list

(config)# interface Ethernet slot/port

ip dhcp snooping trust

Control Plane

מישור אבטחה זה עוסק באבטחת הקישורים והפרוטוקולים השונים המשמשים לקבלת החלטות ניתוב והפצה של מידע ברשת, בעיקר פרוטוקולי ניתוב שונים המתקשרים בין רכיבי ציוד התקשורת עצמם.

DTP - Dynamic Trunk Protocol

פרוטוקול DTP הוא פרוטוקול שפותח ע"י סיסקו ורכיבי סיסקו משתמשים בו כברירת מחדל. פרוטוקול זה מאפשר הקמת קישור trunk בין מתגים באופן אוטומטי באמצעות ניהול משא ומתן. בפרוטוקול זה נשלחות הודעות DTP בין הצדדים, ומתקבלת החלטה האם יוקם קישור trunk או לא.

נציין כי קישור trunk הינו קישור המאפשר מעבר חבילות מידע (פאקטות) המתויגות כשייכות ל-vlans שונים.

קיימים מספר מצבים שפורט במתג יכול להיות משויך אליהם:

- Access- במצב זה לא נשלחות הודעות DTP.
- Trunk- במצב זה אנו מכריחים את הפורט לאפשר קישור Trunk.
- Dynamic auto - במצב זה הפורט יחליף את מצבו כך שאם חובר מחשב הפורט יהפוך ל-Access ואם חובר מתג הפורט יהפוך ל-Trunk, אך לא ינסה מעצמו להפוך ל-trunk. במצב זה לא נשלחות הודעות DTP אלא מתבצעת רק הקשבה לפניות של הצד השני בקישור.
- Dynamic desirable- הפורטים מוגדרים במצב זה כברירת מחדל. במצב זה אנו

גורמים לפורט להיות במצב Trunk ובנוסף הוא שולח הודעות DTP באופן יזום על מנת להקים קישור Trunk עם הצד השני.

- Non negotiate - ברגע שעולה קישור trunk פקודה זו מפסיקה את שליחת הודעות ה-DTP.

הסכנות הטמונות בהגדרת DTP

פרוטוקול DTP עלול לאפשר מתקפת VLAN hopping. הפורטים במתג משויכים כברירת מחדל למצב Dynamic desirable. המשמעות היא שהפורטים ינסו להקים קישור Trunk עם הרכיב שיחובר בצד השני. תוקף עלול להתחבר לרשת ולבצע משא ומתן עם הפורט עד להקמת קישור Trunk, דבר שיאפשר לו קבלת תעבורה מכל ה- VLANS המוגרים תחת TRUNK זה.

איך מתמודדים

יש להגדיר כל פורט במתג ידנית ולא להשאירם תחת הגדרות יצרן.

על מנת לא לאפשר משא ומתן ליצירת קישור Trunk יש להגדיר את כל הפורטים כ- Access ולבטל את פרוטוקול ה- DTP.

הפקודות הן:

```
switch(config) #    interface X/Y
switch(config-if) # switchport mode access
switch(config-if) # switchport nonegoatiate
```

VTP - Vlan Trunking Protocol

פרוטוקול VTP מבצע רפליקציה (שכפול) של vlans בין מתגים בתחום מסוים. ברשתות תקשורת גדולות בהן קיימים מספר רב של מתגים, הפרוטוקול מקצר את זמני התגובה בעת הוספת VLAN חדש לרשת או לחלופין בעת הוספת מתג חדש.

מתגים מגיעים עם vlan ברירת מחדל שה-ID שלו הוא 1, ועם revision number שווה ל-0.

בעת הגדרת vlan חדש ה-revision number עולה ב- 1.

כאשר מגדירים VTP המתג יכול להימצא באחד משלושת המצבים הבאים:

- Server - בכל רשת צריך להימצא מתג אחד שהוא Server, בדרך כלל יהיו אלו מתגי ה-Distribution.
- במצב זה ניתן להוסיף או למחוק vlans במתג. לאחר מכן יישלח עדכון לשאר המתגים

באותו התחום.

- Client- במצב זה לא ניתן להוסיף או למחוק vlans במתג. ה- Client יכול רק לקבל עדכון מה-Server.
- Transparent - משתמשים במצב זה כאשר לא רוצים להשתמש בפרוטוקול ה-VTP. במצב זה ניתן להוסיף או למחוק Vlan-ים. עדכוני VTP המתקבלים במתג זה לא חלים עליו אלא רק מועברים הלאה ברשת.

על מנת למנוע מצב בו תוקף הנגיש לרשת הפנימית מפעיל רכיב מתחזה עם פרטי ה-VTP של הארגון, כך שיכול לשנות את ה- vlan database של המתגים ברשת, יש להכניס את כל ההתקנים למצב transparent.

על ידי הפקודה :

```
switch(config)# vtp mode transparent
```

Data Plane

עוסק באבטחת המידע המועבר ברשת עצמו.

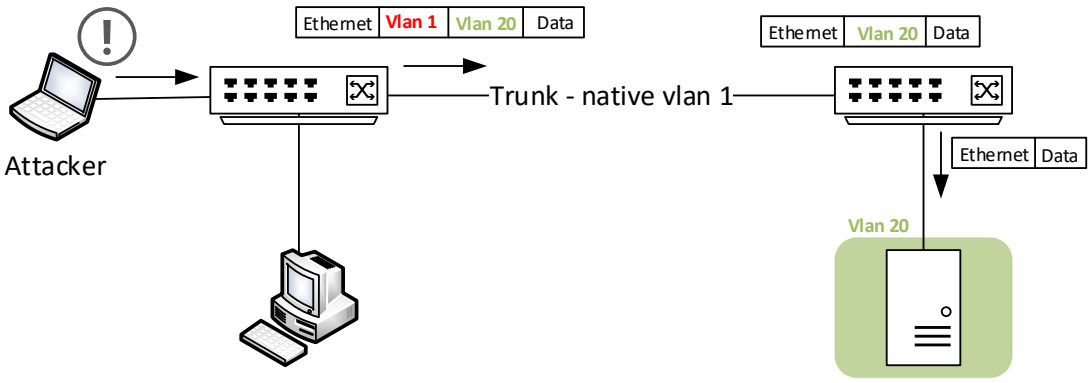
Native vlan

בכל מתג מוגדר 1 native vlan כברירת מחדל, המשמעות הינה שחבילות מידע שאינן מתויגות יועברו על גבי ה-native vlan. הסכנה הטמונה בלהשאיר את ה-native vlan כברירת המחדל היא פגיעות למתקפת double tagging.

תוקף שולח מסגרת מידע המתויגת פעמיים. השדה החיצוני מכיל את ה Vlan של התוקף שהינו זהה לערך ה-native vlan ברירת המחדל במתג. בנוסף לתיוג של Vlan 20, אותו התוקף רוצה לתקוף.

המסגרת המגיעה למתג הראשון אשר מסתכל על ה- 4 byte השייכים לתיוג ומגיע למסקנה כי המסגרת שייכת ל-native vlan . המתג שולח את מסגרת המידע דרך כל הפורטים המעבירים את Vlan 1 (ממשקי trunk תמיד מעבירים את ה-native vlan) לאחר שהוא הסיר את ה-4 byte של התיוג החיצוני. על ממשק ה-Trunk עוברת המסגרת ללא תיוג של vlan 1, והמסגרת לא מקבלת תיוג מחדש מכיוון שהיא הייתה שייכת ל native vlan. בשלב זה התיוג של vlan 20 נשאר ולא נבדק במתג הראשון.

המתג השני מתבונן רק בשדה התיוג הפנימי שהתוקף שלח, ורואה כי המסגרת מיודעת ל-vlan 20. המתג שולח את המסגרת לכיוון הממשק של הקורבן.



על מנת לשמור על אבטחת המידע יש לשנות את ה-ID של ה- native vlan ולא להשתמש בהגדרת ברירת מחדל. את השינוי של ה- vlan id מבצעים תחת ממשקי ה-Trunk.

ע"י הפקודה :

```
switch(config) #     interface X/Y
switch(config-if) # switchport trunk native vlan <vlan number>
```

Port Security

מתקפת macof dsniff גורמת למתג ללמוד ולהגדיר בטבלאותיו הפנימיות כתובות mac ראנדומליות רבות בפרק זמן קצר מאוד, כ-155,000 כתובות mac בדקה. טבלת ה-CAM של המתג מוצפת והמתג לא יכול ללמוד כתובות mac יותר. במצב זה המתג עובר לעבוד כ-Hub. Hub הינו התקן שמעביר את התעבורה שעוברת דרכו אל כל הפורטים שלו. באמצעות מתקפה זו התוקף יכול לקרוא את כל התעבורה העוברת דרך המתג המותקף. המשמעות הינה שבזמן שטבלת ה-CAM מלאה, הודעה הנשלחת מ VLAN מסוים משודרת לכל הפורטים המשויכים לאותו ה-VLAN.

על מנת למנוע מתקפות על טבלת ה-CAM של המתג יש להשתמש ב-Port Security. מטרת מנגנון זה הינה לאבטח את הפורטים של המתג ולמנוע מגורם זר להתחבר אליהם.

מנגנון אבטחה זה מגביל את מספר כתובות ה-mac שניתן ללמוד דרך פורט מסוים. בנוסף ניתן לבצע קיבוע של כתובת mac מסוימת לפורט כך שרק אותה הכתובת יכולה להתחבר לפורט הספציפי עליו מוגדרת ההדבקה. **חשוב לציין כי** Port Security **יש להגדיר רק על פורטים לכיוון**

תחנות קצה.

בהפעלת Port Security ניתן להגביל את מספר כתובות ה- mac שניתן ללמוד דרך הפורט וכיצד הפורט יתנהג במקרה של חריגה ממספר הכתובות שהוגדר.

```
switch(config) #   interface X/Y
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum <number>
Switch(config-if)# switchport port-security violation <protect / restrict / shutdown>
```

במידה ובפורט יילמדו יותר כתובות mac ממה שהוגדר, הפורט יפעל באחת משלושת הדרכים הבאות (תלוי בהגדרה):

Protect - במצב זה המתג יסנן Frames של תעבורה אשר הגיעו מכתובת mac לא מאושרת. מסגרות מידע מכתובות mac מאושרות לא יושפעו.

Restrict - מצב זה דומה מאד בפעולתו למצב Protect אך מודיע למערכת באמצעות הודעת Syslogעל ההפרה, ומעלה את ה - Counter Violation.

Shutdown - מצב ברירת מחדל, ברגע שבו יתקבל בפורט Frame אשר הגיע מכתובת MAC לא מאושרת, הפורט ייכנס למצב שגיאה וינוטרל. לא יהיה ניתן להשתמש בפורט עד שמנהלן של הציוד יפעיל אותו מחדש.

תשומת לב כי הפעלת מצב זה עלול לאפשר לתוקף יכולת קלה לביצוע מתקפת מניעת שירות, באמצעות משלוח FRAME עם MAC כלשהו שאינו מוכר לפורט.

Secure Mac Address

ישנם 3 מצבים באמצעותם ניתן ללמוד כתובות mac:

- Dynamic - מצב ברירת מחדל במתגים. כתובות ה- mac נלמדות באופן דינמי.
- Static - ניתן להגדיר ידנית את כתובת ה- mac שמורשית להתחבר לפורט ספציפי.

```
Switch(config-if)# switchport port-security mac-address <mac-address>
```

- Sticky - במצב זה המתג לומד עצמאית את כתובת ה- mac הראשונה של ההתקן המחובר לפורט ומקשיח את הפורט לכתובת ה- mac הספציפית שנלמדה.

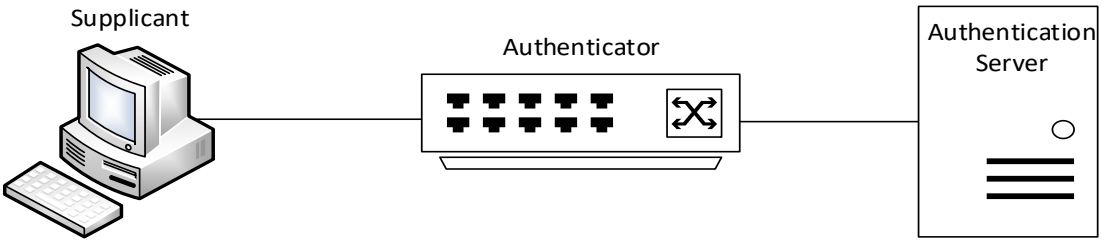
```
Switch(config-if)# switchport port-security mac-address sticky
```

השאיפה היא להגדיר את כל הפורטים המתחברים לתחנות קצה לעבוד במצב sticky. כך אנו מונעים התחברות פיזית של גורמים עוינים לרשת.

802.1X

פרוטוקול המגדיר בקרה על הגישה של מחשב למתג התקשורת, ומונע גישה של ציוד קצה לא מורשה אל הרשת באמצעות השגת נגישות פיזית לפורטים זמינים. שרת האימות (authentication), מוודא את זהותו של כל לקוח המנסה להתחבר לרשת, ורק לאחר אימות הלקוח, יחידת הקצה יכולה לתקשר ברשת דרך הפורט.

802.1X מופעל בדרך כלל עם פרוטוקול אימות בשם EAPOL - Extensive Authentication Protocol Over Lan.

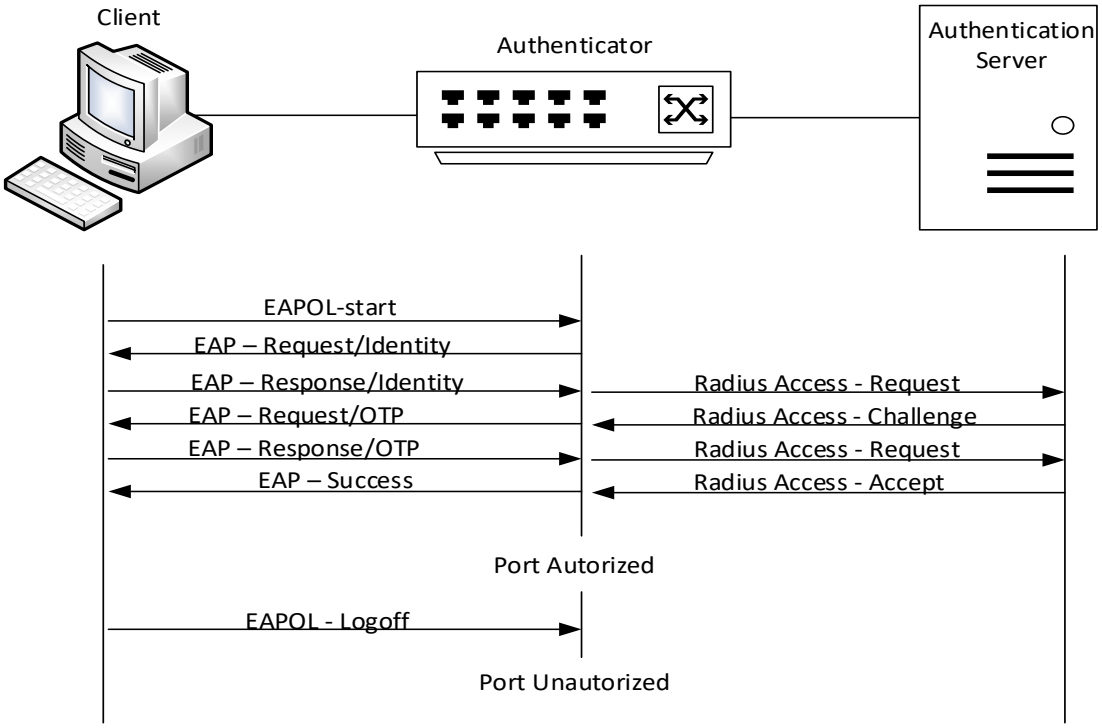


- Supplicant / Client - משתמש קצה המתחבר למתג ברשת הפנימית.
- Authenticator / Switch - המתג משמש כמתווך (proxy) בין שרת האימות ללקוח. המתג מבקש מידע לאימות מהלקוח, מאמת את המידע מול השרת, ולבסוף מחזיר את התשובה אל הלקוח.

המתג כולל את לקוח ה RADIUS, האחראי להוסיף למסגרות EAP header מתאים, ומצד שני להוציא את המידע הנחוץ ללא ה header, וכן לעבוד מול שרת האימות. כאשר המתג מקבל חבילות EAPOL (extensible authentication protocol over LAN), הוא מוריד את ה Ethernet header ובמקומו מוסיף header בפורמט המוכר ע"י ה RADIUS. התוכן עצמו אינו משתנה, ולכן שרת האימות חייב לתמוך ב EAP. ובכיוון ההפוך, כאשר חבילות מתקבלות במתג משרת האימות, הheader שהוסף ע"י השרת נמחק, המתג מוסיף במקומו Ethernet header ונשלח ללקוח.

- Radius / Authentication Server - מבצע את אימות הזהות של הלקוח, ומודיע למתג אם לתת הרשאה ללקוח להשתמש בשירותים שהרשת מספקת. המתג משמש כ proxy ולכן שירות האימות שקוף ללקוח. ישנו שימוש בשרת RADIUS (remote authentication dial in user service) על מנת לבצע את תהליך האימות של המשתמש. השרת עובד במודל לקוח - שרת, בו המידע על הלקוחות מועבר בין שרת ה- RADIUS ללקוחותיו.

נתאר באמצעות השרטוט את התהליך המתרחש בעת התחברות תחנה לרשת הפנימית.



ההגדרות שיש לבצע על פורטים לכיוון התחנות:

(config)# interface type number

(config-if) # authentication order mab dot1x

(config-if) # authentication priority dot1x mab

(config-if) # authentication port-control auto

(config-if) # authentication periodic

(config-if) # authentication timer reauthenticate server

(config-if) # mab

(config-if) # dot1x pae authenticator

(config-if) # dot1x timeout server-timeout <number>

(config-if) # dot1x timeout tx-period <number>

(config-if) # dot1x timeout supp-timeout <number>

(config-if) # dot1x max-req <number>

(config-if) # dot1x max-reauth-req <number