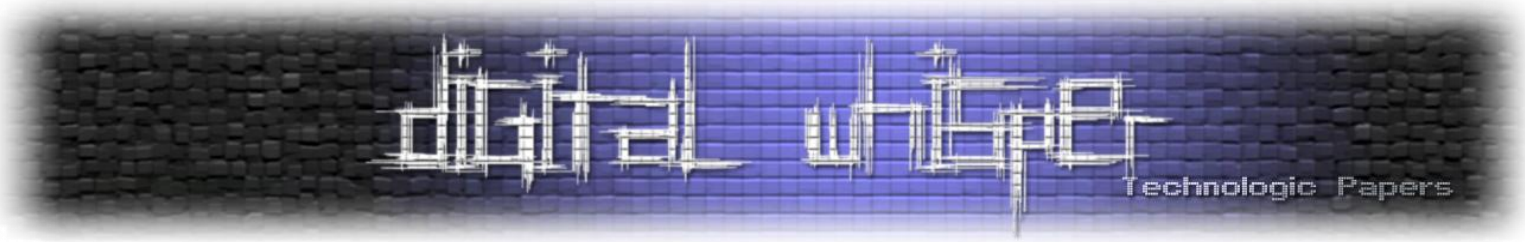


סקירת טכנולוגיות Firewalling שונות

מאת יגאל סולימאני ואפיק קסטיאל (cp77fk4r)

הקדמה

כידוע לכל, Firewall הוא כלי הנועד למדר את הסקטורים השונים ברשת שלנו, בין אם מדובר במידור חלקים שונים ברשת הפנים-אירגונית שלנו, ובין אם מדובר במידור שבין רשת האינטרנט לבין הרשת הפרטית בבית שלנו.

למרות שהכלי עצמו מוכר , לא כולם מכירים לעומק את השיטות השונות הקיימות לביצוע פעולה זאת ובכך עוסק מאמר זה . טכנולוגיית ה-Firewall אמורה להוות מעין פילטר שתפקידו להעביר אך ורק את חבילות המידע העומדות בסטנדרטים שקבענו מראש ולסנן את שאר חבילות המידע. המשימה יחסית פשוטה, אך כאשר מדובר במשימות שדורשות יותר מחסימת גישה לערוצים ספציפיים, או חסימת גישה לכתובת מסוימת, המשימה נעשית קצת יותר מורכבת. ישנו מספר לא קטן של דרכים לענות על המשימות השונות - ולכן ישנם סוגים רבים של טכנולוגיות Firewalling. במסגרת מאמר זה נציג את הטכנולוגיות הנפוצות כיום הנמצאות בשימוש, נסביר את ייעודן, את יתרונותיהן ואת חסרונותיהן.

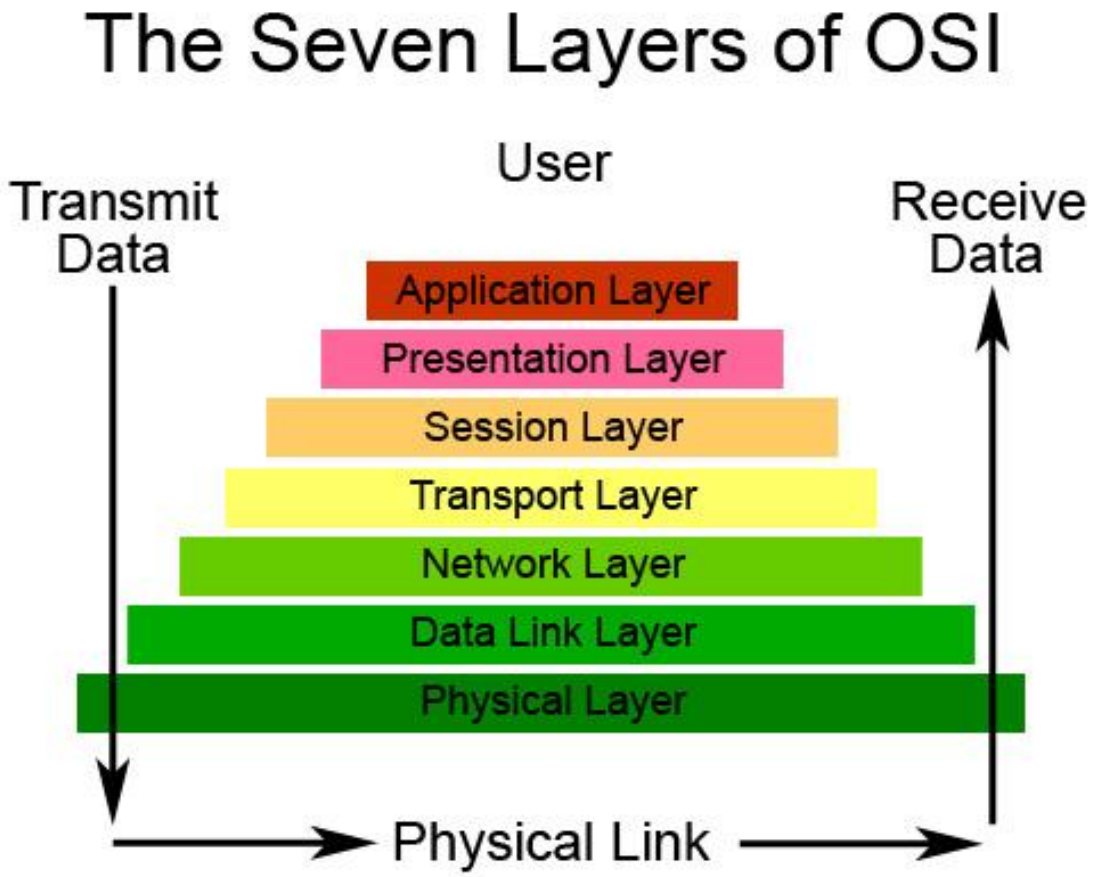
כידוע, בכדי לממש העברת נתונים על גבי הרשת אנו משתמשים במודל ה-OSI או "מודל שבע השכבות":

> מודל ה-OSI (קיצור של: Open Systems Interconnection) הוא מודל שכבתי אשר נוצר על ידי ארגון התקינה הבינלאומי. מטרת המודל היא להציג את הפעולות השונות הנדרשות על-מנת להעביר נתונים ברשת תקשורת ,ואת הסדר בין הפעולות השונות. המודל מתייחס לחומרה , לתוכנה ולשידור וקליטת הנתונים, ובין השאר, מספק הסבר כללי על מרכיביה השונים של הרשת. במודל שבע שכבות, והוא מכונה לעתים "מודל שבע השכבות."
>
> (צוטט מוויקיפדיה תחת הערך: מודל ה-OSI)

לא נכנס ונסביר את תפקיד כל שכבה (את זה אפשר לקרוא בויקיפדיה), אך להמשך הבנת המאמר חשוב להבין דבר אחד - ככל שנעלה בשכבות (נתרחק מהשכבה הפיזית ונתקרב לשכבה האפליקטיבית) כך

נקבל יותר מידע לגבי תעבורת הרשת , וככל שיהיה בידינו יותר מידע לגבי תעבורת הרשת - כך נוכל להיות יעילים יותר בעת מימוש טכנולוגיית Firewalling.

כך נראה מודל 7 השכבות:



(במקור: http://www.washington.edu/lst/help/computing_fundamentals/networking/img/osi_model.jpg)

השכבה הנמוכה ביותר במודל , שבה טכנולוגיות ה- Firewalling פועלות (להוציא מקרים מיוחדים) היא השכבה השלישית (שכבת הרשת, Network). בשכבה זו ניתן לנתח את נתוני חבילות המידע לפי נתוני התקשורת הבסיסיים ביותר - מקורה וייעדה של חבילת המידע. במידה ואנו עובדים בשכבה השלישית, לא נוכל לבצע בדיקות על תוכן חבילת המידע (בכדי למנוע מתקפות ספציפיות), בנוסף, לא נוכל לקשור חבילת מידע אחת לחברתה (Indexing) - וכך למנוע מתקפות הנחשבות למתקדמות יותר. בשכבה זו פועלות טכנולוגיות Firewalling בסיסיות ביותר.

Packet Filtering

הטכנולוגיה הראשונה שבה ניגע במאמר זה היא טכנולוגיית ה- Packet Filtering. טכנולוגיה זו סורקת כל חבילה שיוצאת או נכנסת, על פי טבלת החוקים המוגדרת לה, ומחליטה האם החבילה הזו מורשת לעבור הלאה או שהחבילה נחסמת ונשמטת.

את טבלת החוקים ניתן לקטלג רק על פי כתובת היעד או כתובת המקור, פורט המקור והיעד וסוג הפרוטוקול שבו מועבר המידע (TCP /UDP). טכניקה זאת הוצגה לראשונה בשנת 1988, לאחר מחקר שביצעו מספר מפתחים מחברת DEC ואז טכנולוגיה זו נחשבה כפריצת דרך בתחום אבטחת המידע.

טכניקה זו היא הנפוצה ביותר (והזולה ביותר) מכיוון שאין צורך בתוכנה נוספת שתעמיס על הציוד, ולכן רוב הנתבים תומכים בטכניקה זו. לדוגמא, אם נרצה לחסום כתובות IP מסוימות או סגמנטים מסוימים לשימוש FTP, בטבלת החוקים נחסום את כתובות היעד (Any) והמקור לשימוש בפורט 21 . לרב, טכנולוגיות Firewalling אלו, מאופיינות בממשק ניהול הכולל "Access List" – רשימה המאפשרת למנהל היישום לקבוע לאילו כתובות תאופשר גישה ולאלו כתובות לא.

<u>יתרונות ב Packet Filtering:</u>

- **שקטה** - לא דורשת משאבים רבים מפני שהיא לא נכנסת לעומקה של חבילת המידע.
- **זריזה** - היא אינה מתעכבת על ניתוח נתוני החבילה על פי חוקים ורגולציות.

<u>חסרונות:</u>

- **לא חכמה -** הטכנולוגיה אינה לומדת את כלל מאפייני התקשורת (State) ולכן היא פגיעה למתקפות כגון IP Spoofing, Data Driven Attack, Source Route Attack, SYN Flood וכו'.
- **לא פשוטה לניהול -** במערכות גדולות, קשה מאוד לנהל את טבלת החוקים ויכולות להיות סתירות, מכיוון שחבילה עוברת/נחסמת על פי הכלל הראשון שמתאים לחבילה זו. למשל, כתובת IP מסויימת יכולה להשתייך לקבוצה A וגם לקבוצה B, לשתי הקבוצות הרשאות שונות בטבלת החוקים. כשחבילה מכתובת ה- IP הזו תגיע ל-Firewall, היא תגיע לשורה של קבוצה A שחסומה ליציאה ולכן החבילה תחסם ותישמט למרות שבקבוצה B היא מוגדרת כאחת שכן יכולה לצאת החוצה.
החבילה מועברת הלאה או נזרקת על פי השורה הראשונה בטבלת החוקים שמתאימה לחבילה, אם אף שורה לא מתאימה החבילה נשמטת.

השכבה הבאה במודל, שבה מופעלות טכנולוגיות ה- Firewalling, היא השכבה החמישית (שכבת ה-SESSION), שכבה זו עדיין נחשבת שכבה "נמוכה" ולא נדרשים משאבים רבים בכדי לבצע את החישובים בה.

Circuit-Level Gateway

טכנולוגיית ה- Firewalling המוכרת ביותר הפועלת בשכבת הרשת החמישית (שכבת ה-SESSION), הינה טכנולוגיית ה-Circuit Gateway הידועה גם כ-Relay firewall Circuit. משום שהטכנולוגיה פועלת בשכבת ה-SESSION, היא אינה נתונה למגבלות הקיימות בטכנולוגיות הממוקמות מתחתיה ושימוש בה מאופיין בניתוח מאפיינים שונים בתקשורת.

שלא כמו בשכבה השלישית במודל, בשכבה החמישית ניתן ללמוד את כל הנתונים בחבילת התקשורת ולא רק את נתוני מקור החבילה או את יעדה. בעזרת ניתוח של כלל נתוני חבילת התקשורת ניתן לייעל את סינון המידע ולאפשר למנהל היישום לממש חוקים מורכבים יותר. מתקפות המבוססות על אי-יכולת ה- Firewall לזהות קשרים בין חבילות התקשורת יפלו כנגד הטכנולוגייה הזאת, כמו כן גם מתקפות כגון DoS המבוססות על מנגנון הרכבת חבילת המידע השלמה וניתוחה ע"י ה-Firewall. לעומת זאת מתקפות Stateless, כגון העברת נתונים זדוניים בחבילת נתונים אחת מתוך State שלם של חבילות נתונים לא תזוהה על ידי טכנולוגיה זו מפני שאין כאן בדיקה של חבילת הנתונים הבודדת, אלא של כלל ה-State.

<u>היתרונות הקיימים בטכנולוגיה זו:</u>

- **שקטה** - הטכנולוגיה אינה דורשת משאבים רבים מפני שאינה נכנסת לעומקה של חבילת מידע אחת אלא לעומקו של כלל ה-State.
- **זריזה** - הטכנולוגיה אינה מתעכבת על ניתוח נתוני החבילה הבודדת.
- **חכמה-** לומדת ומסיקה מסקנות על ידי כלל State התקשורת ולא על פי חבילות מידע בודדות.

<u>והחסרונות הם:</u>

- **פזיזה -** הטכנולוגיה אינה מסוגלת לבצע בדיקת חבילת נתונים יחידה ועל כן נופלת במתקפות כגון מתקפות המבצעות שימוש Tunneling דרך פרוטוקול תקשורת מאושר אחר.

Filtering Gateway

טכנולוגיית ה-Stateful Packet Filtering הראשונה שנכיר היא מסוג Application Filtering. ישנן שתי דרכים לממש טכנולוגיה זו:

- שימוש מקומי של המערכת.
- שימוש בשרת חיצוני המהווה שרת Proxy לתקשורת הרשת.

שימוש בשרת פרוקסי לסינון וניטור תעבורת הרשת נקרא- Filtering Gateway. הרעיון הוא להקצות שרת ייעודי אשר ימוקם בקצה (או במרכז, תלוי בתפקידו) של רשת התקשורת - בנקודה בה הרשת מתחברת לרשתות השונות בארגון המסכנות אותה (הרשת הכללית של הארגון, רשת האינטרנט, DMZ וכו') וכך לבצע ניטור של המידע הנכנס או היוצא מהרשת.

במידה והתוקף ירצה לבצע מתקפה על משאב רשת הממוקם ברשת הפנימית (המוגנת) של הארגון, הוא יחוייב לעבור דרך ה-Filtering Gateway. לפיכך אנו יכולים להבטיח שכל הנתונים היוצאים והנכנסים לאותה הרשת יעברו דרך שרת הפרוקסי שלנו. כך, למשל, אפשר להימנע ממתקפות כגון Source Route Attack.

היתרונות בטכנולוגיה זו:

- **יציבה -** הטכנולוגיה רצה בדרך כלל על שרתים ייעודיים נפרדים שלא משתמשים לעבודה רגילה ולכן אין בעיה שתוקצה לה כמות גבוהה של משאבי מחשוב.
- **אבטחה גבוהה -** שימוש בשרת Filtering Gateway עבור גישור בין רשתות הארגון השונות, מחייבות את מנהלי הרשתות בארגון לעבוד באופן מאובטח ויכולות למנוע הרבה "טעויות אנוש" המהוות חלק נכבד מבעיות האבטחה הנפוצות ביותר כיום.
- **גמישה -** Application Filtering איכותי מגיע כיום עם מגוון אפשרויות לניהול הרשת, ביסוסו על טכנולוגיית ה-Stateful Packet Filtering מאפשרת למנהל הרשת לקבוע חוקים המשלבים מאפייני תקשורת רבים.
- **חכמה -** ביסוסה על טכנולוגיית ה-Stateful Packet Filtering מונעת ממנה ליפול למתקפות Spoofing בסיסיות בשל למידתה את כלל ה-State של התקשורת.

החסרונות בטכנולוגיה:

- **לא פשוטה לניהול -** בהרבה מהמקרים ישנם קורסים שלמים והסמכות שצריך לעבור בכדי לדעת לתפעל שרת שכזה באופן איכותי.
- **כבדה -** דורשת משאבי חישוב רבים (לרוב משאב רשת ייעודי).
- **זמינות -** השרת אמנם יציב אך בשל תצורתו, הוא מהווה את החוליה היחידה המקשרת בין הרשת הפנימית לכלל הרשת של הארגון או רשת האינטרנט. כך, במידה והוא ייפול- **כלל הרשת הפנימית** לא תהיה זמינה עד שיקימו את השרת בחזרה.

IPTables

טכנולוגיית ה-Stateful Packet Filtering שנציג היא טכנולוגיית ה-IPTables, טכנולוגיה זו מיושמת ברוב הפצות הלינוקס כיום ומהווה אחד מגורמי האבטחה המרכזיים בהפצה. טכנולוגיה זו מבוססת על קבוצות חוקים, המשורשרים במספר סוגי טבלאות, כדוגמת:

- **FILTER** – טבלת ברירת המחדל, הטבלה הכי בסיסית, במידה ולא תקבע שום טבלה שתוגדר כאחראית לטיפול באירוע, ה-Packet יגיע לכאן.
  בטבלה זו קיימות שלוש שרשראות:
  1. **INPUT**- שרשרת המוגדרת לטפל ב-Packets אשר נכנסים למערכת.
  2. **OUTPUT**- שרשרת המוגדרת לטפל ב-Packets אשר יוצאים מהמערכת.
  3. **FORWARD**- שרשרת המוגדרת לטיפול ב-Packets המיועדים לניתוב.
- **NAT** - הטבלה האחראית לניתוב ה-Packets, בטבלה קיימות שלוש שרשראות:
  1. **PREROUTING**- שרשרת המוגדרת לטפל ב-Packets לפני הניתוב.
  2. **POSTROUTING**- שרשרת המוגדרת לטפל ב-Packets לאחר הניתוב.
  3. **OUTPUT**- שרשרת המוגדרת לטפל ב-Packets היוצאים.
- **MANGLE**- טבלה לטיפול מתקדם ב-Packets. בקרנלים החדשים (מ-2.4.18) קיימות חמש שרשראות:
  1. **PREROUTING**- שרשרת המוגדרת לטפל ב-Packets לפני הניתוב.
  2. **POSTROUTING**- שרשרת המוגדרת לטפל ב-Packets לאחר הניתוב.
  3. **INPUT**- שרשרת המוגדרת לטפל ב-Packets אשר נכנסים למערכת.
  4. **OUTPUT**- שרשרת המוגדרת לטפל ב-Packets היוצאים.
  5. **FORWARD**- שרשרת המוגדרת לטיפול ב-Packets המיועדים לניתוב.

(נלקח מהמאמר "שימוש ב-IPTables" ע"י אפיק קסטיאל הפורסם בגליון השלישי של Digital Whisper)

לכל שרשרת היכולה להכיל מספר חוקים שני מאפיינים:

- הגדרות לזיהוי חבילת המידע.
- גורל חבילת המידע.

אירועים

במידה ויווצר אירוע רלוונטי חבילת המידע תגיע לטבלה הרלוונטית (חבילות מידע יוצאות- OUTPUT, חבילות מידע נכנסות-INPUT וכו') ותעבור מול שרשראות החוקים הקיימות באותה הטבלה. במידה ותמצא התאמה בין חוק הקיים בשרשרת לבין חבילת המידע: גורל חבילת המידע יקבע לפי המצויין בטבלת החוקים. במידה ולא תמצא התאמה תתבצע בדיקה מול החוק הבא ברשימה.

<u>היתרונות של טכנולוגיה זו:</u>

- **גמישה -** ביסוסה על טכנולוגיית ה-Stateful Packet Filtering מאפשרת למנהל הרשת לקבוע חוקים המשלבים מאפייני תקשורת רבים. בנוסף, הטכנולוגיה תוכל לרוץ גם על עמדת הקצה.

- **פשוטה (יחסית)** - השימוש בה פשוט יחסית ובכדי ליצור בה חוקים בסיסיים אין צורך בהבנה עמוקה של המערכת.

- **חכמה-** ביסוסה על טכנולוגיית ה-Stateful Packet Filtering מונעת ממנה ליפול למתקפות Spoofing בסיסיות מאחר והטכנולוגיה לומדת את כלל ה-State של התקשורת.

<u>החסרונות:</u>

- **לא פשוטה לניהול -** במידה ומדובר באירגונים גדולים המכילים משאבי מערכת ותצורות רשתות הדורשות אילוצים שונים, יהיה קשה לנהל טבלאות ניתוב. שינוי של טבלה או חוק אחד בטבלה עלול לגרום לפגיעה בשרשרת חוקים שונים.

- **כבדה-** במידה ומדובר ביישום הטכנולוגיה כ-Filtering Gateway ולא ניהול של עמדת קצה- יש להקצות כוח מחשוב רב.

Application level gateways

כפי שראינו בתחילת המאמר, מודל ה-OSI מחולק לשכבות, השכבה העליונה ביותר היא שכבת האפליקציה ("Application Layer"), טכנולוגיות Firewalling שיושבות על השכבה הזאת נקראים בדרך כלל "Application level gateways" או בקיצור- ALG. לרוב מדובר באפליקציות הצורכות משאבים רבים (כמובן שהרבה תלוי באופן מימושה של הטכנולוגיה) - אך האפשרויות שהן מציעות רבות.

טכנולוגיה כזאת יכולה להיות ממומשת באופן של Session flow או כ-Packet flow. מפני שהטכנולוגיה יושבת באופן הקרוב ביותר למשתמש (מבחינת שכבות המודל) היא מסוגלת לקחת בחשבון את כלל נתוני התקשורת, במקומות שטכנולוגיות אחרות יכולות רק למנוע או לאפשר למשתמש לגלוש באתר אינטרנט. למשל, טכנולוגיה זו מאפשרת למנהל הרשת גם לקבוע מאילו כתובות יהיה ניתן לקבל מידע ואילו כתובות ספציפיות יהיו חסומות לגלישה.

<u>היתרונות בטכנולוגיה זו:</u>

- **חכמה -** בשל מיקומה הגבוהה במודל היא מסוגלת להייחס לכלל נתוני התקשורת ובאפשרותה להתייחס לכלל ה-State של התקשורת.
- **גמישה-** מפני שהטכנולוגיה מסוגלת להתחשב בכלל נתוני התקשורת, היא מאפשרת למנהל הרשת לקבוע חוקים המשלבים מאפייני תקשורת רבים.

החסרונות הם:

- **כבדה-** רוב צורות המימוש של הטכנולוגיה דורשים משאבי מיחשוב רבים.
- **איטית –** טכנולוגיה זאת מתחשבת בכלל נתוני התקשורת ובודקת את כלל שדות חבילת המידע, שימוש בהרבה חוקים יורגש בשל האטה משמעותית של התקשורת.

סיכום

במאמר זה הצגנו את הדרכים הנפוצות בהן ניתן לממש טכנולוגיות Firewalling להגנה על עמדת הקצה או כלל הרשת. כיום ישנם לא מעט יישומי Firewalling המבצעים שימוש במספר טכנולוגיות Firewalling בכדי לשאוב מכל טכנולוגיה את יתרונותיה וכך להגביר את האבטחה שהם מספקים. כאשר רוכשים יישום Firewalling לאירגון או למחשב האישי יש להתחשב במספר גורמים כגון תצורת כלל הרשת, סוג השימוש בחיבור האינטרנט (הורדת/העלאת קבצים, גלישה, שליחת מיילים וכו') והיקף השימוש.