

עבודת גמר בתכנון ותכנות מערכות – התמחות סייבר

5 יח"ל – שאלון 883589

****

**מערכת ReverseProxy**

* **מגיש:** עידן אפלבום (ת"ז 215917378)
* **מורים מנחים:** אריק וינשטיין ושרית שוורץ
* **בית הספר:** אמי"ת גוש-דן בר-אילן
* **שנת הגשה:** 2024, תשפ"ד

# מבוא

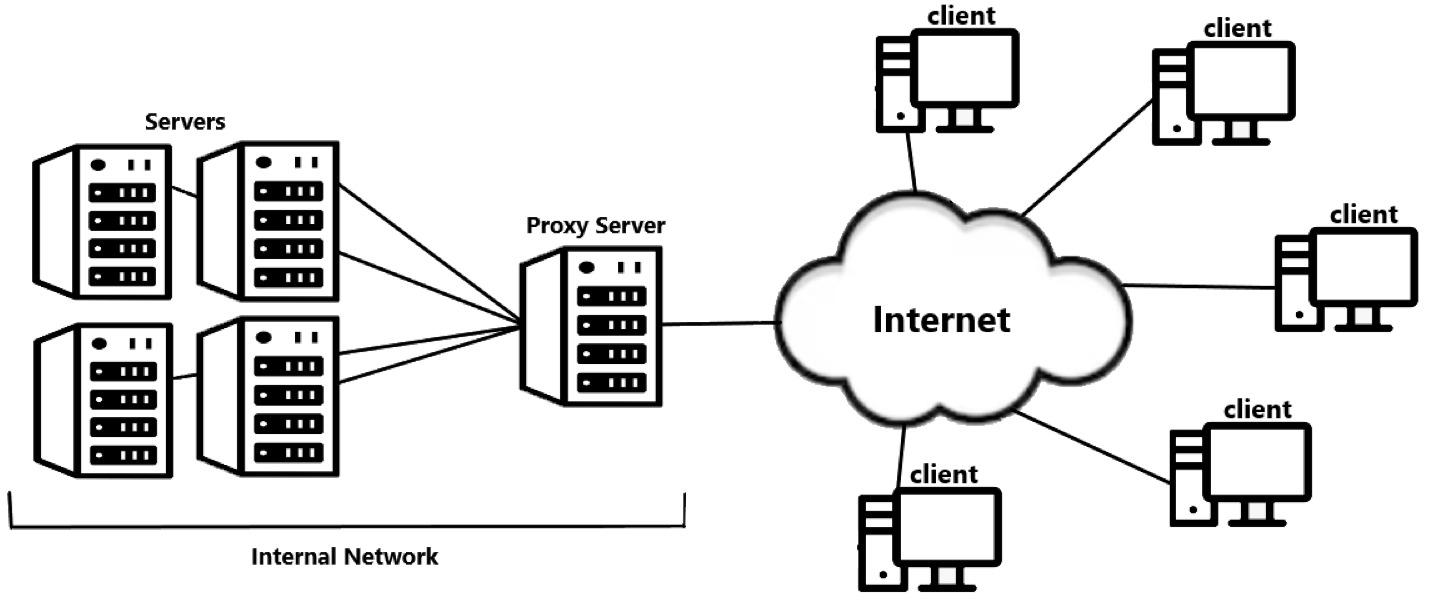
## נושא הפרויקט

RP - מערכת להגנה על שרתי web מבוססת שרת reverse proxy.

## תקציר הפרויקט

תוכנת RP היא שרת פרוקסי הפוך לניהול תקשורת רשתות שרתים לאינטרנט. שרתי פרוקסי ככלל הם שרתים המשמשים middleman בין רשת האינטרנט לשאר המכשירים ברשת מקומית (LAN). כלומר, תעבורת הרשת היוצאת והנכנסת לרשת המקומית עוברת דבר ראשון דרך הבקרה של שרת הפרוקסי. שרתי פרוקסי משמשים בעיקר לשיפור האבטחה והפרטיות על הרשת המקומית, אך גם למספר מטרות משניות כגון שיפור ביצועים עבור הגלישה באינטרנט.

בעוד שרתי פרוקסי בד"כ משמשים למשתמשים פרטיים (בצד הלקוח) ורשתות ביתיות, שרת פרוקסי הפוך משמש לרשתות שרתים של חברות מסחריות. שרת פרוקסי הפוך, כמו תוכנת RP, מספק רמות אבטחה ושיפור הפרטיות לרשת השרתים ומרכיביה. דוגמה לכך הוא חסימת נסיונות התקפות DoS כמו Resource Exhaustion וTCP Flood. שירותים נוספים הניתנים ע"י הפרוקסי ההפוך הם היכולת לעקוב ולשמור פעילות של משתמשים, חלוקת זרימת הבקשות באופן שווה על מנת למנוע עומס על שרת יחיד, הסרת הצורך בהתקנת תוכנות אבטחה על כל שרת בנפרד ועוד.



## סיקור מצב השוק כיום

1. **שרת Apache** – שרת אינטרנט שיכול לשמש כפרוקסי הפוך. השרת מבצע מספר פעולות כגון load balancing ע"י יצירת workers שמטפלים במשתמשים, שיפור האבטחה ע"י NAT, שיפור היעילות בעזרת static data caching וחיבורי SSL המאפשרים תקשורת ברשת הפנימית ללא הצפנה.
2. **שרת NGINX** – דומה לשרת Apache, אך בא אחריו. NGINX הוא תוכנת שרת אינטרנט בקוד פתוח שיכול לשמש כשרת פרוקסי הפוך. יתרונו על Apache הוא שהוא יותר פשוט, מה שמשפר יעילות ומהירות הריצה שלו. אך כתוצאה מכך, הוא יותר מוגבל ביחס לשרת Apache.

המטרה של תוכנת ReverseProxy היא לספק שירותי אבטחה מהתקפות DoSנפוצות כגון Resource Exhaustion וTCP Flood. בנוסף תאסוף ותציג התוכנה מידע אודות פעילות המשתמשים בשרתים השונים, תחלק את פניות המשתמשים בין השרתים ותתן שירותים נוספים לניהול תקשורת רשת השרתים מול האינטרנט.

## הגדרת לקוח

התוכנה מיועדת לאנשים בעלי אתר אשר רוצים להגן על השרת/ים שלהם, או שמעוניינים לנהל את שרתיהם בצורה פשוטה ובטוחה. ReverseProxy תאפשר להם לאבטח את האתר שלהם ולנהל את התקשורת שלו מול הרשת בצורה נוחה.

## תיחום הפרויקט

התוכנה תאפשר הגנה על שרתי אינטרנט מפני שלל התקפות DoS, ותציע מספר שירותים לניהול יעיל של השרתים. עם זאת, התוכנה לא תיצור worker עבור כל משתמש בפני עצמו, אלא תשתמש בשרתים הנתונים. בנוסף, התוכנה לא תוכל למנוע התקפות DDoS (Distributed DoS) ולא התקפות SQL Injection.

## אתגרי הפרויקט

1. **מחקר ופיתוח** – כחלק מפיתוח התוכנה, אצטרך לחקור וללמוד על נושאים חדשים כמו התקשורת בין הרכיבים שברשת, סוגי התקפות נפוצות ועבודה מול שרתי אינטרנט.
2. **בחירת התחברות התוכנה לרשת** – יש לבחור את ספרייה להתחברות לרשת שתתאים ביותר למטרות התוכנה. צריך ספרייה שתתמוך בהתחברות למספר שרתי אינטרנט בו זמנית ובהתחברות לרשת.
3. **המצב הנוכחי בישראל** – בעקבות מלחמת חרבות ברזל שאנו נמצאים בה כרגע, עולים הרבה חששות וקשיים עקב מצב החוסר וודאות שכולנו נמצאים בו.

## תיאור המערכת

תוכנת ReverseProxy היא שרת פרוקסי הפוך שמטרתה לאבטח ולסדר חיבור של שרת/י אינטרנט לרשת.

התוכנה תבצע מספר שירותים:

User data logging – השרת יאסוף וינתח מידע אודות המשתמשים הגולשים בשרתים שברשת המקומית, ויציג בפני משתמש admin את הדוחות.

Load Balancing – התוכנה תחלק את כניסות המשתמשים בצורה כמה שיותר שווה כדי להפחית עומס מהשרתים. כשמגיעה בקשת התחברות מלקוח חדש, RP תמצא את השרת הכי פחות עסוק ותפנה את הבקשה אליו.

פרטיות – כאשר נשלחת תגובה מהשרת, הלקוח רואה רק את כתובת הIP של שרת הפרוקסי, כך שאין לו כל מידע על השרת המקורי.

נוחות – כאשר יש צורך בהוספת תוכנת אבטחה, שינויים בקריפטוגרפיה או כל שינוי המשפיע על תקשורת השרתים עם האינטרנט – תוכנת RP מבטלת את הצורך לבצע שינויים בכל שרת ושרת. במקום זה, ניתן לבצע את השינויים אך ורק על שרת הפרוקסי, וכתוצאה מכך כל המערכת תושפע מהחידושים.

הגנה – שרת הפרוקסי RP יעצור ניסיונות של התקפות (Denial of Service) DoS, שהן התקפות שמטרתן להציף את השרת בבקשות עד שלא יוכל לקבל פניות ממשתמשים אמיתיים או שיאט משמעותית. התקפות הDoS הנפוצות ביותר הן Resource Exhastion, שבה התוקף מעמיס על משאבי השרתים ומונע מהם טיפול בבקשות אחרות, וTCP SYN Flood, שבה התוקף שולח לשרת המון בקשות SYN לפתיחת חיבורים ובכך מונע ממנו ליצור חיבורים עם לקוחות המנסים להתחבר.

SSL Termination – בכך שהתוכנה מטפלת בהצפנות הSSL, הרכיבים ברשת המקומית (VLAN) יכולים לתקשר ביניהם ללא הצורך בהצפנה, מה שמאיץ את ביצועי המערכת ככלל.

תהליכים בתוכנה:

* קבלת בקשות התחברות מהמשתמשים ברשת
* קישור לקוח לשרת והעברת התקשורת ביניהם
* חיפוש אחר התקפות DoS
* איסוף וניתוח פעילות המשתמשים בשרתים

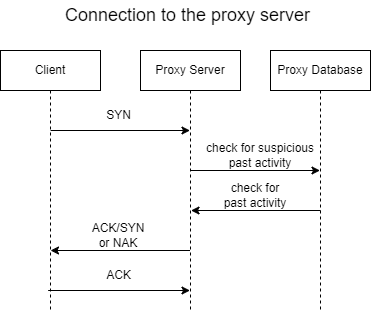
## בדיקות התוכנה

מספר בדיקות יבוצעו על מנת לבדוק שכל התהליכים במערכת עובדים כראוי, לדוגמא:

1. **טיפול בתקשורת השרת והלקוח:** בדיקה שהחיבור מאפשר לתוכנה להעביר בקשות של לקוחות ומידע אל השרתים, וששרת הפרוקסי מצליח להחזיק כמה TCP tunnels באותו הזמן.
2. **בדיקת חיבור השרתים לתוכנה:** בדיקה שהתוכנה מפנה בקשות התחברות לשרת המתאים, ודואגת לבדיקה מתמידה של מצבם לקבל התחברויות חדשות.
3. **בדיקת התקפת DoS:** בדיקה האם התוכנה יודעת להבדיל בקשות חיבור רגילות מבקשות שמטרתן לתקוע את השרת, וחסומת את מקור ההתקפה.
4. **בדיקת קבלת User Data Log:** בדיקה ששרת הפרוקסי RP מתעד באמינות את פעילות המשתמשים בשרתים ומדווח אותם בצורה מסודרת למשתמש admin המבקש את דו"ח הפעילות.

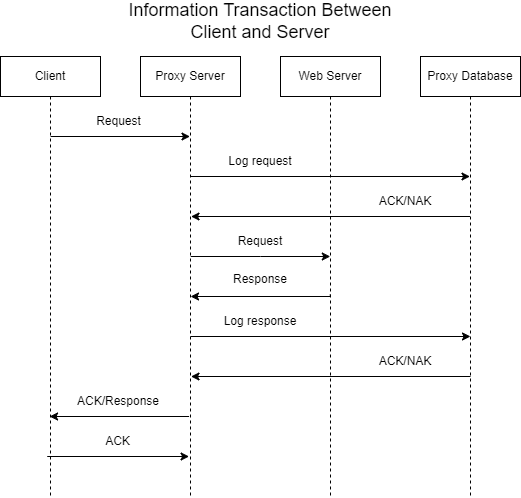
## תהליכים ראשיים במערכת

1. **קבלת בקשות התחברות מהמשתמשים ברשת:** המשתמש שולח בקשת התחברות לאתר, שתגיע אל שרת הפרוקסי. התוכנה תבדוק האם כתובת הIP שלו לא חשודה ע"פ מאגר הכתובות החשודות. לאחר שביררה שלכתובת לא הייתה היסטוריה בעייתית, התוכנה תבדוק האם הבקשה היא עצמה חלק מהתקפה פוטנציאלית. אם השרת מקבל המון פניות מאותה כתובת IP, הכתובת תיחסם. אם התוכנה אישרה את אמינות המשתמש, היא תיצור איתו TCP tunnel.
2. **קישור לקוח לשרת והעברת התקשורת ביניהם:** שרת הפרוקסי שולח בקשת ההתחברות לשרת המתאים, ויוצר איתו TCP tunnel. בנוסף מוסיפה התוכנה את המשתמש לUser Data Log ומתעדת את פעילותו בשרת. כשהלקוח שולח בקשה לשרת, התוכנה בודקת שהלקוח לא שולח בקשות מרובות בזמן קצר, ואם הוא כן, היא תנתק את התקשורת ותחסום אותו.לאחר הבדיקה תעביר התוכנה הבקשה לשרת, ותעביר בחזרה ללקוח את הack/response מהשרת.
3. **חיפוש אחר התקפות DoS:** התוכנה בודקת גם במהלך ההתחברות וגם בזמן התקשורת עצמה שלא מתרחשת התקפת מניעת שירות מהלקוח על השרת. שרת הפרוקסי מוודא שהמשתמש לא מעמיס המון בקשות בזמן קצר על השרת. כשהתוכנה מזהה ניסיון התקפת DoS, היא חוסמת את הכתובת מלתקשר עם השרתים ומוסיפה אותו למאגר הכתובות החשודות.
4. **איסוף וניתוח פעילות המשתמשים בשרתים:** במהלך התקשורת של הלקוח עם השרת, התוכנה אוספת מידע אודות פעילותו בשרת, כגון זמן החיבור לשרת ותוכן הפעילות. את המידע מסדרת התוכנה בטבלאות ומציגה אותם לadmin שמבקש לראות את הדוחות.

****

**A black screen with white text

Description automatically generated**

****

