

**עבודת גמר 5 יח"ל**

**נושא העבודה :**  רשת VPN למשתמשים פרטיים

**שם תלמיד :** פימה פנחס מוצמכר

**ת.ז תלמיד :** 325118693

**שם בית ספר ועיר :** קריית החינוך ע"ש עמוס דה-שליט, רחובות

**שם המנחה :** ערן בינט

**מועד הגשה :** 9.3.2018

תוכן עניינים

[1. מבוא 3](#_Toc509432052)

[2. תיאוריה 4](#_Toc509432053)

[3. תוצר סופי 5](#_Toc509432054)

[4. תהליך כתיבת הפרויקט 11](#_Toc509432055)

[5. מרכיבי פתרון 11](#_Toc509432056)

[6. תסריטי בדיקה 13](#_Toc509432057)

[7. רפלקציה 13](#_Toc509432058)

[8. הוראות התקנה ותפעול 14](#_Toc509432059)

[9. ביבליוגרפיה 14](#_Toc509432060)

[10. נספחים 14](#_Toc509432061)

1. מבוא
   1. נושא העבודה

נושא העבודה הוא שירות Enterprise VPN למשתמשים פרטיים. השירות יכלול חיבור לשרת VPN אשר יצפין את התעבורה העוברת דרך המכונה של המשתמש. בנוסף השירות יציע גם שימוש בשרת FTP לשם העברת קבצים ובשימוש באזור מנוטר ברשת (DMZ). השירות יכלול האמתה אשר תאמת משתמשים לפי שם משתמש וסיסמא ותעניק JWT לכל אחד מהם.

* 1. מטרות מרכזיות

המטרות המרכזיות של העבודה הן:

* הקמת שירות שרת – לקוח אשר יאפשר ניהול תקשורת מאובטחת ואנונימית של הלקוח עם העולם.
* לאפשר ללקוח לשתף קבצים עם משתמשים שונים בצורה מאובטחת.
  1. רציונל

המוטיבציה שלי לפיתוח הרעיון הינה ליצור ממשק, פשוט נח ושמיש אשר יאפשר למשתמש לבצע גלישה בטוחה ברחבי הרשת הכלל עולמית. לדעתי, שירות שכזה יכול להבטיח את בטיחותם של כלל המשתמשים ואכן לתת תועלת רבה. באמצעות הפרויקט אני מקווה להבין יותר את כלל נושא אבטחת התקשורת ברמות הגבוהות של ה – OSI ובנוסף להצליח לשפר את יכולותי בשפת Python במגוון האפשרויות השונות שהיא מציעה בתחום תקשורת הנתונים.

* 1. קישור לחומר הנלמד

העבודה מתקשרת לחומר הנלמד במספר תחומים שונים. ראשית, ...

1. תיאוריה
   1. תיאוריה
   2. מוצרים קיימים - ExpressVPN

ExpressVPN הוא שירות VPN בתשלום שמציע את שירותיו ברחבי העולם. ExpressVPN מגנים על החיבור של משתמשיו עם **הצפנת AES-256-ביט ברמה צבאית**, אותר רמת הצפנה הנמצאת בשימוש על ידי סוכנויות ממשלתיות רבות, כדי לסבר את האוזן בנוגע לכמה אלגוריתם ההצפנה הזה מאובטח. ExpressVPN מציעים גם מנהור מפוצל. משמעותה של האפשרות הזו היא שאתם יכולים לבחור אתרים שלא יהיו מוצפנים, וישתמשו באינטרנט "הרגיל", במקום להעביר את כל התעבורה שלכם דרך ה-VPN. תוכלו גם להגדיר את המכשיר שלכם כדי שיתמוך במצב של מנהור מפוצל הפוך, ולבחור לשלוח תעבורה מאתרים מסוימים רק דרך ה-VPN. מנהור מפוצל זמין רק עבור התוכנות של ExpressVPN לווינדוס, מק OS, אנדרואיד, ונתבים.

לאחרונה ExpressVPN עלו לרמה אפילו גבוהה יותר עם טכנולוגיית TrustedServer החדשנית. במהותו, המשמעות של TrustedServer היא ש-ExpressVPN מפעילים את השרתים שלהם רק באמצעות RAM. זה מפחית את הסיכון של נקודות תורפה אבטחתיות בשרתי ExpressVPN בהשוואה לרשתות שרתי VPN אחרות.

אמנם האפליקציה שלי לא תהיה כה משוכללת ומתוחכמת, אך היא תהיה חינמית ותאפשר גישה למגוון תכנים נוספים מלבד גלישה בטוחה באינטרנט, כגוון שיתוף קבצים ו – DMZ.

1. תוצר סופי
   1. תיאור הפרויקט

המשתמש פותח את קליינט הVPN במחשבו האישי אשר מריץ חלונות. חובה על שרת הVPN ושרת ההתחברות להיות פעילים לשם פעילות התכנית. הקליינט מתחבר לשירות ומקבל גישה לכל המוזכר לעיל, לרבות התחברות מאובטחת לאינטרנט, התחברות לשרת FTP, התחברות לשרת DMZ. כמו כן, כל פרק זמן מוגדר יצטרך המשתמש לחדש את

המערכת מאפשרת מספר פעולות:

* הצפנה מוחלטת של המידע המועבר בין המשתמש לממשק בעזרת חיבור SSL
* אנונימיות במרחב בעקבות החיבור לשרת ה VPN.
  1. אלגוריתמים עיקריים

אלגוריתמים מרכזיים במערכת

1. JWT (ראשי תיבות באנגלית של: JSON Web Token) הוא תקן פתוח מבוסס JSON ליצירת מפתח גישה (Access Token) המשמש לולידציה של "טענות" (לדוגמה שם משתמש, הרשאות, סיסמה). המפתחות חתומים על ידי מפתח ייחודי של השרת, כך שהלקוח והשרת מסוגלים כל אחד בנפרד לוודא שהמפתח לגיטימי. האלגוריתם אחראי על התחברות לקוחות באופן בטוח ומוודא את

היותם מקבלי שירות מורשים.

1. "מנהור HTTP" הוא התהליך בו מתקבלות תקשורת באמצעות פרוטוקול HTTP. מנהור HTTP מיועד בעיקר לרתיעה מפני חומת אש. מנהור HTTP מבצע אנקפסולציה של פרוטוקול, על ידי סגירת מנות נתונים של פרוטוקול אחד (SOAP, JRMP וכו ') בתוך מנות HTTP. לאחר מכן נשלחים מנות ה- HTTP דרך חומת האש כתעבורת אינטרנט רגילה. במקרה שלי, המנהור מאפשר לקיים אנונימיות והצפנה של המידע המועבר לשרת ה-VPN.
   1. ממשק משתמש
   2. תרחישים עיקריים
2. אחד
3. שתיים
4. תהליך כתיבת הפרויקט
   1. תהליך הפרויקט
   2. אתגרים ואופציות שונות למימוש
5. מרכיבי פתרון
   1. תיחום הפרויקט

* תקשורת - בתקשורת נתונים, מִנְהוּר, וגם תיעול, הוא השימוש בפרוטוקול תקשורת המאפשר הכמסה של פרוטוקול אחר בתוכו, באופן בו שדה המטען (payload) של פרוטוקול המעטפת, מכיל למעשה הודעות המקודדות על פי פרוטוקול הליבה. המונחים תיעול ומנהור נובעים מכך שלמעשה נוצרת תעלה או מנהרה מבודדת שבה עוברות הודעות של פרוטוקול הליבה. שימוש בפרוטוקול תיעול מאפשר לדוגמה חצייה של רשתות שאחרת לא היו מאפשרות מעבר של הפרוטוקול לו מבוצעת הכמסה. דוגמת שימוש נפוצה בפרוטוקול תיעול היא הכמסה של פרוטוקול שאיננו תומך בהצפנה באחר שכן, דבר המאפשר את אבטחת ערוץ מעבר ההודעות ללא כל שינוי בהגדרת הפרוטוקול הגלוי.
* אבטחת מידע - SSL/TLS הוא פרוטוקול ורסטילי שמטרתו אבטחת שיחת שרת/לקוח בשיטות קריפטוגרפיות חזקות והוא אמור למנוע ציתות, זיוף, או חבלה (שינוי זדוני) של המידע העובר בין השרת והלקוח. מאפשר חיבור אנונימי, אימות שרת (חד-צדדי) או אימות דו-צדדי, תוך שמירה על דיסקרטיות ושלמות המסרים.
  1. סביבת העבודה (טכנולוגיה)
* שפות התכנות:

האפליקציה עצמה כתובה בפייתון

* סביבות פיתוח:

Visual Studio Code

* 1. מבט טופולוגי
  2. מבט מודולרי
  3. פירוט מודלים עיקריים

1. תסריטי בדיקה
   1. דגשים בבדיקה
   2. תסריטי בדיקה עיקריים
2. רפלקציה
   1. לוח זמנים מוערך לניהול הפרויקט:

|  |  |
| --- | --- |
| נובמבר |  |
| דצמבר |  |
| ינואר |  |
| פברואר |  |
| מרץ |  |
| אפריל |  |

* 1. אתגרים ותרומה אישית
  2. תובנות

1. הוראות התקנה ותפעול
   1. תצורה ודרישות קדם

* שימוש במערכת הפעלה Windows
* Python 2.7.9 Installed
* Flask, jwt
  1. התקנה

1. ביבליוגרפיה

במהלך כתיבת הפרויקט הסתמכתי על מספר מקורות מידע:

* ויקיפדיה : <https://en.wikipedia.org/wiki/HTTP_tunnel>
* GitHub
* YouTube (PyQt4 Learning)

1. נספחים