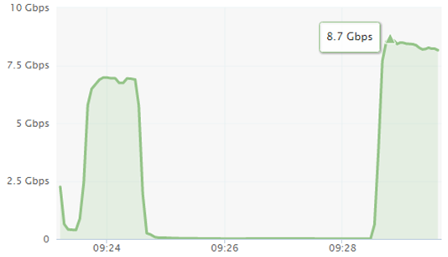
DoS and DDoS Attacks

התקפות DoS ו DDoS:

התקפות DoS הן התקפות על שרתים ומטרתן למנוע שירות (Denial of Service). בצורה פשוטה, נוכל לומר שהתגנבות למקור השרת וחבלה בחוטים - או אפילו הוצאת תקע החשמל מהשקע היא תקיפת מניעת שירות, אך בהקשר האינטרנט ואבטחת המידע, אנו עוסקים בעיקר בתקיפות המתרחשות מרחוק ולא על ידי חבלה פיזית. התקפות DDoS הן התקפות דומות ואף אותן התקפות, והכוונה שלהם הוא מופץ - Distributed, כלומר שההתקפה מגיעה לא ממקור אחד, אלא ממספר רחב של תחנות קצה – לרוב מופעלות על ידי התוקף בצורה של מעין וירוס הנמצא על תחנות קצה אלו. לרוב התקפות ה DDoS הן הרבה יותר חזקות ומשמעותיות. חשוב להבין כי גם התקפה המגיעות על ידי 2-3 תחנות קצה, בדרך כלל עדיין נחשבת כהתקפת DoS, מאחר ואין באמת הצפה משמעותית של השרת.

את התקפות ה DoS ו DDoS נוכל לחלק ל2 סוגים:

* התקפות המציפות ומעכבות את השירות.
* התקפות המשביתות לגמרי את השירות (ובה נרצה להתעסק בפרוייקט).

כרגע נכליל את שתי סוגי ההתקפות להתקפות DoS ו DDoS באופן כללי, ונפצל את סוגי ההתקפות לסוגים שונים עיקריים, על פי מודל שבע השכבות (OSI):

1. התקפות בשכבת ה Application.  
   התקפות בשכבת האפליקציה לרוב מיוצרות על ידי בקשות Post. גם הן מחולקות לתת פרוטוקולים בשכבת האפליקציה - http / https.  
   Http Post Flood - יוצרים כמות גדולה מאוד של מתודות post מהשרת, עד כדי כך שהוא אינו מספיק לענות לכולן ולכן שירות למשתמשים האמיתיים של השרת נפגע.  
   Https Post Flood - זוהי הצפה של מתודות Post שעוברות ב SSL Session. מטרת ה SSL היא לקחת כל הודעה, לפענח את ההצפנה שלה ולוודא שהיא אכן ההודעה שהייתה אמורה להגיע. הצפה של מתודות אלו תפגע בשירות.  
   Http Get Flood – התוקף יוצר כמות ענקית של בקשות Get. השרת צריך לנתח את כולן ולהחזיר מידע. יש המבחינים בהתקפה זו כהתקפה בשכבת ה Transport, מאחר והשרת צריך לשלוח נתונים אל המשתמש / תוקף. כלומר, התעבורה ופס הרשת מוצף. אופן מניעת השירות תלוי בהספק השרת – אם הוא אכן מצליח לעמוד בכמות עצומה של בקשות – התעבורה תיפגע, ואם אינו מצליח, מראש הבקשות אשר הוא מקבל ממשתמשים אמיתיים לא יטופלו.  
   Https Get Flood – הצפה של בקשות Get בפרוטוקול Https מצריך עבודה רבה מה SSL Session לטובת פיענוח ההודעות המוצפנות ומכאן העומס והחבלה בשירות.
2. התקפות DoS בשכבת ה Transport.  
   הצפות בשכבת התעבודה מתאפיינות בעיקר בפקטות אשר השרת מקבל ונדרש לתת שירות ולענות אליהן – בדרך של שליחת Data מתבקש או פקטת מענה.  
   Syn Flood – בהתקפה זו התוקף מנצל את עקרונות ה TCP שאליהן השרת תמיד רוצה להגיע. כאשר שרת מקבל פקטת Syn, עבורו זוהי בקשה מלקוח לפתיחת קשר, והוא הרי מחוייב למענה ועליו להחזיר ללקוח אישור Syn – Ack. כל הודעת Syn מצריכה מהשרת עבודה, לנתח את הפקטה (להבין מי פנה אליו, לחשב Csum) ואז ביכולתו להשיב, מכאן שהצפת הודעות כאלו גורמות להאטה ופגיעה ביכולת השירות של השרת.  
   Rst Flood – בדומה ל Syn Flood, התוקף מנצל את עקרונות ה TCP ובראשם תקשורת אמינה. במצב שהסוקט נסגר \ מצב שאחד מהצדדים ניתק את הקשר אך לא כל המידע עבר (ובעוד מספר מצבים), מופיע בפרוטוקול TCP פקטת עם דגל Rst. לפיכך, הצד השני עדיין רוצה להמשיך את החיבור (מאחר ולא התקיים תהליך סגירת קשר), ושולח פקטה עם דגל Rst ומכאן עליהם לפתוח קשר מחדש. בדוצה להצפת פקטות Syn, גם הצפת פקטות Rst דורש מהשרת עבודה רבה ובהצפה עצומה גם למניעת שירות.
3. התקפות DoS בשכבת ה Network.  
   בהתקפות DoS בשכבת הרשת, התוקף שולח כמות גדולה של פקטות כדי להעמיס את רוחב הפס ולמצות את משאבי הרשת. משאבי הרשת יכולים להיות נתבים, חומות אש ושרתים, וכמובן שיכולתם סופית.  
   ICMP Flood – פרוטוקול ICMP משמש בדרך כלל עבור הודעות שגיאה ולא להחלפת נתונים בין מערכות. הצפה של הודעות מפרוטוקול ICMP – לדוגמא ping, נועדות כדי להעמיס את רוחב הפס של הרשת.

APDoS:

זוהי התקפה המשלבת התקפות Dos ו DDoS שונות ורבות ומבוצעת על ידי גורמים עוינים רבים לאורך זמן. במידה מסויימת היא מייצגת את התקפת מניעת השירות הגרועה ביותר שיכולה להתרחש. הרעיון העומד מאחוריה, הוא שילוב של התקפות רבות מתקחות קצה רבות, ולאורך זמן, ומכאן שמה – Advanced Persistent DoS. בהתקפה זו התוקפים לרוב עוברים בין מספר תחנות על מנת ליצור הסחת דעת של הגנות DoS, אך מתרכזים בקורבן אחד ראשי בארגון.