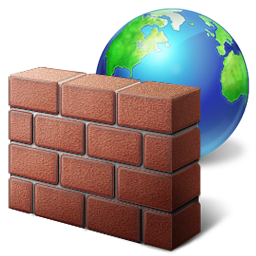
tfשיעור 6 – UDP

**תרגיל: ככה בונים חומה**

בתרגיל זה נכיר את רכיב ה-Firewall (חומת אש), המאפשר לנטר ולשלוט על התעבורה הנכנסת והיוצאת מהמחשב שלכם, ובכך להגן עליו מפני תוכנות זדוניות, תקיפות של האקרים ותכנים בלתי ראויים.

**אז מה זה Firewall בעצם?** 

Firewall (חומת אש) הוא רכיב תוכנתי או חומרתי שמטרתו להגן על מחשב או רשת ע"י ניטור ובקרה על התעבורה היוצאת ונכנסת ממנו (בניגוד לתוכנת אנטיוירוס למשל, שמתעסקת יותר בזיהוי קבצים זדוניים שנמצאים בזיכרון של המחשב). ה-Firewall באופן בסיסי עובר על כל חבילת מידע שנשלחת מהמחשב ואל המחשב, ומחליט האם היא תקינה וניתן להעביר אותה הלאה למערכת ההפעלה.

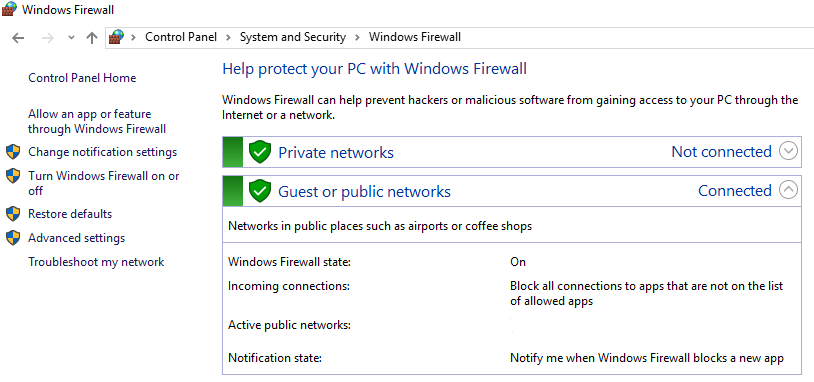
ה-Firewall משמש גם כתוכנת אבטחה למחשבים אישיים, אבל קיימים גם מוצרים מתוחכמים יותר שמקבלים תעבורה של רשת ארגונית שלמה ושומרים על כל המחשבים שנמצאים מאחוריה, וגם יודעים להגן מפני התקפות על שרתים של ארגון, כמו התקפות DDoS. הרכיב יכול לנתח את התעבורה על שלל השכבות שלה (לסנן לפי סוגי אפליקציות, תוכן שמועבר, פורטים, כתובות IP ועוד), אך בתרגיל זה נתמקד בסינון לפי פורטים.

ה-Firewall בעצם עובד עם חוקים – כל חבילת מידע או סשן תקשורת נבדק אל מול החוקים השונים של התוכנה, ובמידה והחבילה מתאימה לחוק כלשהו (למשל, חבילת HTTP מתאימה לחוק "תחסום את כל התעבורה מפורט 80"), אז הפעולה המתאימה מתבצעת.

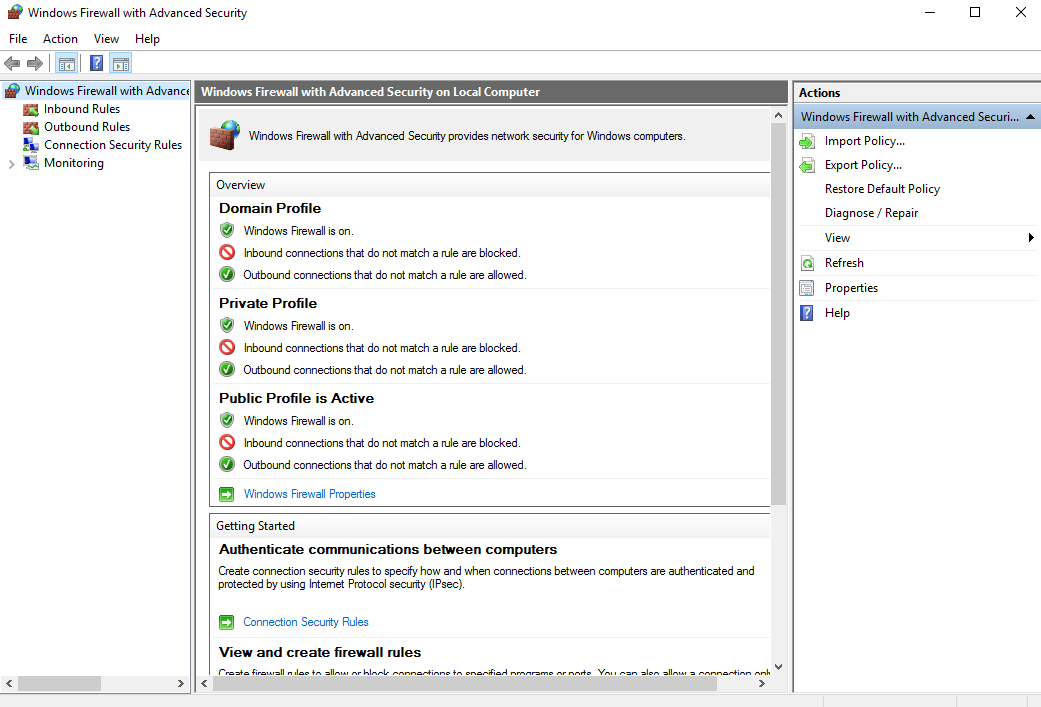
**איך מתקינים Firewall ומגדירים חוקים?**

כבר מותקן לכם Firewall על המחשב!

מחשבי Windows באים עם תוכנת Firewall בסיסית מותקנת, הנקראת בשם המקורי Windows Firewall. ניתן להגיע לתוכנה דרך Control Panel -> System and Security -> Windows Firewall. לחלופין אפשר לכתוב **firewall.cpl** במסך Run. אמור להיפתח לכם מסך כזה:

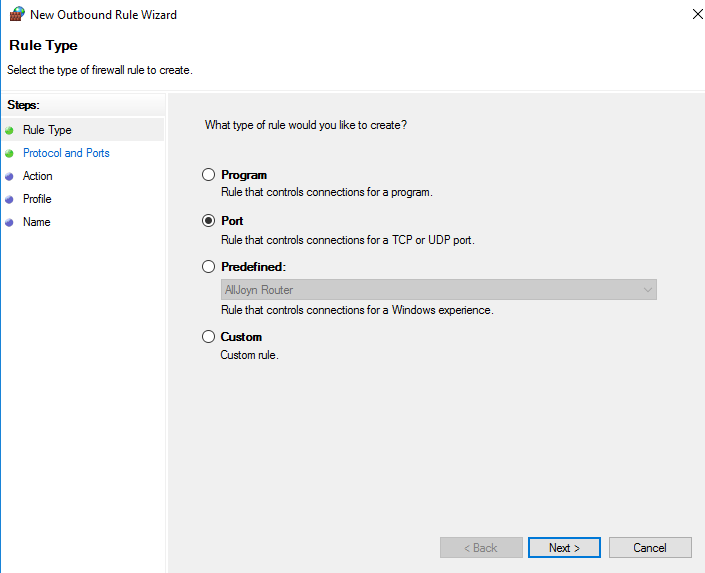


כדי להגדיר חוקים ספציפיים וללמוד יותר לעומק על התוכנה, ניכנס ל-Advanced Settings בצד שמאל. יפתח המסך הבא:

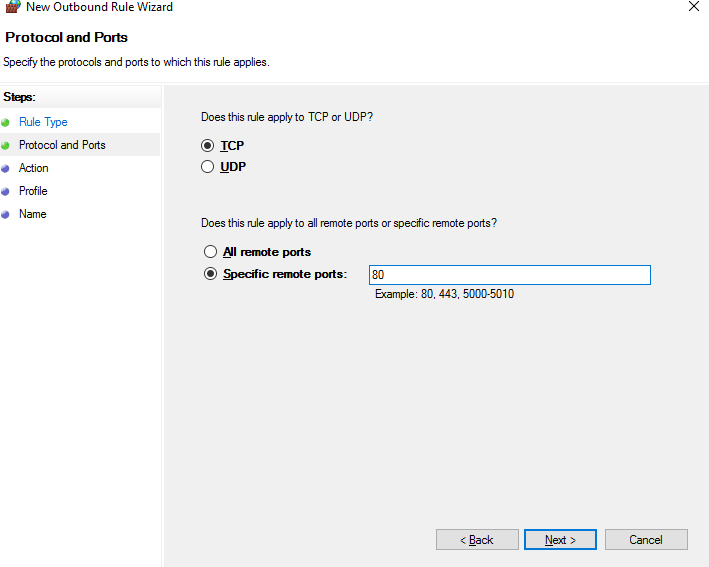


בחלון הראשי ניתן לראות את ההגדרות הכלליות של ה-Firewall שלנו, שמכילות את הפעולות הדיפולטיות שמתבצעות עבור חבילות מידע שלא מתאימות לאף חוק. ניתן לראות למשל שחיבורים נכנסים למחשב נדחים אלא אם כן הם מתאימים לחוק מסוים, בעוד שחיבורים יוצאים מהמחשב מאופשרים אלא אם כן הם מתאימים לחוק מסוים. אלו הם שני סוגים של הגדרות שמופיעות באופן נרחב בעולם אבטחת המידע ועולם המחשוב באופן כללי – **Black List או White List**. רשימה שחורה היא מצב בו דיפולטית אנחנו מאפשרים לכל התעבורה לעבור, פרט למי שנמצא ברשימה השחורה שלנו. רשימה לבנה היא ההפך – אנחנו חוסמים את כל התעבורה פרט למי שנמצא ברשימה הלבנה שלנו.

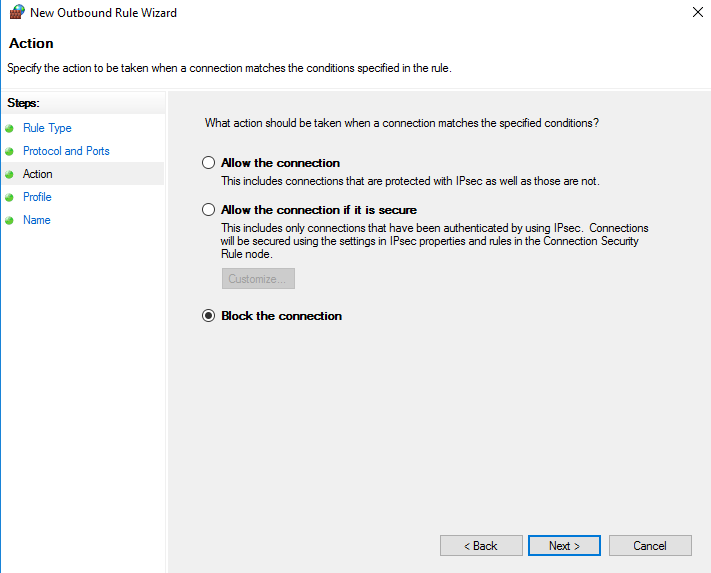
כדי להגדיר חוקים לתעבורה היוצאת מהמחשב שלנו ניכנס ל-Outbound Rules ואז יוצגו על המסך כל החוקים שכרגע פועלים בתוכנה. נלחץ בצד ימין על New Rule כדי ליצור חוק חדש:



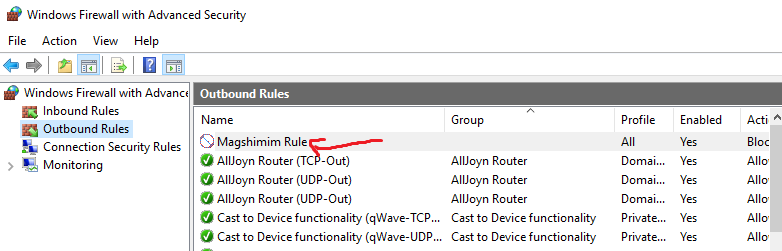
כדי לבצע חסימה על בסיס פורט, נבחר בחוק מסוג "Port" ונלחץ על Next:



במסך כעת נוכל לבחור איזה פרוטוקול בשכבת התעבורה נרצה שהחוק יהיה תקף לגביו (בדוגמה הזאת נבחר לחסום את פורט 80, ולכן נבחר ב-TCP ונרשום את פורט 80).   
שימו לב: remote port = פורט בצד השרת.

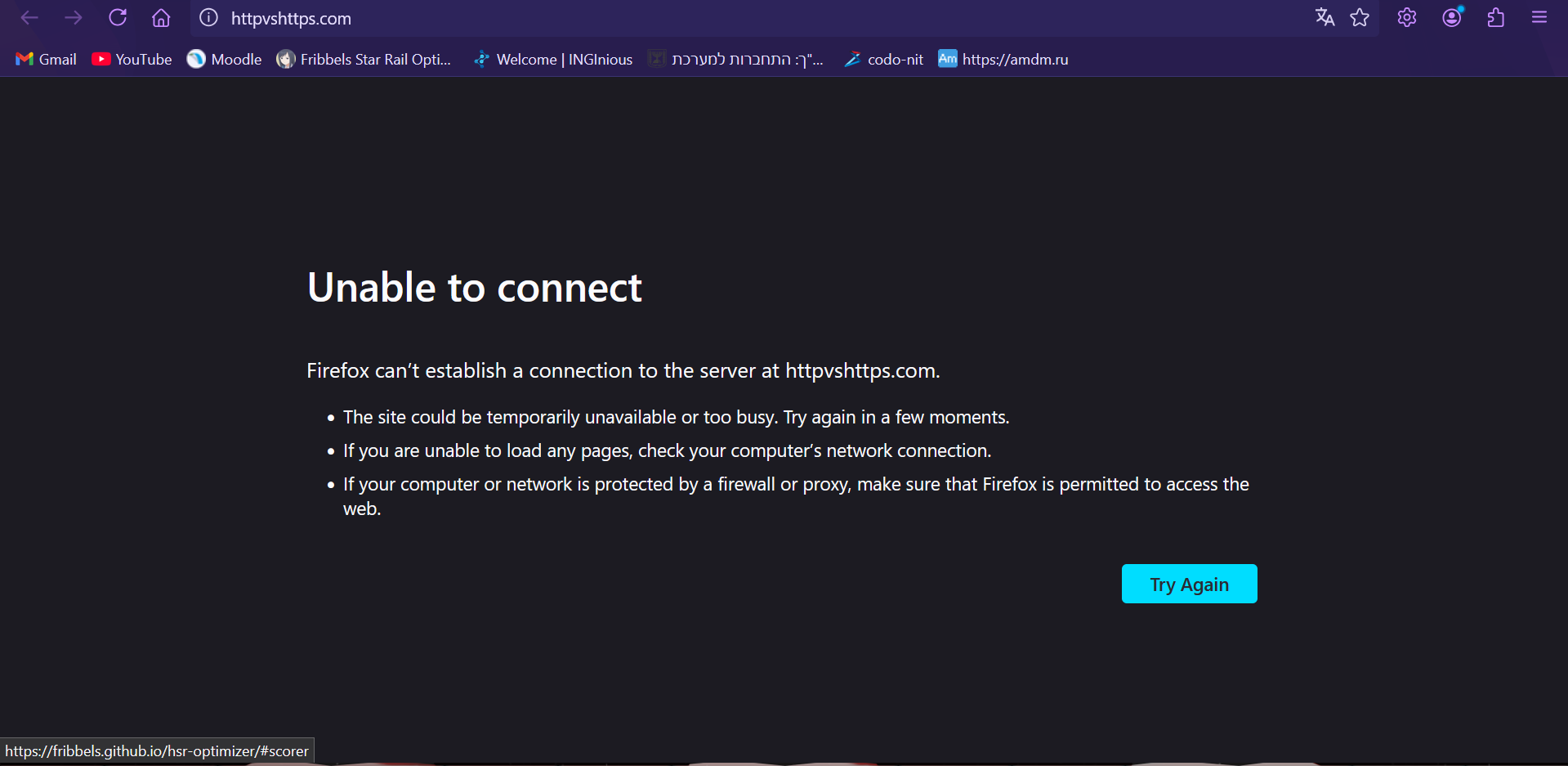


כעת ניתן לבחור מה יקרה לחבילות מידע שיוצאות מהמחשב עם ה-dstport שבחרנו, ואנחנו נגדיר שחבילות מהסוג הנ"ל ייחסמו. שני החלקים האחרונים של בניית החוק הם הגדרה באילו רשתות החוק יפעל (נבחר את כולן) ובחירת שם לחוק (נבחר שם מגניב). לבסוף נלחץ Finish כדי לאשר את החוק. כעת נוכל לראות אותו ברשימה החוקים שלנו:



## כתיבת חוק ראשון

1. כנסו ל-Firewall שלכם ובנו חוק חדש שחוסם תעבורת HTTP יוצאת מהמחשב, בדומה לדוגמה.
2. העתיקו את הכתובת הבאה לדפדפן: <http://httpvshttps.com>   
   מה קרה? צרפו צילום של התוצאה.

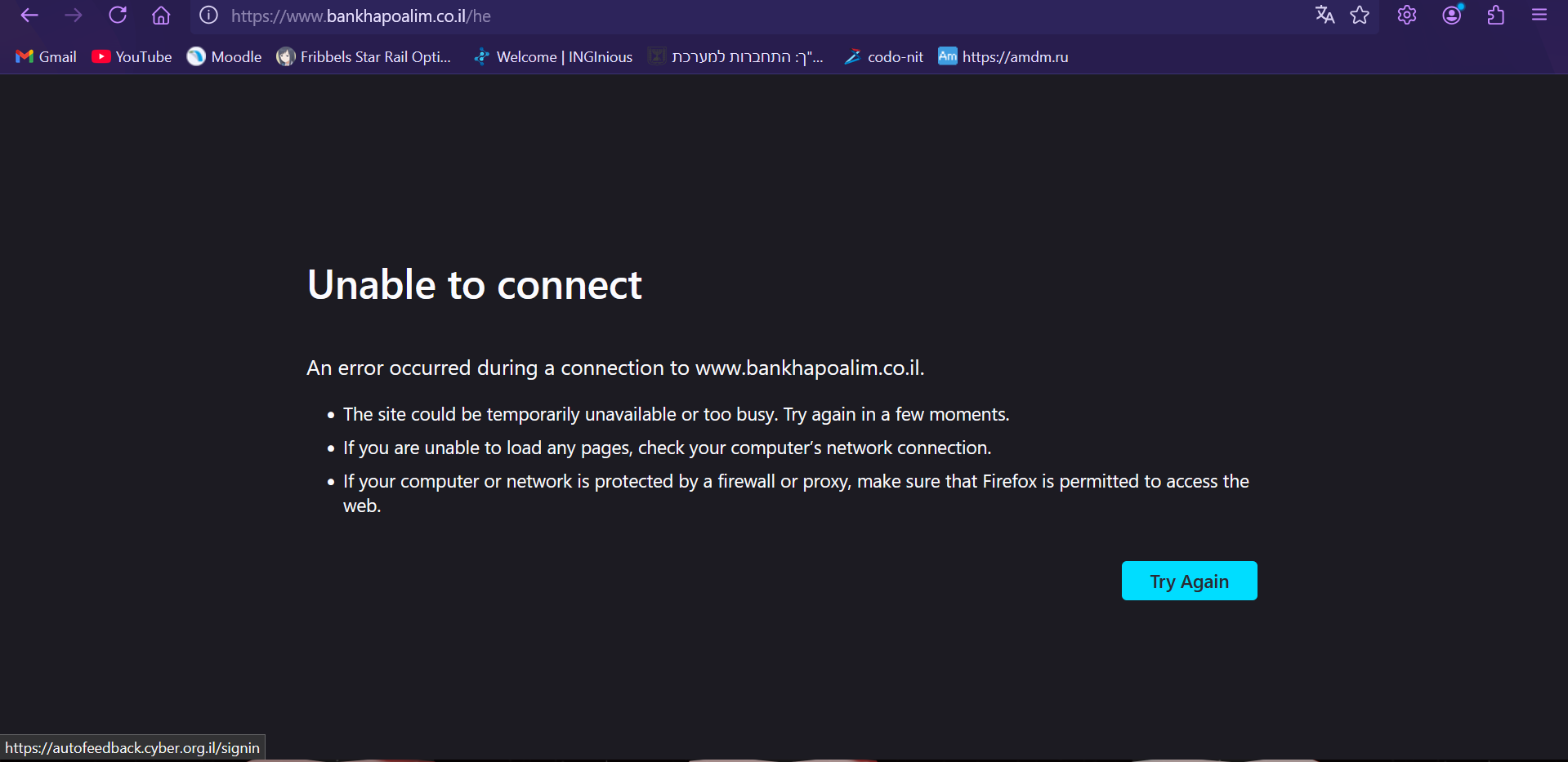


1. כעת, נסו להיכנס לאתר של בנק הפועלים ע"י העתקת הכתובת הבאה: [https://www.bankhapoalim.co.il](https://www.bankhapoalim.co.il/). הצלחתם?

נסו להסביר מדוע קיים הבדל בין שני האתרים (רמז – **Wireshark** זה לא בושה):

| כי אנחנו סגרנו את אפשרות להיכנס לכול האתרים שמשתמשים בhttp והבנק הפועלים פועל בhttps |
| --- |
| *תשובה* |

1. כעת, צרו חוק נוסף כך שגם האתר של בנק הפועלים ייחסם וודאו שהוא אכן חסום. צרפו צילום של השגיאה בדפדפן



## חסימת DNS

1. בטלו את החוקים שיצרתם בשאלה הקודמת (מקש delete במקלדת).
2. כעת, חסמו את תעבורת ה-DNS היוצאת מהמחשב שלכם בעזרת חסימת הפורט הרלוונטי.
3. פתחו חלון בדפדפן חדש או באינקוגניטו של כרום (Ctrl+Shift+N).
4. נסו לגלוש לאתר www.cnn.com – הצלחתם?
5. כעת, נסו לגלוש לאתר <http://httpvshttps.com> - הצלחתם?

מד וע הצלחתם לגלוש לאתר אחד אבל לשני לא? (אם שני האתריםנטענו, בצעו טעינה מחודשת עם Shift+F5)

(גם כאן – **ווירשארק** עשוי לעזור לכם להבין מה קורה מאחורי הקלעים...)

| הצלחנו לגלוש לאתר הראשון אך לא לאתר השני בגלל שחסימת פורט dns מונעת תרגום שמות דומיין לכתובות IP, ולכן HTTP מפסיק לעבוד. HTTPS עשוי להמשיך אם כתובת ה-IP נשמרה בcache . |
| --- |

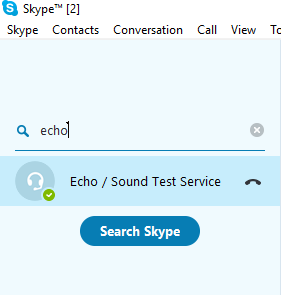
## שרת מגשימייל

כבר נפגשנו עם שרת המייל של מגשימים בשבוע שעבר ושלחנו דרכו מיילים.

צרו חוק חדש מסוג Custom, שיחסום התחברות SMTP לשרת המיילים הספציפי של מגשימים (magshimail.com). כדי לבדוק שהצלחתם, ודאו שהגישה לשרת של מגשימים חסומה אבל גישה לשרת SMTP אחר (למשל mailgw.netvision.net.il) צריכה לעבוד. כיצד עשיתם זאת?  
(שימו לב – כדי לבחור ב-Port של החסימה יש לבחור קודם כל בפרוטוקול TCP)  
תזכורת: על שרת פיזי אחד יכולים לרוץ מספר שירותים. חסימת כתובת IP תחסום את כל השירותים, לא רק SMTP, וזה לא מה שאנחנו רוצים שיקרה.

| לאחר יצירת של החוק החדש שסוגר את כול הsmtp הנכנס, אני נכנסתי לתוך הscope ושם הקלדתי את האיפי של המגשימייל שבקדתי באמצעות nslookup mail.magshimail.com.  את השאר הדברים השארתי אותו דבר. |
| --- |
| *תשובה* |

## סקייפ

1. בטלו את החוקים הקודמים שיצרתם.
2. כעת, במידה ולא התקנתם עדיין, [התקינו את התוכנה סקייפ](https://www.skype.com/en/download-skype/skype-for-computer/), והפעילו אותה. במידה ועליכם לפתוח חשבון חדש, עשו זאת.
3. במסך הראשי של Skype, הקישו echo בשדה החיפוש מצד שמאל.
4. כעת יופיע הפרופיל Echo / Sound Test Service. זהו פרופיל "מזויף" שנועד לבדוק שאתם מסוגלים לבצע שיחה בסקייפ. 
5. התקשרו אל Echo בעזרת הלחצן הכחול מצד ימין וודאו שאתם שומעים את ההודעה המוקלטת.
6. כעת עליכם להבין כיצד לחסום את תעבורת Skype כך שהשיחה ל-Echo לא תעבוד. ניתן להשתמש בכל סוגי החסימה שהפיירוול מציע.  
   כתבו כיצד עשיתם זאת ומה החסימה שנדרשה:

| אני הוספתי 2 חוקים נוספים, אחד סוגר את האיפי של הסקייפ שמצאתי באמצעות הסנפה בוירשרק, החוק השני סוגר את הפורט 53 שעליו פועל הסקייפ, כאשר סגרנו את שני הדברים אלו, הecho הפסיק העבוד. |
| --- |
| *הקש תשובה* |



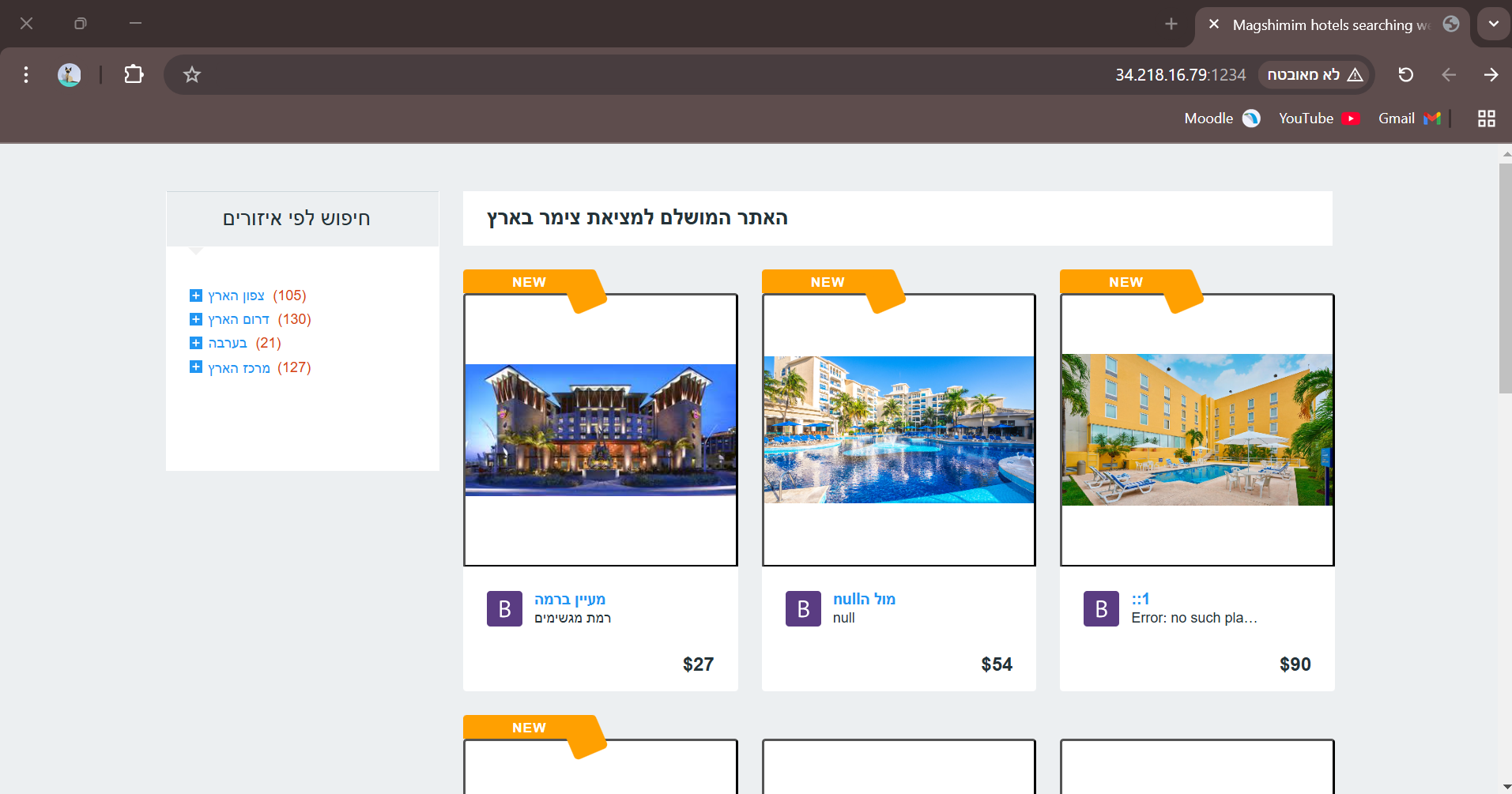
## חוסמים פרסומות!

Ad Blockerהוא סוג של תוכנות אשר מטרתן לחסום פרסומות המופיעות באתרי אינטרנט. המובילה מביניהן היא תוסף דפדפנים הנקרא AdBlock. המנגנון של AdBlock כולל דרכים רבות לזהות פרסומות ולחסום אותן, ביניהן לפי מילים נפוצות (ad למשל), לפי התנהגות בעמוד וגם לפי **רשימות שחורות** של כתובות IP.

בתרגיל הבא עליכם להיכנס לאתר הזמנת הצימרים של מגשימים (<http://34.218.16.79:1234>) ובעזרת הפיירוול של חלונות, להגיע למצב בו לא מופיעות בו כלל פרסומות.

\* שימו לב, אם בדפדפן שלכם פועל כבר חוסם פרסומות עליכם להשעות אותו לפני פתרון התרגיל על ידי לחיצה על Don’t run on pages on this site.

1. אם הצלחתם, צרפו צילום מסך של האתר "הנקי".



1. בנוסף, תארו את החוקים שהוספתם וכיצד גיליתם שיש להוסיף אותם.

| אני הוספתי 2 חוקים, אחד מהם סוגר את כול האיפי של הפרסומות וסוגר את הפורט 1234 הוא הפורט של הרוב הפרסומות, ואז סגרתי את הפורט 80 בחוק אחד והוא הפורט של הפרסומת זזה. |
| --- |
| *תשובה* |

**לאחר סיום התרגיל לא לשכוח למחוק את כל החוקים שהוספנו בפיירוול!!!**