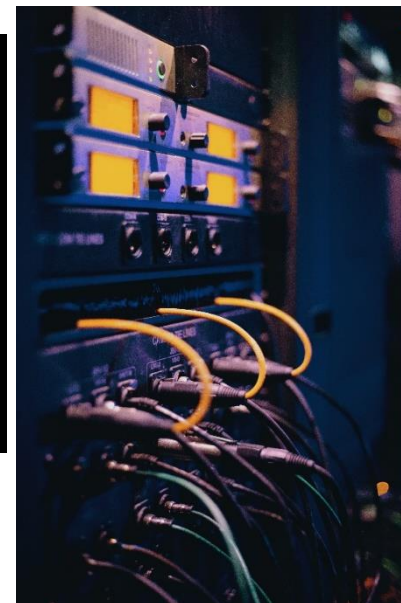


# מושגי ייסוד בסייבר – חלק א



Yosi Shavit MBA, CISM - Information Security & Cyber Expert

Cellular: 058-6662242

Mail: [yosish@gmail.com](mailto:yosish@gmail.com) , [yosish@sviva.gov.il](mailto:yosish@sviva.gov.il)



# נושאי הלימוד

- רבדים בהגנת סייבר, מעגלי אבטחת המידע והסייבר
- מבנה רשת ארגוני, כיצד גולשים לאינטרנט
- כתובות IP – כתובות פרטיות, כתובות ציבוריות
- חומת אש – עקרונות, שימושים
- גישה מרחוק לארגון
- סיסמאות, פריצת סיסמאות
- הזדהות חזקה – מהי הזדהות חזקה, דוגמאות
- הגנה מפני התקפות – IDS , IPS
- ווירוסים – סקירה על סוגי הווירוסים השונים ודרכי התגוננות
- התקפות ZERO DAY ודרכי התגוננות

# רבדים בהגנת סייבר



הגנה פיזית ✓



הגנה לוגית ✓



מודעות עובדים ✓

# הגנה רב שכבתית – מודל ה-PPP

הגנה רב שכבתית – תהליך המשלב שלושה מרכיבים עיקריים:

The PPP Model (3 P's Model)

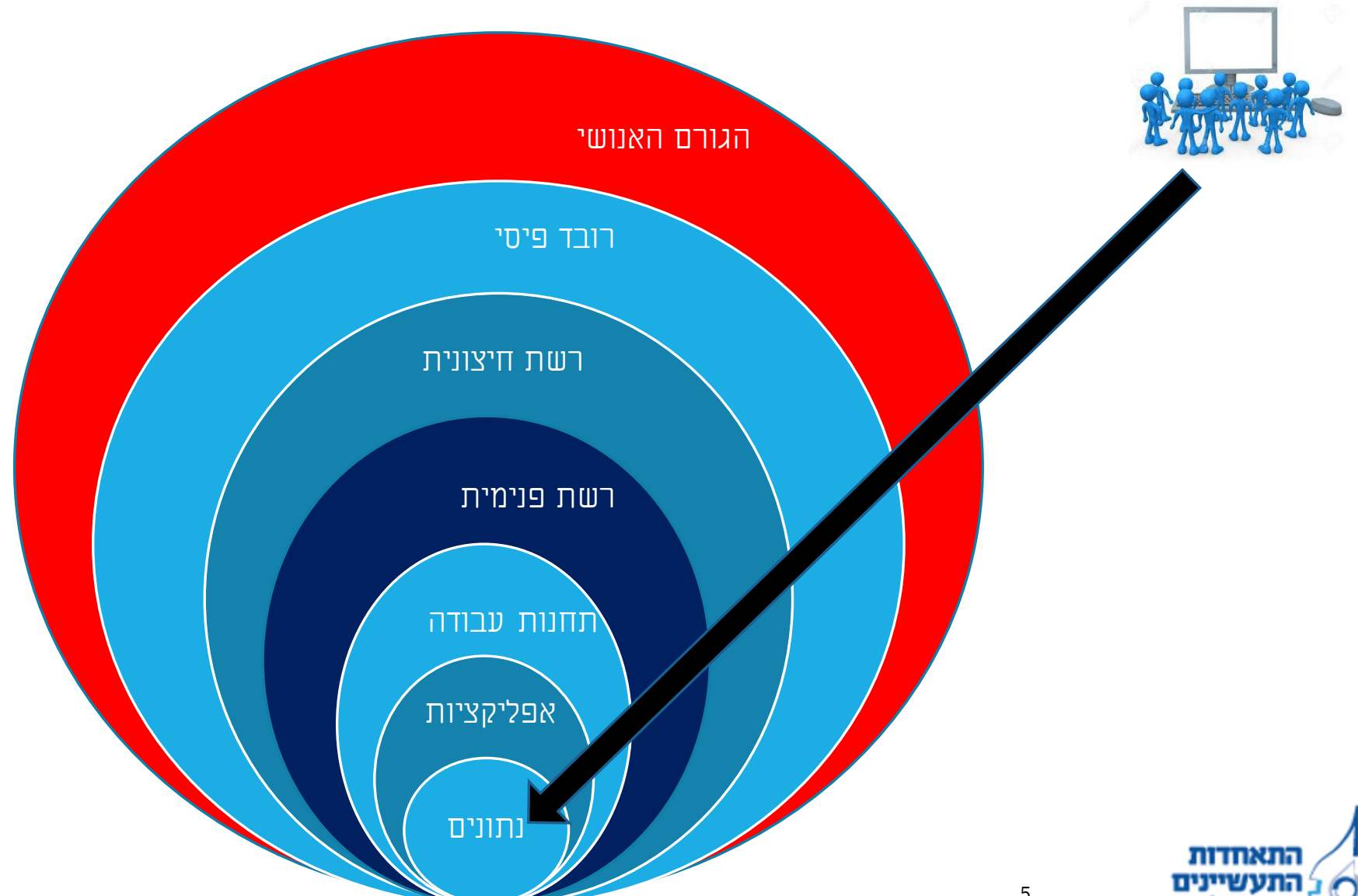
People, Process, Products



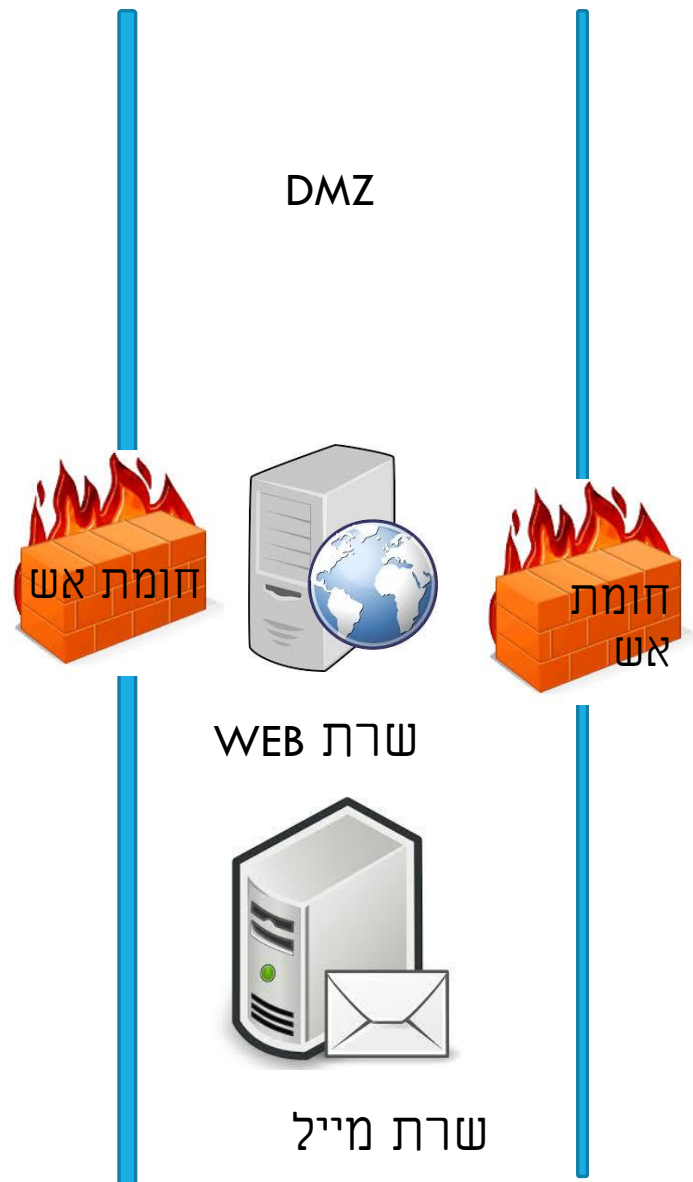
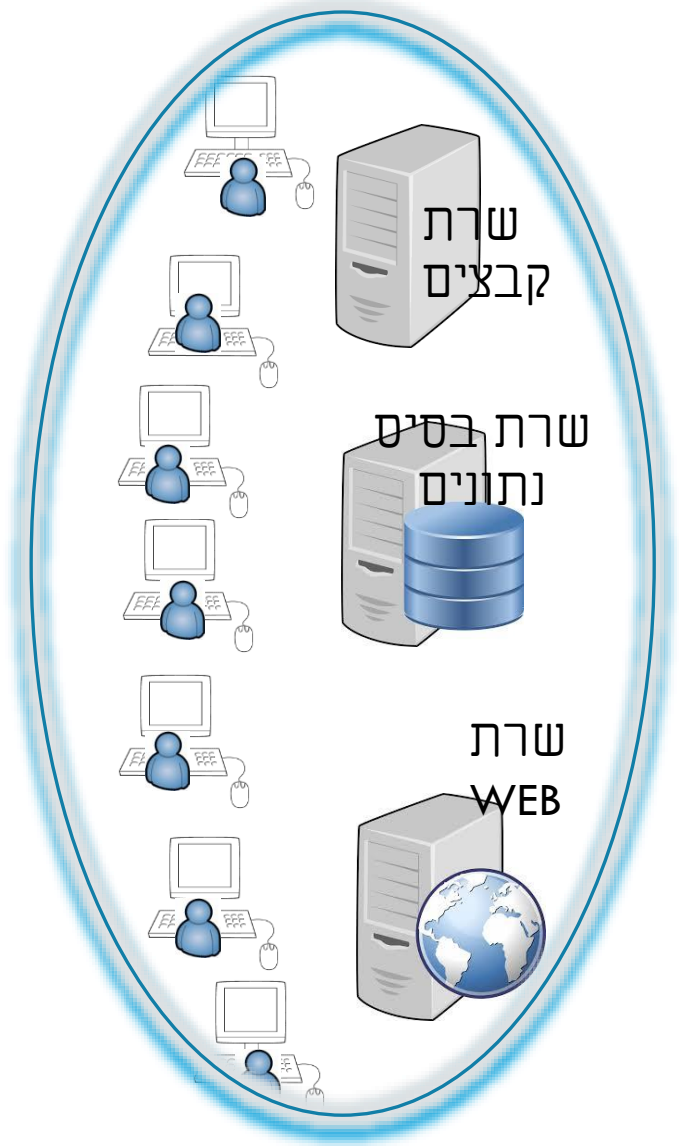
✓ אנשים  
✓ טכנולוגיה  
✓ תהליכים

ניתן למצוא מודל זה גם בראשי התיבות: PPT People, Process, Technology

# מעגלי אבטחת המידע והסייבר

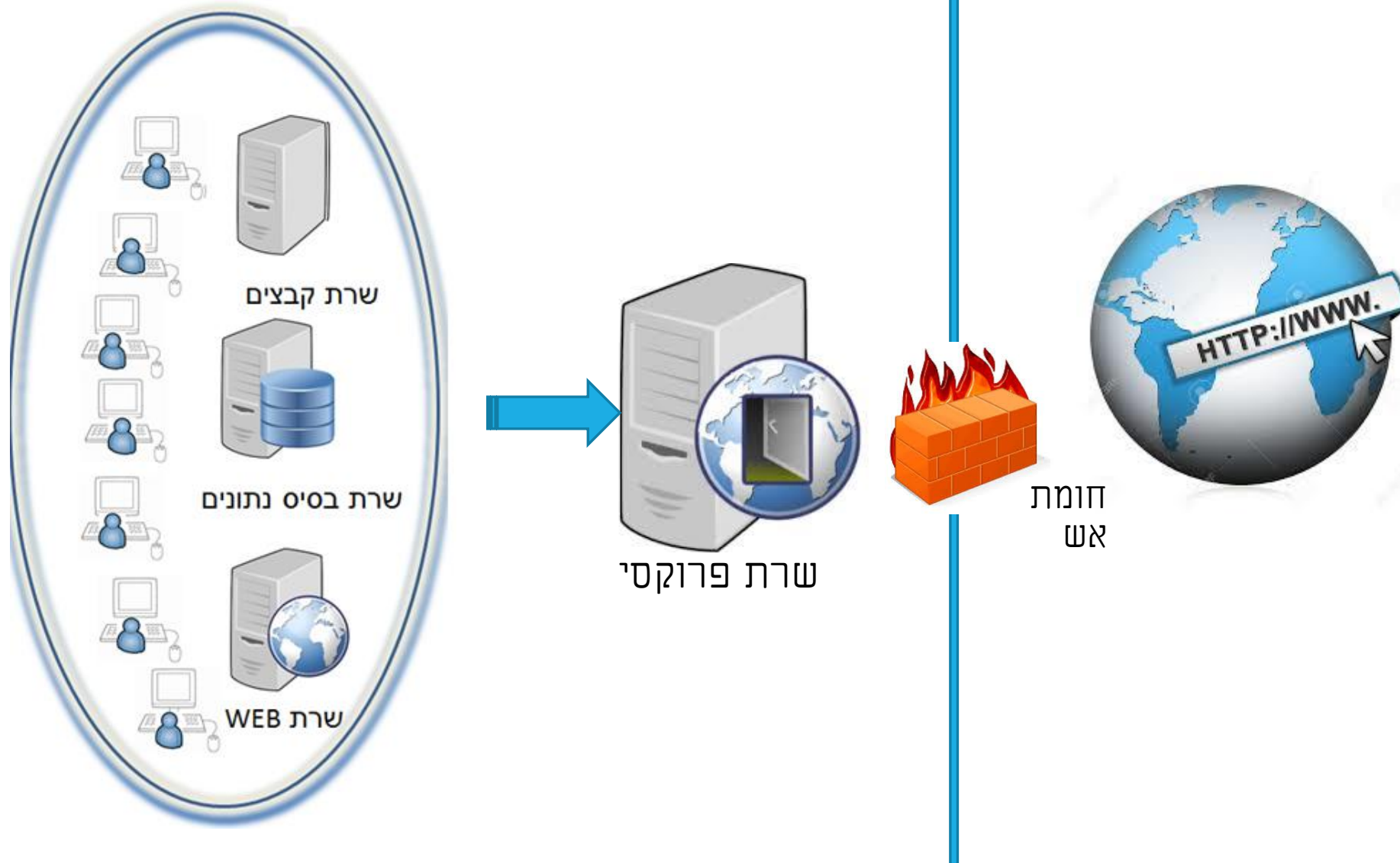


# כיצד נראית רשת ארגונית?





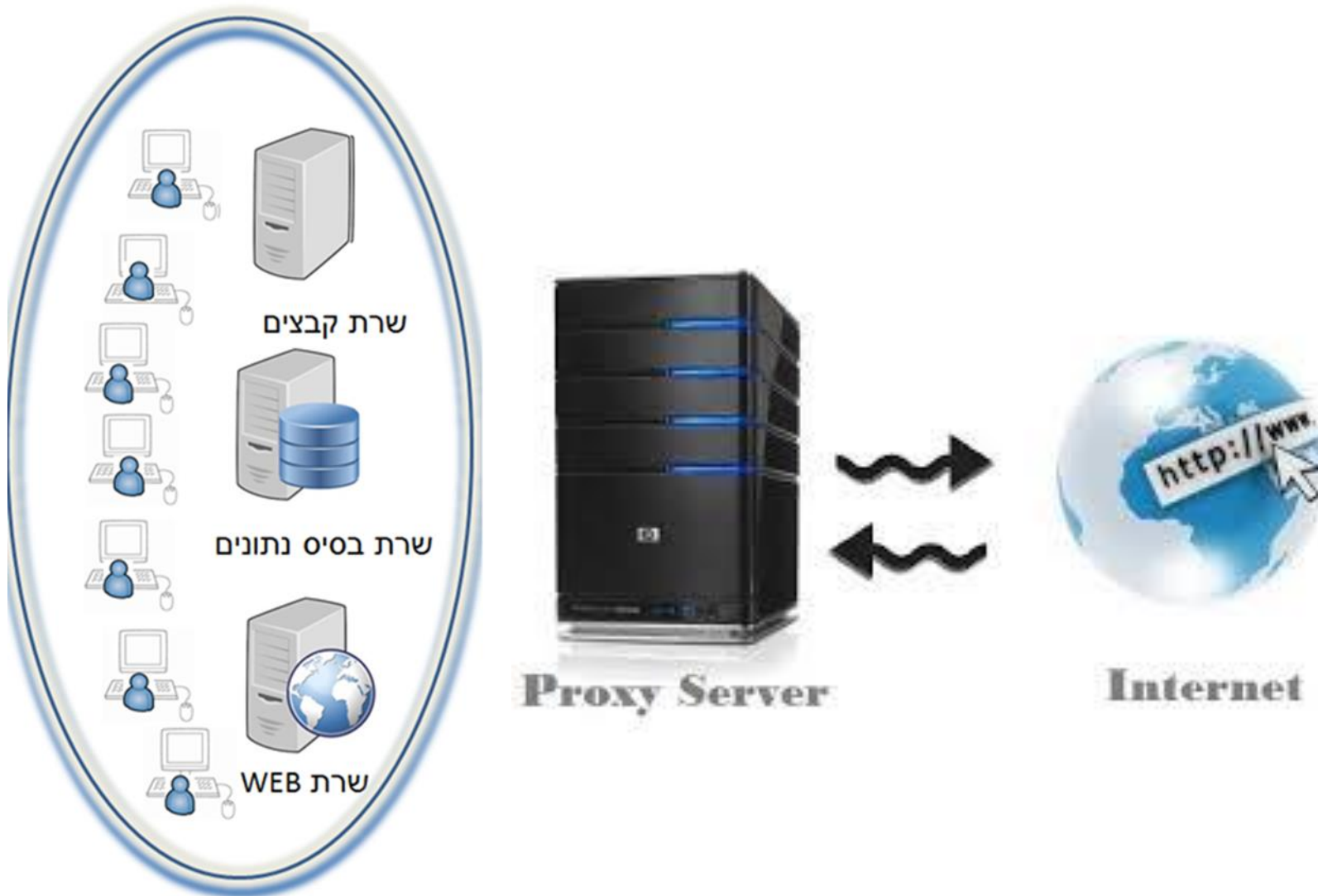
# גלישת משתמשים



# גלישת משתמשים - שרת פרוקסי

מטרות:

- ✓ גלישה מאובטחת - סינון תוכן
- ✓ הסתרת כתובות IP ארגוניות
- ✓ חסכון בכתובות IP ציבוריות



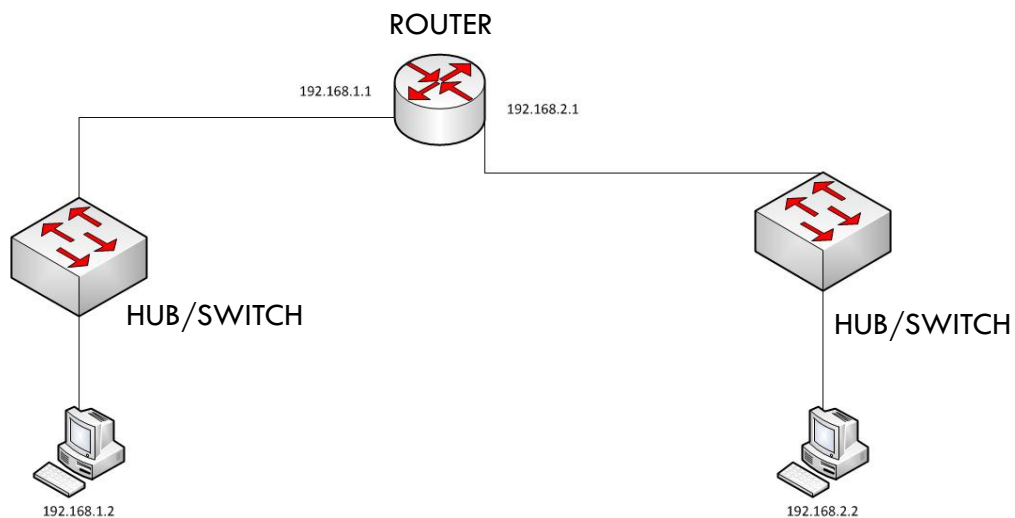


# כתובות IP על קצה המזלג

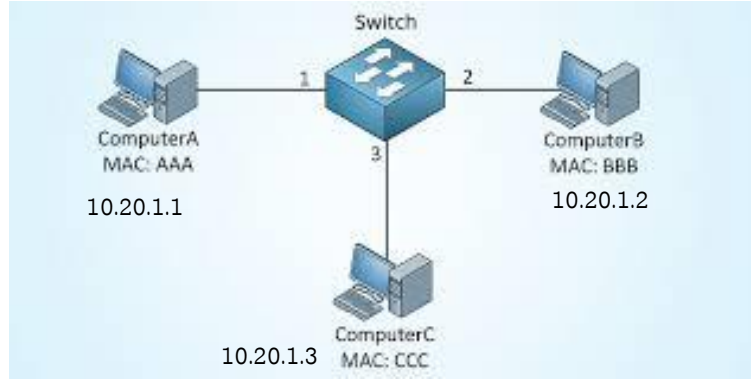


כמה עובדות חשובות לגבי כתובות IP

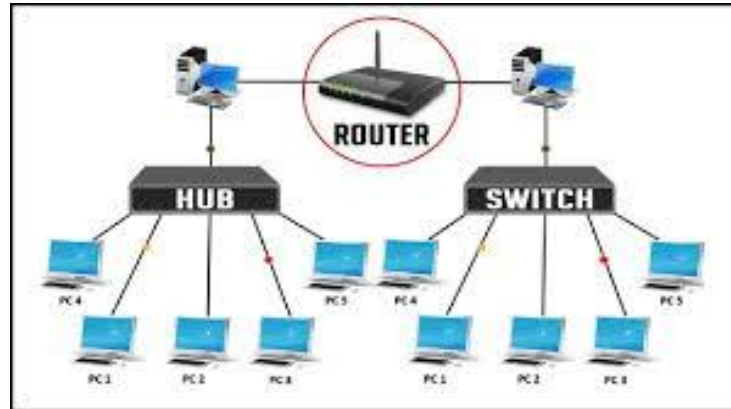
- ❑ כשמחשב א' רוצה להגיע למחשב ב' הוא פונה לכתובת שלו
- ❑ כתובת IP כמוה ככתובת מגורים – חייבים לדעת לאן רוצים להגיע
- ❑ 2 סוגי כתובות IP – פרטית וציבורית



# איך מתבצעת התקשורת?



תקשורת פנים ארגונית  
כתובת IP פרטיות



תקשורת חוץ ארגונית  
כתובת IP ציבוריות

# כתובות IP פרטיות מול ציבוריות

כתובות פרטיות – תחום הכתובות פרטיות (נקבעו ע"י IANA\*)

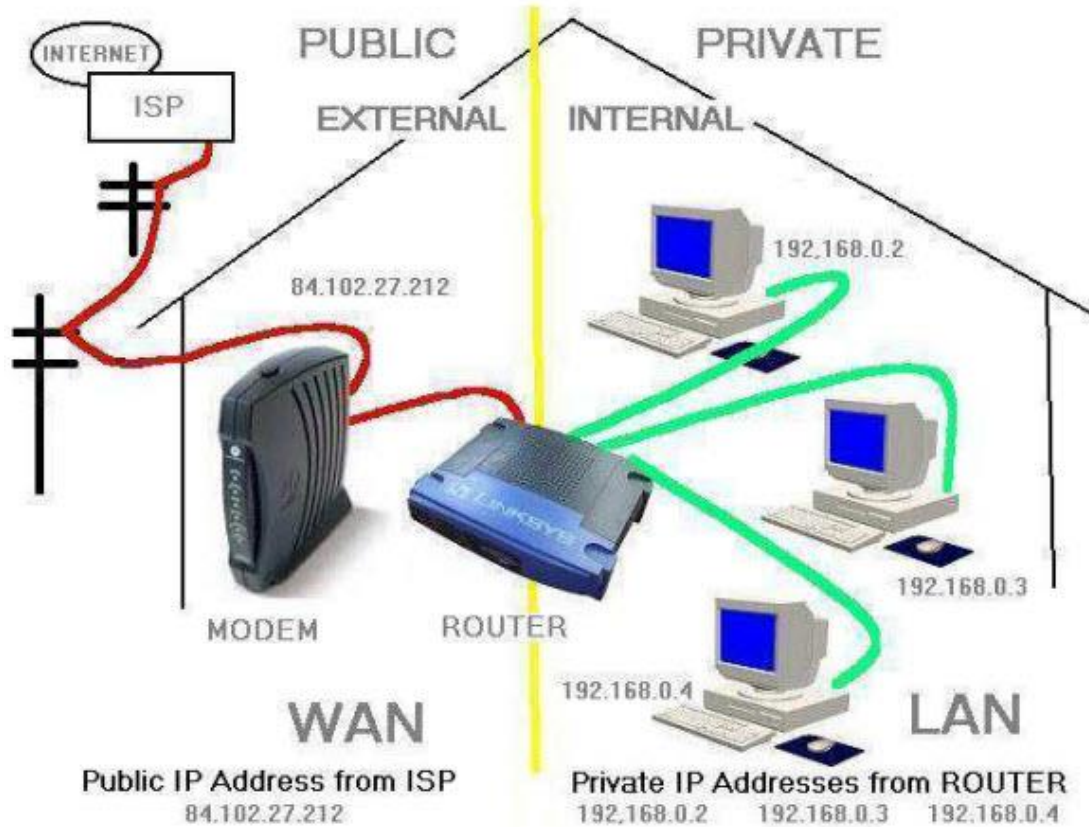
לשימוש בתוך ארגון.  
אין להן אפשרות לצאת לעולם (גלישה, מיילים)  
אין הגבלה במספר הכתובות

מחלקה	מסכת משנה	התחלה	סיום	כמות כתובות ברשת
A	255.0.0.0	10.0.0.0	10.255.255.255	16,777,216
B	255.255.0.0	172.16.0.0	172.31.0.0	65,536
C	255.255.255.0	192.168.0.0	192.168.255.255	256

\*The Internet Assigned Numbers Authority (US-based organization)

# כתובות ציבוריות

כתובות שיכולות להיות מנותבות ברשת יש מספר מוגבל של כתובות בעולם שהולך להיגמר.



## Public IP Addresses

Cisco.com

Class	Public IP Ranges
A	1.0.0.0 to 9.255.255.255 11.0.0.0 to 126.255.255.255
B	128.0.0.0 to 171.255.255.255 173.0.0.0 to 191.255.255.255
C	192.0.0.0 to 195.255.255.255 197.0.0.0 to 223.255.255.255
D	224.0.0.0 to 247.255.255.255 Multicast Addresses
E	248.0.0.0 to 255.255.255.254 Experimental Use

© 2004 Cisco Systems, Inc. All rights reserved.

INTRO v2.0-5-10

# פרוטוקולים – CONNECTION LESS VS CONNECTION ORIENTED

פרוטוקול (Protocol) – זה בעצם הערוץ התקשורת שיכול לבצע תקשורת בין מחשבים

פורט (Port) – זה הכביש – המספר המזהה של הפרוטוקול

שירות (Service) – סוג השירות שנגזר גם מהפרוטוקול

דוגמאות

פרוטוקול	פורט	שירות
HTTP	80	גלישה בדפדפן
HTTPS	443	גלישה בתעבורה מוצפנת



# חומת אש - הגנה ברמת תקשורת

## ברירת מחדל: הכל סגור - אין תקשורת



פורט = כביש

### אז מה בכל זאת מאפשרים?

- ✓ תעבורת מיילים (SMTP) - פורט 25
- ✓ גלישה לאינטרנט (HTTP) - פורט 80
- ✓ גלישה מאובטחת (HTTPS) - פורט 443
- ✓ התחברות מרחוק (RDP) פורט 3389
- ✓ הזדהות לארגון (AD) פורט 389 או 636 (מוצפן)
- ✓ העברת קבצים (FTP) - פורט 21
- ✓ העברת בסיסי נתונים: (SQL) - TCP1433 , UDP1434
- ✓ העברת בסיס נתונים: (ORACLE) - 1521

# חוקים בחומת האש

עוברים ברשימת החוקים מלמעלה כלפי מטה על ש"נופלים" על חוק שמתאים



מקור (Source)	יעד (Destination)	שירות (Port)	מצב חסימה	תיאור (Description)
כולם	לכל מקום	80	מותר	גלישה לאינטרנט
כולם	לכל מקום	25	מותר	מייל
מנהל רשת 10.20.10.1	שרתים במשרד 172.16.1.0	389	מותר	שליטה מרחוק
מנהל בסיס נתונים 10.20.12.3	שרתי DB 172.16.1.5-172.16.1.16	1521	מותר	ניהול בסיס נתונים
כולם	כולם	כל השירותים	אסור	חסימה

## שימוש שני: חציצה בין רשתות בארגון (סגמנטציה)



## שימושים לחומת אש בארגון

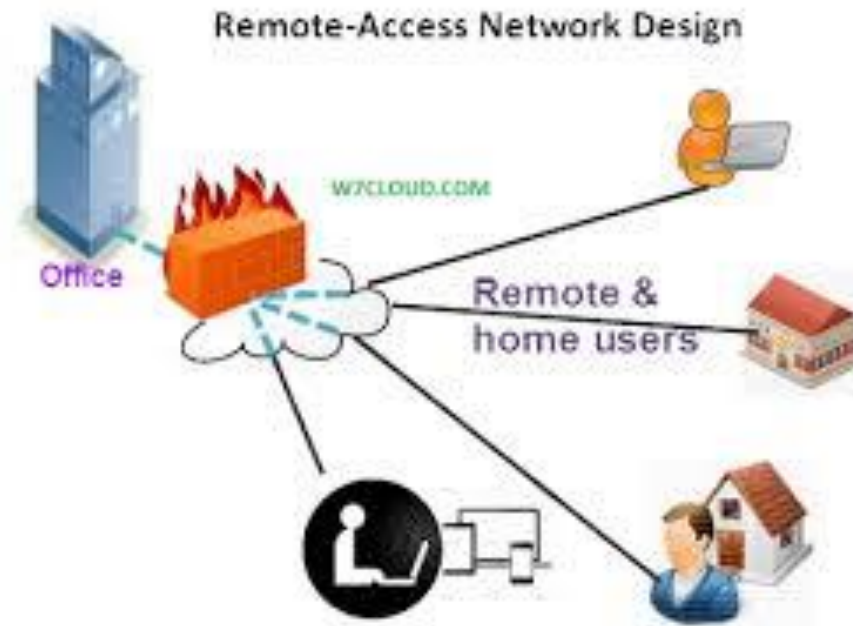
## שימוש ראשון: לאפשר תקשורת בטוחה לאינטרנט



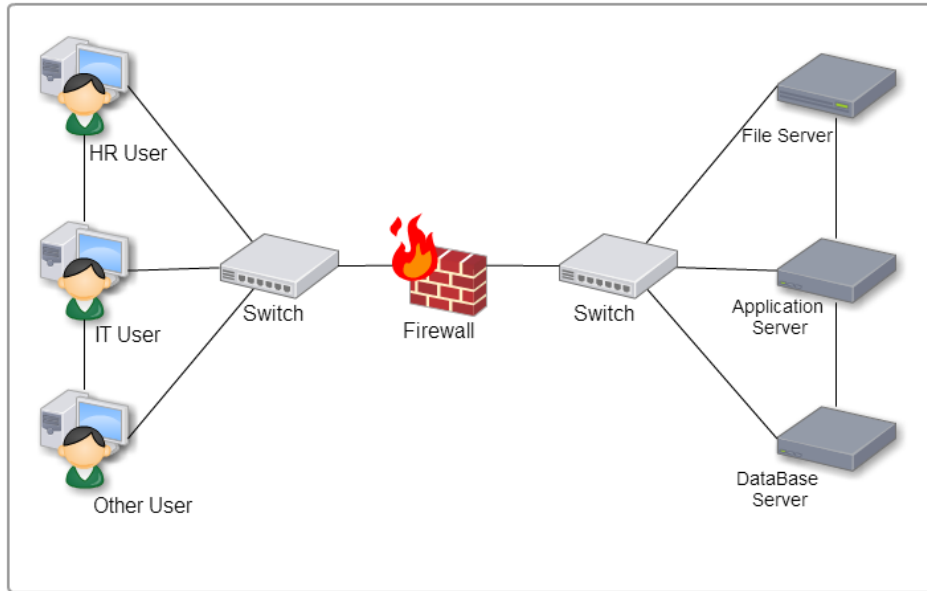
# שימושים לחומת אש בארגון

שימוש שלישי:

גישה מרחוק לארגון – (VPN)

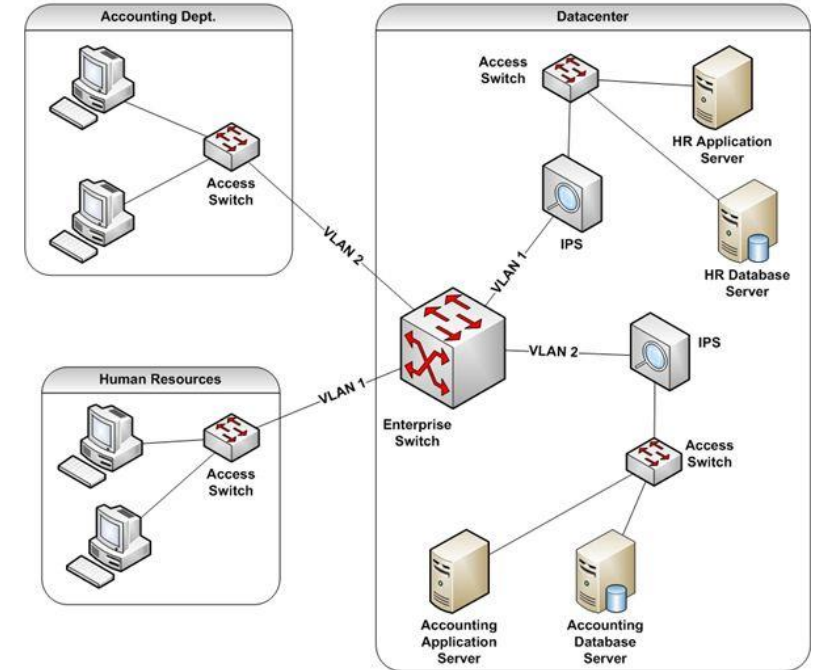


## בין משתמשים לשרתים



רק משתמשים שחומת האש תאפשר להם יוכלו להגיע ישירות לשרתים לצורך תחזוקתם

## בין מחלקות שונות בארגון

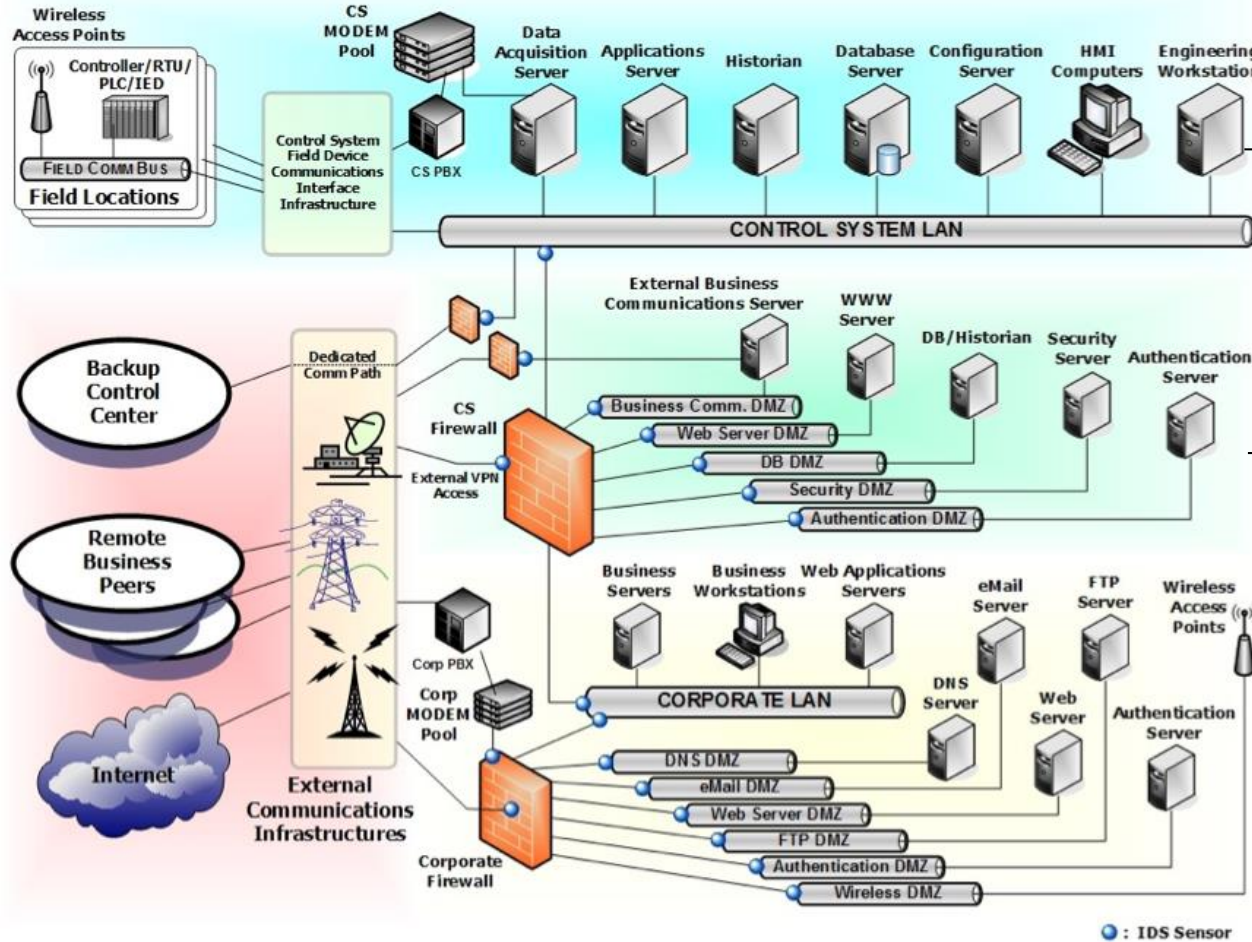


מחשב מהנהלת חשבונות לא יכול ליצור קשר עם מחשב ממחלקת כח אדם אלא אם מאפשר בחומת האש

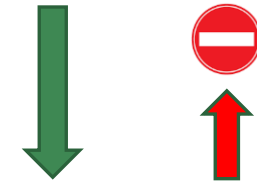


# חציצה - סגמנטציה בעולם ה-OT - (מערכות תעשייתיות)

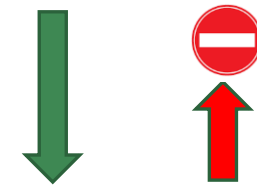
OT – Operation Technology  
ICS – Industrial Control System



רשת ה-OT (ייצור)



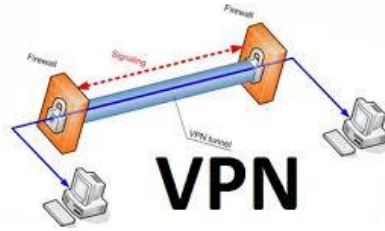
רשת מנהלתית



יציאה לאינטרנט

# גישה מרחוק

לצורך גישה מרחוק נדרשים 3 דברים עיקריים:



1. תקשורת **מוצפנת** מהאינטרנט אל הארגון VPN



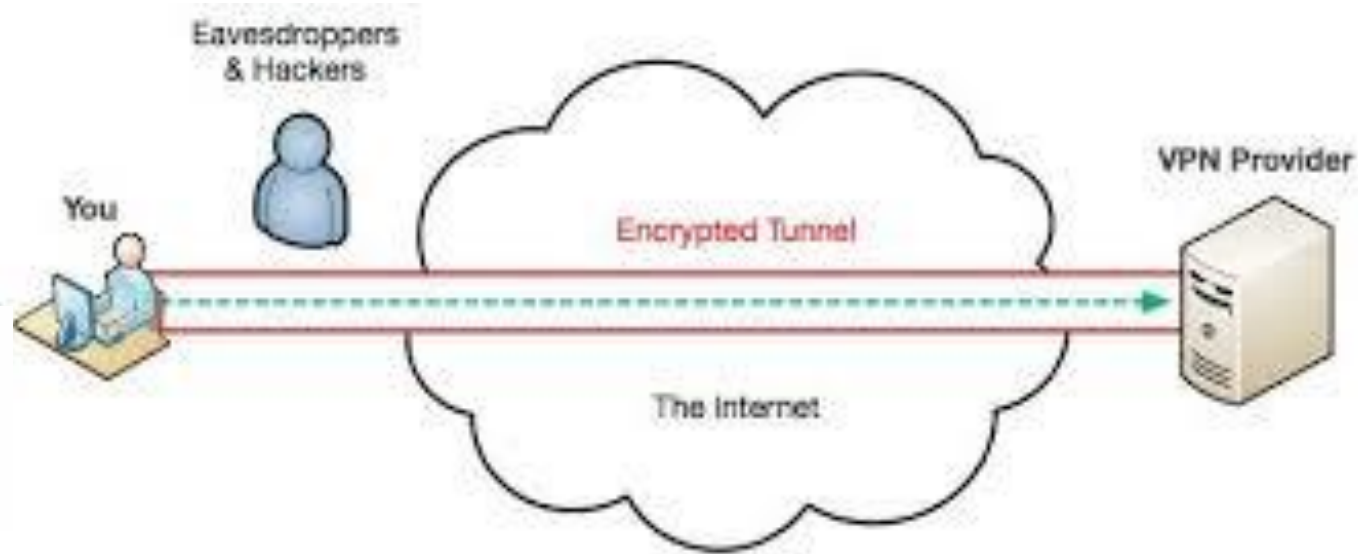
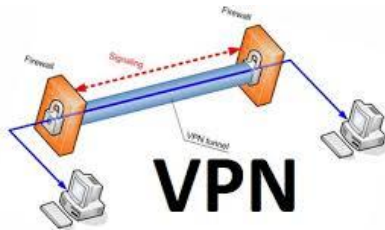
2. זיהוי **חד-חד ערכי** של הגורם הניגש

3. רישום לוגים : מי התחבר, מתי נכנס, מתי יצא, לאיזה מערכות נכנס וכדומה.

שאלה: האם סיסמא מהווה זיהוי חד חד ערכי??

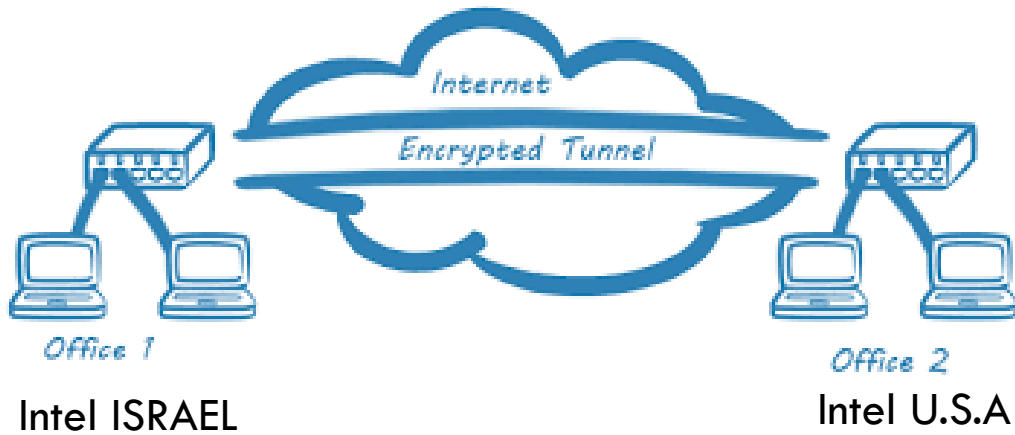
# תקשורת אל הארגון - באמצעות VPN

**VPN = VIRTUAL PRIVATE NETWORK**

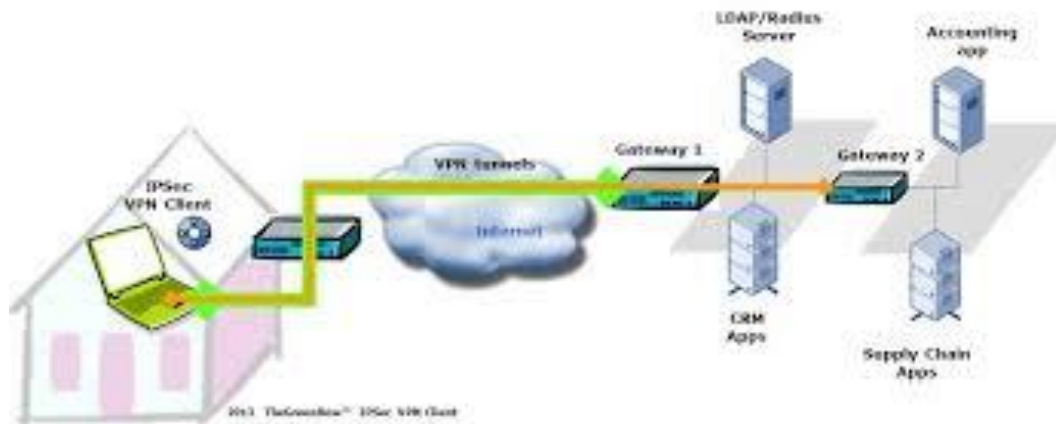


# תקשורת אל הארגון - באמצעות VPN - שימושים

ארגון מפורז על פני שטח גיאוגרפי גדול



גישה מרחוק של משתמשים

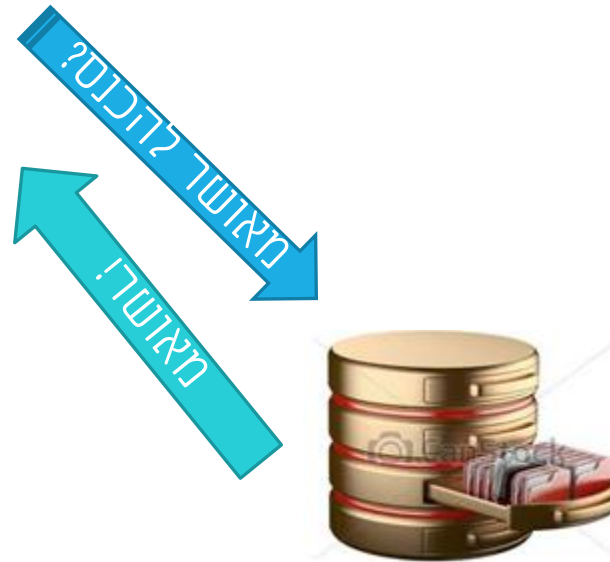


# הזדהות למערכת



שם משתמש: BG105  
 סיסמא: 123456

איך עובדת הזדהות ?



מאושר	סיסמא	שם משתמש
	123123	Uv451
	11qq11	Db633
✓	<b>123456</b>	<b>Bg105</b>
	password	tp423
	-----	-----
	-----	-----



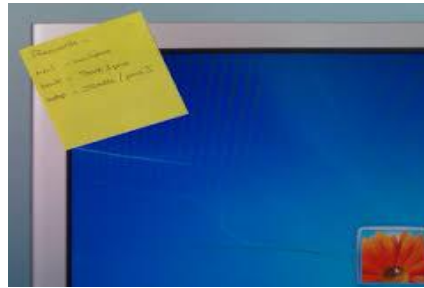
208 הסיסמאות הנפוצות לפי נתונים שנאספו על ידי פורצים טורקיים רוב הסיסמאות נאספו, ככל הנראה, מהומלס ומפיצה האט, יש לא מעט סיסמאות שקשורות לשני האתרים האלה. המידע מבוסס על סט של כ-110,000 סיסמאות, ואפשר להוריד אותו כאן: [files.ranh.co.il/passwords.csv](https://files.ranh.co.il/passwords.csv) (כבר לא.....)

מספר סידורי	סיסמה	מופעים
1	123456	2419
2	1234	1875
3	12345	1115
4	12345678	445
5	123123	218
6	1111	216
7	qazwsx	189
8	1234567	164
9	0	155
10	123	154
11	121212	152
12	1212	139
13	111111	122
14	55555	109
15	pizza	100

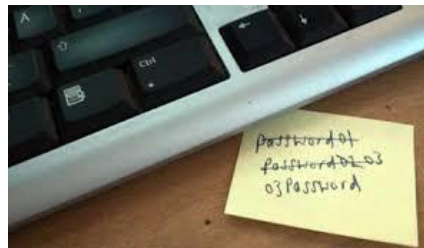
הבעיה:  
שימוש בסיסמאות חלשות



➤ סיסמא קלה



➤ תולים על מסך המחשב



➤ שמים מתחת למקלדת

יש לזכור:

**קיימות טכנולוגיות BRUTE FORCE וטכנולוגיות DICTIONARY מתקדמות לזיהוי סיסמאות ברשת**

פתרון:

- ✓ רצוי מאד 8 תווים אך לא פחות מ- 6 תווים
- ✓ מורכבות סיסמא (אות גדולה, קטנה, מספר, תו מיוחד) 3 מתוך ה-4

דוגמאות לסיסמאות שקל לזכור וקשה לפרוץ:



P@55w0rd  
Pשדד'סרג

# הפתרון: הזדהות חזקה



הזדהות ב-2 רמות (2 Factor Authentication)

הזדהות ב-3 רמות (3 Factor Authentication)

רמה I – משהו שאתה יודע – **Something you know**

רמה II – משהו שיש לך – **Something you have**

רמה III – משהו בך – **Something you are**

# הזדהות ברמה שניה - משהו שיש לך



➤ מכשיר סלולרי - קבלת SMS



➤ טוקן ייעודי



➤ כרטיס חכם



# הזדהות ברמה שלישית - משהו בך



טביעת אצבע ✓

זיהוי רשתית ✓

תווי פנים ✓

זיהוי קולי ✓

מאפייני התנהגות ✓

# סרטון בנושא 2 FACTOR

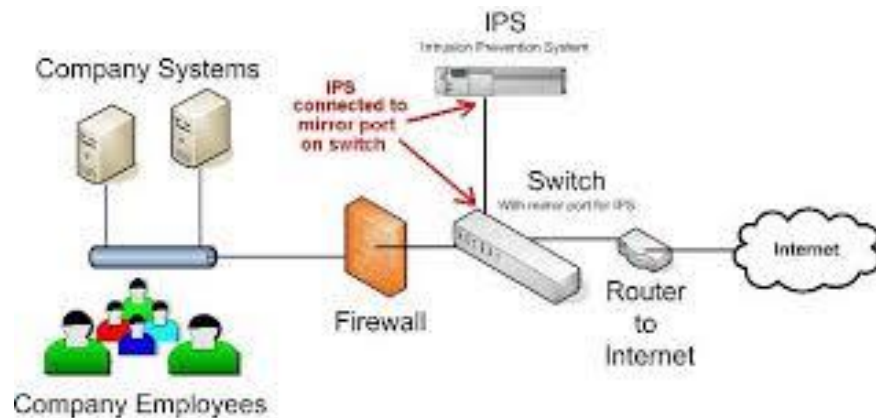


IDS = INTRUDER DETECTION SERVICE

IPS = INTRUDER PROTECTION SERVICE

IDS - במקרה של התקפה על הארגון - מתריע בלבד

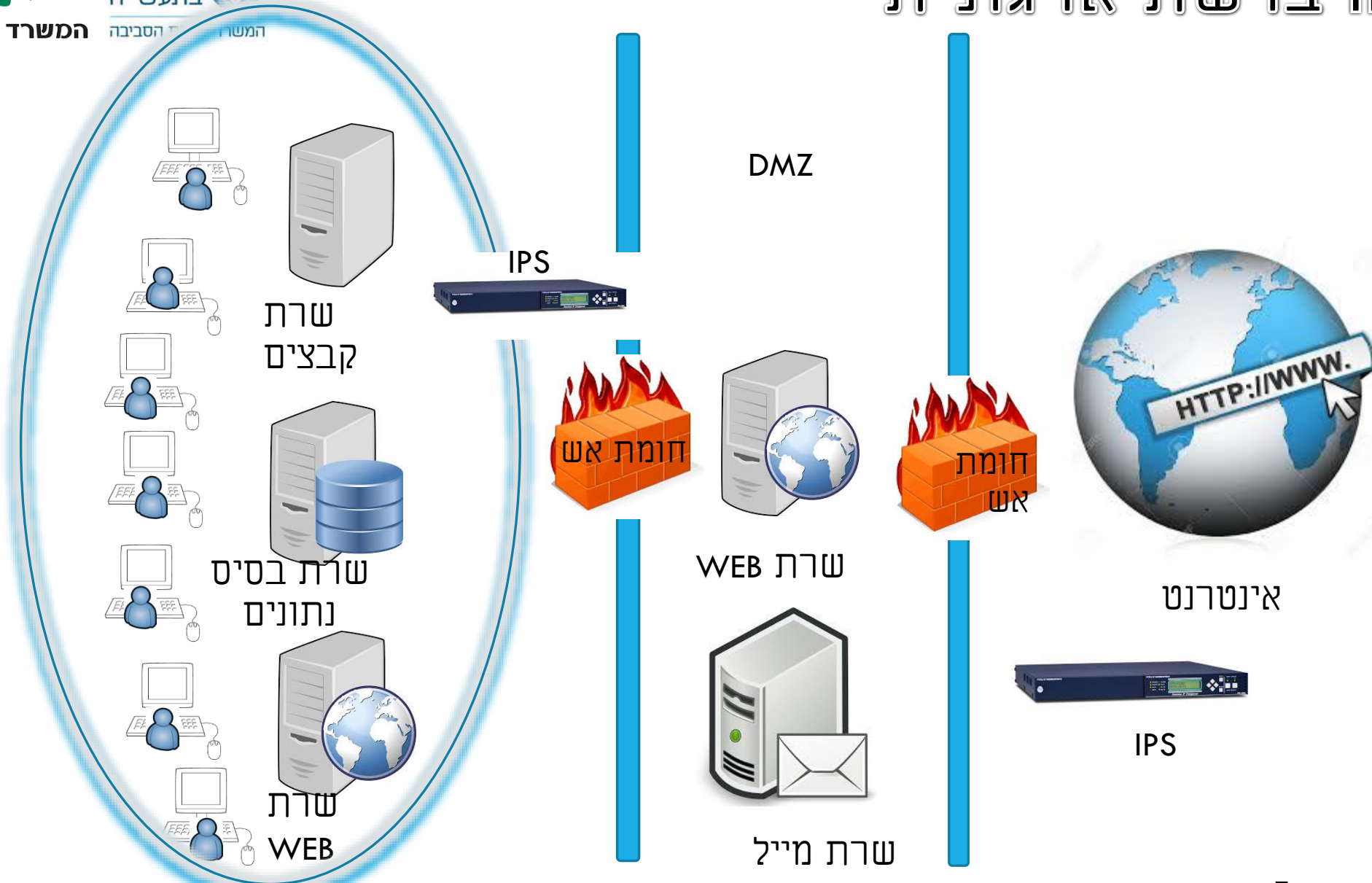
IPS - מתפקד כ-IDS ובמידת הצורך, אם קינפגנו אותו כך - יכול לחסום התקפות בצורה אקטיבית



הצורך:

- חסימת התקפות מחוץ לארגון
- חסימת התקפות מתוך הארגון

# מיקום IPS ברשת ארגונית



# בעיות בחסימת התקפות

ב-IPS יש לקחת בחשבון **חסימת תעבורה לגיטימית\***

מצב חסימה	סוג התעבורה	מצב
מאפשר	לגיטימית	1
1 בעיה חוסם	לגיטימית	2
2 בעיה מאפשר	לא לגיטימית (התקפה)	3
חוסם	לא לגיטימית (התקפה)	4

מי יותר גרוע לארגון ??

בעיה 1 או בעיה 2?



בעיות בחסימת התקפות במערכת IPS

תאריך	שעה	מקור	מטרה	סוג אירוע	רמת חומרה	תיאור
2015/02	10:00	192.168.1.1	192.168.1.1	התקפת DDoS	גבוהה	התקפת DDoS מאת 192.168.1.1
2015/02	10:05	192.168.1.1	192.168.1.1	התקפת DDoS	גבוהה	התקפת DDoS מאת 192.168.1.1
2015/02	10:10	192.168.1.1	192.168.1.1	התקפת DDoS	גבוהה	התקפת DDoS מאת 192.168.1.1

בעולם ה-oz – השבתת גישה למערכת מידע



בעולם ה-oz – השבתת גישה למערכת ייצור

הפתרון הראשוני: הפעלת IDS + שיקול דעת אנושי מה לחסום בפועל



מה זה וירוס?

וירוס זה תוכנה העשויה מקוד מסוים שהיא בתוך קובץ הרצה מסוים ויש לו יכולות שכפול.



2 סוגים עיקריים:

- ❑ וירוס אקטיבי-וירוס שעובר ממחשב למחשב
- ❑ וירוס פאסיבי-שנשאר רק במחשב אחד.

פעולות לדוגמא שמבצעים וירוסים

- ❖ וירוס שיכול למחוק את הקבצים במחשב או לשנות אותם
- ❖ וירוס ששולח מידע מהמחשב לעמדת הבקרה של ההאקר
- ❖ וירוס שמאפשר שליטה מרחוק על המחשב

## 1. תולעים

התולעים פועלים באופן עצמאי ומטרתם העיקרית היא להתפשט בכל המחשב ולהביא לקריסתו התולעת משכפלת מפיצה את עצמה ממחשב ומגיעה לנפחים אדירים.

## 2. סוס טרויאני

סוס טרויאני הוא תוכנה שיכולה לשנות קבצים או למחוק אותם או לגנוב באמצעות שליטה מרחוק ע"י מחשב מרוחק.

## 3. פצצות לוגיות

פצצות לוגיות היא וירוס שפועל ע"פ תאריך/יום/שעה. הפצצה הלוגית עושה פעולה כלשהי שגורמת נזק למחשב.



## 4. תוכנת רוגלה

זוהי תוכנה אשר מסוגלת להציג למישהו במחשב מרוחק מידע על המחשב שתוכנה זו נכנסה אליו. בניגוד לסוס טרויאני, תוכנה זו לא מסוגלת לשנות או למחוק קבצים.



## 5. וירוסי מאקרו

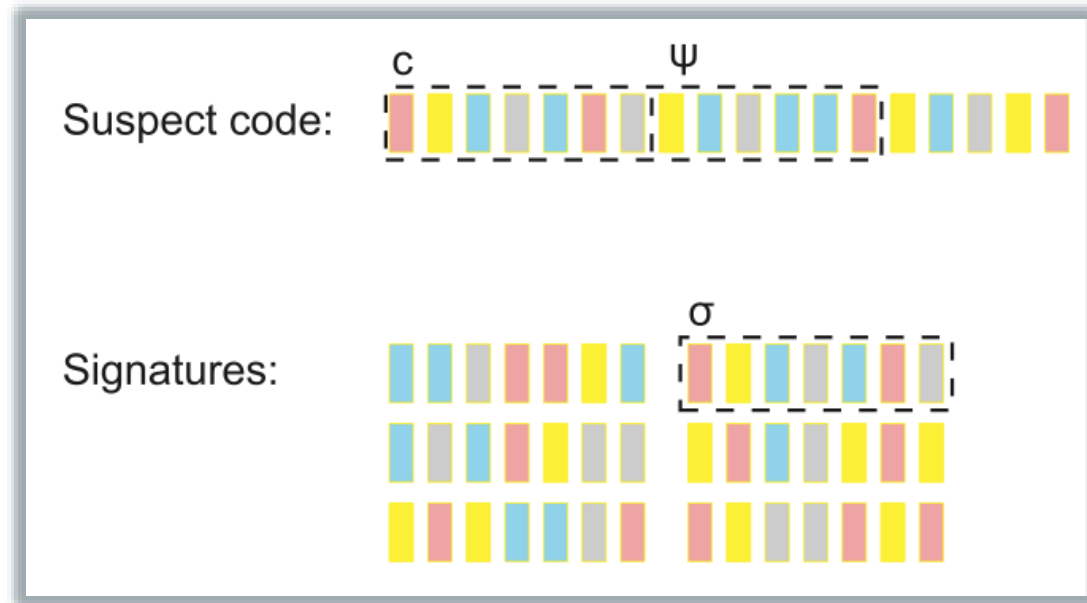
וירוסים אלו מתחבאים בתוך מסמכים סטנדרטיים כמו וורד או אקסל. וירוסים אלו יכולים לגרום למחיקת קבצים או הרס מערכת ההפעלה

**איזה וירוס / וירוסים לא הזכרנו כאן ?? !!!**



# איך מתגוננים ?

חברות אבטחת מידע מייצרות חתימות לוירוסים הידועים



חתימות:

מה החסרונות: מוגנים בפני וירוסים ידועים בלבד



ZERO DAY



מהו וירוס ZERO DAY?

וירוס לא ידוע לחברות האנטי וירוס ולכן לא מופיע בקובץ החתימות של האנטי וירוס המותקן במחשבינו.

איך מייצרים וירוס ZERO DAY?

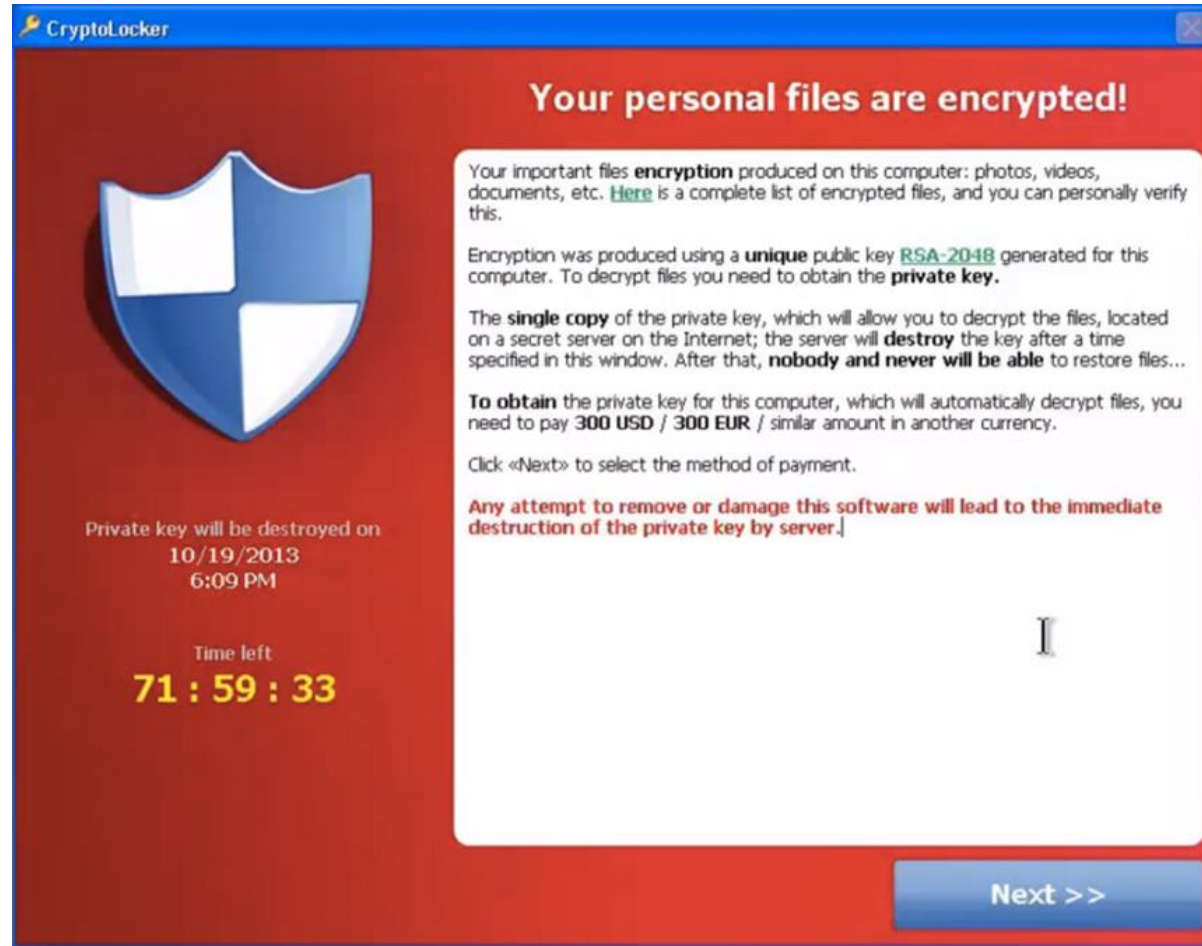
2 אפשרויות:

1. יוצרים וירוס חדש לגמרי שלא מוכר עדיין (לכן נקרא ZERO DAY כי זה היום הראשון שלו בחוץ)

2. לוקחים וירוס קיים ויוצרים ממנו "מוטציה" לעיתים מזוהה ע"י קובץ החתימות של ה-AV ולעיתים לא

# דוגמאות ל-ZERO DAY

ירוסי כופרה שונים





לאחר הצפנת הקבצים ע"י וירוס כופרה הם נראים כך:

