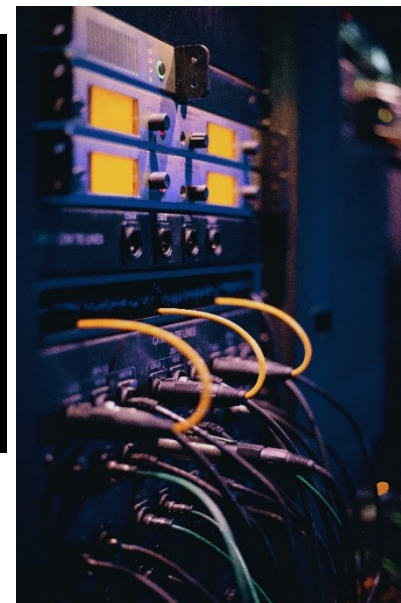


מושגי ייסוד בסייבר – חלק א



Yosi Shavit MBA, CISM - Information Security & Cyber Expert

Cellular: 058-6662242

Mail: yosish@gmail.com , yosish@sviva.gov.il

מתקפת סייבר על חברות ישראליות, בהן חברה-בת של התעשייה האווירית

מתקפת כופרה נעלה מערכות של חברת נס הבינלאומית ויתכן כי חדרה גם למחשבים של חברה-בת של התעשייה האווירית וחברות נוספות בישראל. התוקפים דורשים תשלום כופר, אולם בשלב זה לא מתנהל איתם משא ומתן. בהתמודדות עם האירוע מעורבים צוותים בחו"ל וכן צוותים של חברת נס הישראלית והתעשייה האווירית



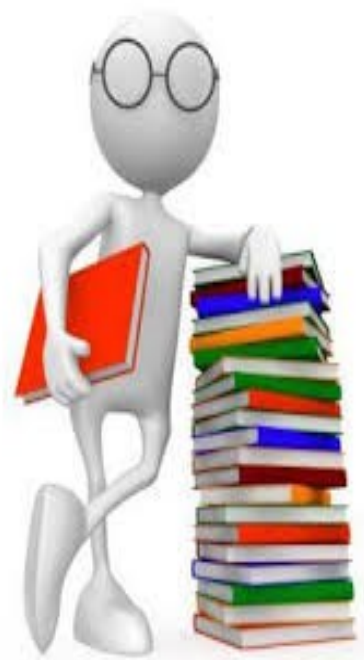
טל שחף פורסם: 08.02.21, 13:27

מתקפת סייבר על חברת Ness Digital Engineering מתרחשת בשעות אלה בארה"ב, הודו וגם ישראל, וייתכן כי מעורבת בה גם חברת TSG, חברה-בת של התעשייה האווירית שנרכשה מנס טכנולוגיות הישראלית. ל-ynet נודע כי האירוע מנוהל על ידי צוותי התערבות ומומחי סייבר בשלוחות החברה בהודו ובארה"ב, וגם בישראל פועלים צוותים פנימיים של נס טכנולוגיות בשיתוף מומחים של התעשייה האווירית כדי להבין אם נפגעו מערכות ומה מידת הנזק.

התוקפים נעלו מערכות מחשבים בחברות המותקפות באמצעות כלי הכופרה RAGNAR LOCKER, שנחשב למסוכן ביותר. הם דורשים כופר בסכום שלא נמסר. ככל הידוע לא מתנהל עדיין משא ומתן עם התוקפים.



היום מלפני חצי שעה...



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
- וירוסים – סקירה על סוגי הוירוסים השונים ודרכי התגוננות
- התקפות ZERO DAY ודרכי התגוננות
- תקיפת DDOS
- מוצרי הגנה : WAF , DAF , NAC , דיודה חד כונית , הלבנה , SIEM – SOC

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)

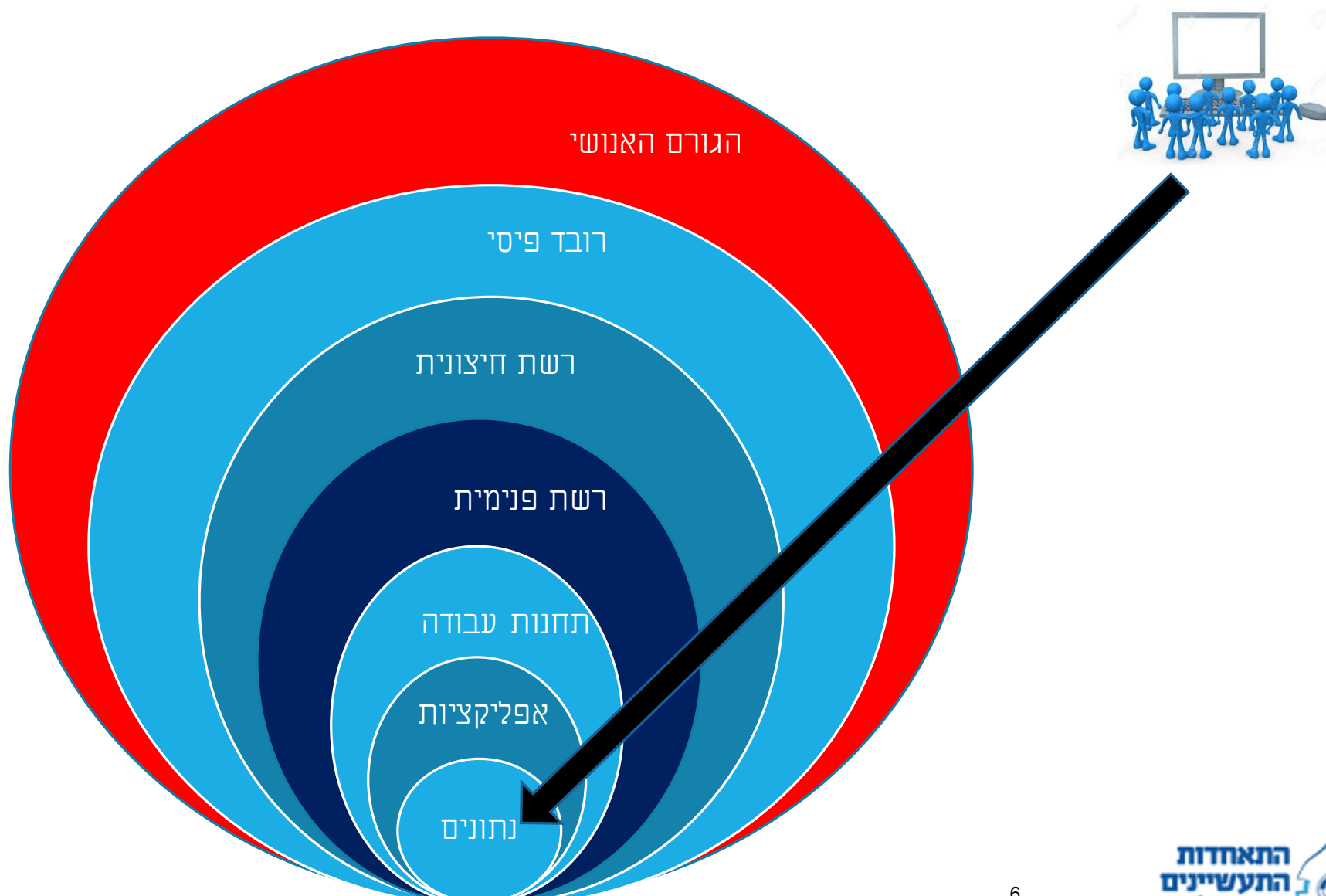
People, Process, Products



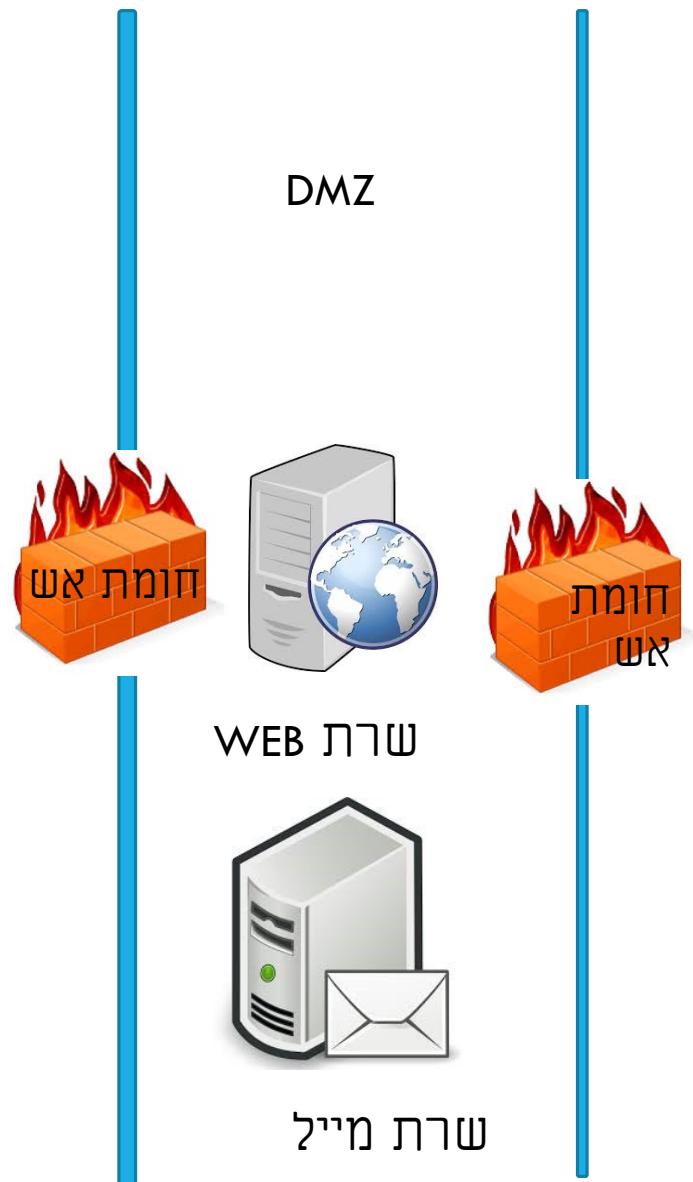
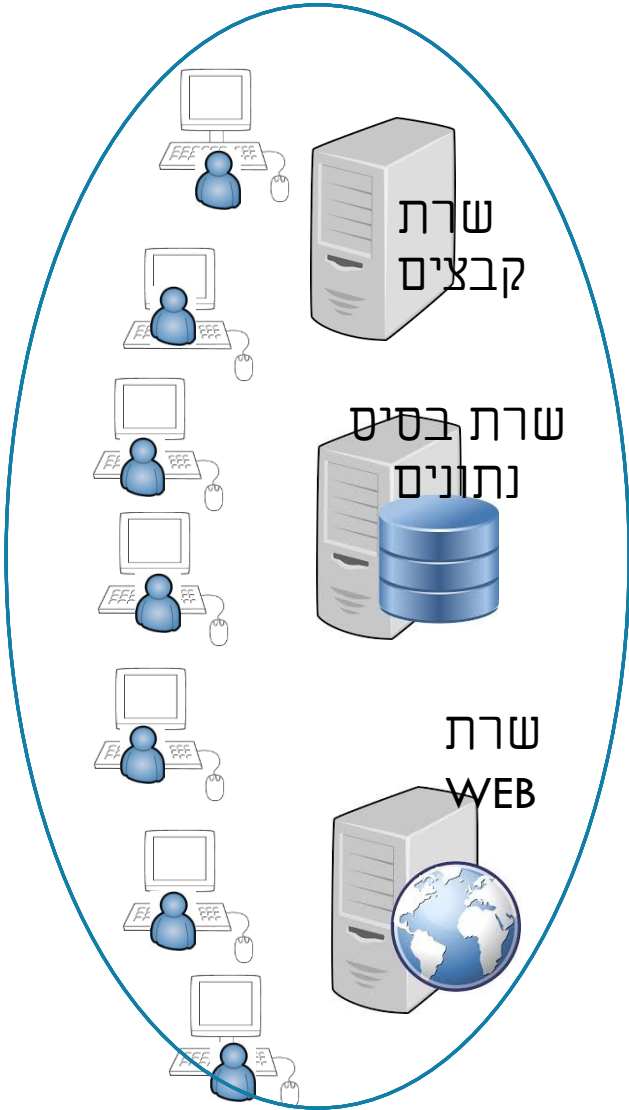
✓ אנשים
✓ טכנולוגיה
✓ תהליכים

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

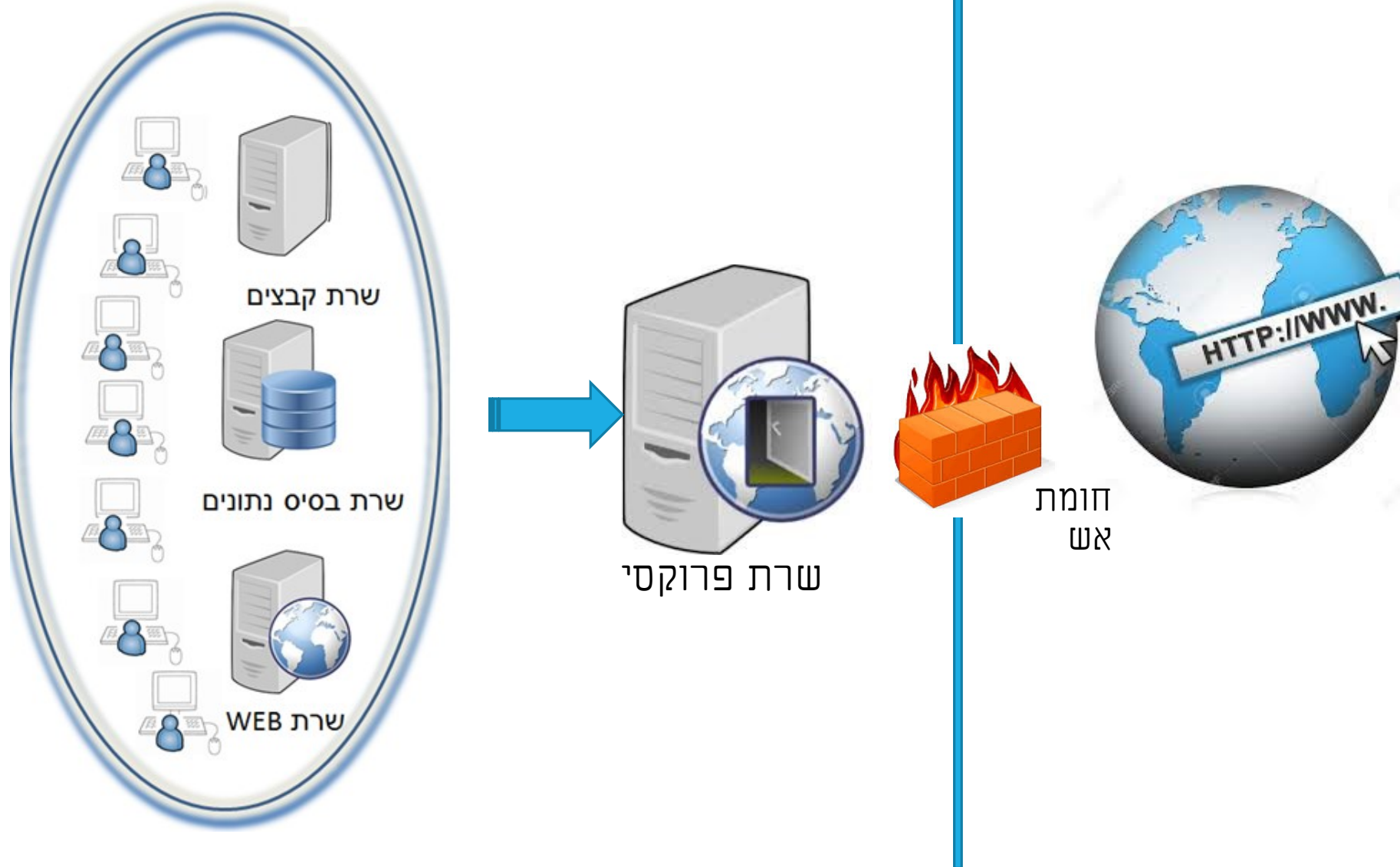
מעגלי אבטחת המידע והסייבר



כיצד נראית רשת ארגונית?



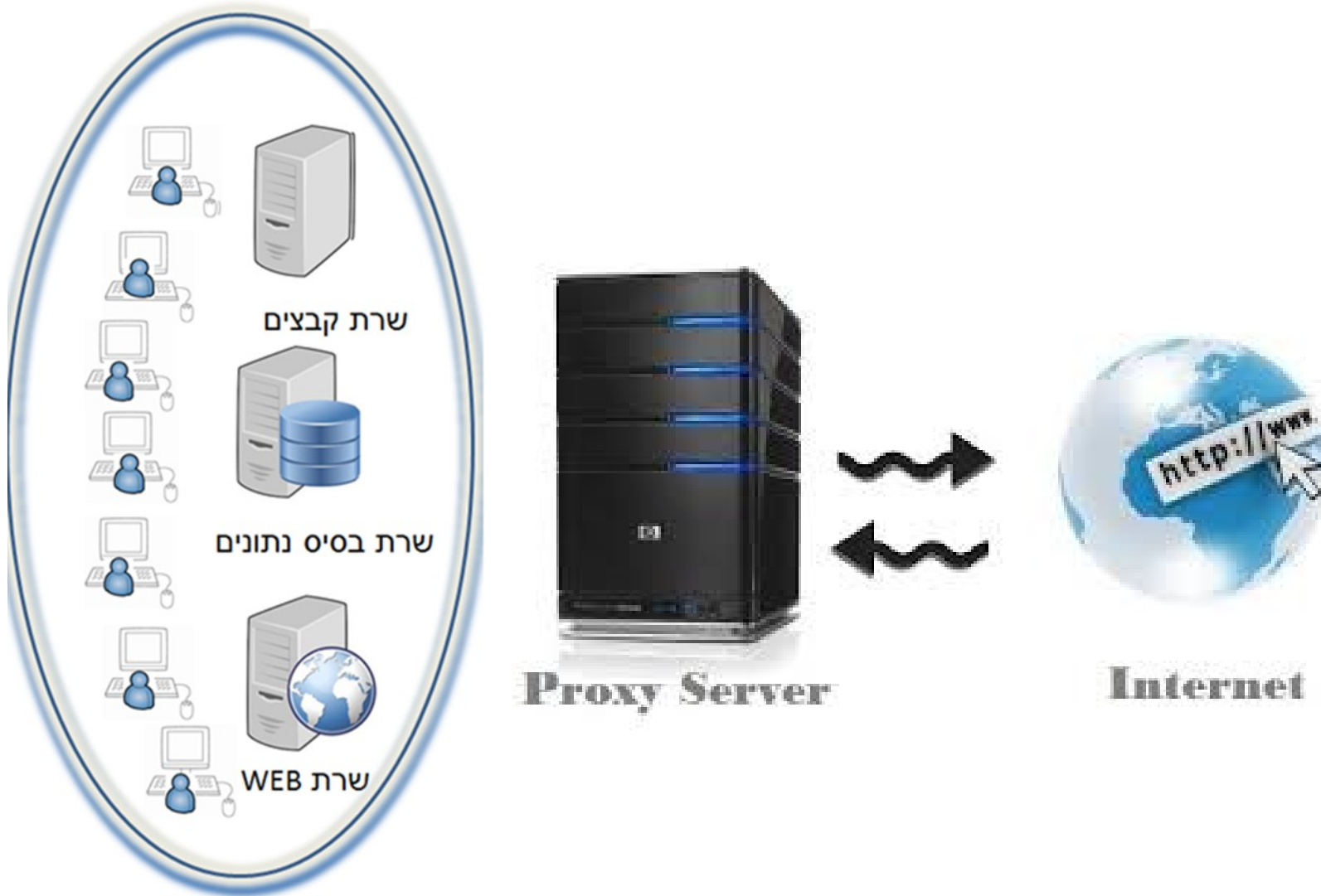
גלישת משתמשים



גלישת משתמשים - שרת פרוקסי

מטרות:

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

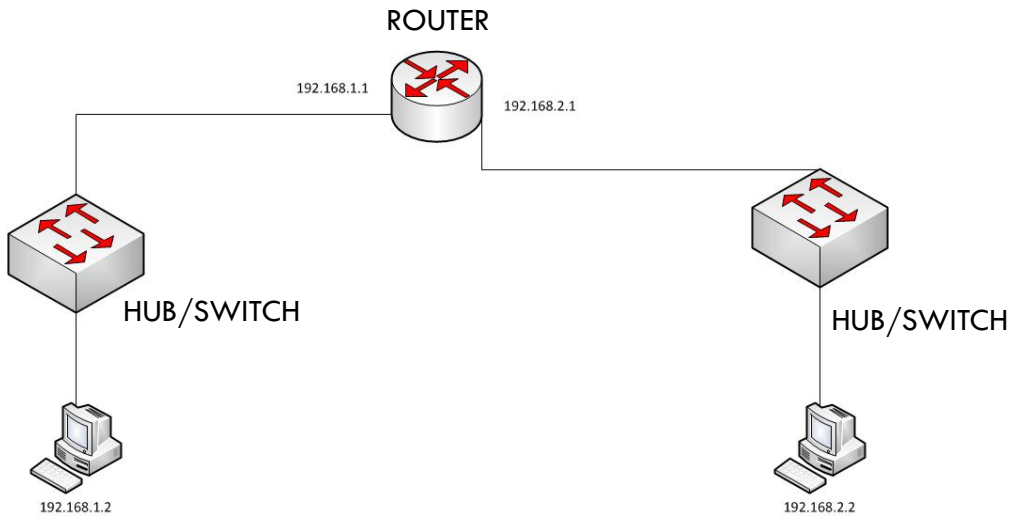




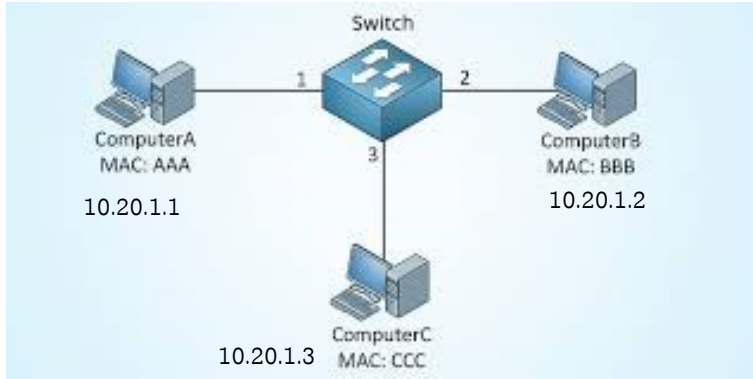
כתובות IP על קצה המזלג

כמה עובדות חשובות לגבי כתובות IP

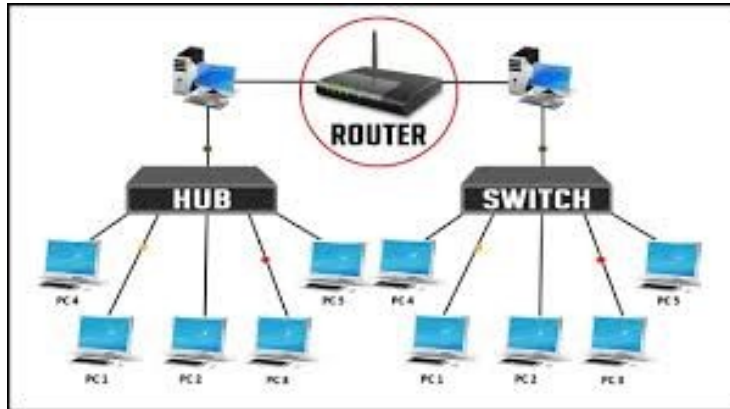
- ❑ כשמחשב א' רוצה להגיע למחשב ב' הוא פונה לכתובת שלו
- ❑ כתובת IP כמוה ככתובת מגורים – חייבים לדעת לאן רוצים להגיע
- ❑ 2 סוגי כתובות IP – פרטית וציבורית



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*)

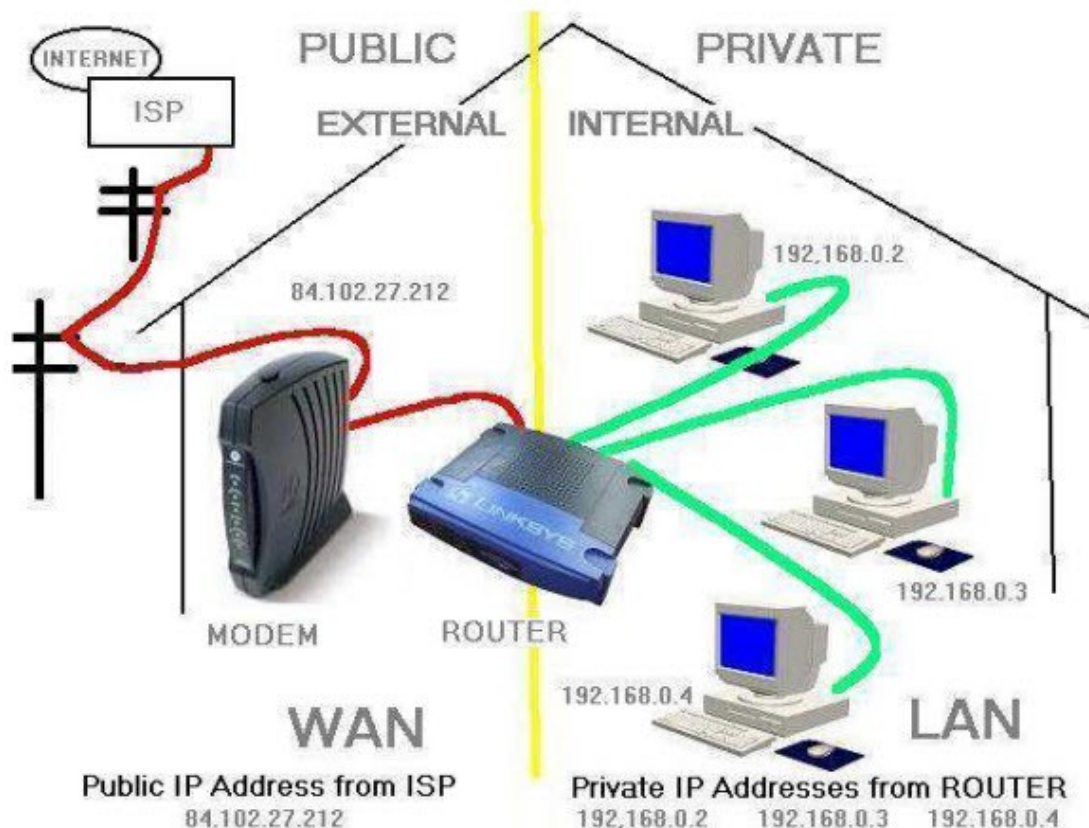
לשימוש בתוך ארגון.
אין להן אפשרות לצאת לעולם (גלישה, מיילים)
אין הגבלה במספר הכתובות

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

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
SMTP	25	תעבורת מיילים
FTP	21	העברת קבצים

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



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

RULES – חוקים

No.	Hits	Name	Source	Destination	Applications/Sites	Action	Track	Install On
1	4M	Block sites which may cause liability	Any	Internet	Potential_liability	Block Blocked Message	Log	All
2	3M	Block High risk applications	Any	Internet	High Risk	Block High Risk Block	Log	All
3	2M	Allow remote admin for IT Dept only	IT_Department	Any	Radmin	Allow	Log	All
4	10K	Allow Facebook only to HR	HR	Internet	Facebook	Allow Download_1Gbps Down: 1 Gbps	Log	All
5	2991	Common Blocked categories	Any	Internet	Streaming Media Social Networki... P2P File Sharing Remote Adminis...	Block Blocked Message	Log	All
6	8441	Log all applications in the organization	Any	Internet	Any Recognized	Allow	Log	All

חוקים – RULES

Policy



Search for IP, object, action, ...

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track
Limit Access to Gateways Rule (Rule 1)								
1	29K	VPN Stealth	Corporate-inte	GW-group	Any Traffic	Any	drop	Alert
VPN Access Rules (Rules 2-5)								
2	392K	Site to site VPN	Any	Any	All_GwToGw	CIFS ftp-port http https smtp	accept	Log
3	0	Remote access	Mobile-vpn-usi	Any	RemoteAccess	CIFS http https imap	accept	Log
4	2K	Clientless VPN	Clientless-vpn-	Corporate-WA-	Any Traffic	https	User Auth	Log
5	21K	Web server	L2TP-vpn-user@ Customers@Ar	Remote-1-web-	Any Traffic	http	accept	Log
Rules for Specific Sites (Rules 6-8)								
6	2M	Outbound HTTP	Remote-2-inter	Any	Any Traffic	http	Client Auth	Log
7	640K	Critical subnet	Corporate-inte	Corporate-fina Corporate-hr-n Corporate-rnd-	Any Traffic	Any	accept	Log

לוגים – LOGS

The screenshot shows the 'All Records (lv_rec.fws)' window in Check Point SmartView Tracker. The interface includes a sidebar with 'Network & Endpoint Queries' and 'Predefined' categories. The main area displays a table of records with columns for No., Date, Time, Origin, Service, Source, Source User Name, and Destination. The records list various network activities such as SMTP, SIP, HTTP, and FTP traffic between different internal and external hosts.

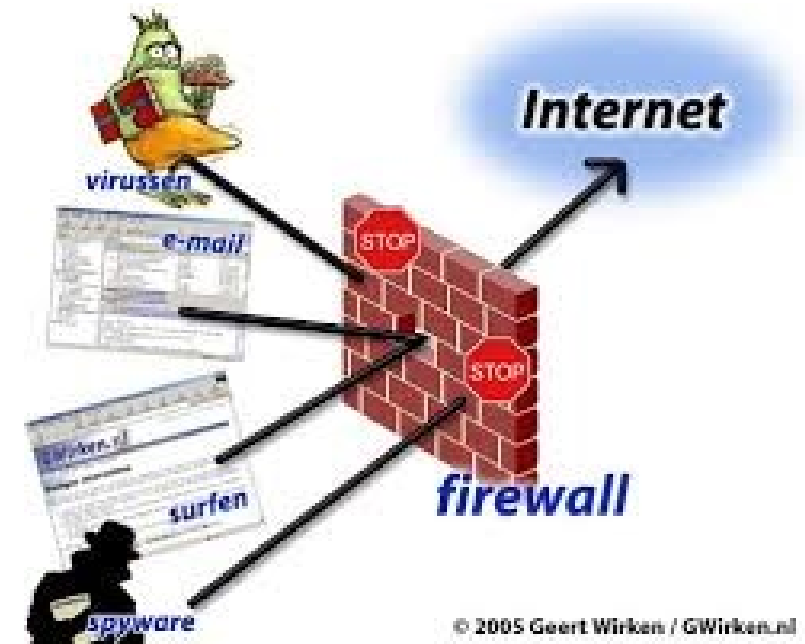
No.	Date	Time	Origin	Service	Source	Source User Name	Destination
1	1Nov2008	1:11:29	Alaska_memb...				
2	1Nov2008	15:00:41	California_GW	TCP smtp	California.LAN.ham...		durden.abc-corp.biz
3	1Nov2008	15:06:33	California_GW	TCP smtp	California.LAN.ham...		durden.abc-corp.biz
4	1Nov2008	15:41:29	California_GW	TCP smtp	California.LAN.kum...		California_GW
5	1Nov2008	16:43:13	California_GW	UDP sip	voip		California_GW
6	1Nov2008	17:43:28	California_GW				
7	1Nov2008	18:35:11	California_GW	TCP smtp	California.LAN.jaco...		pc1.abc-hq.com1
8	1Nov2008	18:35:14	California_GW	TCP 1039	35.12.10.129		California_GW
9	1Nov2008	18:39:42	Alaska_RND_...	TCP http	10.111.254.11		www.ietf.org
10	2Nov2008	8:10:20	Alaska_cluster	TCP ftp	robot.ftps.domain...		Alaska_DMZ_intern...
11	2Nov2008	8:11:22	Alaska_cluster	TCP ftp	robot.ftps.domain...		Alaska_DMZ_intern...
12	2Nov2008	8:11:30	Alaska_cluster	TCP ftp	robot.ftps.domain...		Alaska_DMZ_intern...
13	2Nov2008	8:12:29	Alaska_cluster	TCP ftp	robot.ftps.domain...		Alaska_DMZ_intern...
14	2Nov2008	8:14:36	Alaska_cluster	TCP ftp	robot.ftps.domain...		Alaska_DMZ_intern...
15	2Nov2008	8:14:38	Alaska_memb...				
16	3Nov2008	11:14:26	Alaska_cluster	TCP ftp	robot.ftps.domain...		Alaska_DMZ_intern...
17	15Mar2009	1:00:1	Primary_Mana...				
18	15Mar2009	2:14:36	Alaska_cluster	TCP http	resolved.hosts.com		Alaska_DMZ_intern...
19	15Mar2009	2:19:21	Alaska_Finan...	TCP microsoft-ds	Alaska.IT.Bentli		10.112-254-9
20	15Mar2009	10:9:29	Alaska_RND_...	TCP 8080	10.111.254.31	Jennifer McHenry (jm...	192.168.9.111
21	15Mar2009	10:9:30	Alaska_RND_...	TCP 8080	10.111.254.31	Jennifer McHenry (jm...	192.168.9.111
22	15Mar2009	10:9:31	Alaska_RND_...	TCP 8080	10.111.254.31	Jennifer McHenry (jm...	192.168.9.111
23	16Mar2009	16:35:14	Alaska_cluster	TCP http	scriptskids.inc		Alaska_DMZ_intern...
24	16Mar2009	16:35:19	Alaska_cluster	TCP http-81	scriptskids.inc		Alaska_DMZ_intern...
25	1Jan2009	22:54:13	Alaska_cluster		California.LAN.jaco...		Alaska_cluster
26	1Jan2009	22:54:13	Alaska_cluster	L.	California.LAN.jaco...		
27	15Jan2009	22:59:34	California_GW	TCP nbssession	California.LAN.ham...		Alaska.LAN.Chincilla
28	15Jan2009	22:54:14	Alaska_cluster	TCP http	Alaska.Fin.Deasel		Florida.LAN.euclid
29	29Jan2009	22:53:49	Delaware_ciu...	TCP nbssession	California.LAN.ham...		Alaska.LAN.Chincilla
30	2Feb2009	22:59:35	California_GW	TCP http	Alaska.Fin.Deasel		Florida.LAN.euclid
31	2Feb2009	22:54:14	Alaska_cluster		California.LAN.jaco...		Alaska_cluster
32	4Feb2009	22:59:35	California_GW	TCP http	Alaska.Fin.Deasel		Florida.LAN.euclid

שימוש שני: חציצה בין רשתות בארגון (סגמנטציה)



שימושים לחומת אש בארגון

שימוש ראשון: לאפשר תקשורת בטוחה לאינטרנט

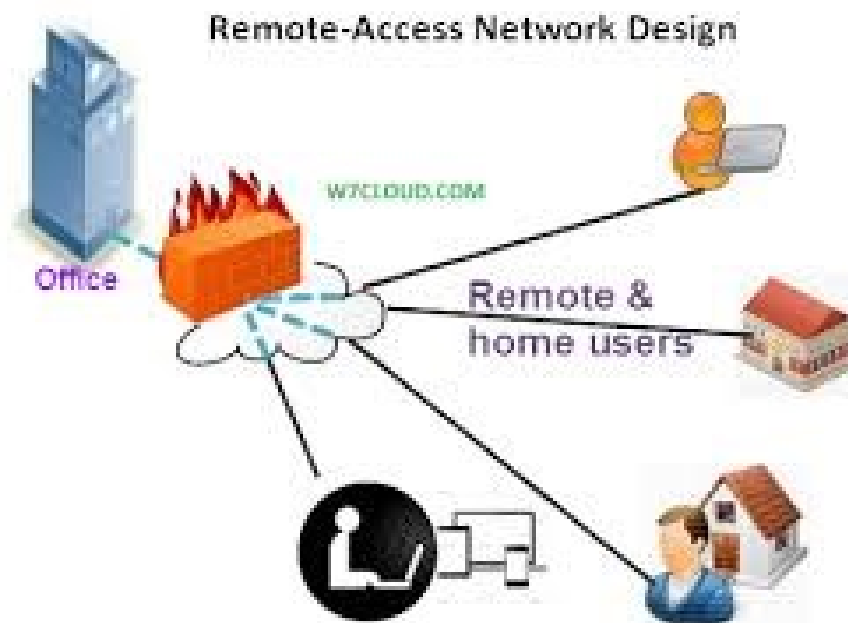


© 2005 Geert Wirken / GWirken.nl

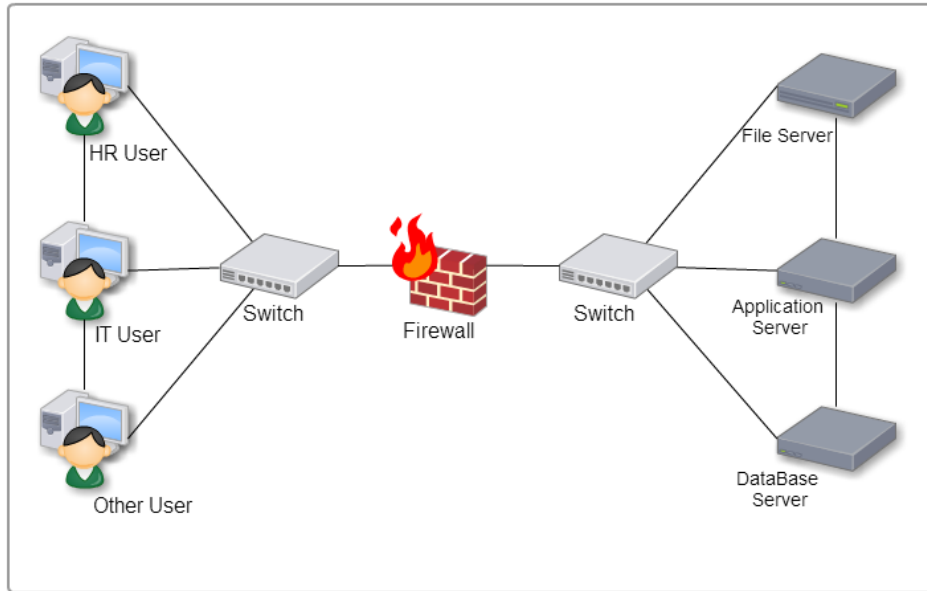
שימושים לחומת אש בארגון

שימוש שלישי:

גישה מרחוק לארגון – (VPN)

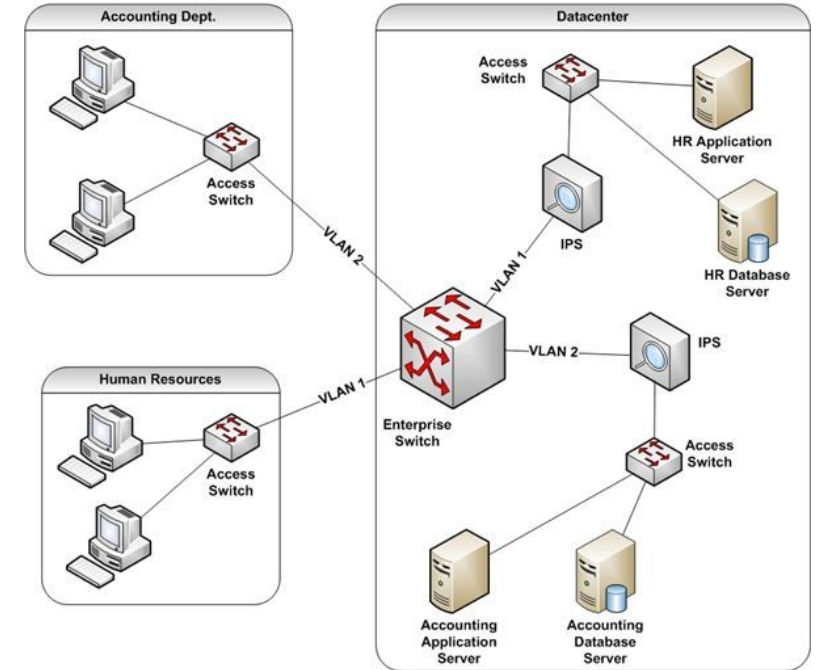


בין משתמשים לשרתים



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

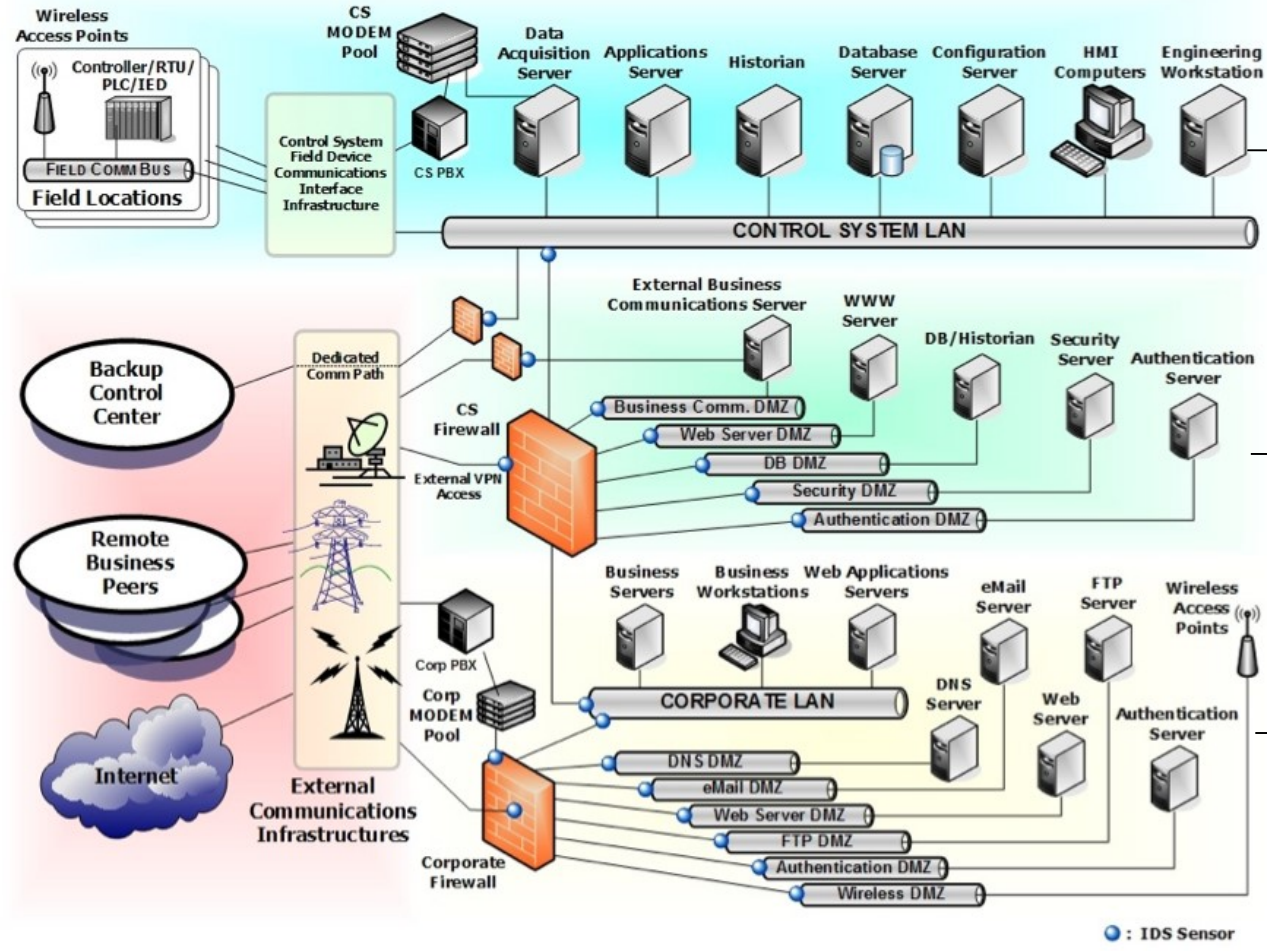
בין מחלקות שונות בארגון



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

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

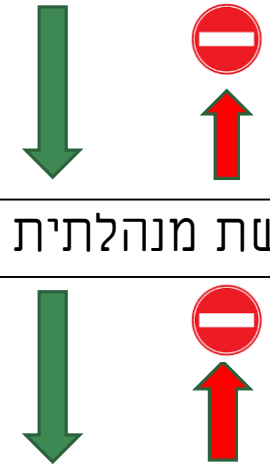
OT – Operation Technology
ICS – Industrial Control System



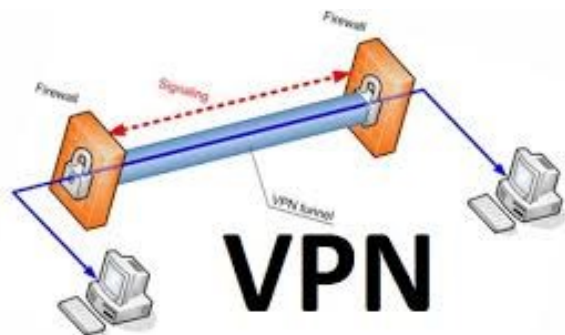
רשת ה-OT (ייצור)

רשת מנהלתית

יציאה לאינטרנט



גישה מרחוק



A screenshot of a network management interface showing a list of firewall rules or logs. The table has multiple columns with various settings and status indicators.

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??

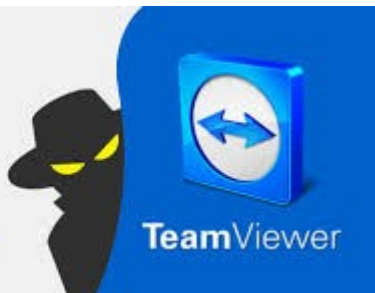
המלצות נוספות להתחברות מרחוק

User Name: matrix
Password: 123456

❑ משתמש חיצוני לארגון (ספק, נותן שירות) – יצירת משתמש חד - חד ערכי

Another
vulnerability,
this time

TeamViewer



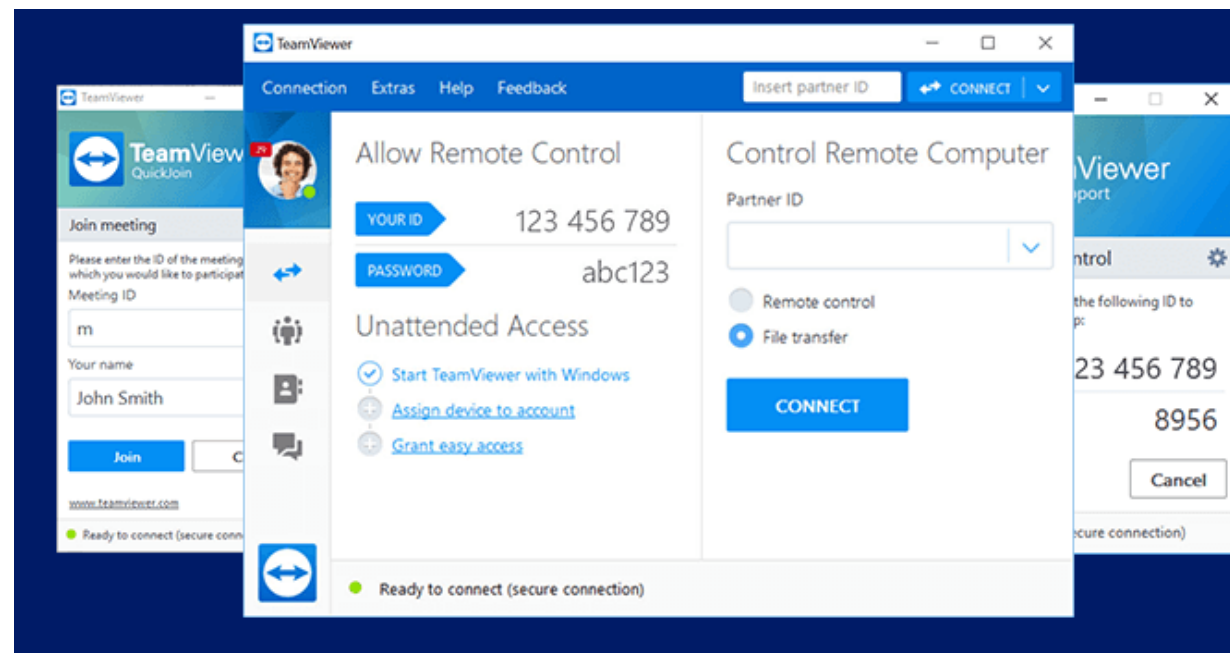
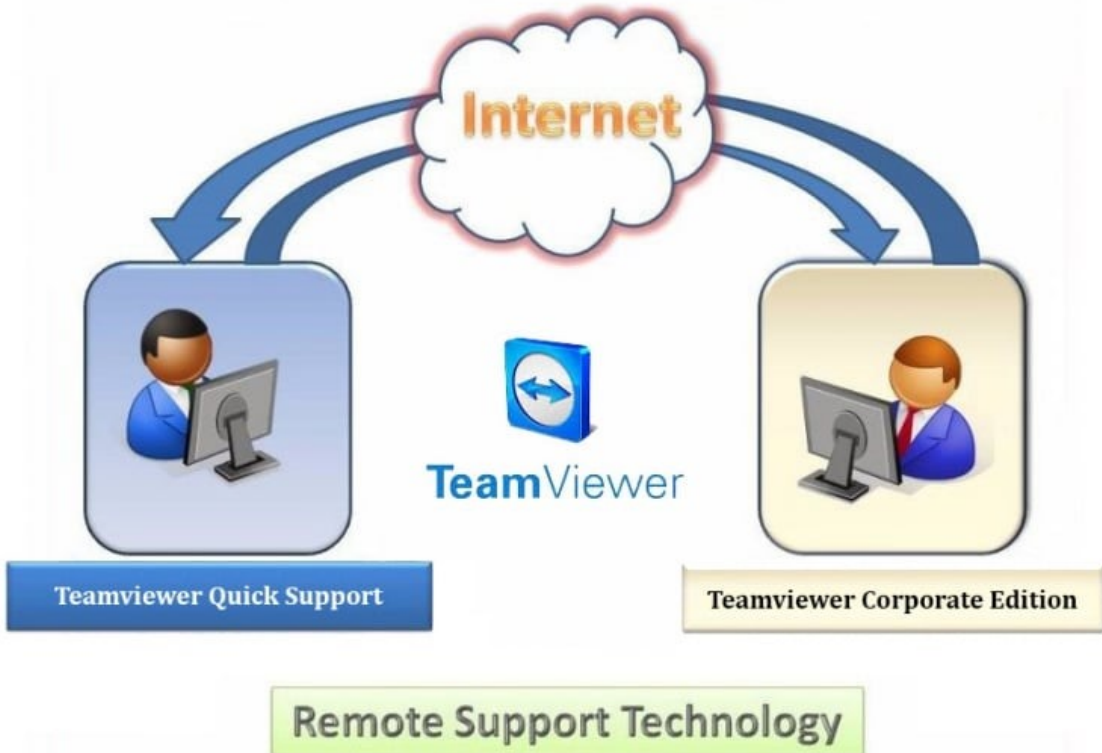
❑ גישה מבחוץ לא באמצעות גלישת WEB

❑ בדיקת תאימות התחנה המתחברת – עדכוני אבטחת מידע ואנטי-וירוס

❑ החתמת משתמש חיצוני על הצהרה התחברות לצורך המטרה הספציפית שלשמה נועד

איך עובד TEAM-VIEWER?

השתלטות ממחשב
השתלטות מטל סלולרי

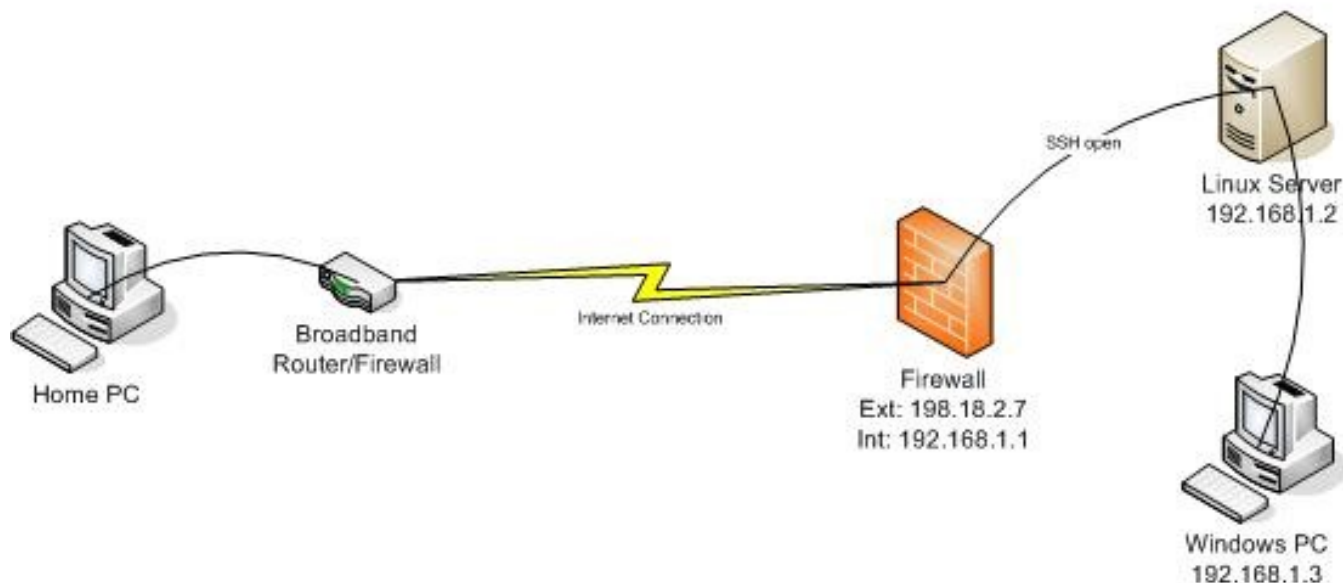


תוכנות נוספות להשתלטות מרחוק מבוססות אינטרנט



גישה מרחוק: איך עושים זאת נכון?

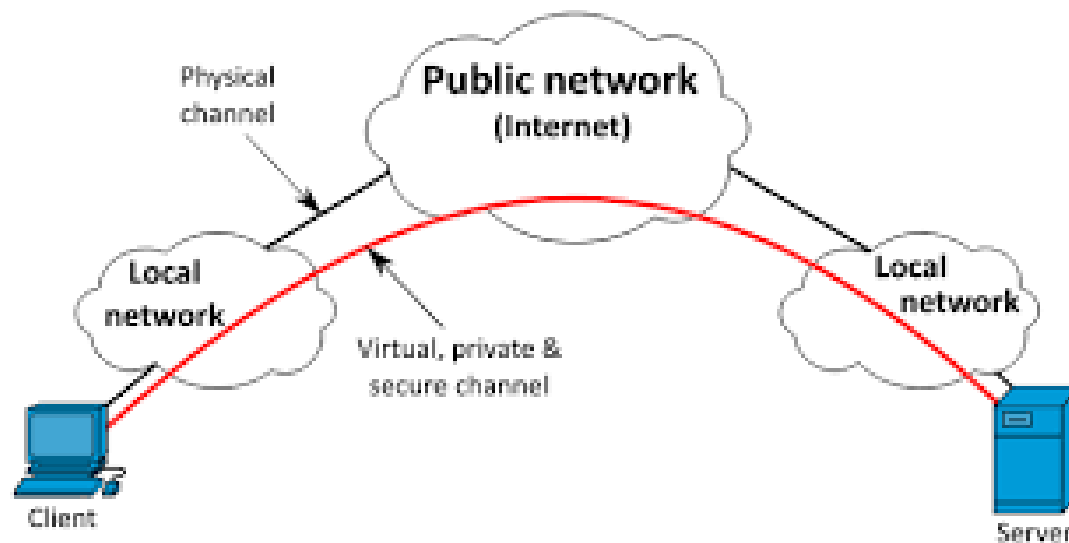
1. גישה ל-GATEWAY הארגוני (FW) – יצירת VPN
2. בדיקת תאימות (COMPLIANCE) למחשב המתחבר (קיום עדכוני אבטחה WINDOWS ואנטי-וירוס מעודכן)
3. הפניה לשרת הזדהות
4. זיהוי חד – חד ערכי
5. משלוח SMS למזדהה



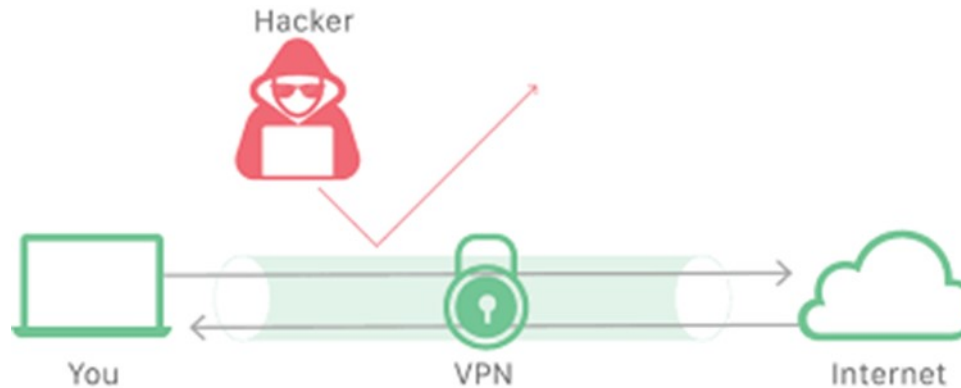
תקשורת אל הארגון - באמצעות VPN



VPN = VIRTUAL PRIVATE NETWORK

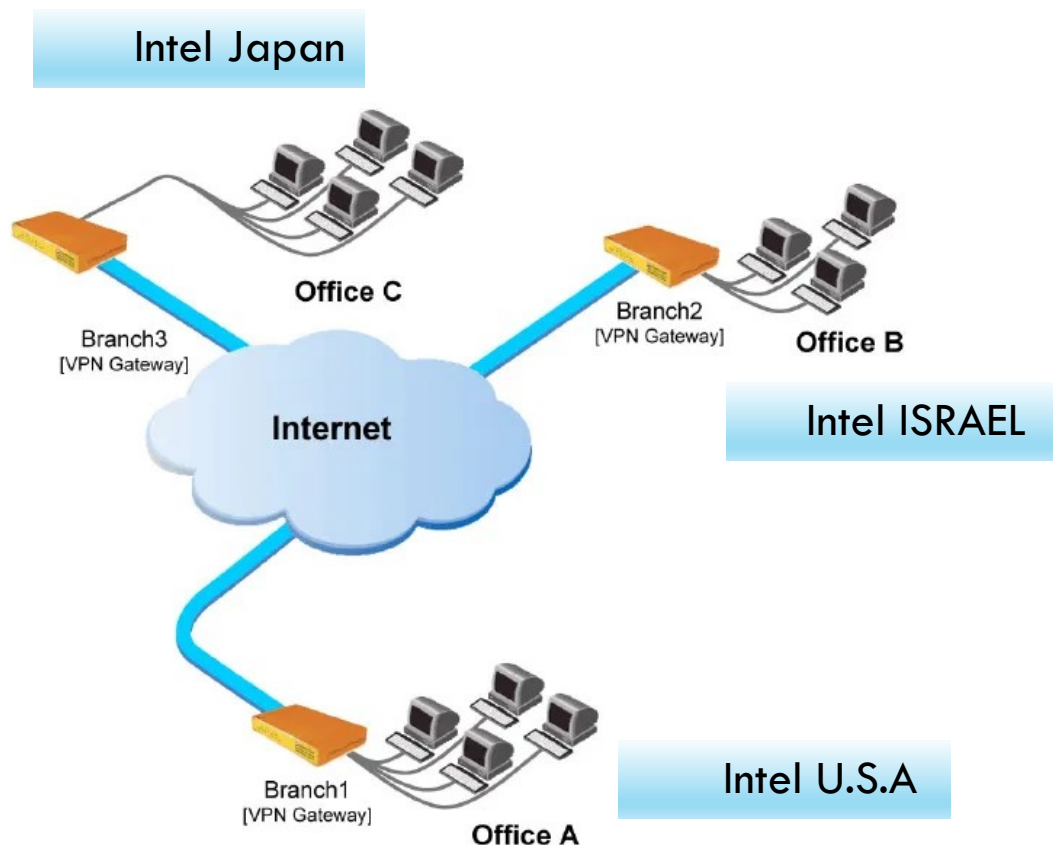


תקשורת עוברת בצינור (TUNNEL) מוצפן

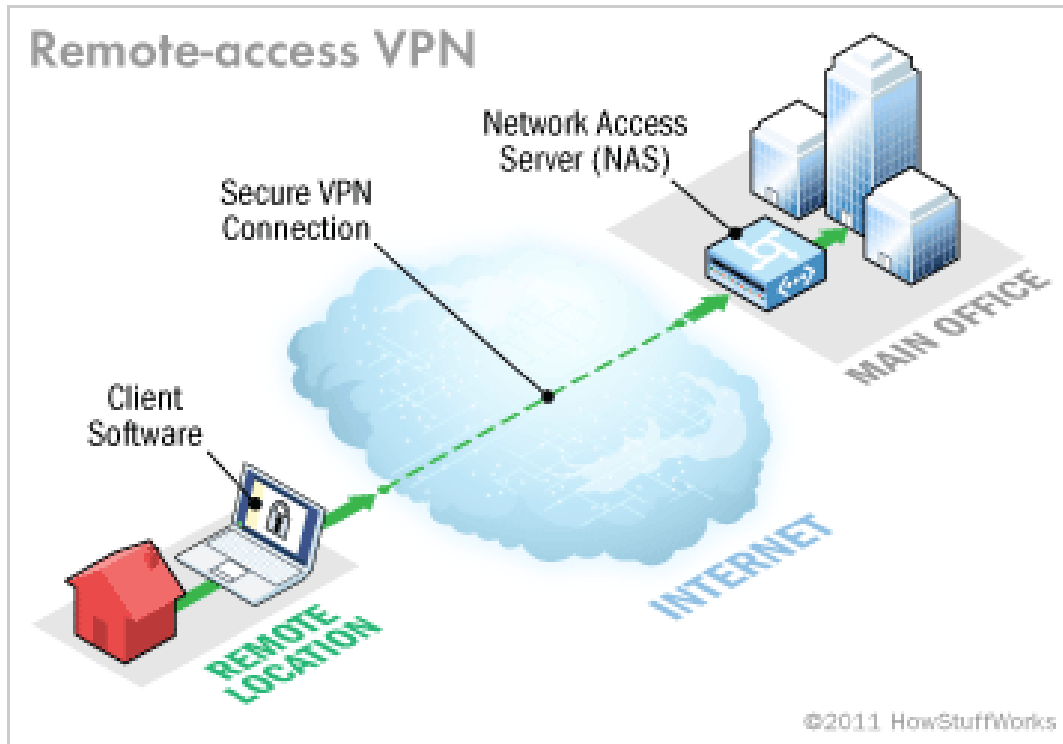


תקשורת אל הארגון - באמצעות VPN - שימושים

ארגון מפורז על פני שטח גיאוגרפי גדול



גישה מרחוק של משתמשים

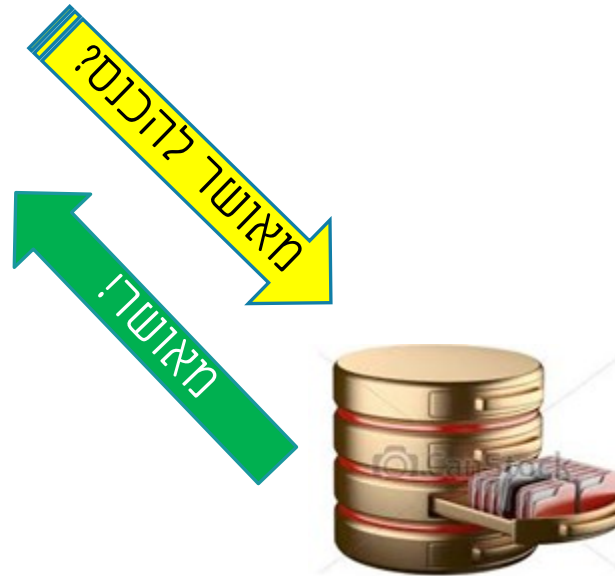


הזדהות למערכת



שם משתמש: Hr105
 סיסמא: 123456

איך עובדת הזדהות ?



שם משתמש	סיסמא	סטטוס אישור
Uv451	123123	
Db633	11qq11	
Hr105	123456	✓
tp423	password	
-----	-----	
-----	-----	

סיסמאות נפוצות

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 (כבר לא.....)

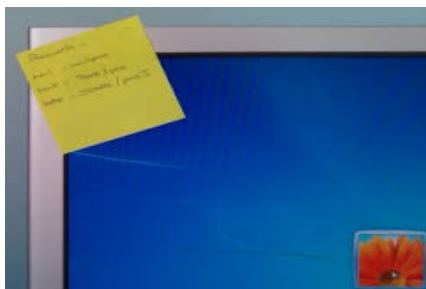
מספר סידורי	סיסמה	מופעים
1	123456	2419
2	1234	1875
3	12345	1115
4	12345678	445
5	123123	218
6	1111	216
7	qazwsx	189
8	1234567	164
9	0	155
10	123	154
11	121212	152
12	1212	139
13	111111	122
14	55555	109
15	pizza	100

הבעיה:
שימוש בסיסמאות חלשות

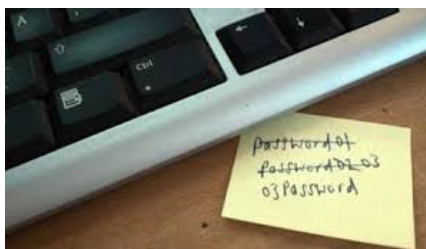
בעיות עם סיסמאות



➤ סיסמא קלה



➤ תולים על מסך המחשב



➤ שמים מתחת למקלדת

יש לזכור:

קיימות טכנולוגיות BRUTE FORCE וטכנולוגיות DICTIONARY מתקדמות לזיהוי סיסמאות ברשת

פתרונות לבעיית סיסמאות

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:



1. P@55w0rd

2. Pשדד'סרג

מהירות הפריצה לסיסמא קלה

(96^8)

P@55w0rd

26^8

password

Test a New Password

Enter in a password to see the maximum time it would take to crack that password. Use the slider under the year to see how much the maximum crack time has increased since 1982. Also slide up to 2020 to see how quickly a password might be cracked in the future.

Password: P@55w0rd Year: 2020

9 YEARS : **6** MONTHS : **2** WEEKS : **4** DAYS : **5** HOURS : **54** MINUTES : **32** SECONDS : **79** JIFFIES : **8** MILLISECONDS

Keys per second in 2020: 17042497.3 kps Word List: On Off

This interactive is not collecting entered passwords and is for entertainment purposes. Estimates made in the interactive will not always be accurate due to evolving technologies and limitations in technology used to create it.

Better Buys

Test a New Password

Enter in a password to see the maximum time it would take to crack that password. Use the slider under the year to see how much the maximum crack time has increased since 1982. Also slide up to 2020 to see how quickly a password might be cracked in the future.

Password: password Year: 2020

0.19 MILLISECONDS

Keys per second in 2020: 17042497.3 kps Word List: On Off

This interactive is not collecting entered passwords and is for entertainment purposes. Estimates made in the interactive will not always be accurate due to evolving technologies and limitations in technology used to create it.

Better Buys

<https://www.betterbuys.com/estimating-password-cracking-times/#:~:text=Nine%2Dcharacter%20passwords%20take%20five,bad%20for%20one%20little%20letter.>

מהירות הפריצה לסיסמאות

Password Length	Numerical 0-9	Upper & Lower case a-Z	Numerical Upper & Lower case 0-9 a-Z	Numerical Upper & Lower case Special characters 0-9 a-Z %\$
1	instantly	instantly	instantly	instantly
2	instantly	instantly	instantly	instantly
3	instantly	instantly	instantly	instantly
4	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	20 sec
7	instantly	2 sec	6 sec	49 min
8	instantly	1 min	6 min	5 days
9	instantly	1 hr	6 hr	2 years
10	instantly	3 days	15 days	330 years
11	instantly	138 days	3 years	50k years
12	2 sec	20 years	162 years	8m years
13	16 sec	1k years	10k years	1bn years
14	3 min	53k years	622k years	176bn years
15	26 min	3m years	39m years	27tn years
16	4 hr	143m years	2bn years	4qdn years
17	2 days	7bn years	148bn years	619qdn years
18	18 days	388bn years	9tn years	94qtn years
19	183 days	20tn years	570tn years	14sxn years
20	5 years	1qdn years	35qdn years	2sptn years

דאגו שהסיסמה תהיה באורך של 8 תווים לפחות ותכלול:

- שילוב של אותיות קטנות וגדולות (a-z, A-Z)
- ספרה אחת לפחות (0-9)
- תו מיוחד אחד לפחות (\$,%,&,@)

השאירו את פרטיכם האישיים ופרטים אודותיכם מחוץ לסיסמה.

שמות משמעותיים: שקלו להשתמש בהקשר - אם מדובר בניח בחשבון מקוון, חישוב על מילה המתקשרת אליו. למשל: אפשר לקשר את הסיסמה של חשבון הבנק, לשם הרחוב שבו הסיני מתנהל בהתחשבות בהמלצות ה"ל".

זכרו: שימוש בתו "רווח" יכול לעזור בהגנת הסיסמה.

קחו משפט שלם וארוך שיהיה לכם קל לזכור והפכו אותו לראשי תיבות. למשל My dog's name is Mooshi. הסיסמה תהיה: MdniM. לאחר הוספת ספרה ותו מיוחד, הסיסמה תהיה: MdniM1!

במידה ואורך הסיסמה מאפשר זאת, שיקלו להשתמש ב Passphrases כסיסמתכם - Passphrase הנה סיסמה המורכבת ממשפט או מחיבור של כמה מילים:

עוד אפשרות הנה סיסמה המבוססת על תרגיל חשבון פשוט עם שילוב מילים במקום ספרות. לדוגמה, הסיסמה 3 Hundred - 3 =297

שקלו להשתמש במחרוזת קבועה - כמו ביטוי, מילים משי, ציטוט מסרט ולהוסיף לה סימנים ותווים מיוחדים, למשל Wish1You@WereHere!

כיצד בונים סיסמא חזקה?

מקור: באדיבות משרד הבריאות

הפתרון: הזדהות חזקה (MFA)



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 (פיסית)



➤ מכשיר סלולרי - קבלת SMS



➤ טוקן ייעודי



➤ כרטיס חכם

הזדהות ברמה שלישית - משהו בכך (ביולוגית)



טביעת אצבע ✓

זיהוי רשתית ✓

תווי פנים ✓

זיהוי קולי ✓

מאפייני התנהגות ✓

סרטון בנושא 2 FACTOR

