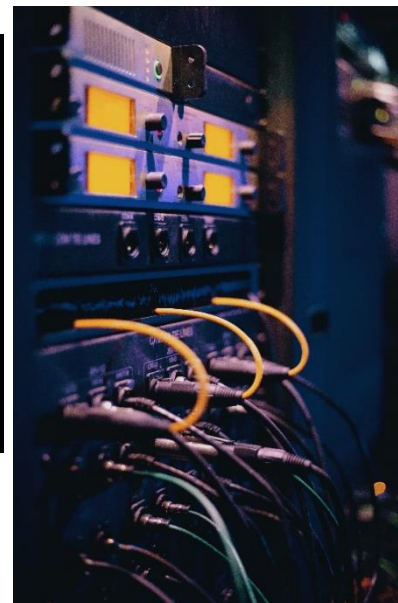


מושגי ייסוד בסייבר – חלק א





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 ✓



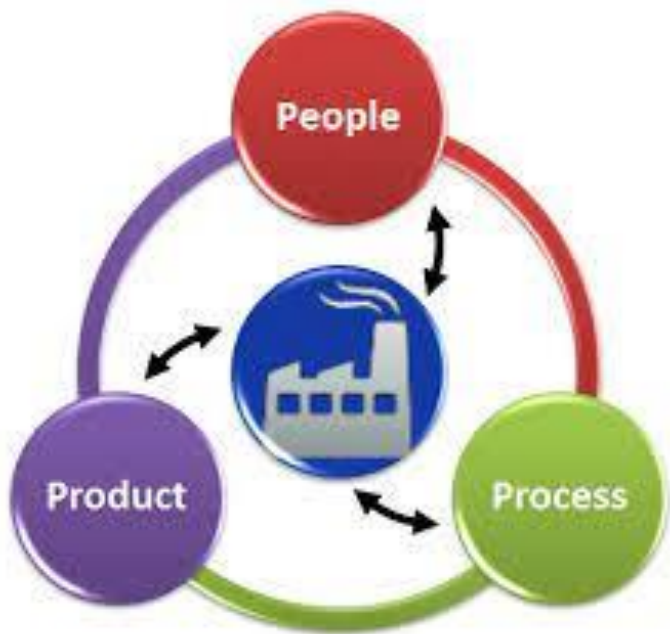
מודעות עובדים ✓

הגנה רב שכבתית - מודל ה-PPP

הגנה רב שכבתית - תהליך המשלב שלושה מרכיבים עיקריים:

The PPP Model (3 P's Model)

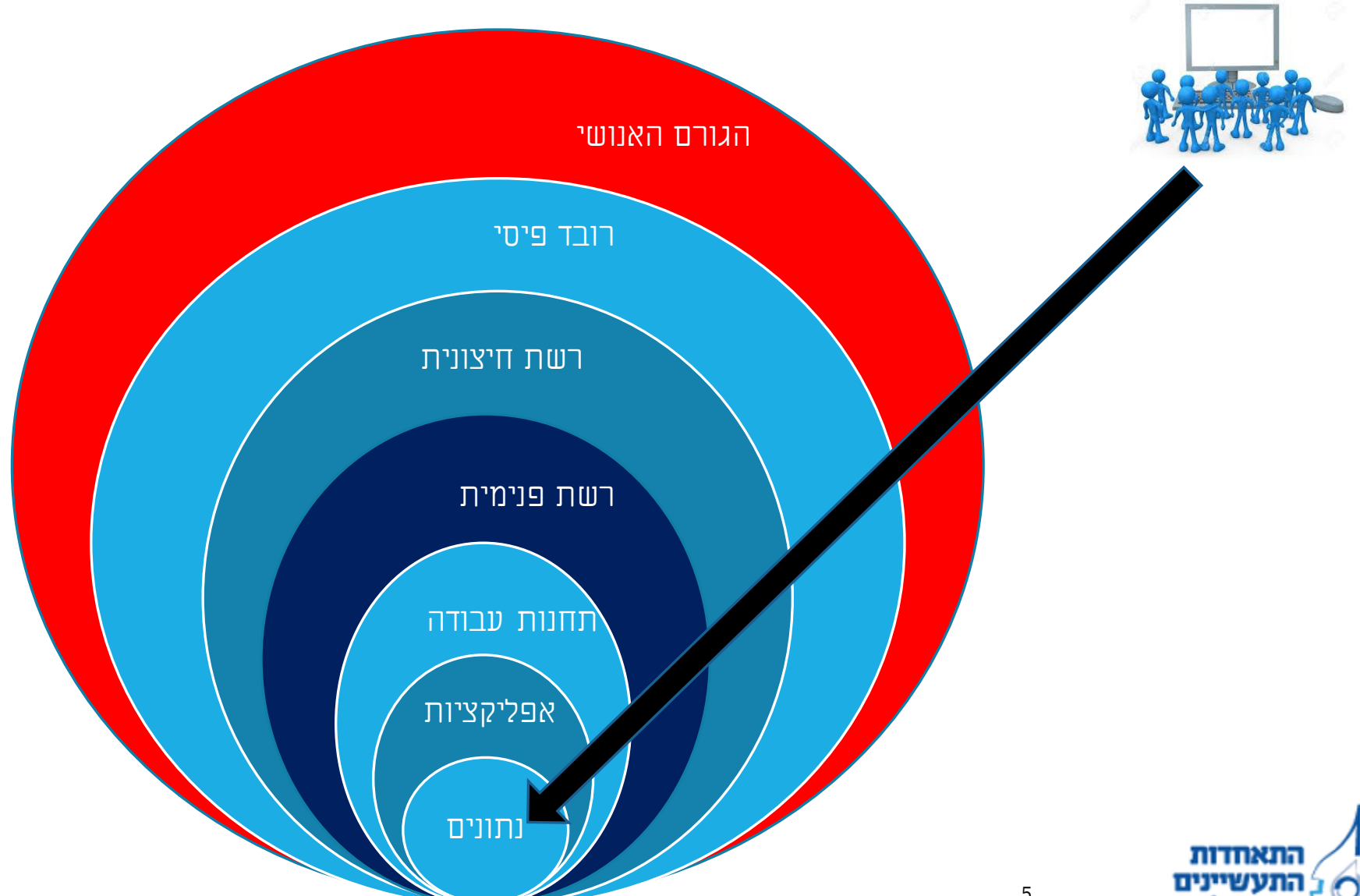
People, Process, Products



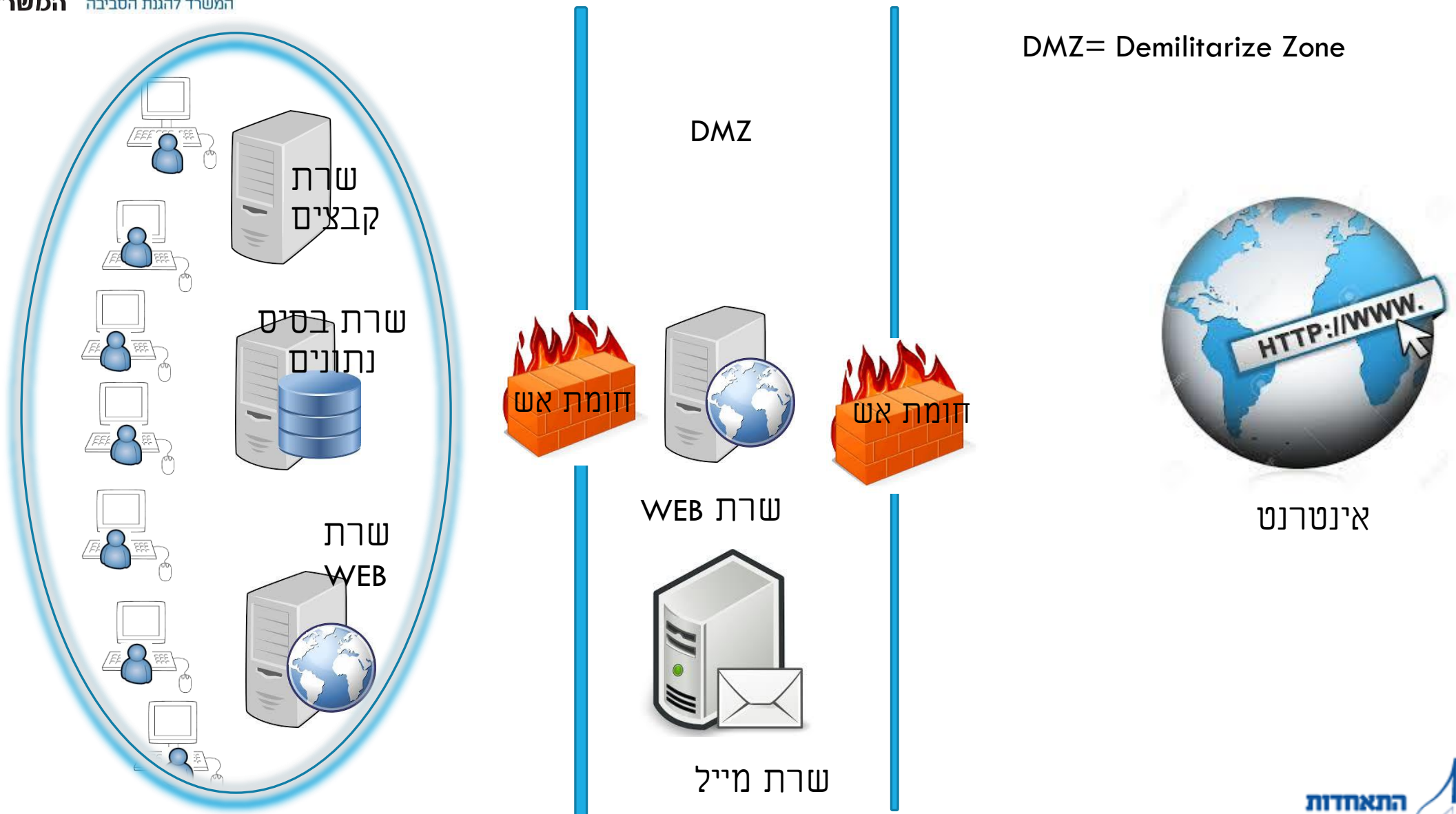
✓ אנשים
✓ טכנולוגיה
✓ תהליכים

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

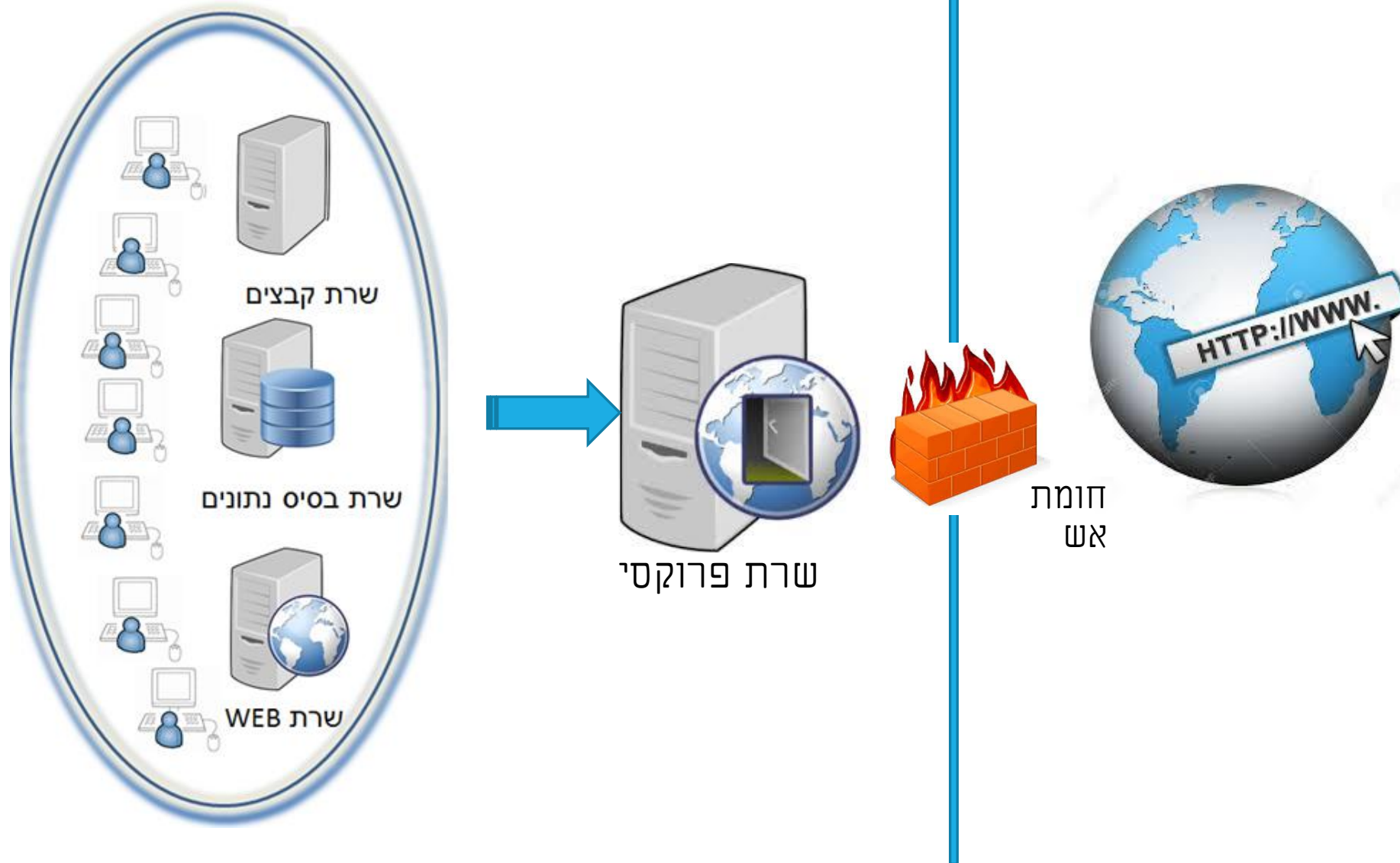
מעגלי אבטחת המידע והסייבר



כיצד נראית רשת ארגונית?



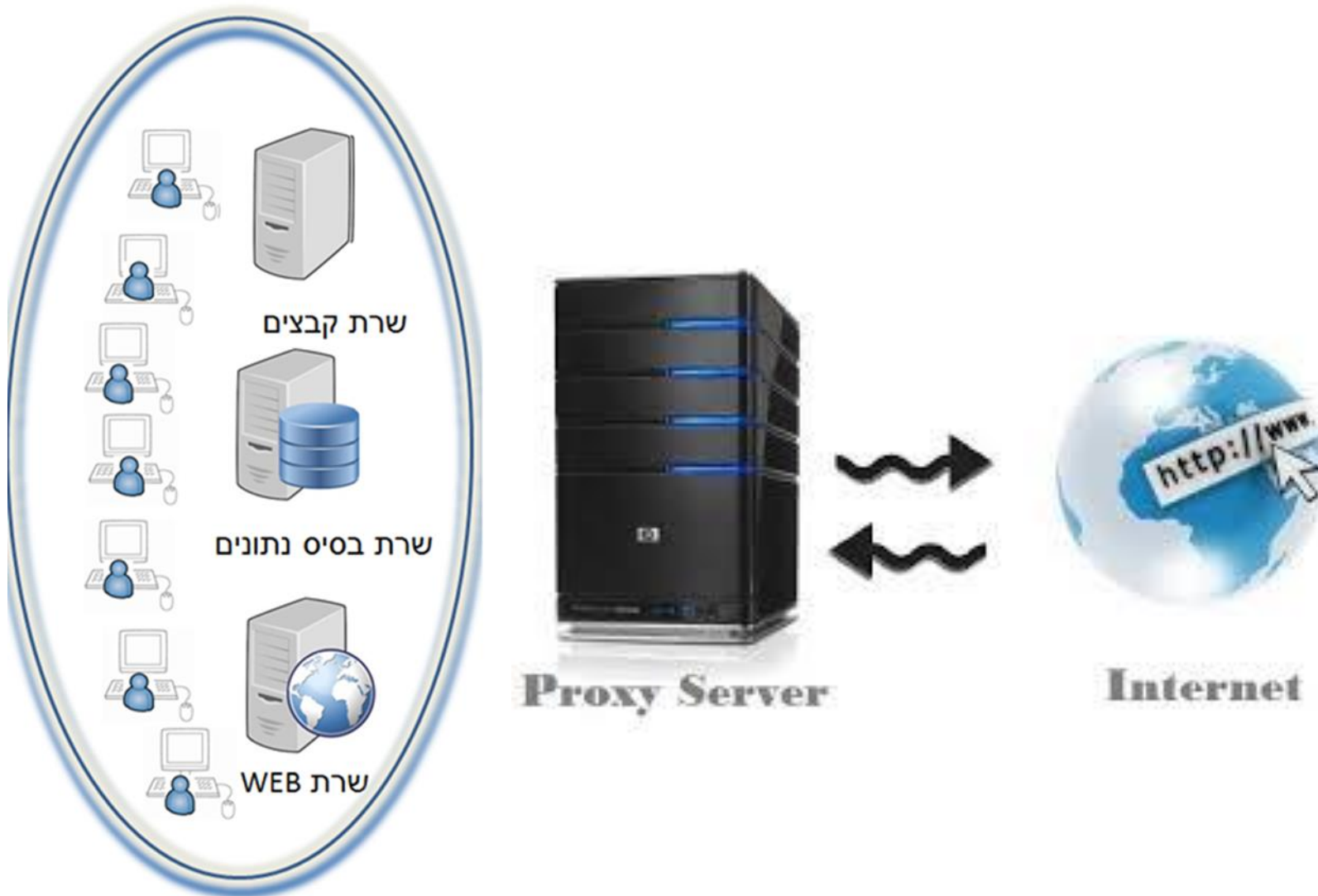
גלישת משתמשים

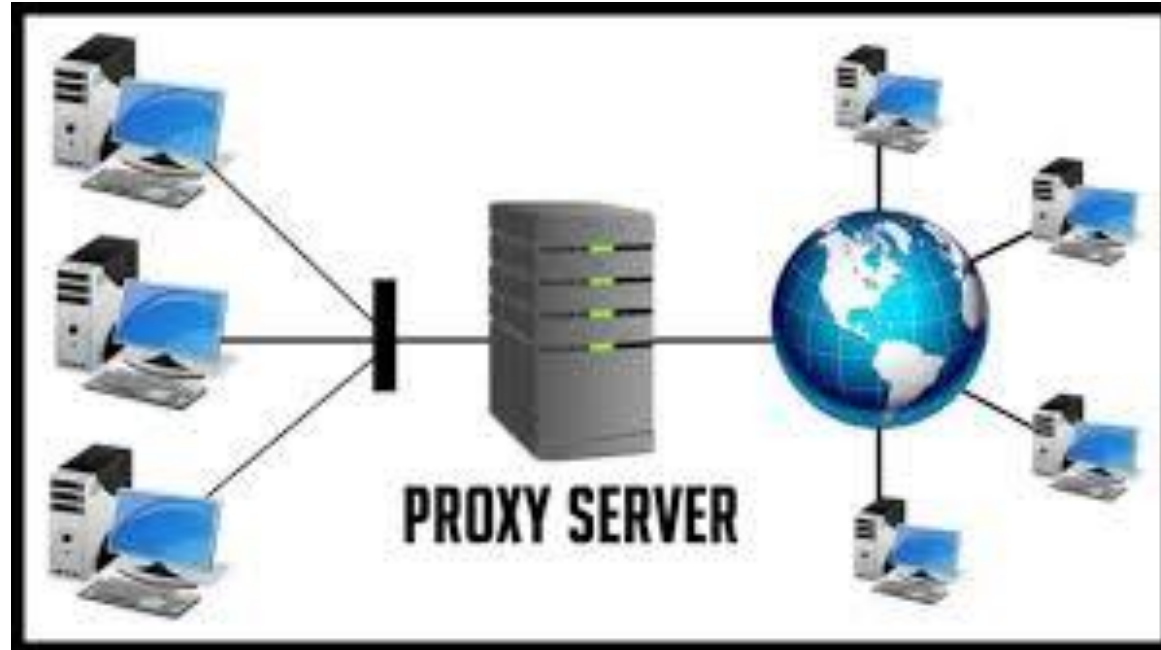


גלישת משתמשים - שרת פרוקסי

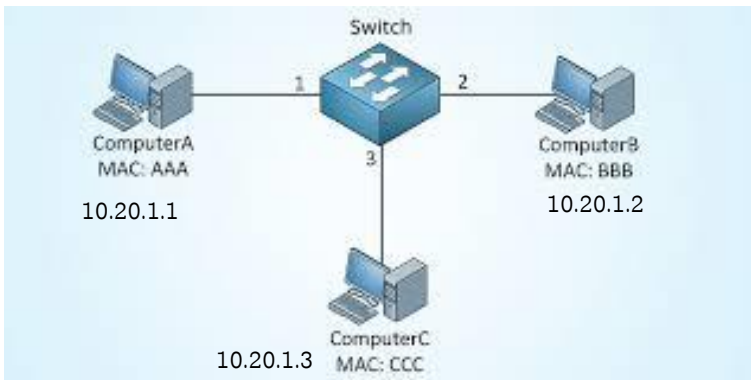
מטרות:

- ✓ גלישה מאובטחת - סינון תוכן
- ✓ הסתרת כתובות IP ארגוניות
- ✓ חסכון בכתובות IP ציבוריות
- ✓ הגדלת ביצועים (CACHE)

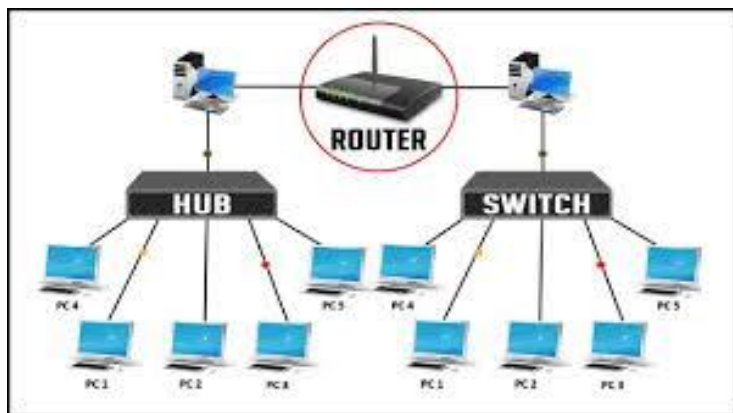




איך מתבצעת התקשורת?



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*)

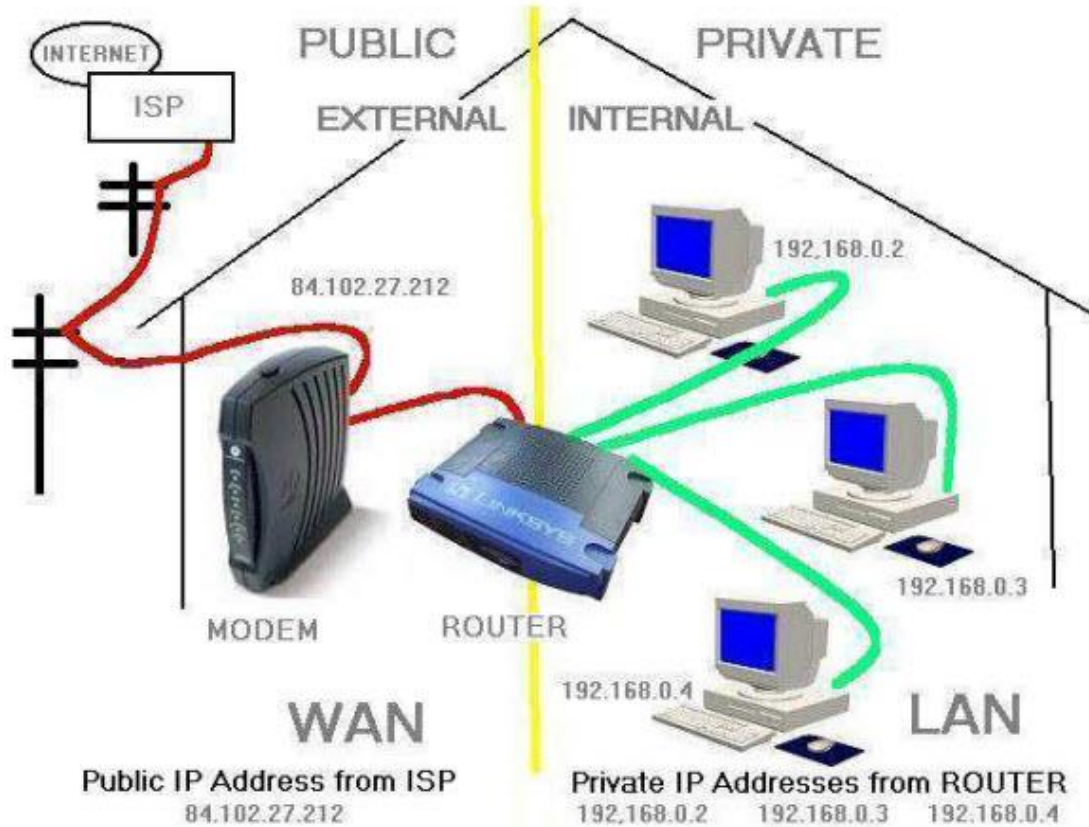
- לשימוש בתוך ארגון .
- אין להן אפשרות לצאת לעולם (גלישה, מיילים)
- אין הגבלה במספר הכתובות

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
RDP	3389	השתלטות מרחוק

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	3389	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	לכל מקום	כולם

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

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

LOGS – לוגים

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...		pci.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	ftp	robot.ftps.domain...		Alaska_DMZ_intern...
11	2Nov2008	8:11:22	Alaska_cluster	ftp	robot.ftps.domain...		Alaska_DMZ_intern...
12	2Nov2008	8:11:30	Alaska_cluster	ftp	robot.ftps.domain...		Alaska_DMZ_intern...
13	2Nov2008	8:12:29	Alaska_cluster	ftp	robot.ftps.domain...		Alaska_DMZ_intern...
14	2Nov2008	8:14:36	Alaska_cluster	ftp	robot.ftps.domain...		Alaska_DMZ_intern...
15	2Nov2008	8:14:38	Alaska_memb...				
16	3Nov2008	11:14:26	Alaska_cluster	ftp	robot.ftps.domain...		Alaska_DMZ_intern...
17	15Mar2009	1:00:1	Primary_Mana...				
18	15Mar2009	2:14:36	Alaska_cluster	http	resolved.hosts.com		Alaska_DMZ_intern...
19	15Mar2009	2:19:21	Alaska_Finan...	microsoft-ds	Alaska.IT.Bentli		10.112.254.9
20	15Mar2009	10:9:29	Alaska_RND_...	8080	10.111.254.31	Jennifer McHenry (jm...	192.168.9.111
21	15Mar2009	10:9:30	Alaska_RND_...	8080	10.111.254.31	Jennifer McHenry (jm...	192.168.9.111
22	15Mar2009	10:9:31	Alaska_RND_...	8080	10.111.254.31	Jennifer McHenry (jm...	192.168.9.111
23	16Mar2009	16:35:14	Alaska_cluster	http	scriptskids.inc		Alaska_DMZ_intern...
24	16Mar2009	16:35:19	Alaska_cluster	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		California.LAN.jaco...		
27	15Jan2009	22:59:34	California_GW	nbsession	California.LAN.ham...		Alaska.LAN.Chincilla
28	15Jan2009	22:54:14	Alaska_cluster	http	Alaska.Fin.Deasel		Florida.LAN.euclid
29	29Jan2009	22:53:49	Delaware_ciu...	nbsession	California.LAN.ham...		Alaska.LAN.Chincilla
30	2Feb2009	22:59:35	California_GW	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	http	Alaska.Fin.Deasel		Florida.LAN.euclid

שימוש שני: חציצה בין רשתות בארגון (סגמנטציה)



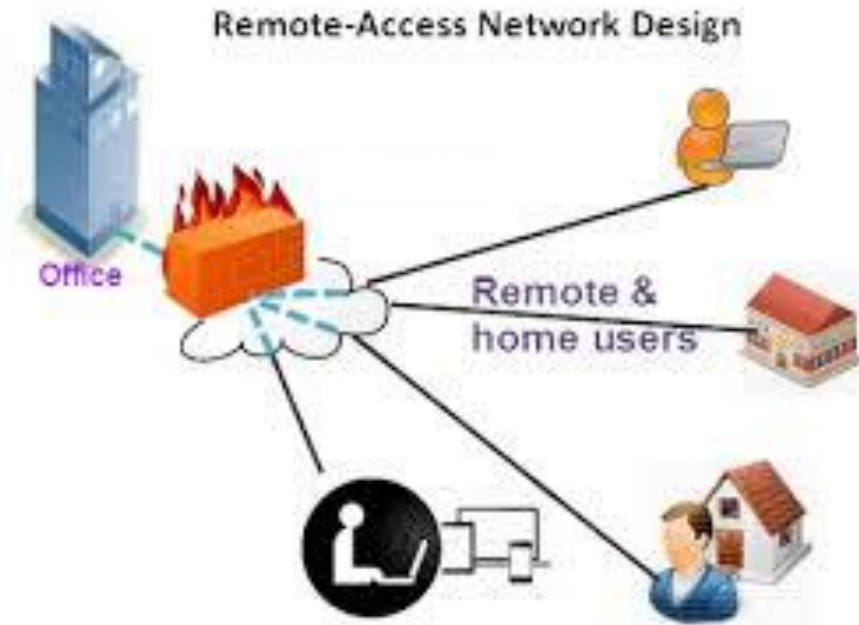
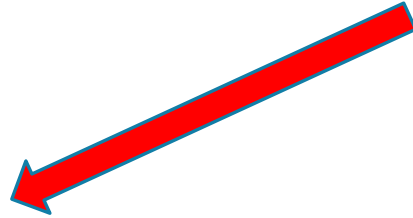
שימושים לחומת אש בארגון

שימוש ראשון: לאפשר תקשורת בטוחה לאינטרנט

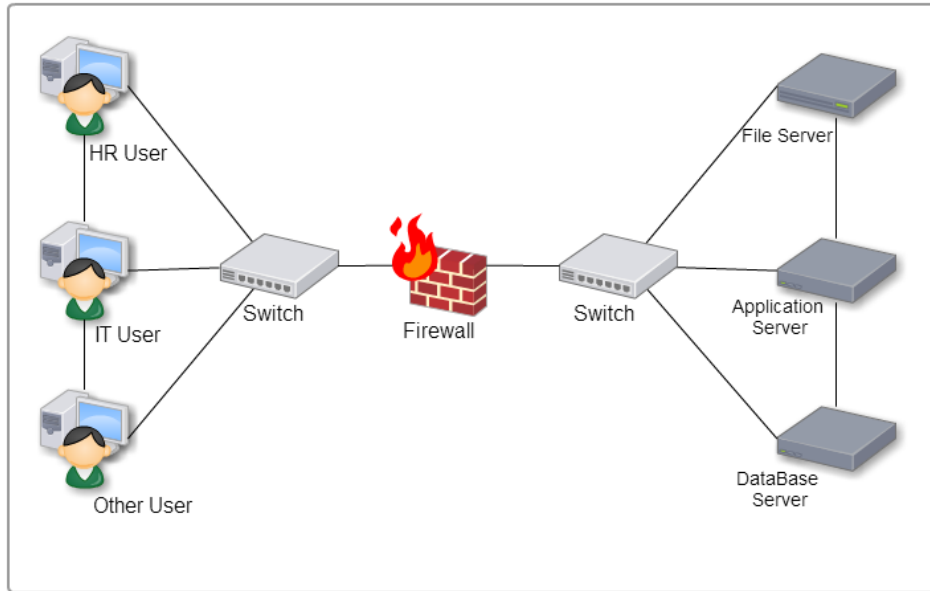


שימושים לחומת אש בארגון

שימוש שלישי:
גישה מרחוק לארגון – (VPN)

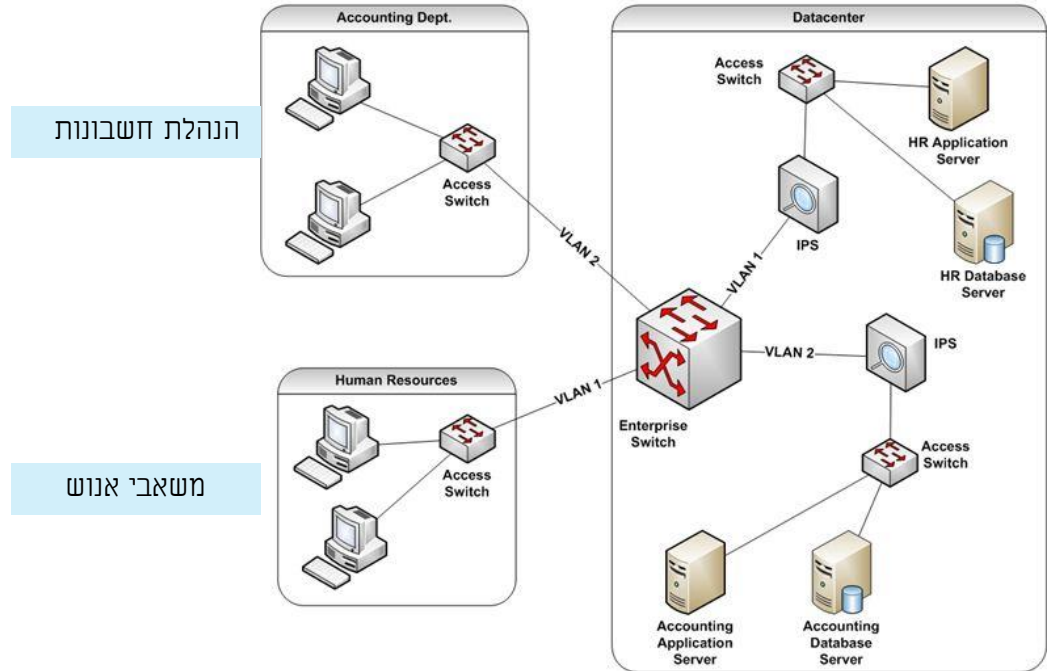


בין משתמשים לשרתים



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

בין מחלקות שונות בארגון



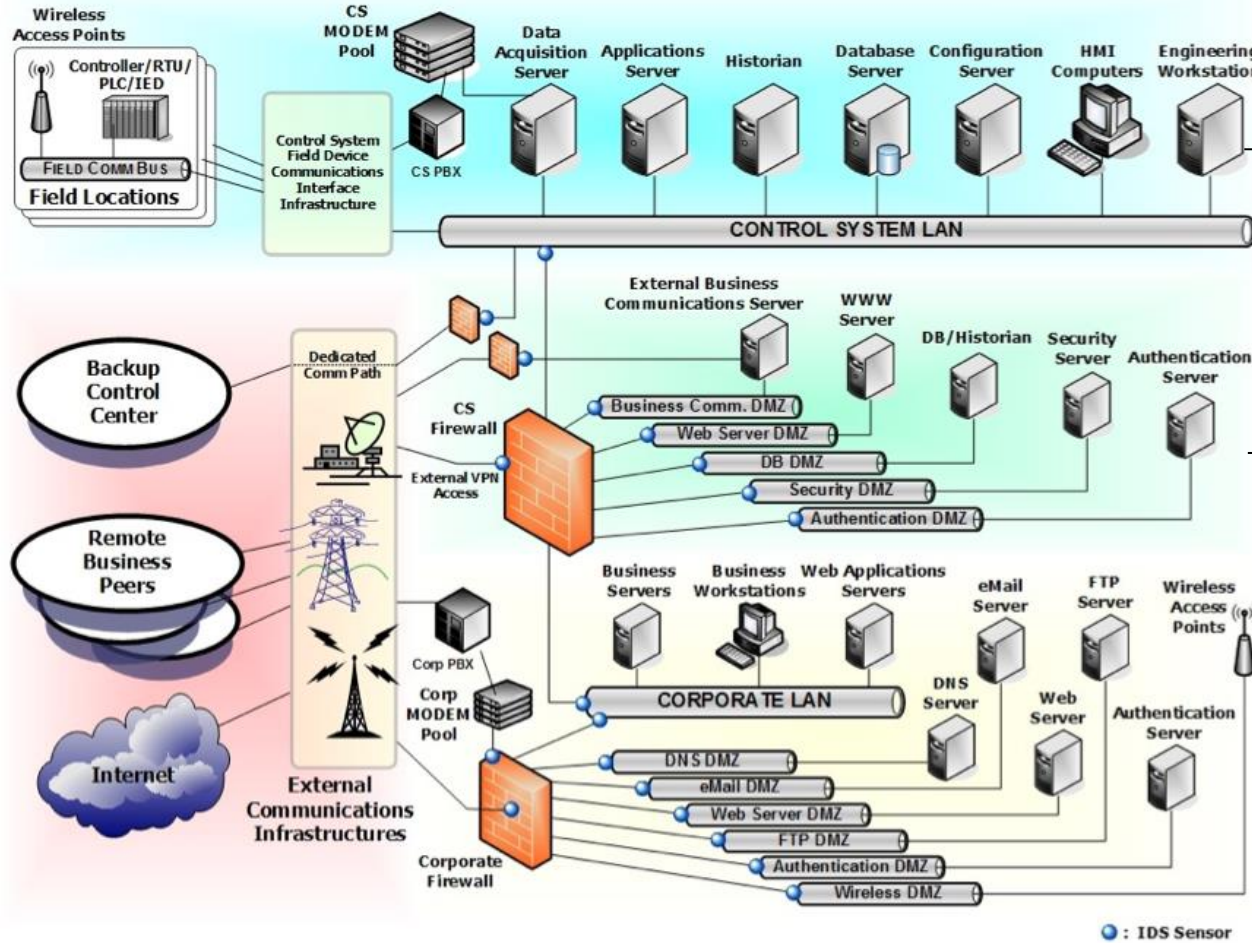
הנהלת חשבונות

משאבי אנוש

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

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

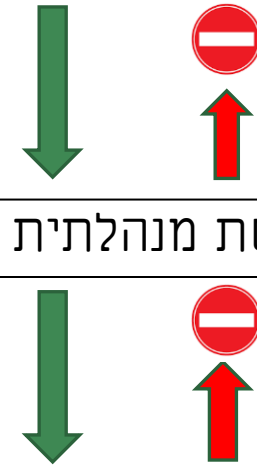
OT – Operation Technology
ICS – Industrial Control System



רשת ה-OT (ייצור)

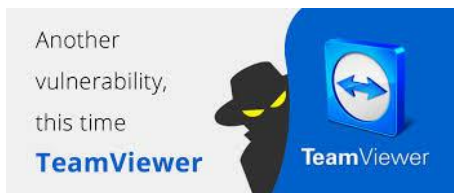
רשת מנהלתית

יציאה לאינטרנט



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

❑ גישה מוצפנת (VPN) מבחון אל ה-GATEWAY (חומת אש) ולא באמצעות גלישת WEB



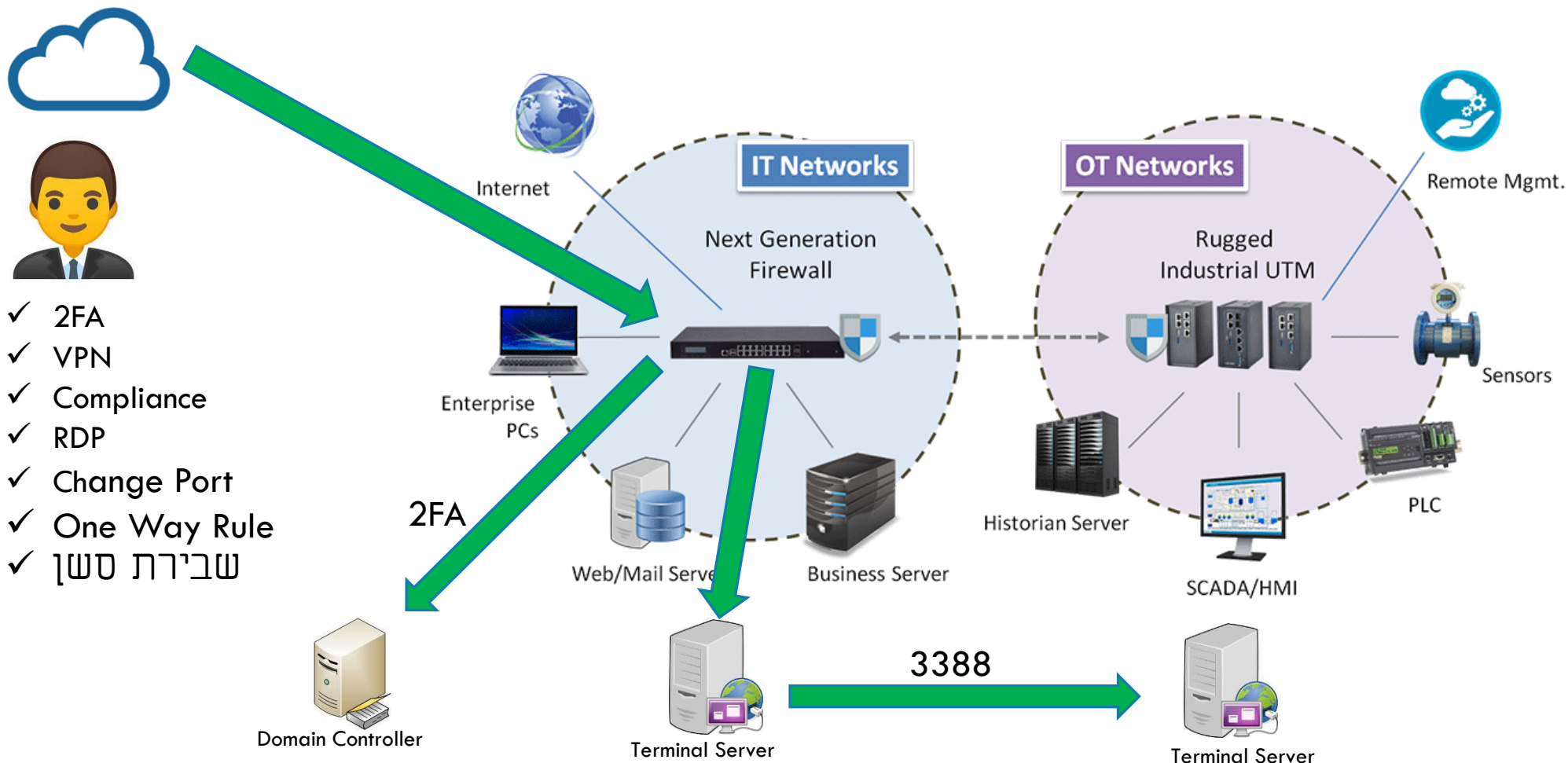
❑ בדיקת תאימות התחנה המתחברת – עדכוני אבטחת מידע ואנטי-וירוס

User Name: matrix
Password: 123456

❑ זיהוי לא גנרי של הספק

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

ארכיטקטורת התחברות מרחוק נכונה

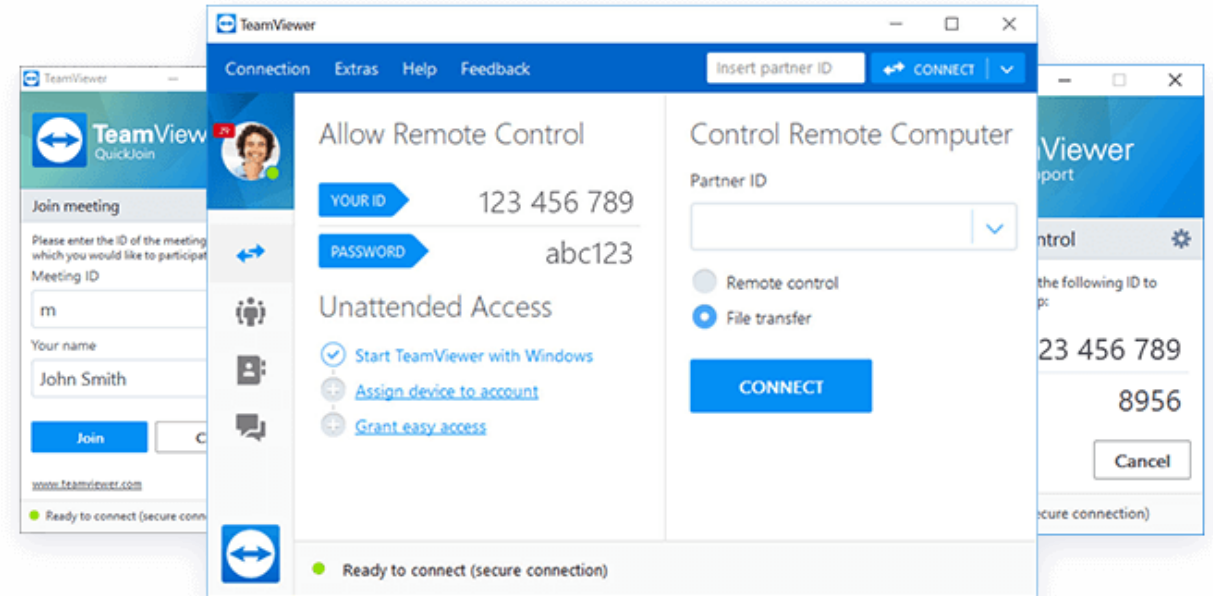
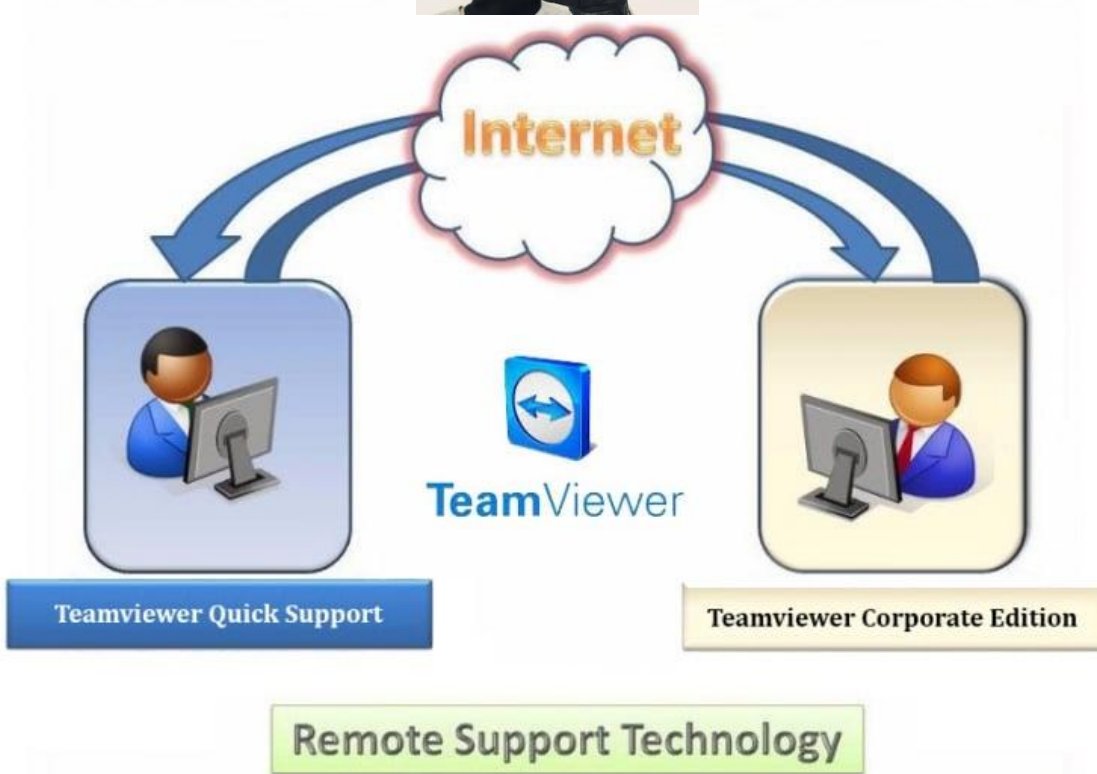


- ✓ 2FA
- ✓ VPN
- ✓ Compliance
- ✓ RDP
- ✓ Change Port
- ✓ One Way Rule
- ✓ שבירת סשן



איך עובד TEAM-VIEWER?

השתלטות ממחשב
השתלטות מטל סלולרי



תוכנות נוספות להשתלטות מרחוק מבוססות אינטרנט



לא לאפשר אלא אם כן השימוש הוא פנימי בלבד למשל תכנת VNC.

