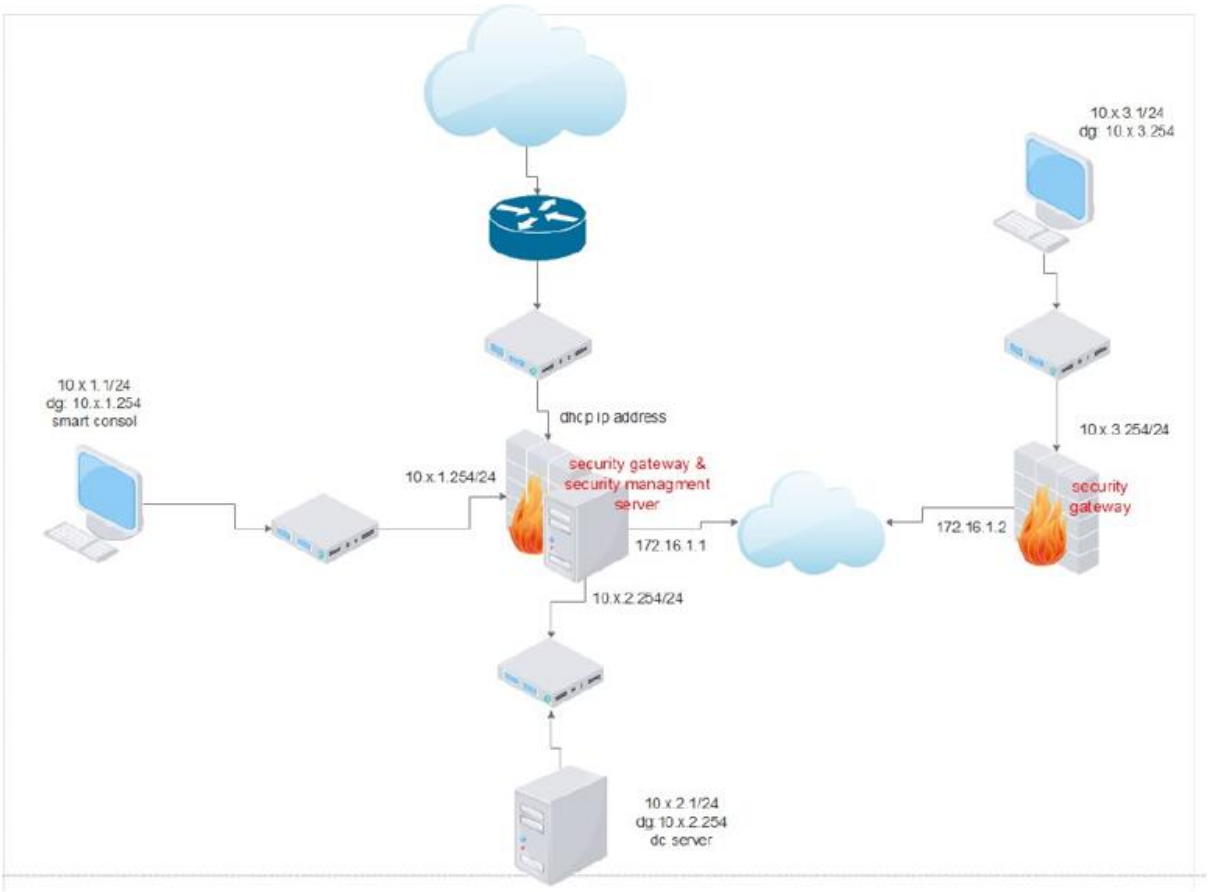
CSP Project

חלק א'- הקמת המעבדה

להלן טופולוגית הרשת:



By Elior Sofer

הקמת והגדרת מכונות PC1 PC2 ו WindowsServerLab

ראשית נתחיל בהקמת המכונה שתשמש אותנו לנהל את ממשקי ה SG (FW) באמצעות ה Smart Console.

פרטי המכונה:

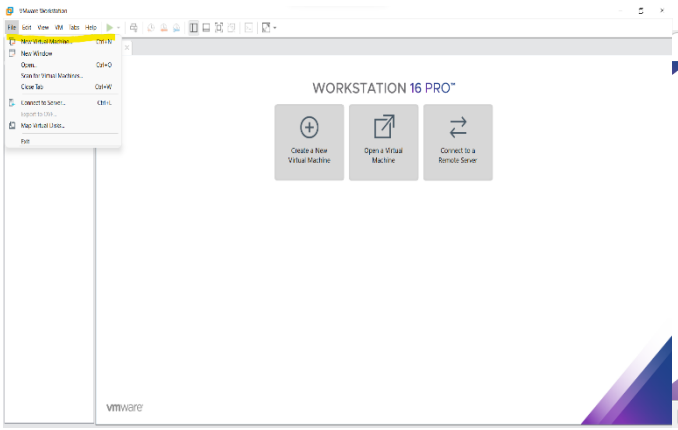
Name: PC1

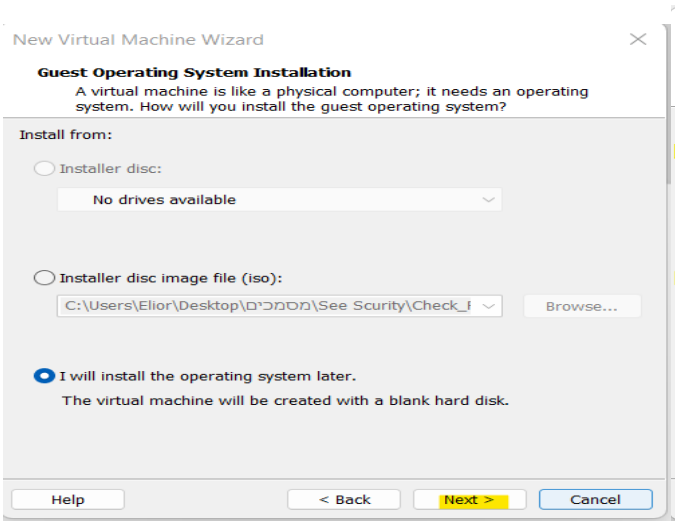
IP: 10.1.1.1/24

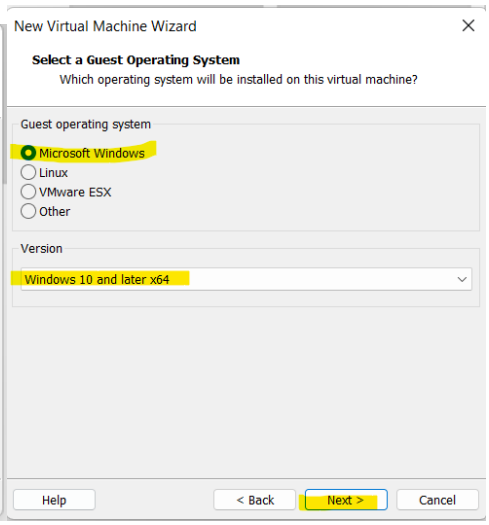
DG: 10.1.1.254

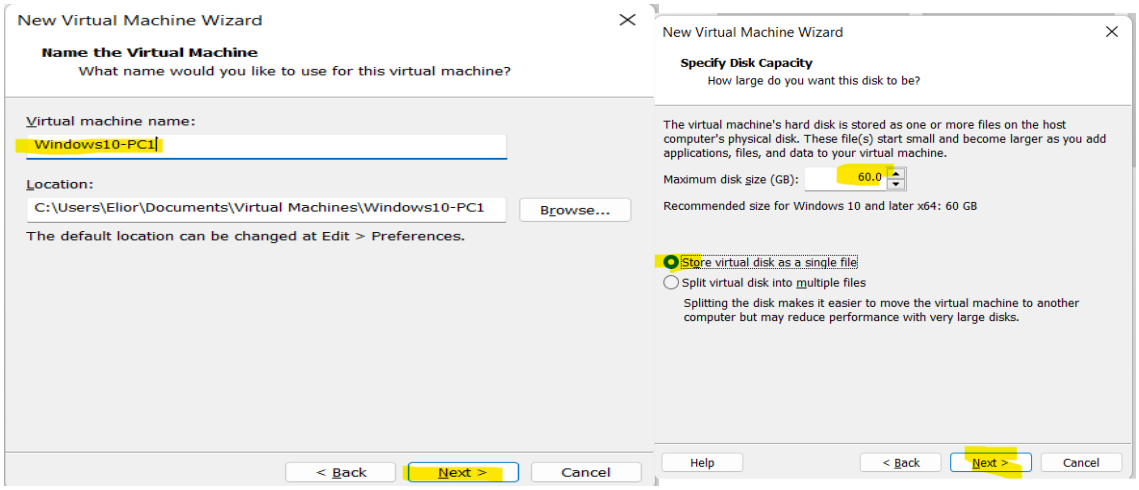
נא לעקוב אחרי השלבים הבאים הדרושים לצורך התקנת המכונה (משמאל לימין):

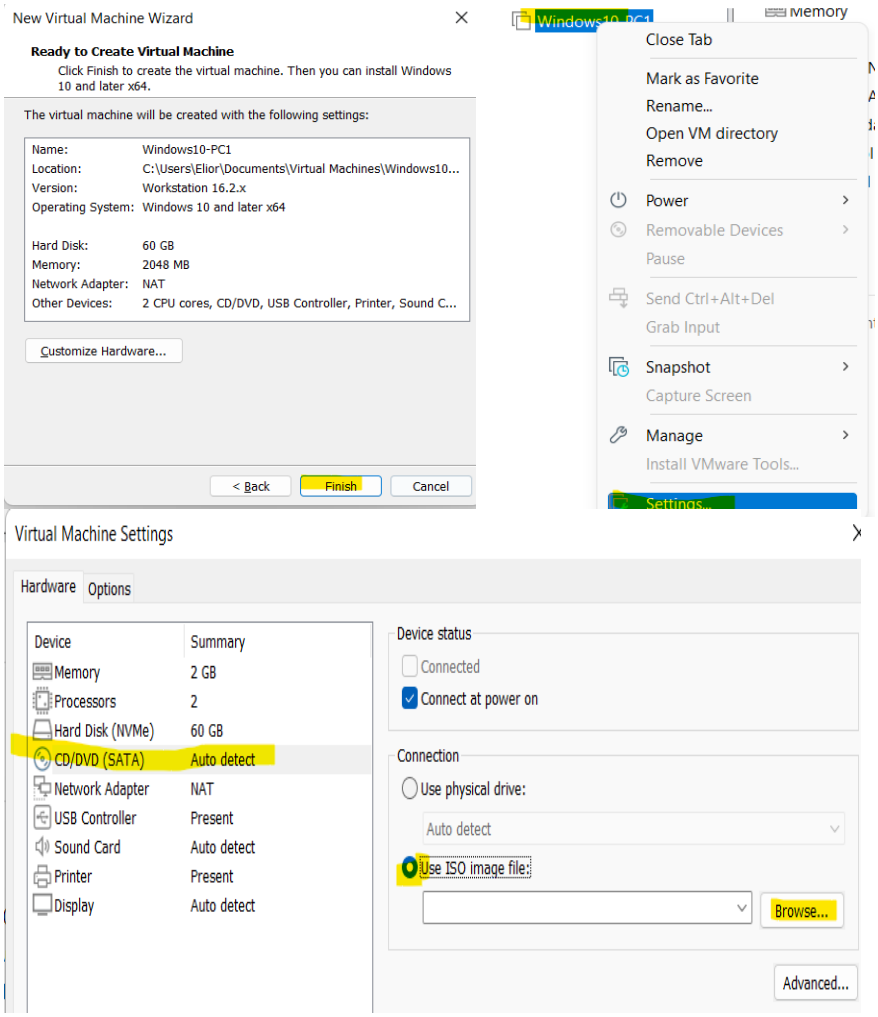
התהליך זהה לכל אחת מהתחנות קצה למעט תחנת הקצה GAIA. כמו כן במערכת הפעלה Windows Server יש צורך לבחור קובץ ISO שמיועד לה ולכל מכונה יש צורך להגדיר את הכתובת IP הרלוונטית לסגמנט שלה.



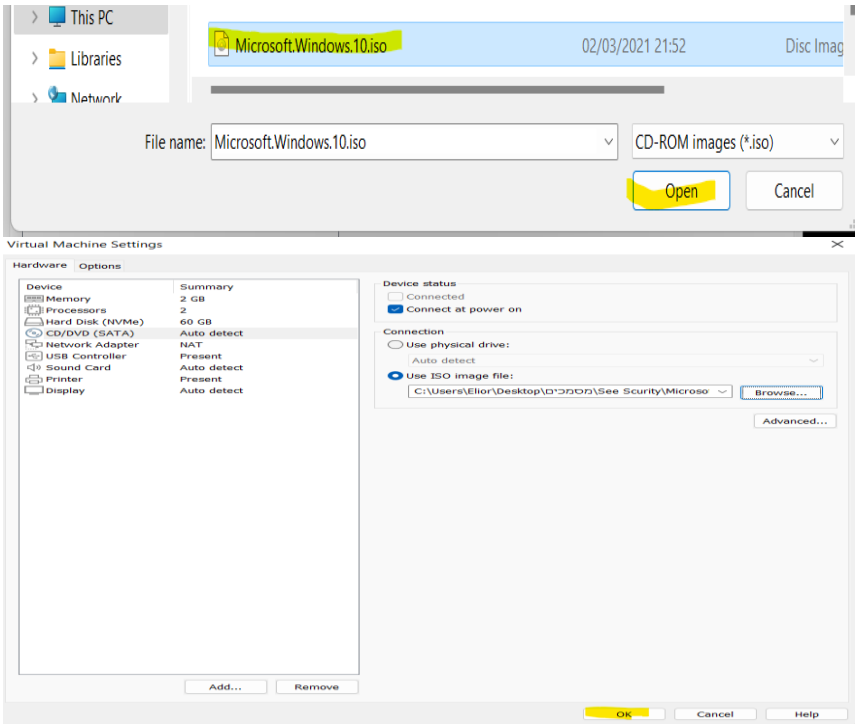


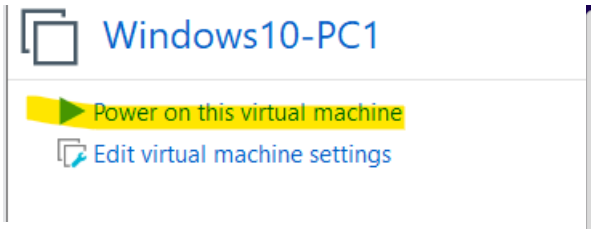


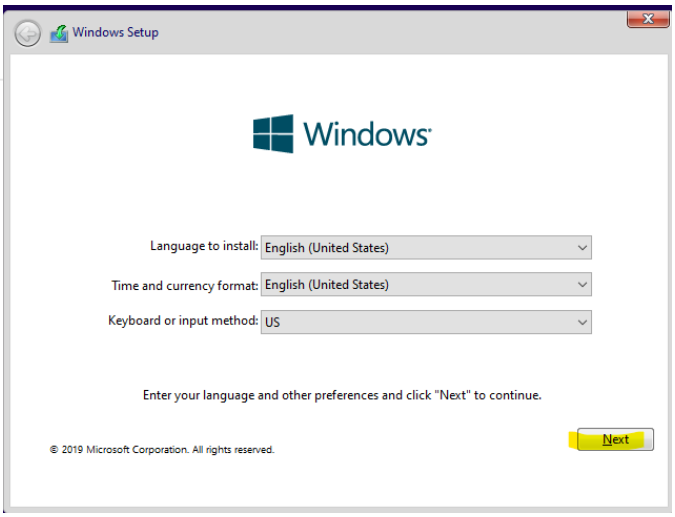


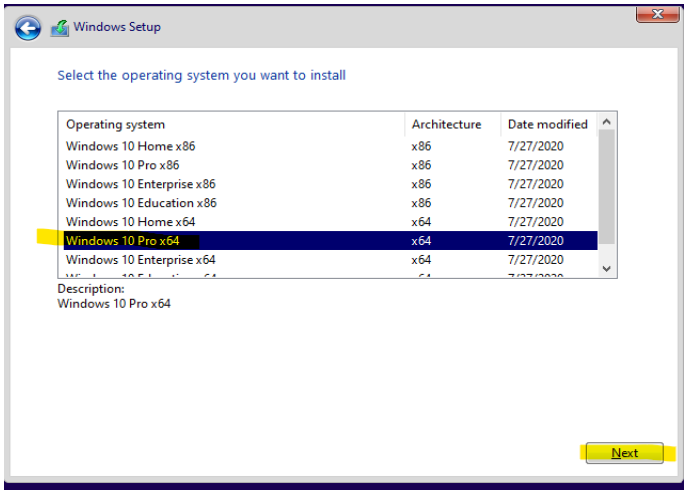


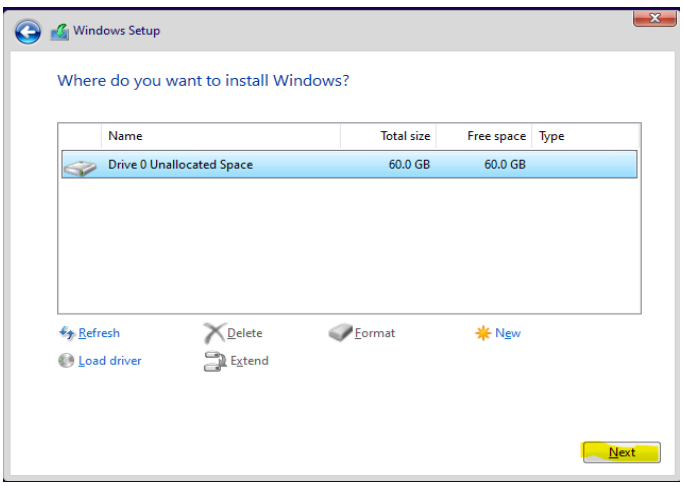
By Elior Sofer



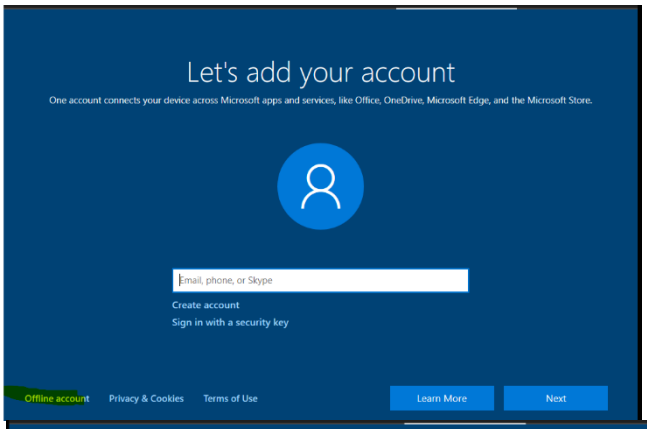


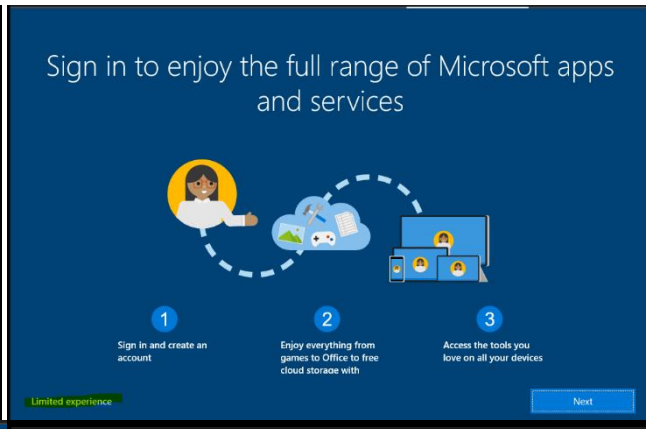


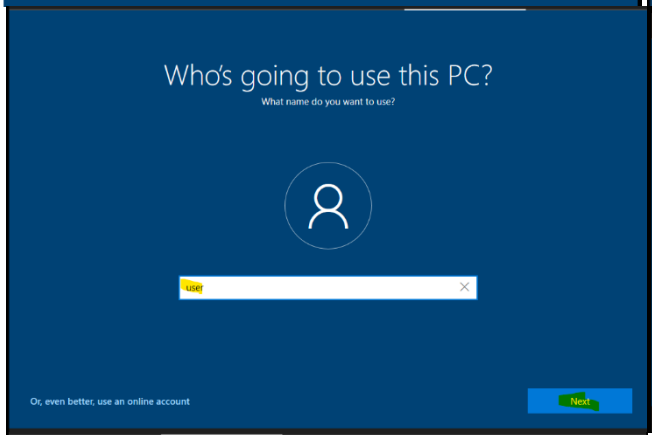


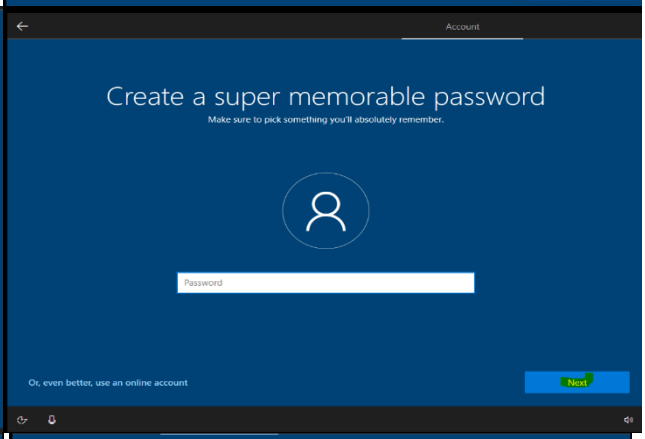


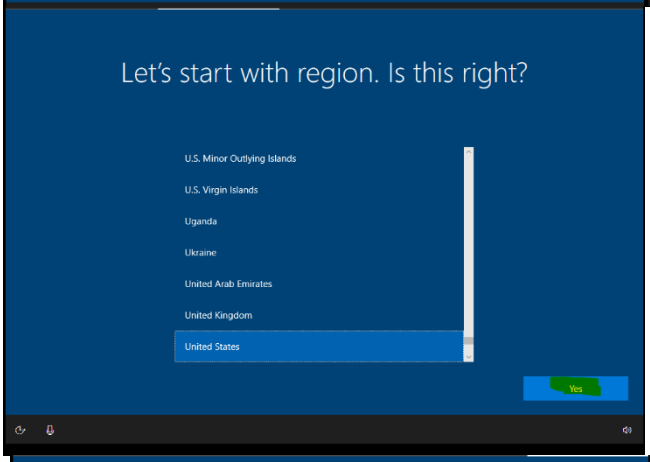
By Elior Sofer

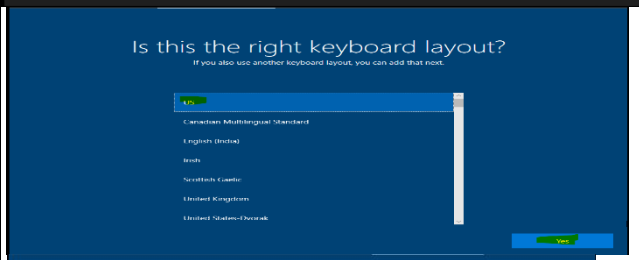


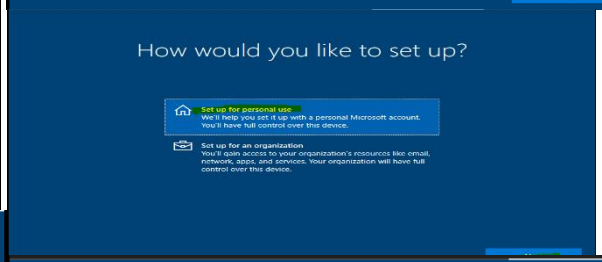


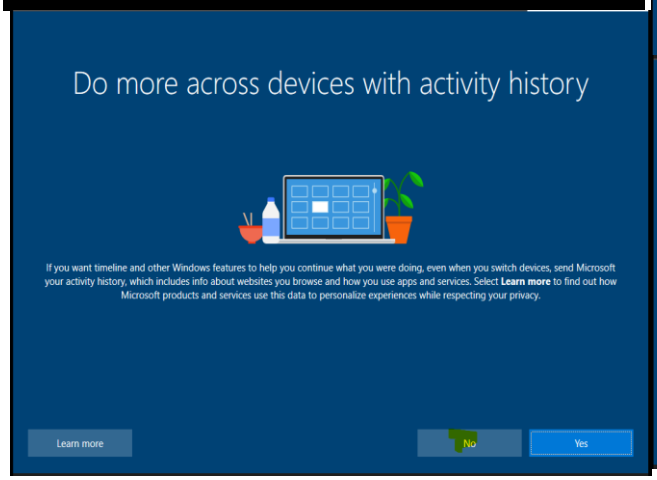


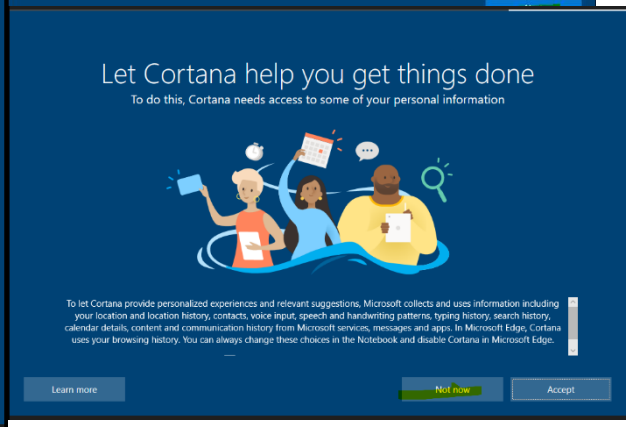






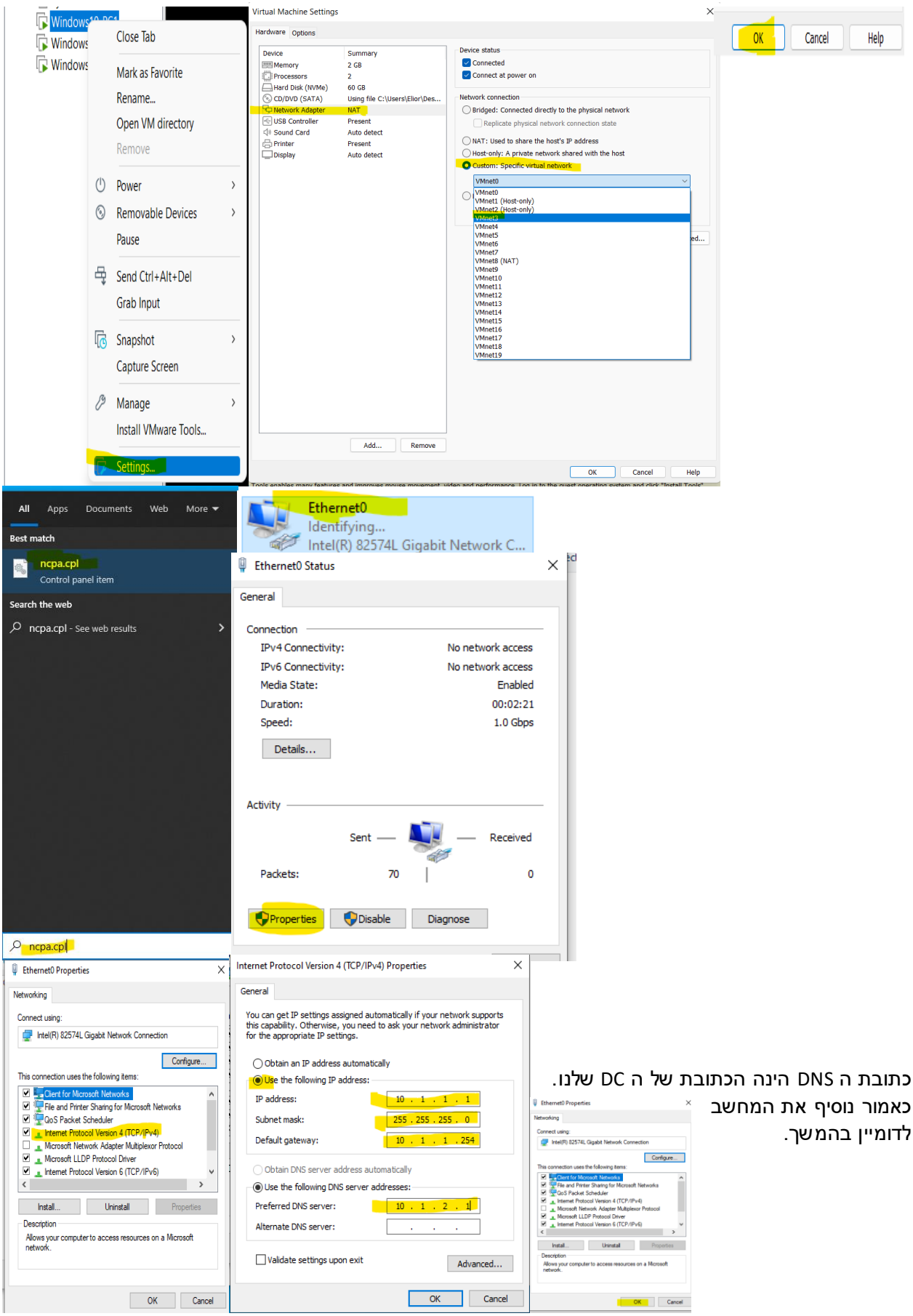






By Elior Sofer

כעת נשייך את המכונה **לסגמנט הרלוונטי אליה** ונגדיר לה כתובת IP:



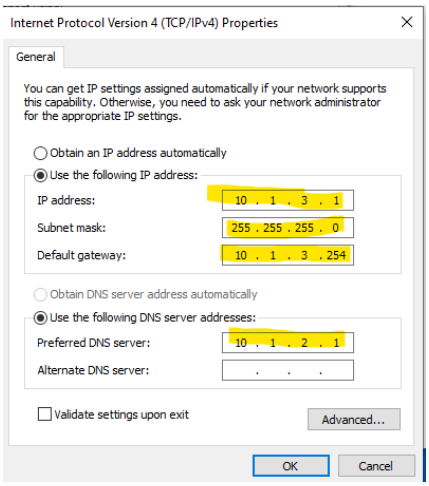
כתובת ה DNS הינה הכתובת של ה DC שלנו.
כאמור נוסיף את המחשב לדומיין בהמשך.

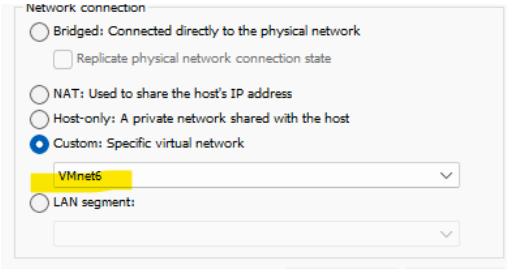
By Elior Sofer

כעת סיימנו להגדיר את המכונה הראשונה.

הגדרתי את המכונה PC2 בדיוק כמו שהגדרתי את המכונה הראשונה, אך שייכתי אותה ל 6VNET והגדרתי אותה לפי הפרטים שלהלן:

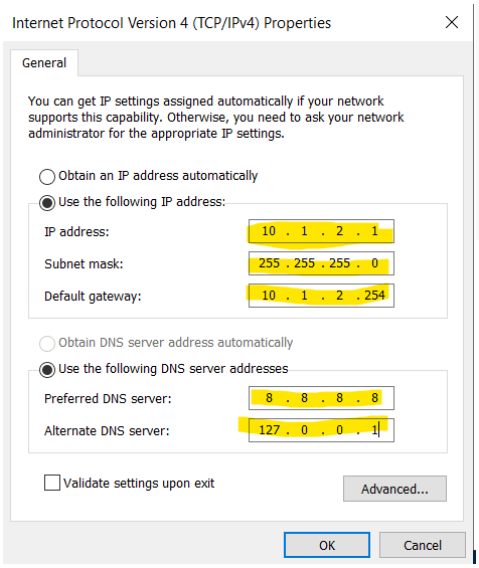
פרטי המכונה:
Name: PC2
IP: 10.1.3.1/24
DG: 10.1.3.254

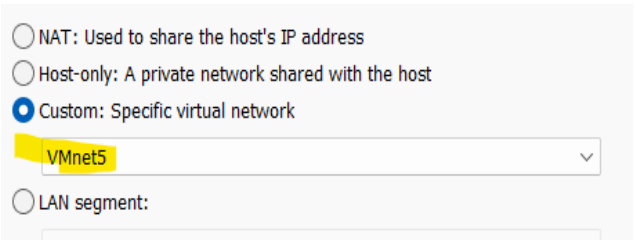




לאחר מכן הגדרתי את המכונה Windows Server אשר תשמש אותנו בתור DC, שרת DNS ושרת IIS. ההגדרה הייתה מאוד דומה להגדרה של המכונה הראשונה והשנייה. שייכתי אותה ל VNET5 והגדרתי אותה לפי הפרטים שלהלן:

פרטי המכונה:
Name: WindowsServerLab
IP: 10.1.2.1/24
DG: 10.1.2.254





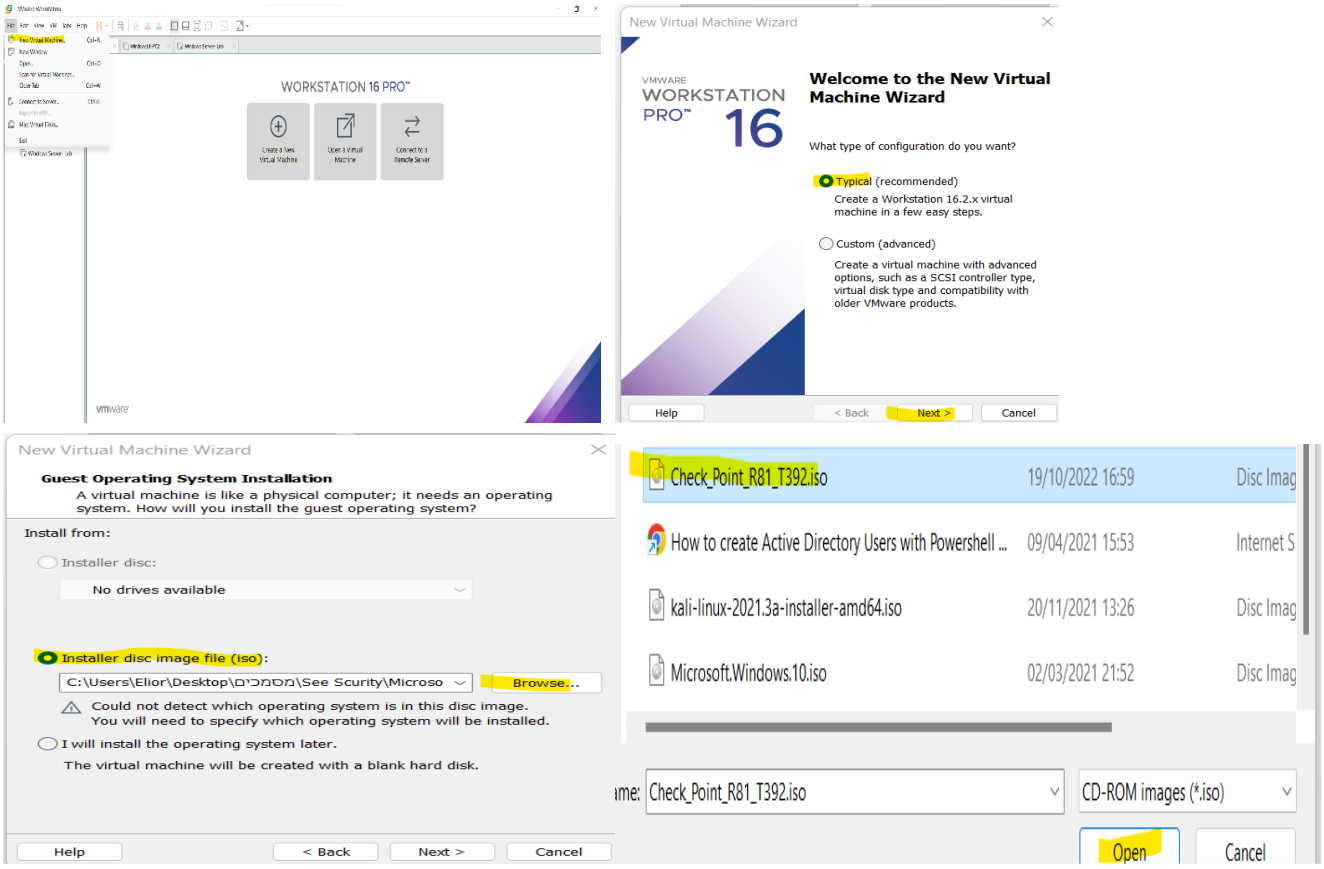
הקמת 2 שרתי Security Gateway ו Security Management Server

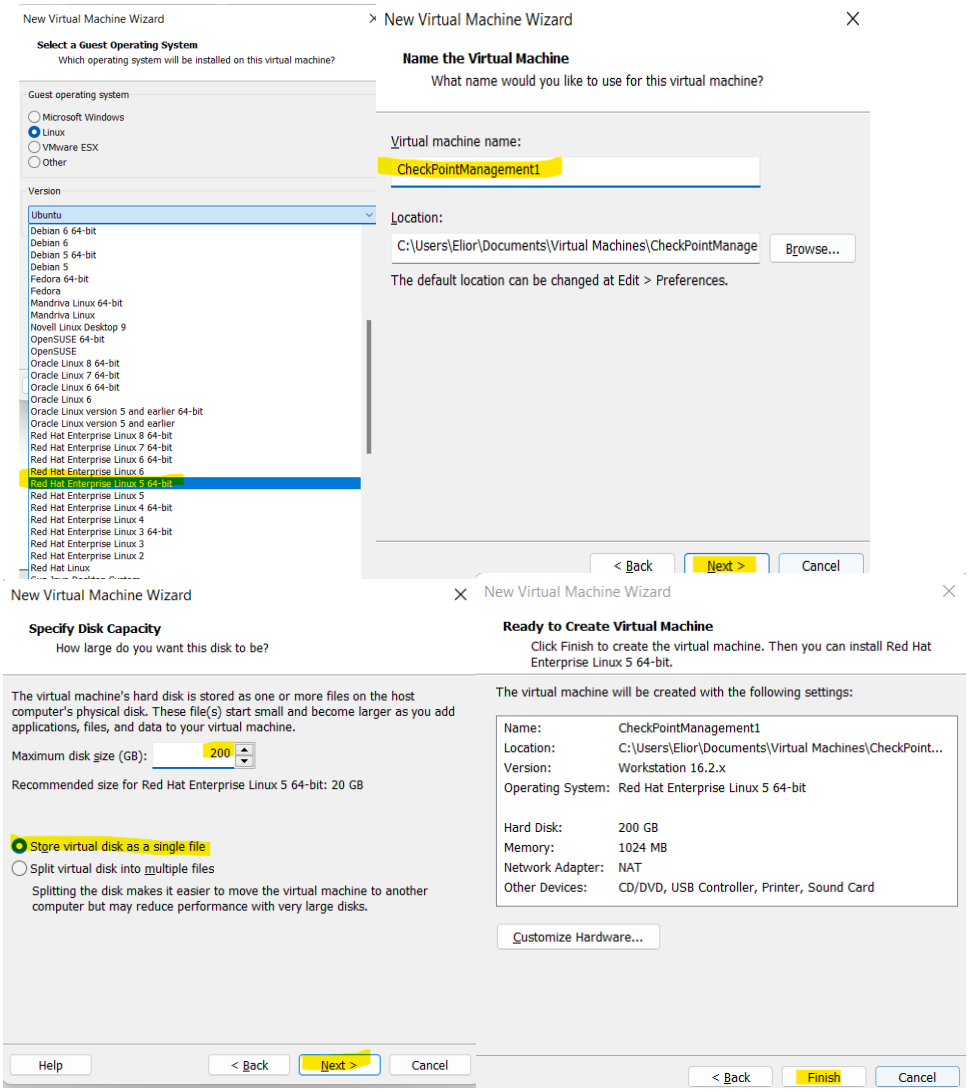
בשלב זה נקים לפי הטופולוגיה SG +Security Management server (Stand Alone) ובסגמנט נפרד SG נוסף (Distributed).

במכונה שתכיל את ה SG יחד עם ה Security Management יהיו 4 ממשקים:

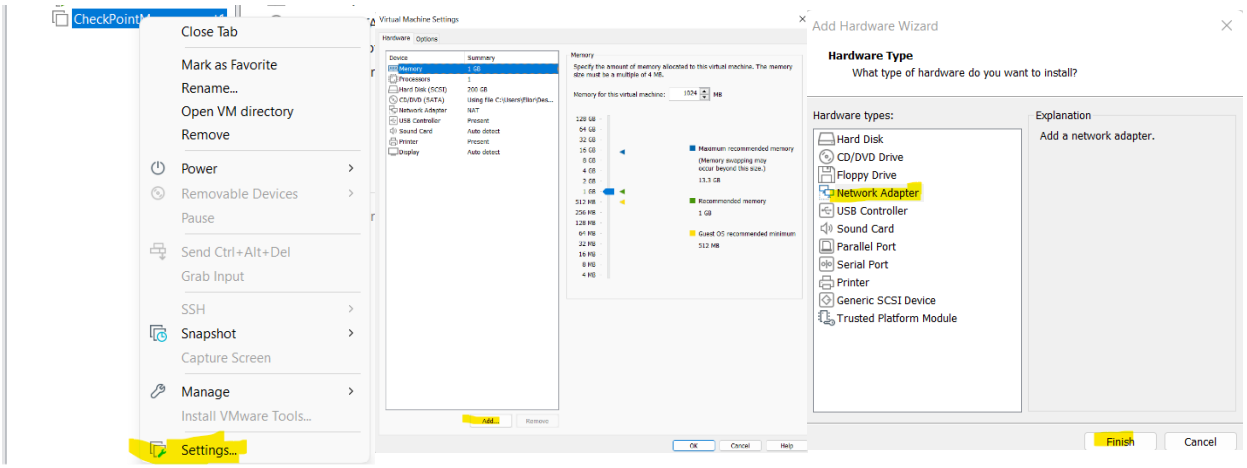
- 10.1.1.254 אשר יתחבר לסגמנט של PC1 ויהווה ממשק ניהול.
- 10.2.1.254 אשר יתחבר לסגמנט של WindowsServerLab
- 172.16.1.1 אשר יתחבר ל SG השני, אשר יתחבר לסגמנט של PC2.
- Bridge אשר יאפשר יציאה החוצה לאינטרנט.

יש לעקוב אחרי השלבים הבאים על מנת להקים את המכונה הראשונה שתכיל את ה SG יחד עם ה Security Management:



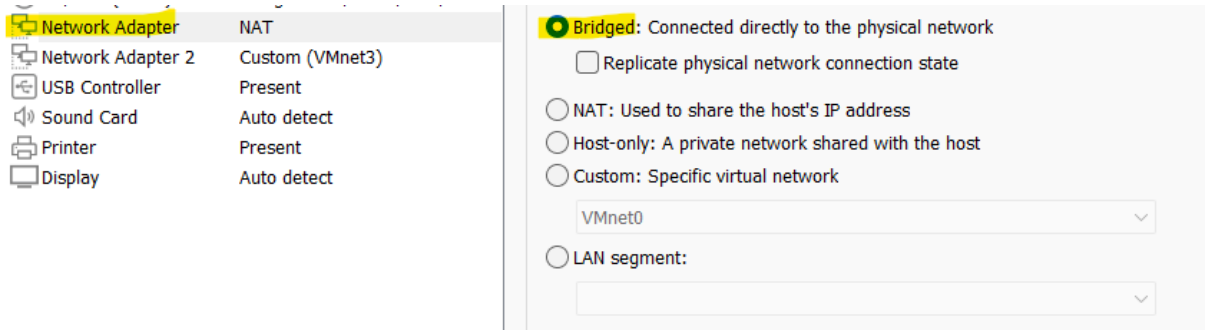


כעת נגדיר את 4 הממשקים במכונה. כל רשת לפי ה VNET הרלוונטי לה (מבצעים את הפעולה 3 פעמים בהתאמה מכיוון שיש כבר כרטיס אחד שמגיע עם המכונה שישמש אותנו ליציאה החוצה לאינטרנט-Bridge Interface):

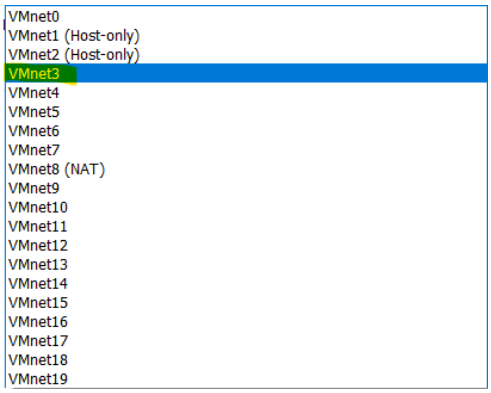


By Elior Sofer

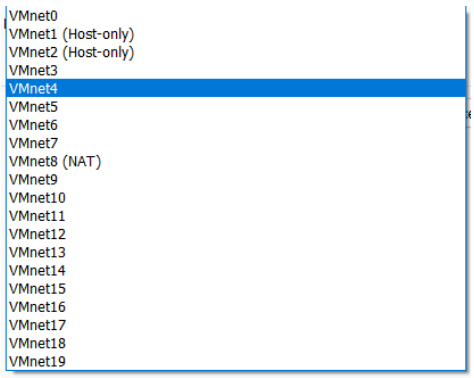
כרטיס הרשת שמשתמש אותנו ליציאה החוצה:



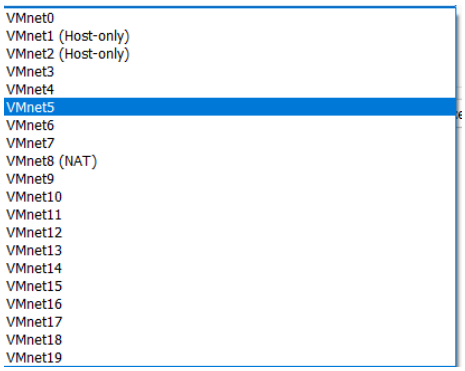
כרטיס הרשת שמשתמש אותנו לניהול הממשק:



כרטיס הרשת שמחבר אותנו למכונת PC2 ול SG השני:

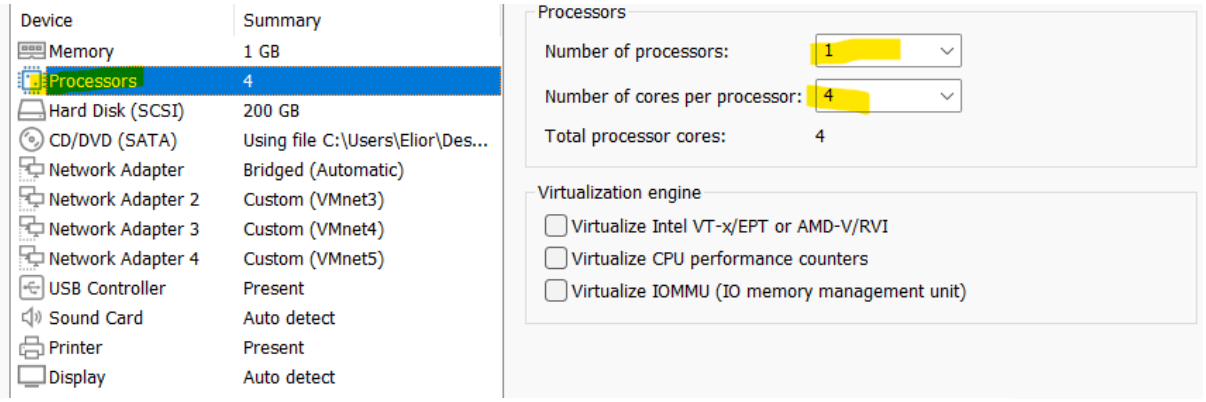


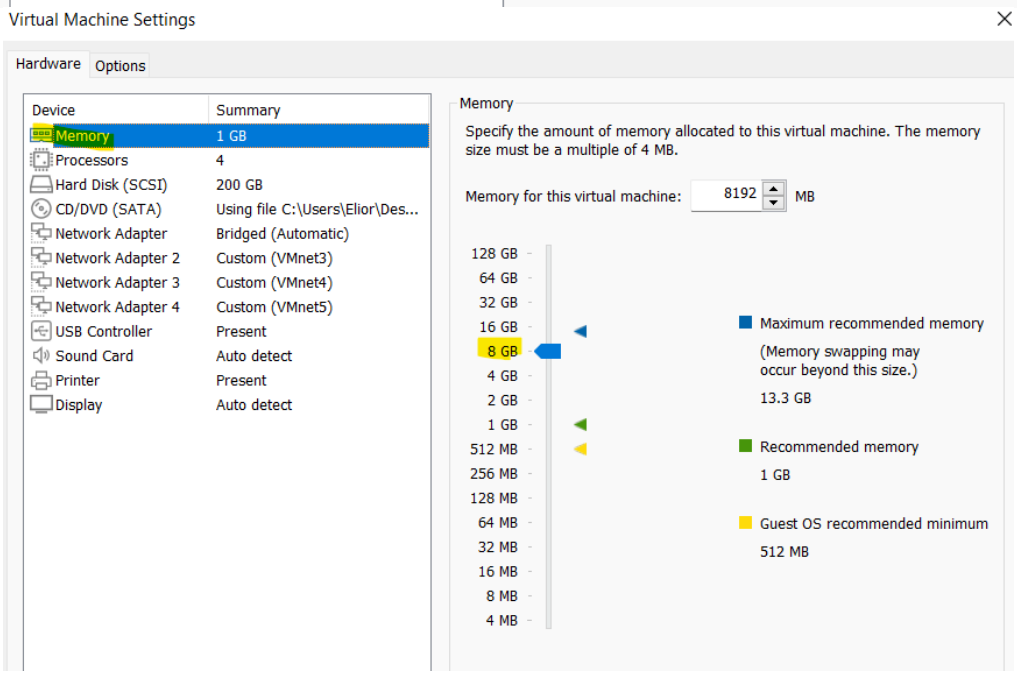
כרטיס הרשת שמחבר אותנו ל WindowsServerLab:

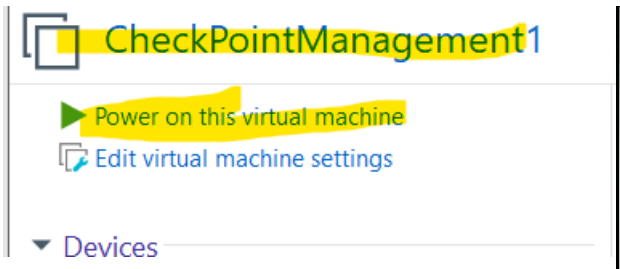


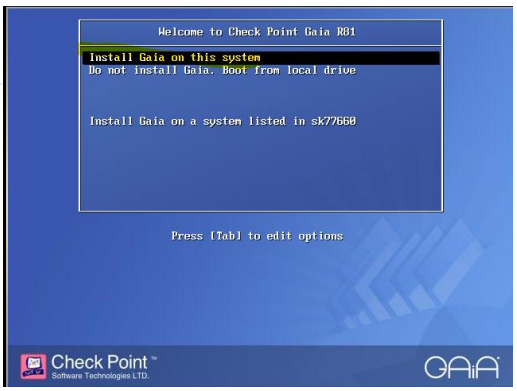
By Elior Sofer

כעת נמשיך בתהליך ההתקנה וההגדרה של המכונה:

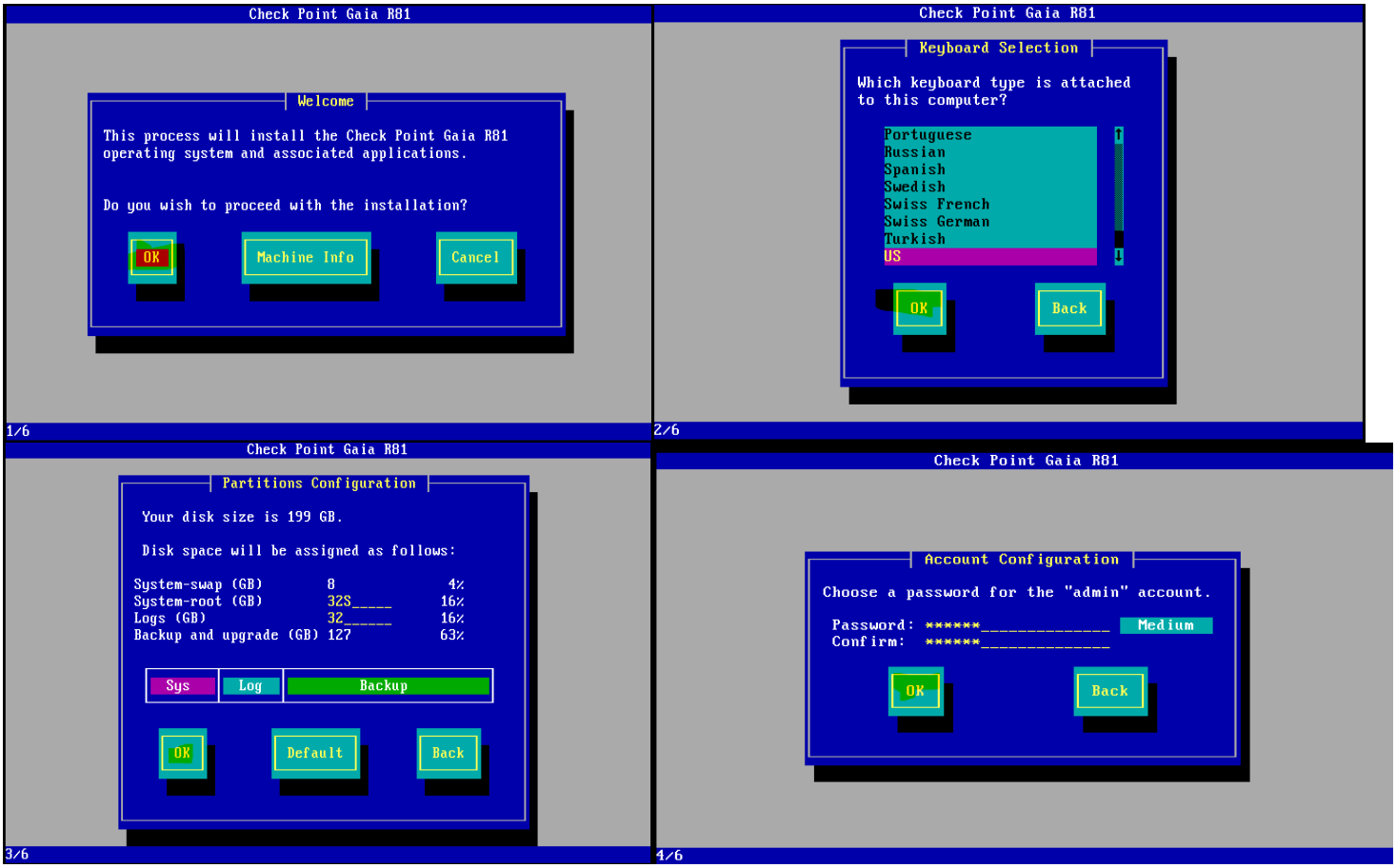




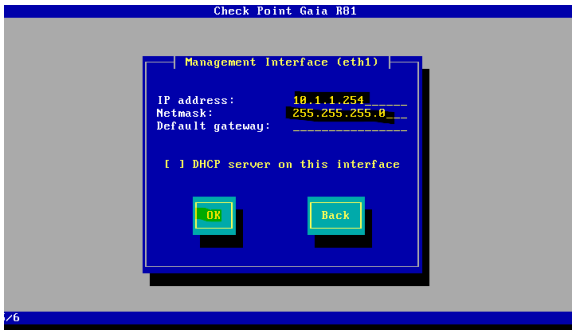




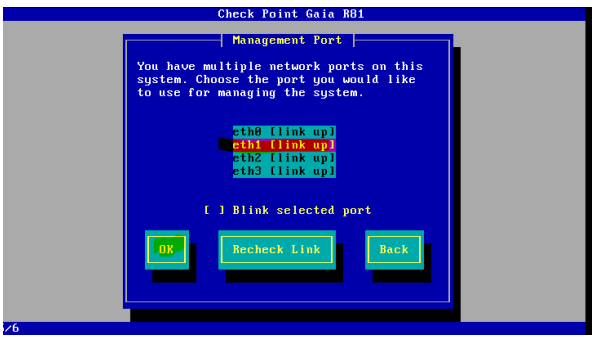
By Elior Sofer



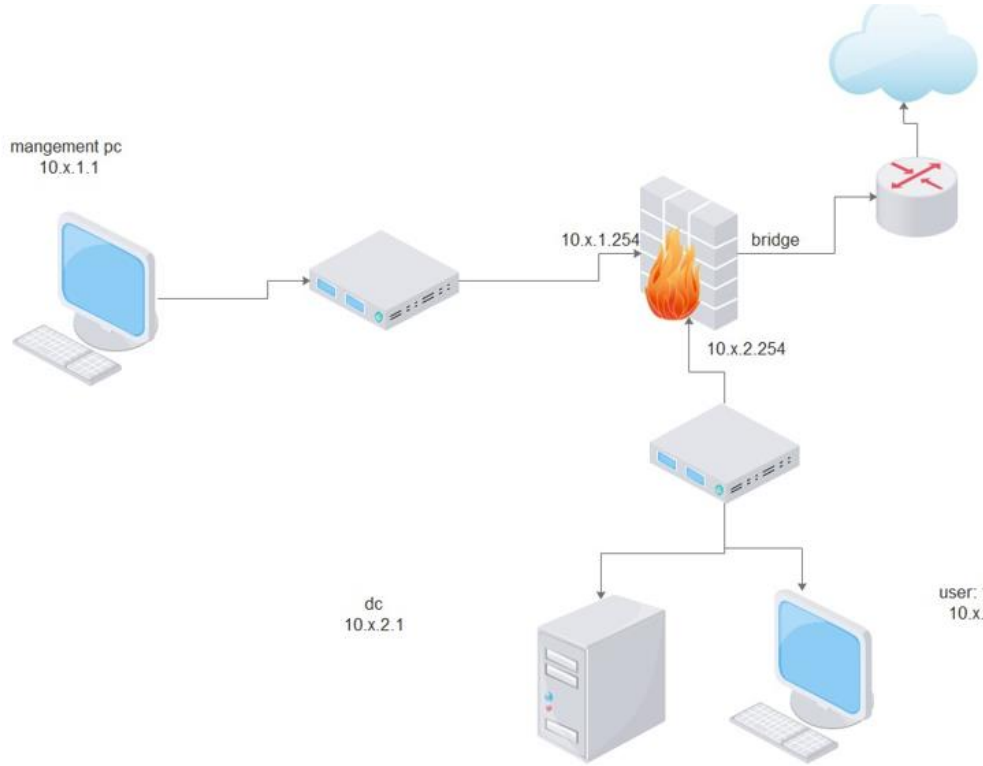
בשלב זה נבחר את הממשק שדרכו נרצה לנהל. במקרה של זה VNET3 והוא נמצא שני. לכן בחרתי ב eth1

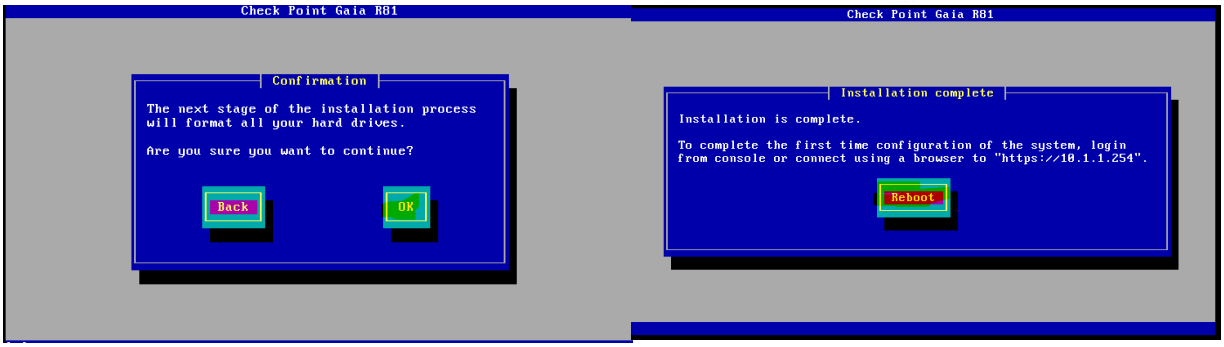


כעת אגדיר בשדה הראשון את הכתובת IP של היציאה לממשק זה מהמכונה:



By Elior Sofer



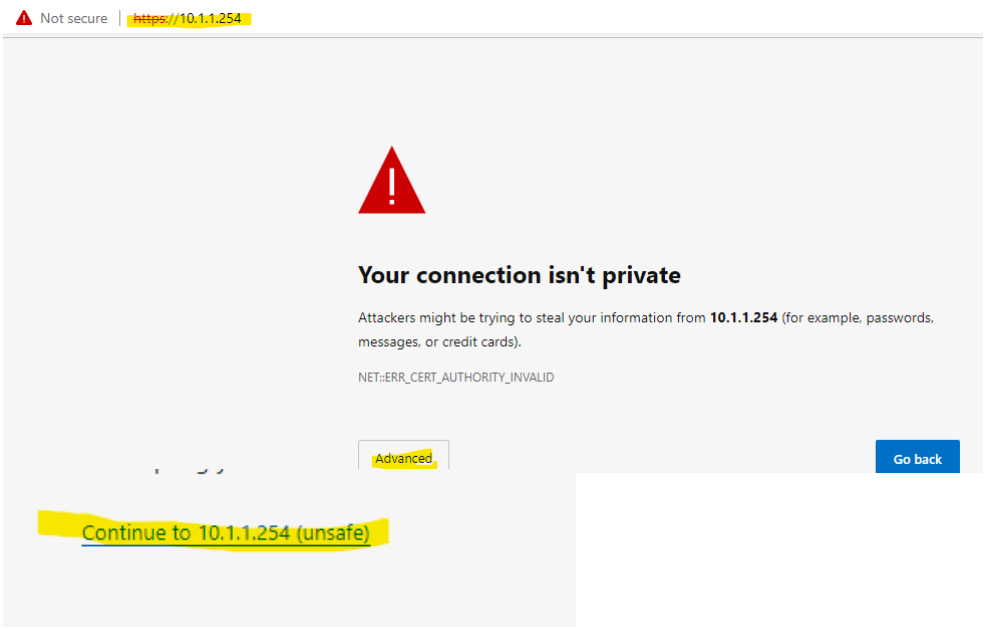


כעת המערכת הפעלה GAIA תעלה. נזין שם משתמש וסיסמא שהגדרנו בתהליך ההתקנה

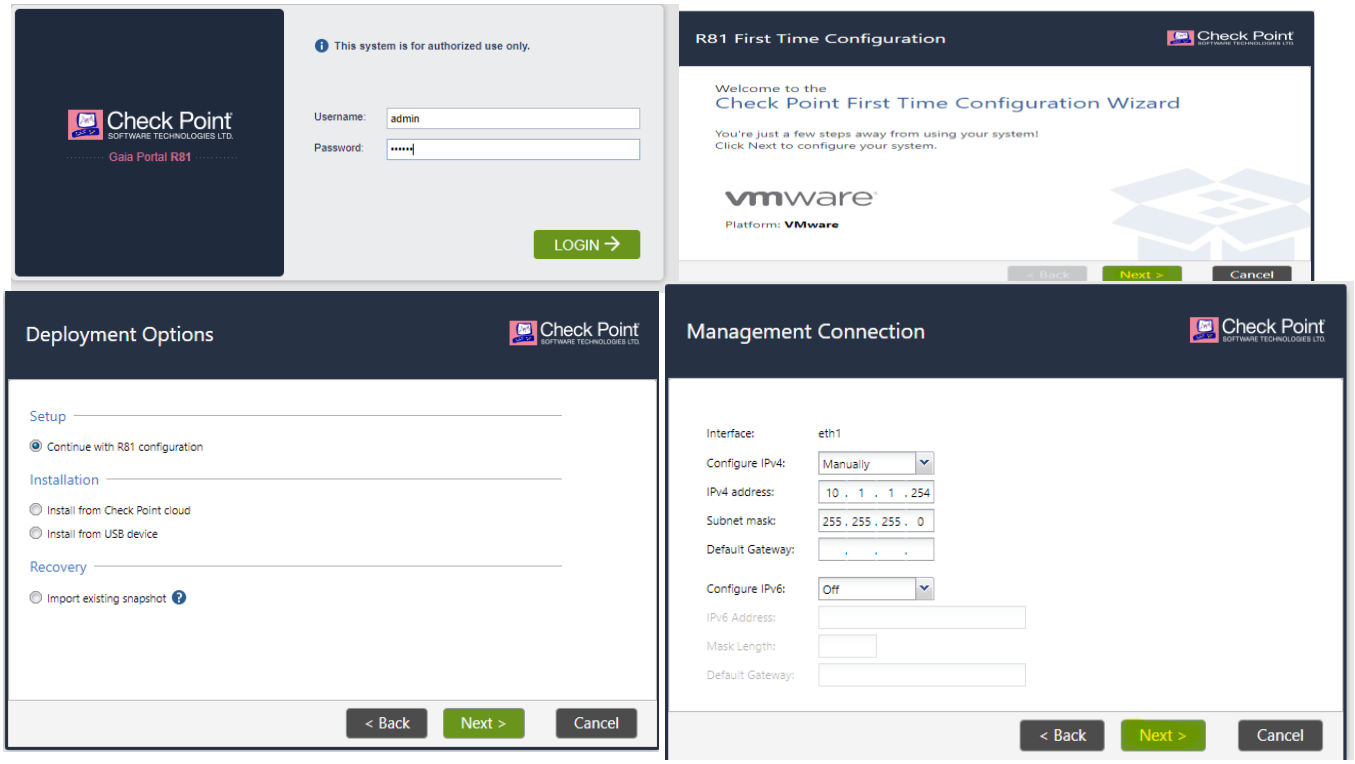
כעת נצטרך להגדיר את ה SMART CONSOLE דרך הדפדפן ב **PC1 אשר נמצא בממשק הניהול:**

נכנס דרך PC1 לכתובת של הממשק: https://10.1.1.254

By Elior Sofer

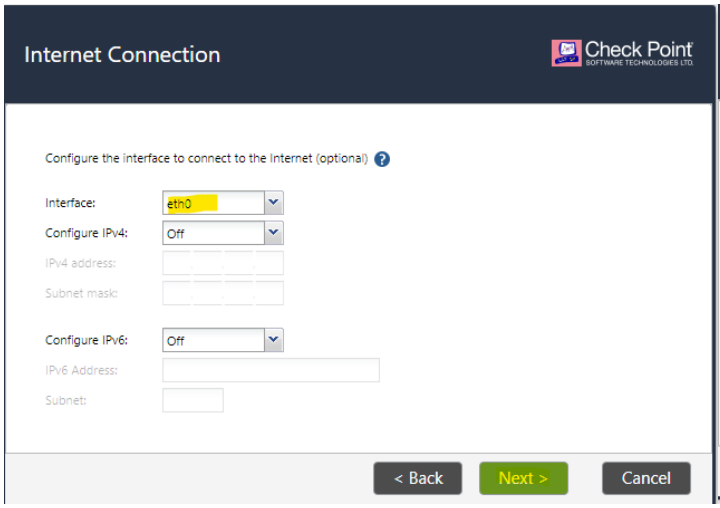


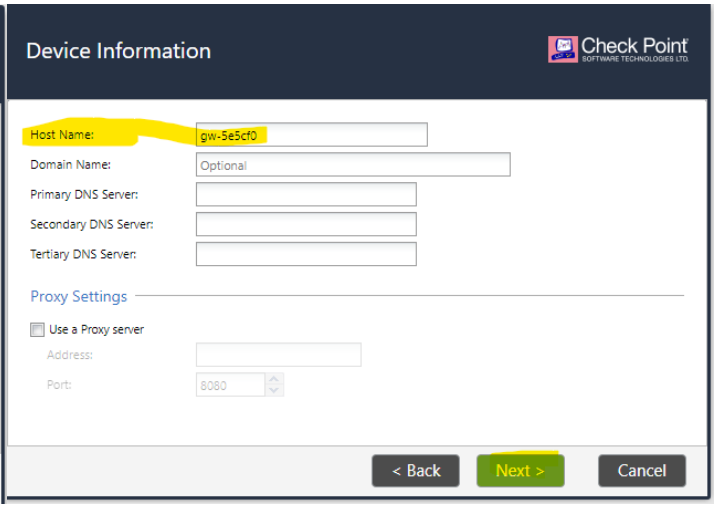
כעת נזין את השם משתמש וסיסמא שהגדרנו בתהליך ההתקנה:

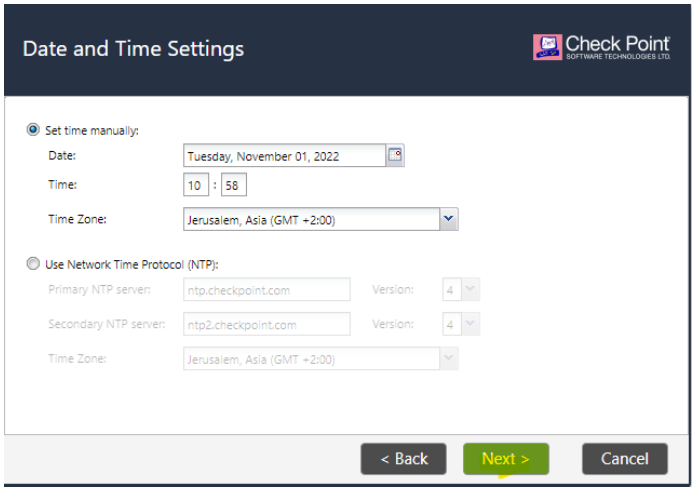


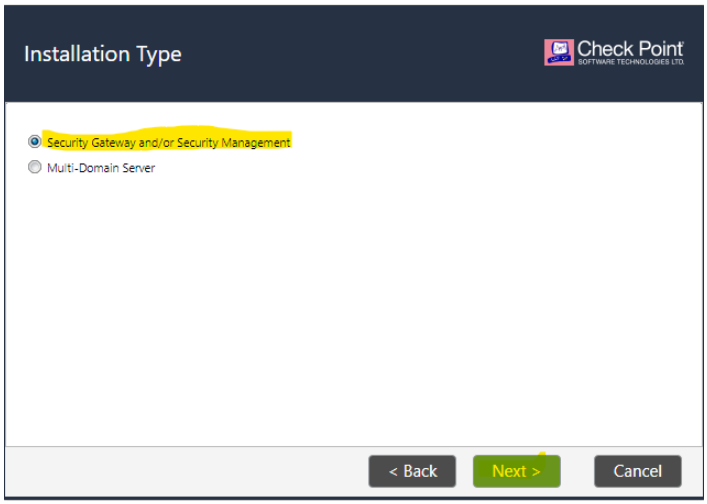
By Elior Sofer

כעת אגדיר תחת Interface את הממשק שמוציא לאינטרנט. במקרה שלי זה eth0

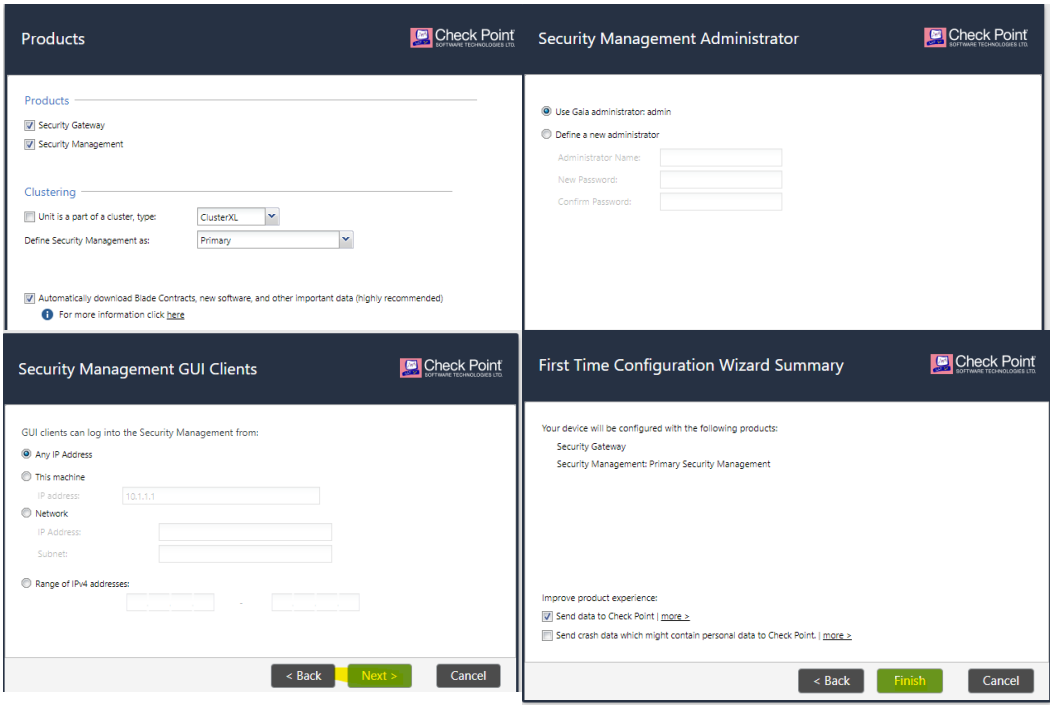




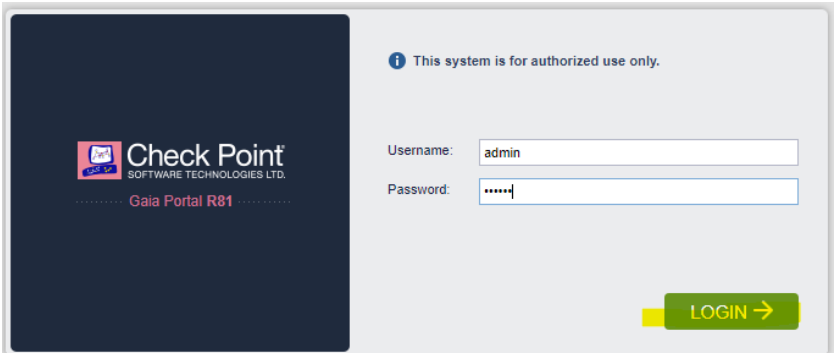




By Elior Sofer

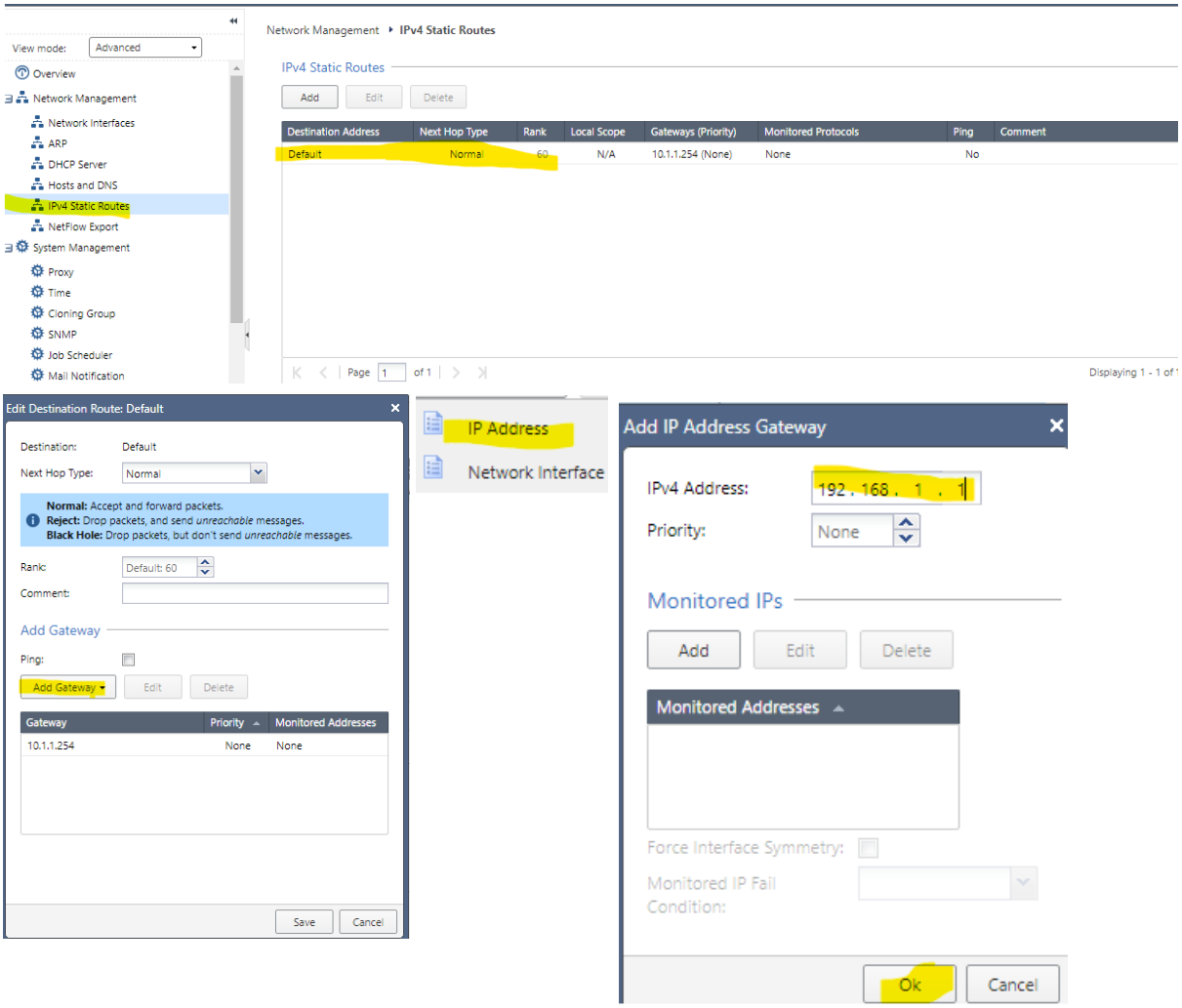


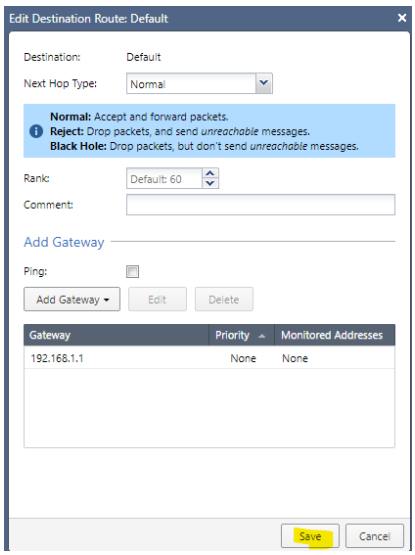
כעת לאחר ההתקנה נתחבר לממשק הניהול:



כעת נצטרך להגדיר את היציאה החוצה לאינטרנט. נזין את הכתובת של ה DG במחשב שלנו (הפיזי):

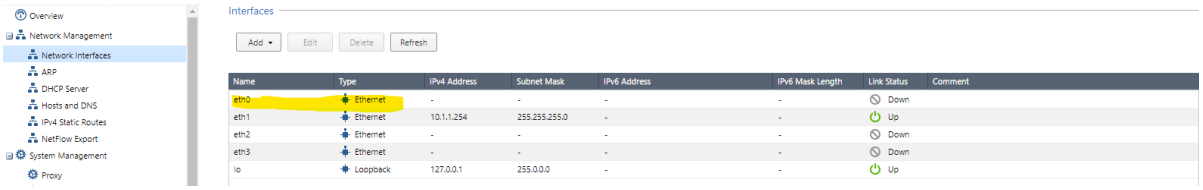
By Elior Sofer

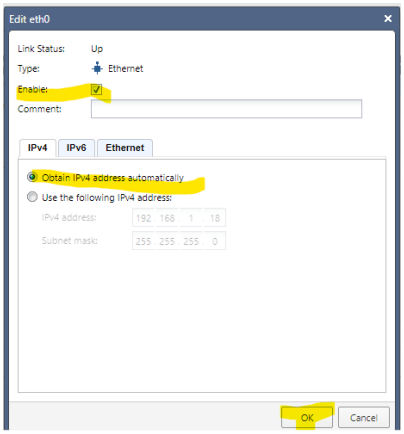




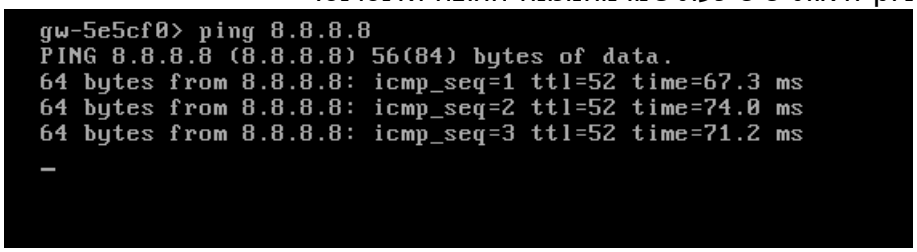
By Elior Sofer

כעת נגדיר את הכרטיסי רשת:

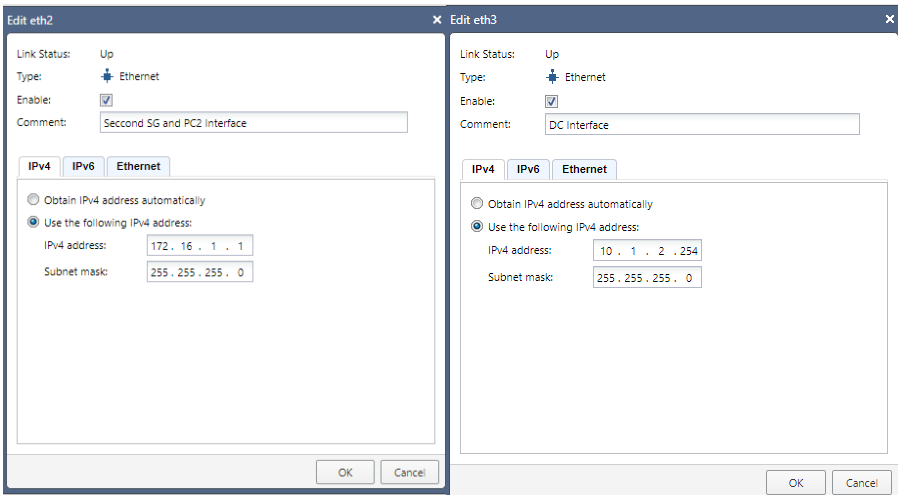




ניתן לראות שיש כעת פינג מהמכונה החוצה לאינטרנט:



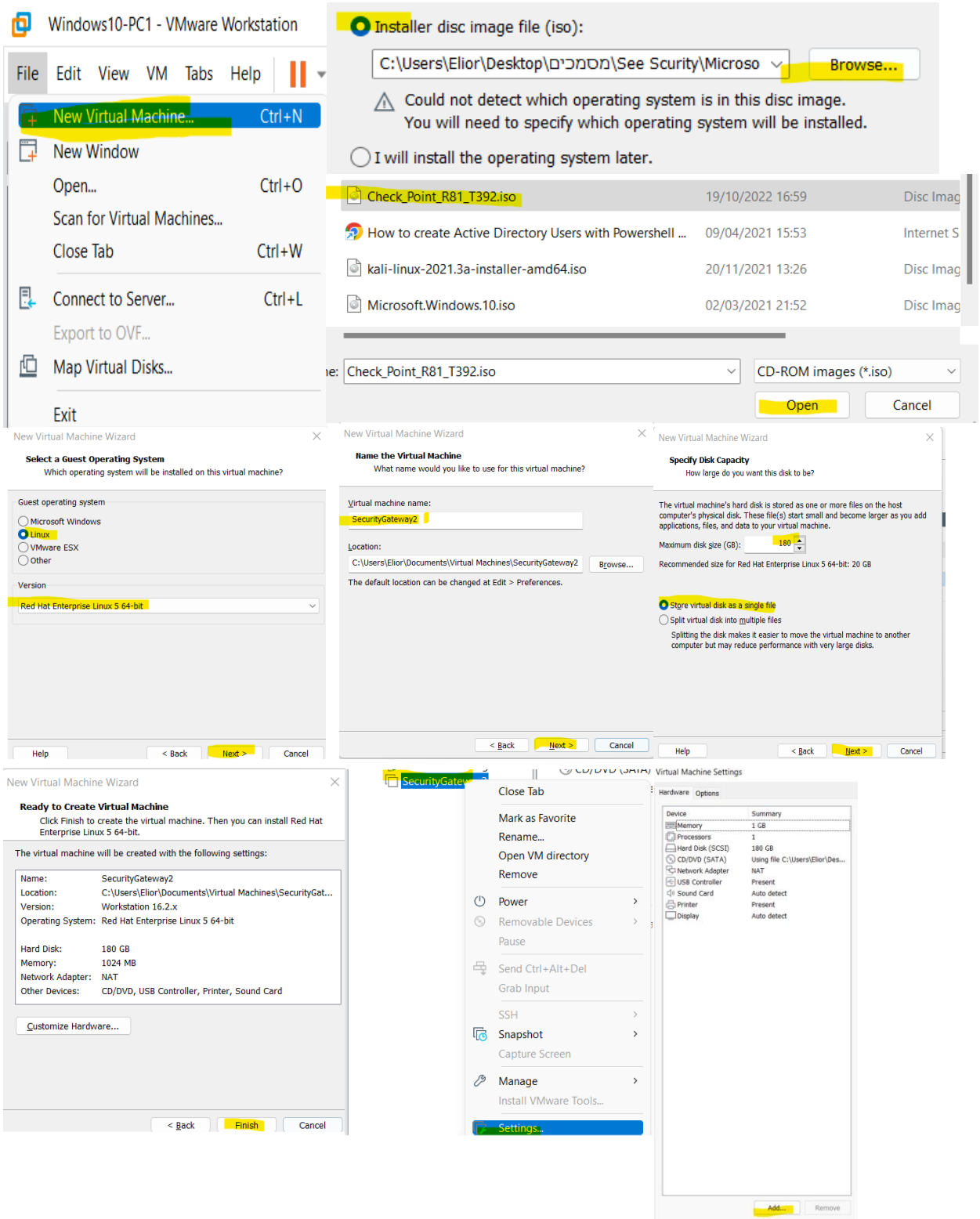
בשני הממשקים השניים נצטרך להזין באופן ידני את הכתובות IP:



By Elior Sofer

Name	Type	IPv4 Address	Subnet Mask	IPv6 Address	IPv6 Mask Length	Link Status	Comment
eth0	Ethernet	192.168.1.18	255.255.255.0	-	-	Up	Int Out
eth1	Ethernet	10.1.1.254	255.255.255.0	-	-	Up	Management Interface
eth2	Ethernet	172.16.1.1	255.255.255.0	-	-	Up	Seccond SG and PC2 Interface
eth3	Ethernet	10.1.2.254	255.255.255.0	-	-	Up	DC Interface
lo	Loopback	127.0.0.1	255.0.0.0	-	-	Up	

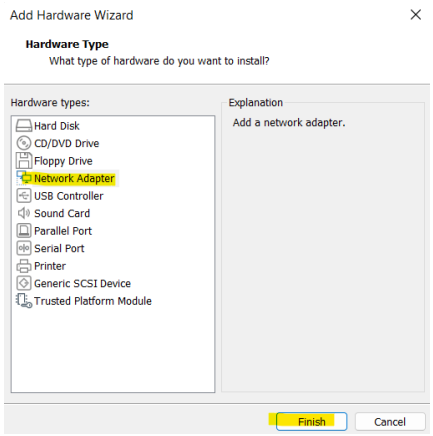
התקנת מכונת ה SG הנפרדת וחיבורה לממשק הניהול Smart Management

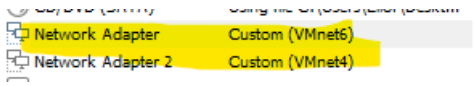


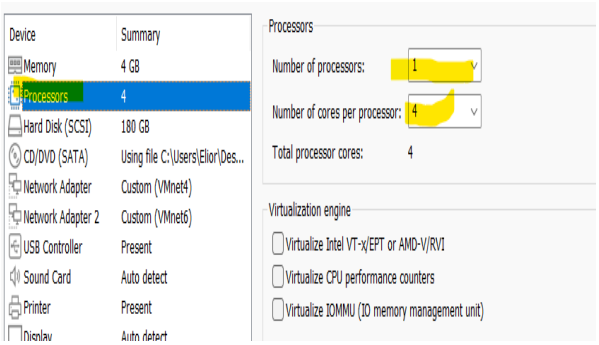
By Elior Sofer

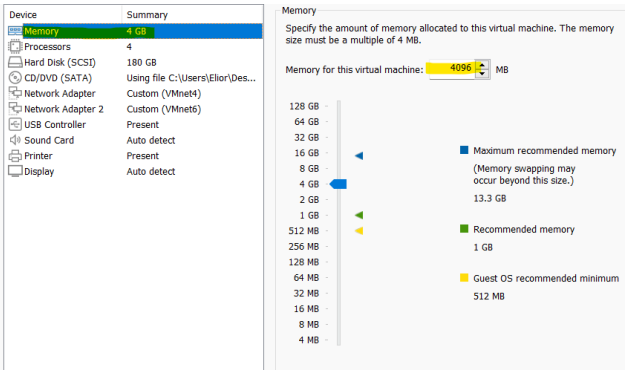
כרטיס הרשת הראשון במכונה יתחבר ל PC2

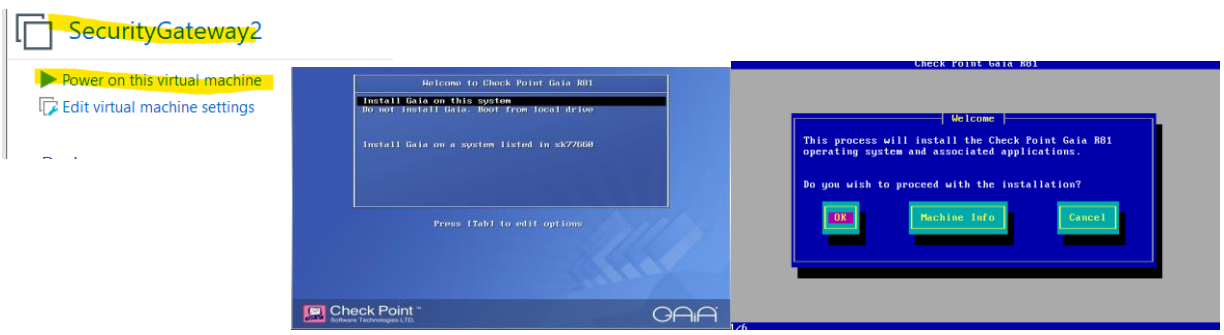
והכרטיס השני יתחבר ל :SG1



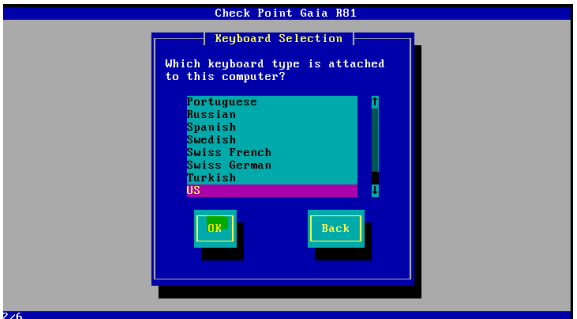


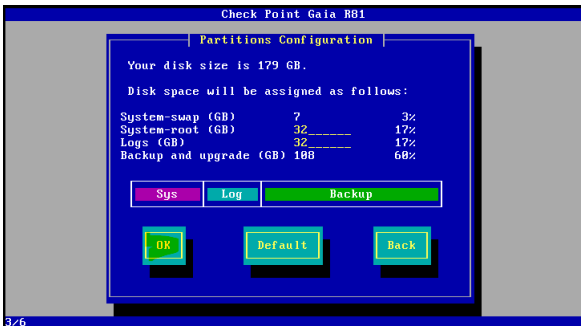


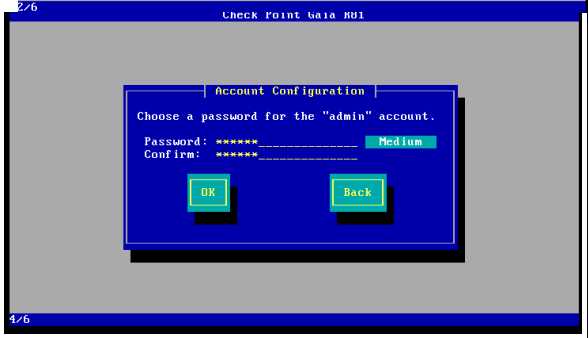


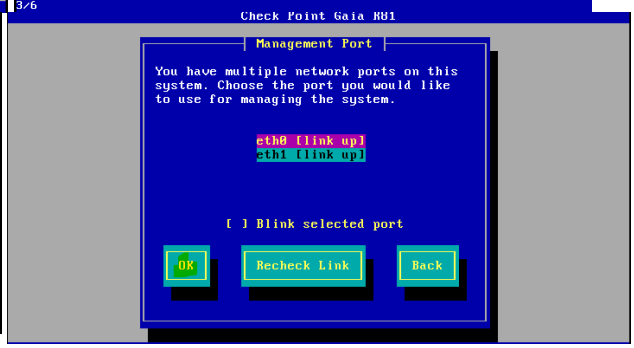


By Elior Sofer

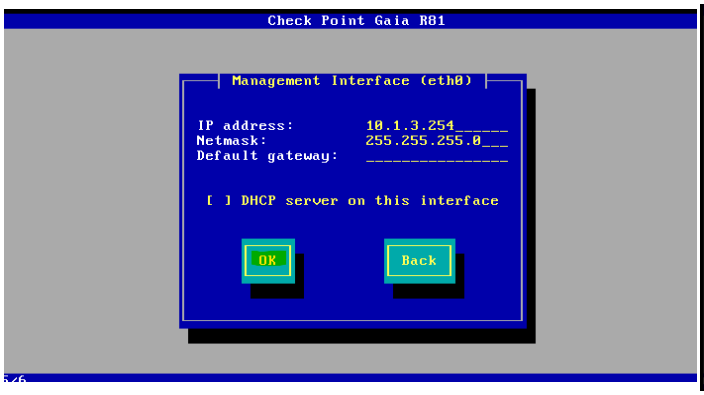


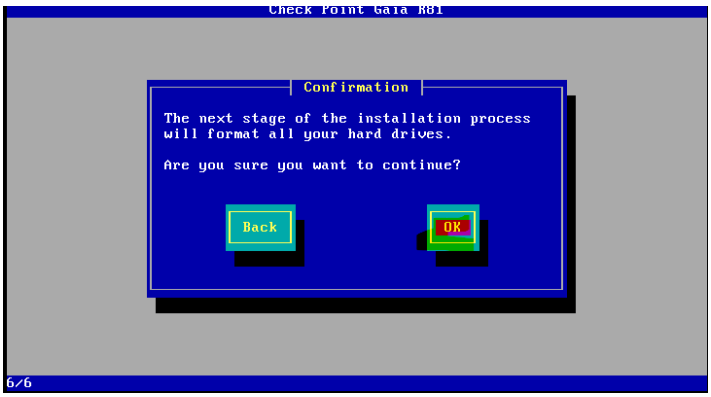




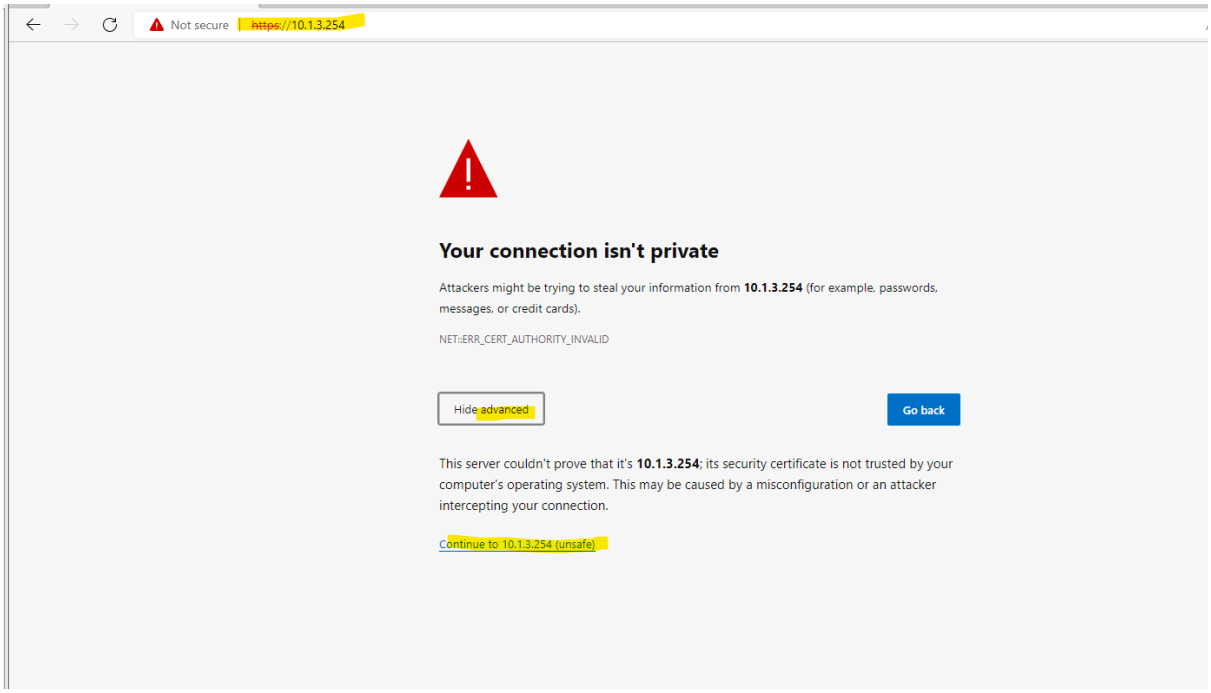


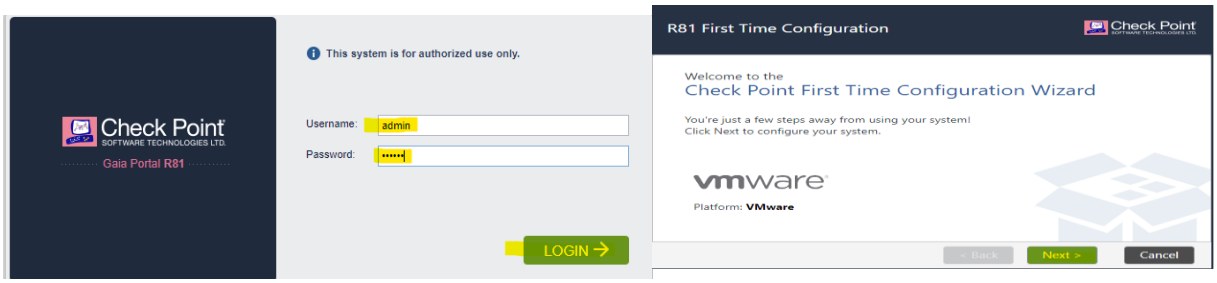
כעת בשדה הראשון נזין את הכתובת IP של הממשק ניהול לפי טופולוגיה:



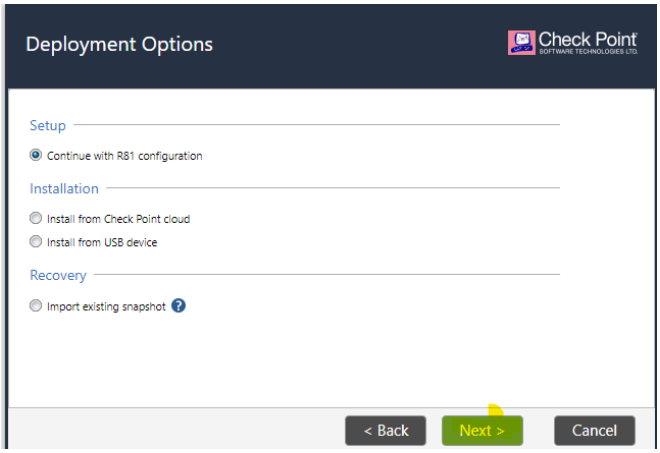


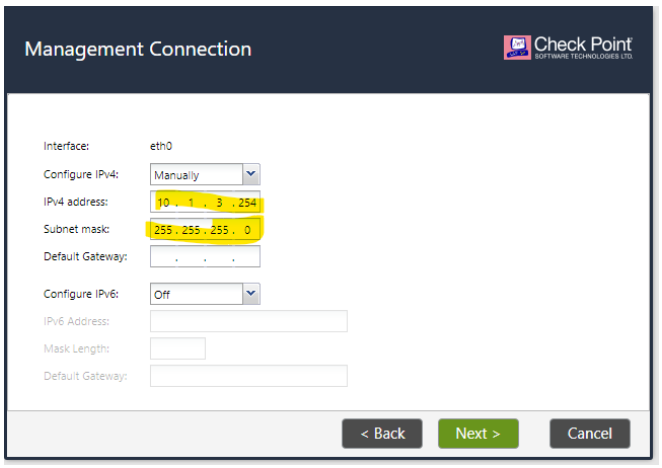
כעת יש צורך להגדיר את SG2. נכנס לממשק דרך PC2:

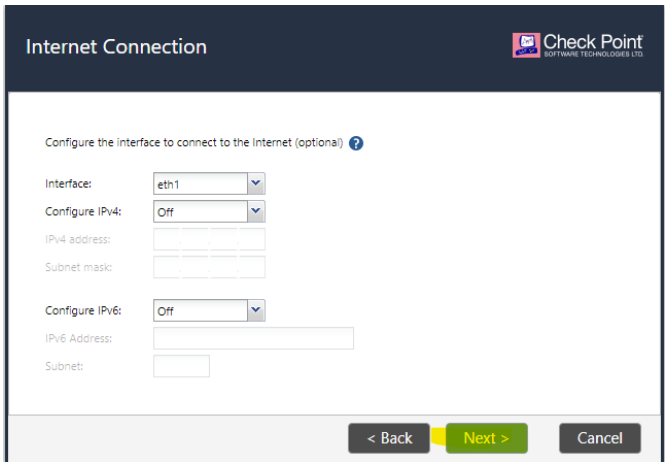


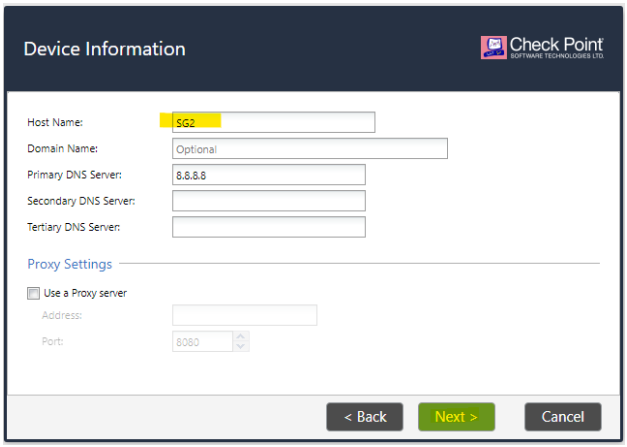


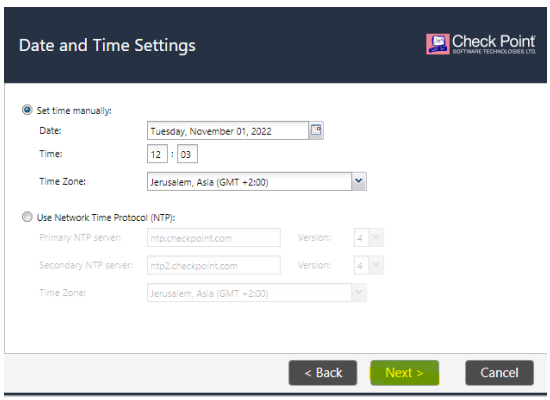
By Elior Sofer

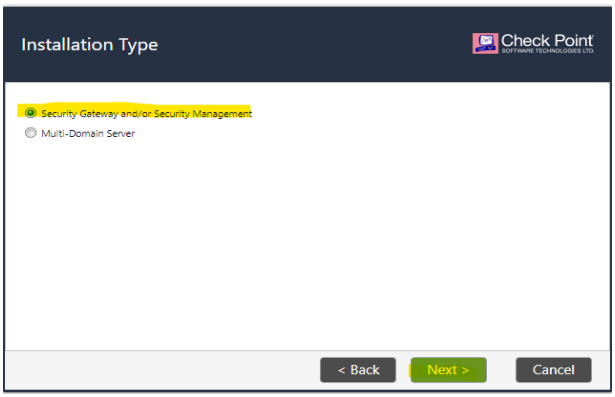






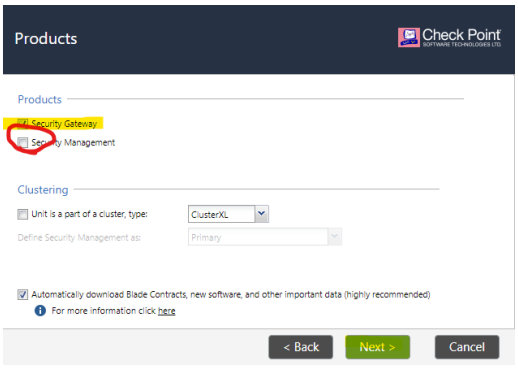


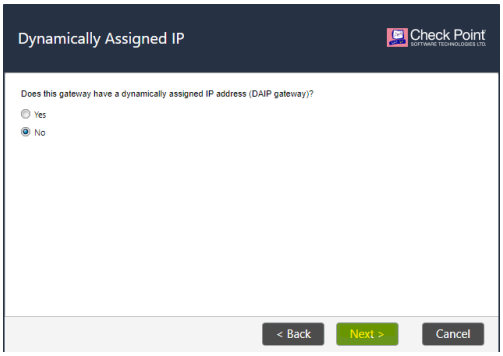




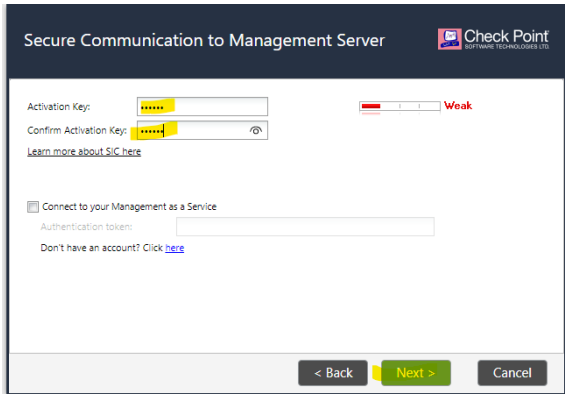
By Elior Sofer

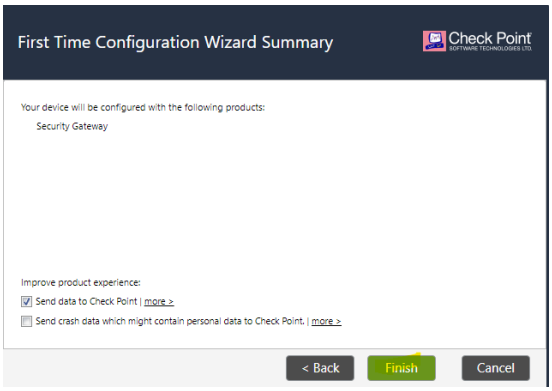
נוודא שאנחנו מורידים את ה V מהאפשרות השנייה!

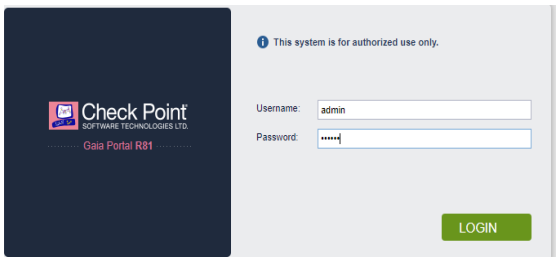




כעת נצטרך להזין SIC-> תפקידו לחבר בין ה SG הנפרד ל Security Management. נזכור אותו ונשתמש בו בהמשך.







כעת נצטרך להגדיר את כרטיסי הרשת:

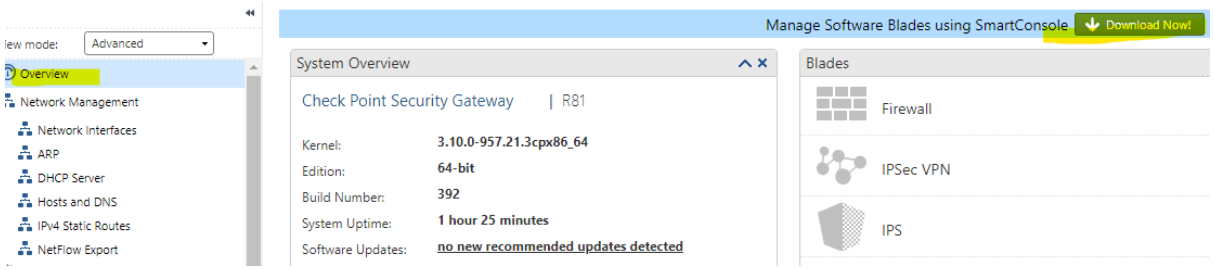
Name	Type	IPv4 Address	Subnet Mask	IPv6 Address	IPv6 Mask Length	Link Status	Comment
eth0	Ethernet	10.1.3.254	255.255.255.0	-	-	Up	
eth1	Ethernet	-	-	-	-	Down	
lo	Loopback	127.0.0.1	255.0.0.0	-	-	Up	

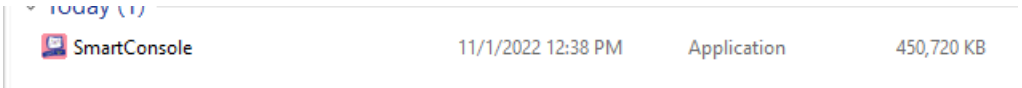
eth0	Ethernet	10.1.3.254	255.255.255.0	-	-	Up	Interface to PC2
eth1	Ethernet	172.16.1.2	255.255.255.0	-	-	Up	Interface to SG1 and out
lo	Loopback	127.0.0.1	255.0.0.0	-	-	Up	

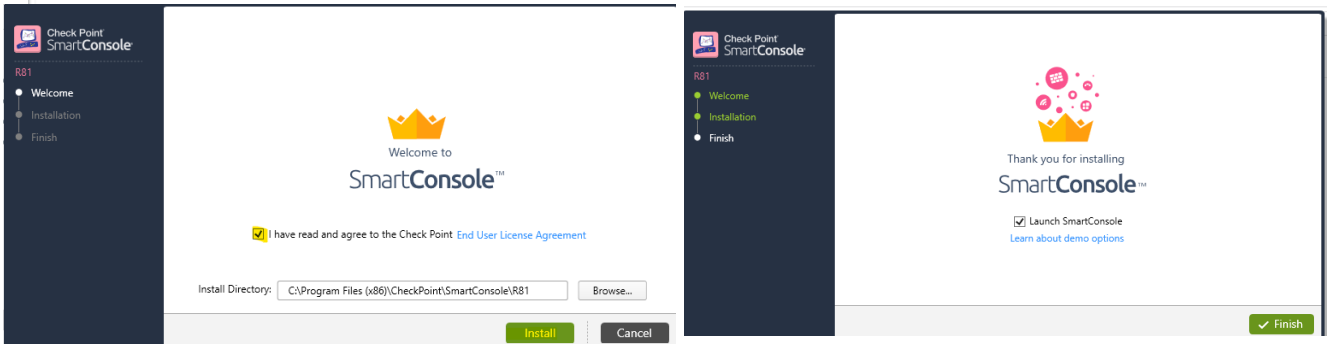
By Elior Sofer

התקנת Smart Console

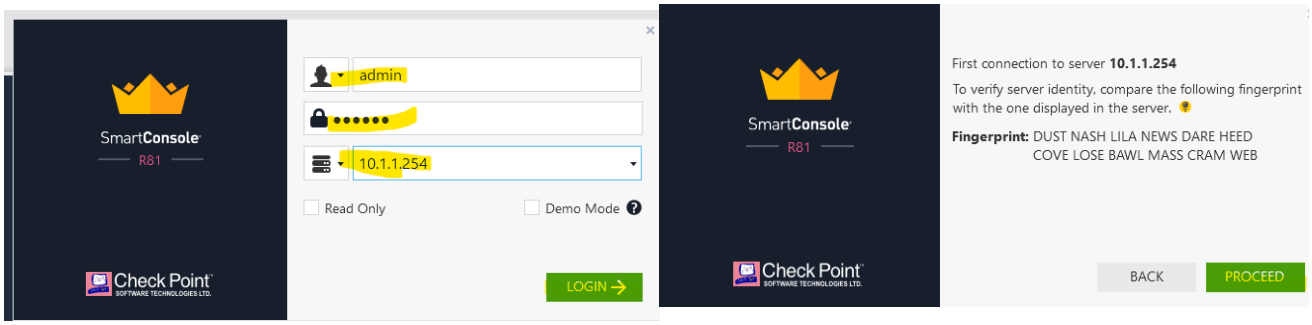
כעת נוריד ונתקין את ה Smart Console אשר למעשה מנהל את כל ה SG:







כעת נתחבר לממשק ניהול ה SG הראשי (SG1)



By Elior Sofer

כעת נצטרך להגדיר מספר חוקים בסיסיים על מנת שנוכל להתחיל לעבוד עם SG1:

חוק מספר 1:

Filter Rule

מטרת החוק: לזרוק חבילות מיד וללא Log. החוק מקל על ה- Firewall ולכן מאיץ את ביצועיו. בנוסף סינון הרשומות שנכנסות ל- Log הופך אותו לקריא יותר.

מיקום החוק: ראשון.

Name	Source	Destination	Services & Applications	Action	Track
Filter rule	* Any	* Any	UDP nbdatagram	Drop	None

חוק מספר 2:

Stealth Rule (התחמקות)

מטרת החוק: להגן על ה- Security Gateway על-ידי חסימת התקשורת אליו.

למרות חוק זה, ניתן ליצור קשר עם ה- Security Gateway בזכות חוקי מערכת וחוק ניהול.

מיקום החוק: בין החוקים הראשונים.

Name	Source	Destination	Services & Applications	Action	Track
Stealth Rule	* Any	firewall1	* Any	Drop	Log

חוק מספר 3:

Management Rule

מטרת החוק: לאפשר ניהול של ה- Security Gateway.

מיקום החוק: מעל Stealth Rule.

Name	Source	Destination	Services & Applicat...	Action	Track	Install On
Management	windows10	gw-2cef02	https echo-request ssh_version_2	Accept	Log	* Policy Targets

חוק מספר 4:

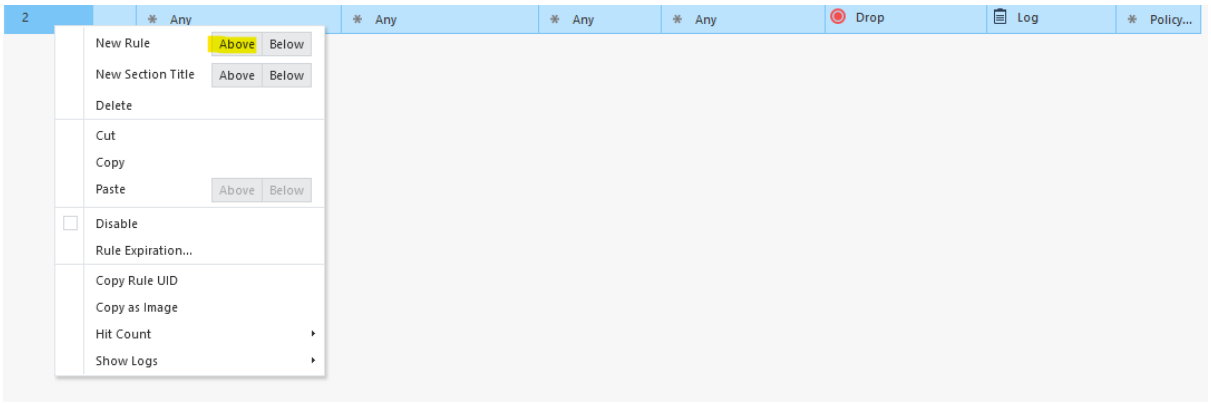
Cleanup Rule

מטרת החוק: **ביצוע Log** ל Packets שנזרקים כתוצאה מחוסר התאמה לשום חוק אחר.

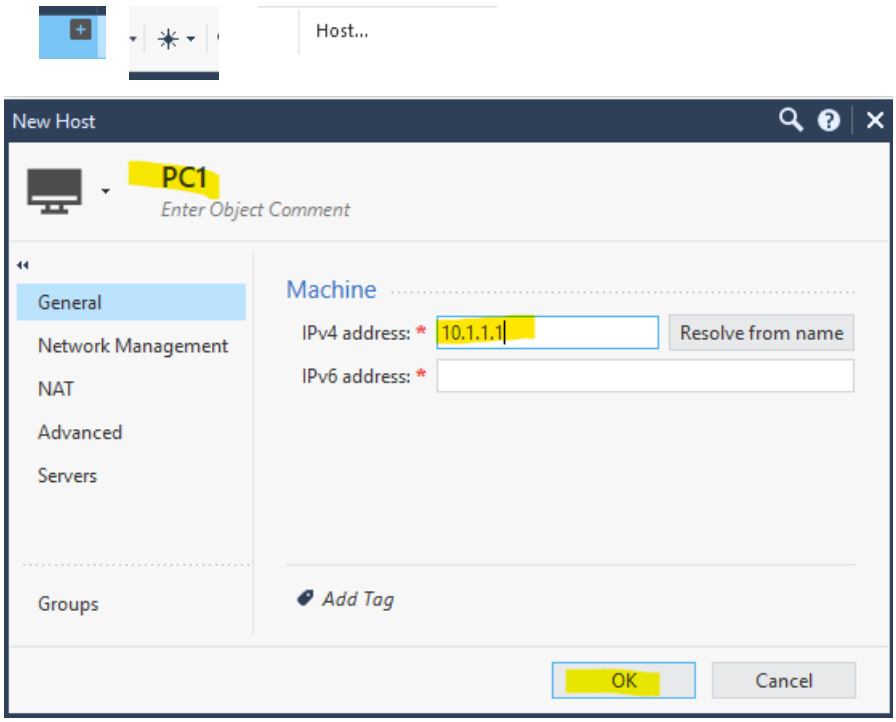
מיקום החוק: תמיד אחרון.

Name	Source	Destination	Services & Applications	Action	Track
Cleanup rule	* Any	* Any	* Any	Drop	Log

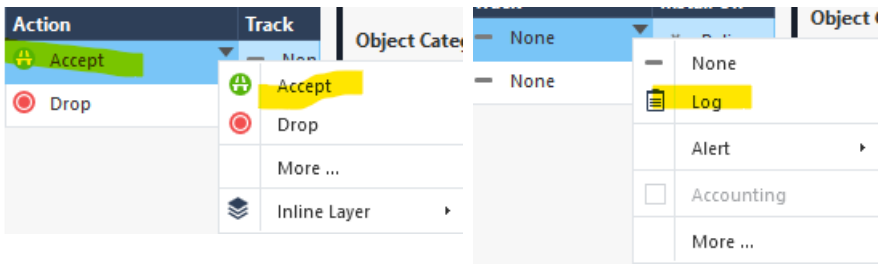
על מנת ליצור חוק יש לעשות את הפעולות הבאות:



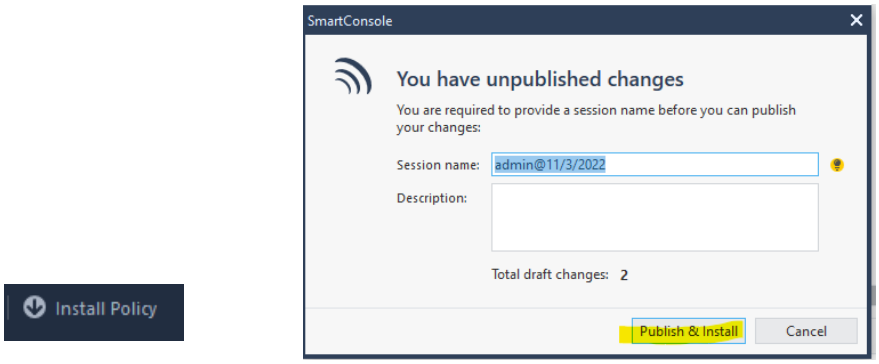
לאחר מכן יש ליצור אובייקט על פי הצורך. לדוגמא בחוק Management Rule אצור אובייקט ל PC1 ואשם אותו ב Source:



לאחן מכן נשנה את ה ACTION ל **ACCEPT** ושנה את ה **TRACK** ל **LOG** על מנת שנוכל לראות לוגים שקשורים לחוק

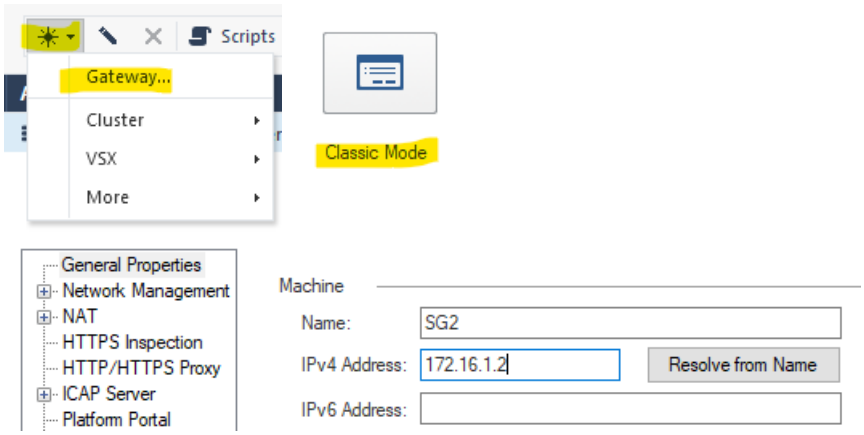


לאחר מכן <u>נגדיר את כל שאר החוקים</u> שתיארתי ונלחץ על **Install Policy** ואז **Publish & Install** על מנת להחיל את הפוליסה החדשה.

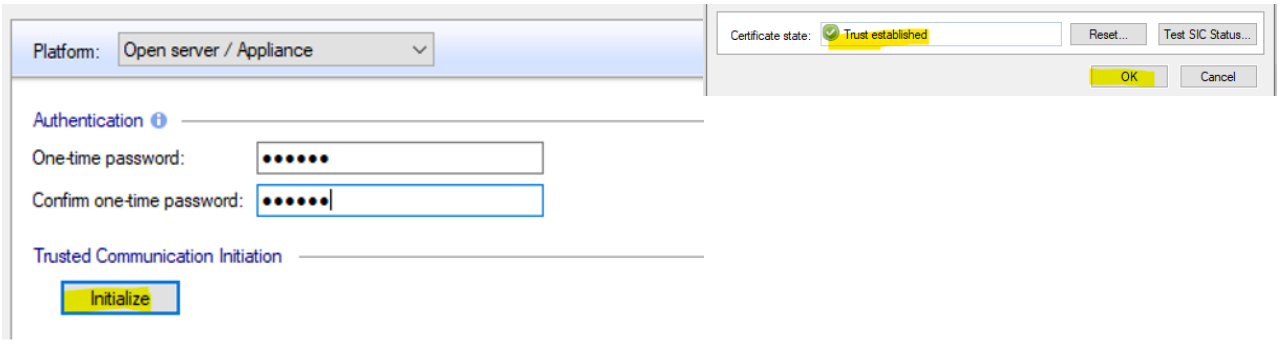


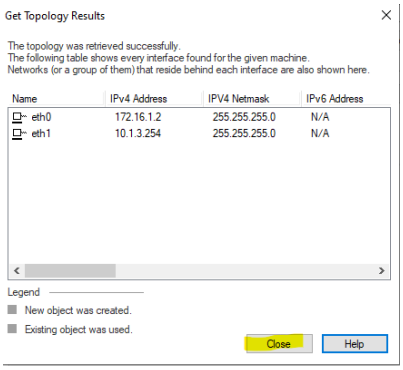
By Elior Sofer

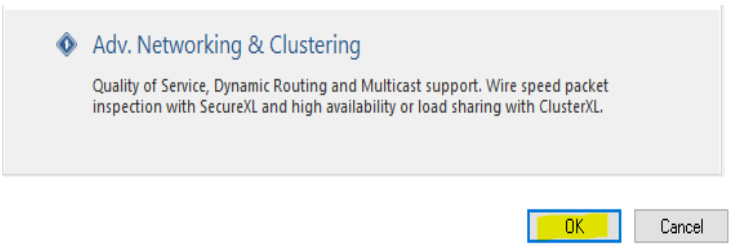
כעת נחבר את SG2 ל Security Management:



כעת נזין את ה SIC שהגדרנו קודם לכן:

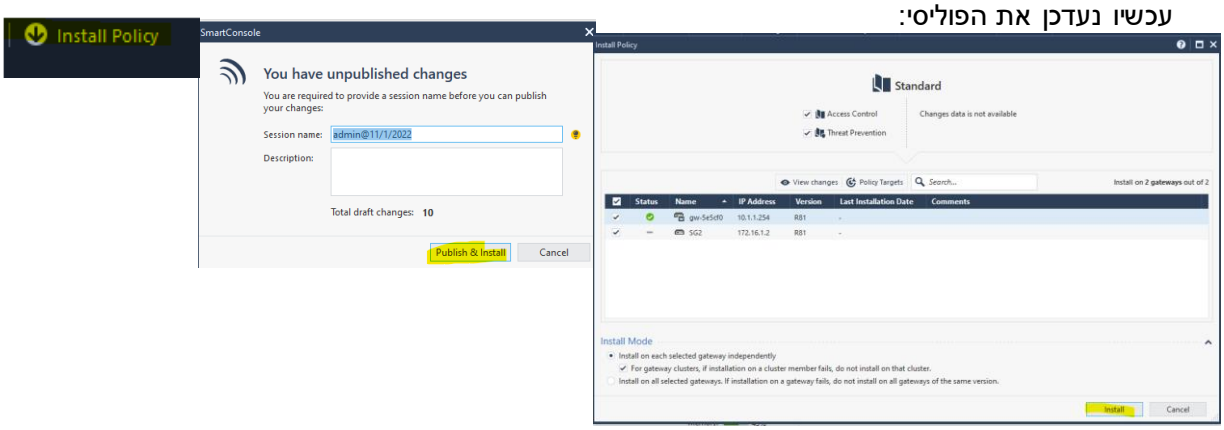




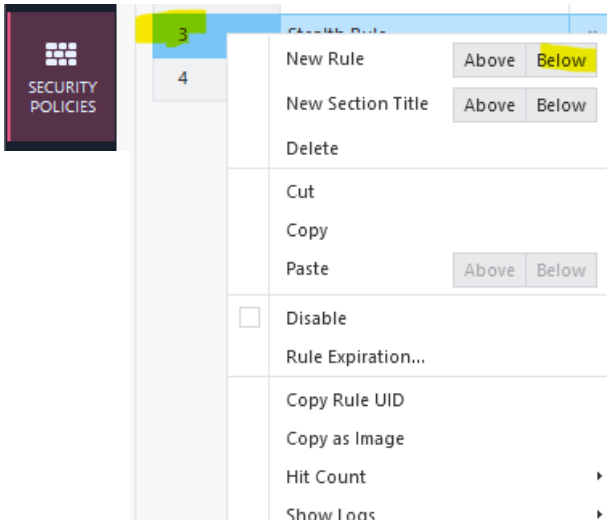


By Elior Sofer

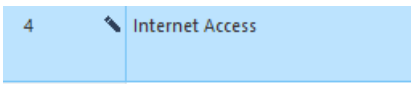
עכשיו נעדכן את הפוליסי:



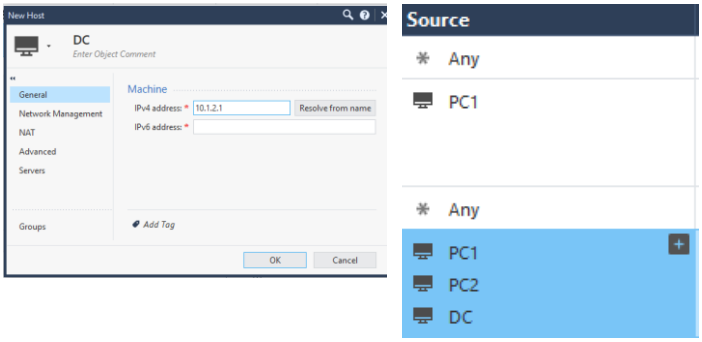
בשלב זה הטופולוגיה מוכנה. כעת ניצור חוקים שיאפשרו לנו חיבור לאינטרנט מכל העמדות קצה:



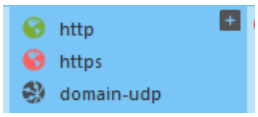
ניתן שם לחוק:



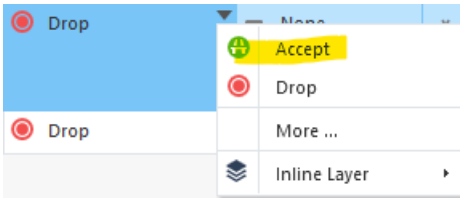
ב Source נשם את האובייקטים PC1 PC2 וניצור גם אובייקט ל DC ונוסיף אותו:



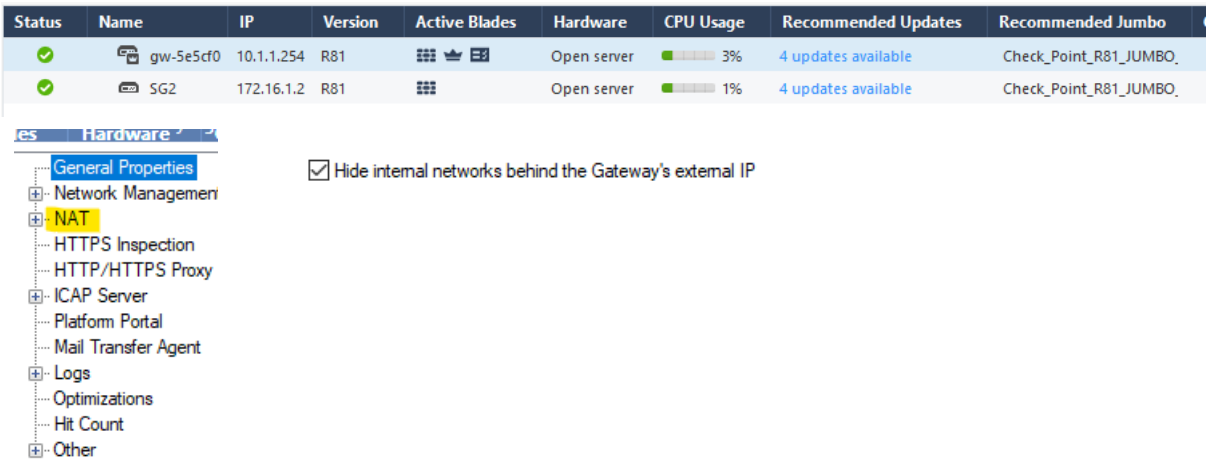
ב Destination לא נגע (נשאיר על ANY בשלב זה) ובעמודת Services & Applications נקבע את הפרוטוקולים הנחוצים לגלוש באינטרנט. במקרה הזה HTTPS,HTTP,DNS



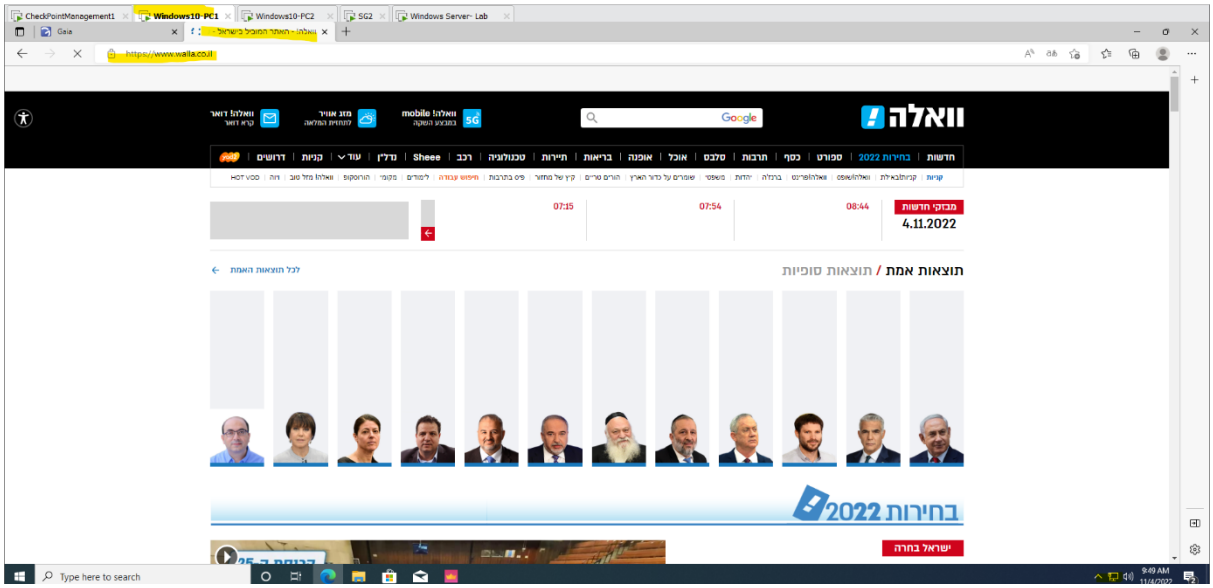
כעת נשנה את ה **Action** ל **Accept**

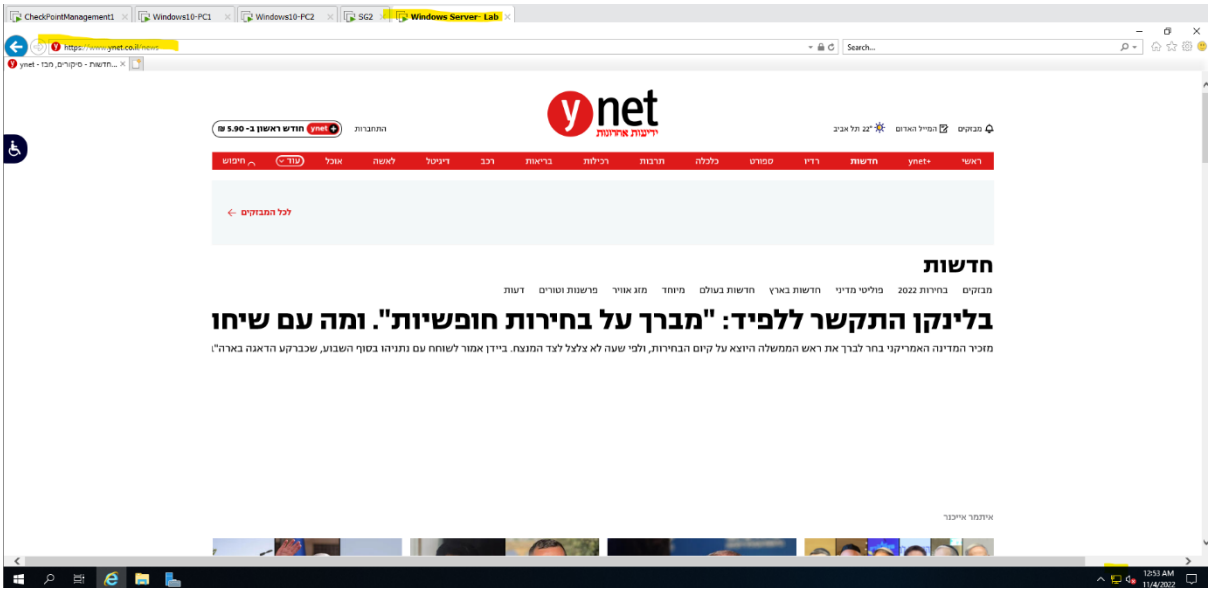


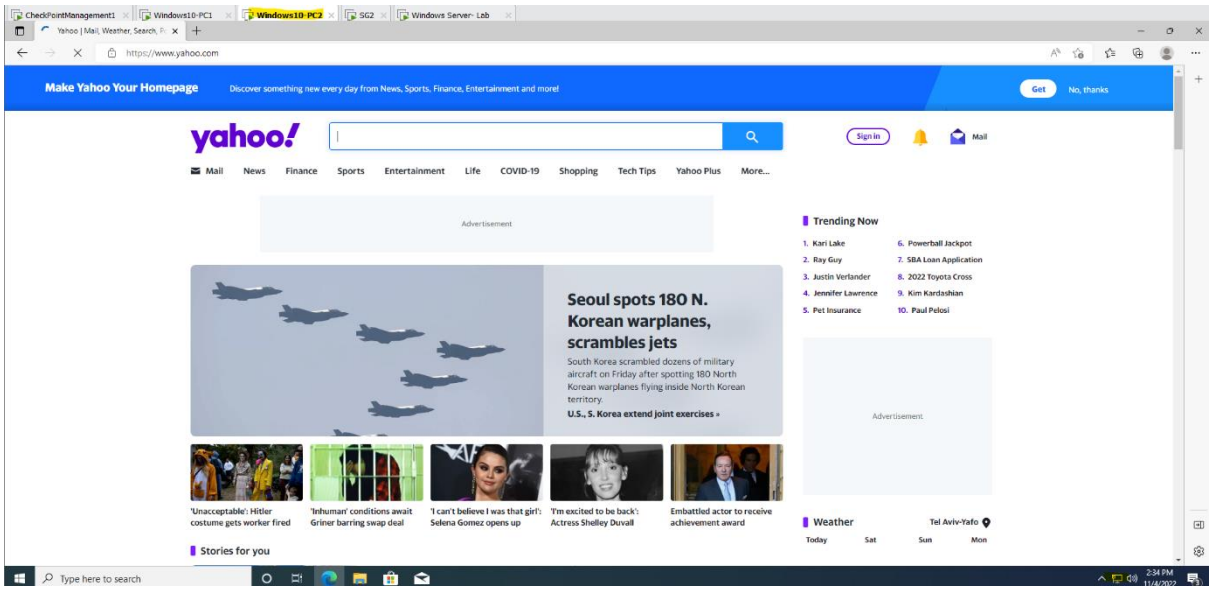
כעת נגדיר NAT לכל אחד מ ה SG:



כעת נתקין את הפוליסה נראה שהאינטרנט עובד בכל העמדות קצה:





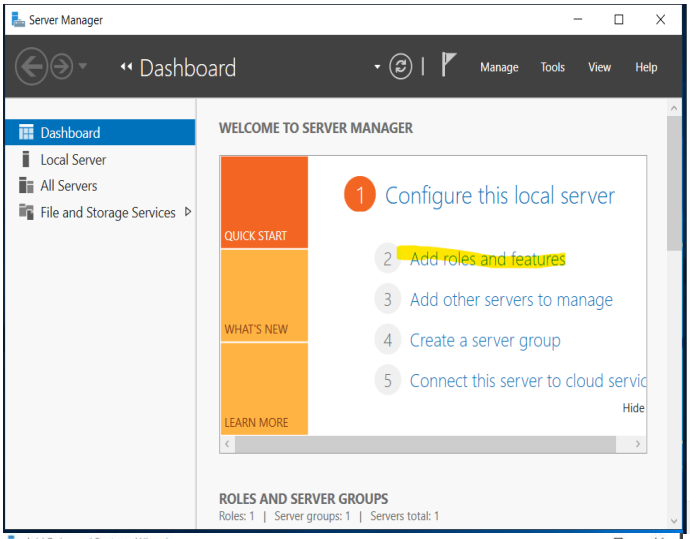


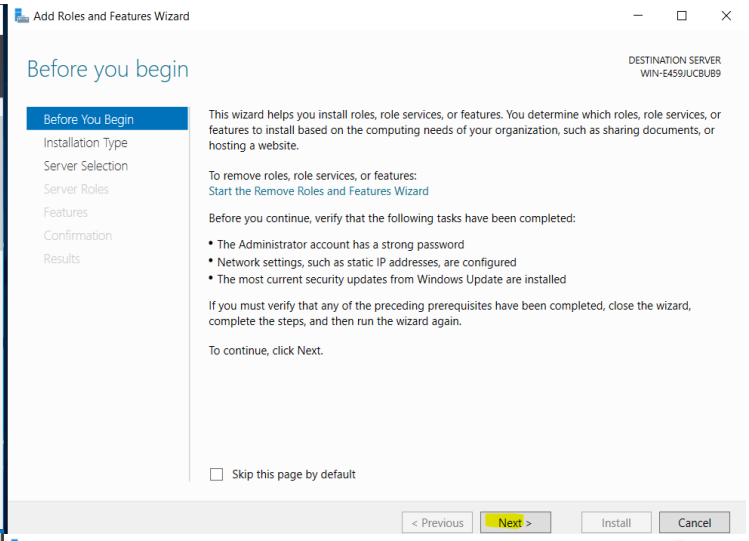
By Elior Sofer

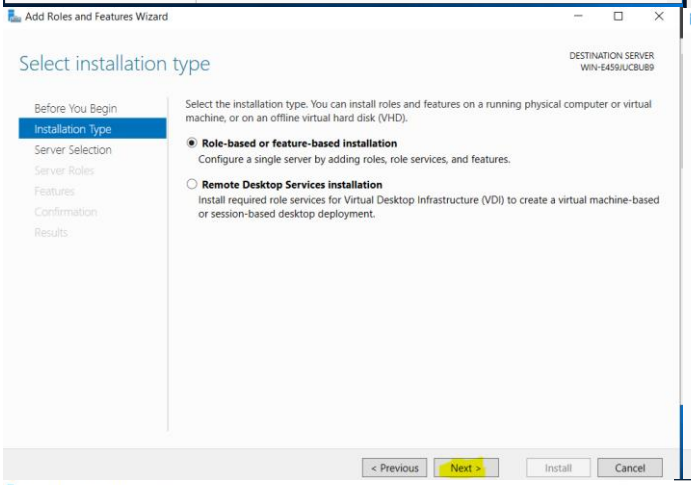
הקמת DC,שרת DNS, IIS והוספת PC1 ו PC2 לדומיין

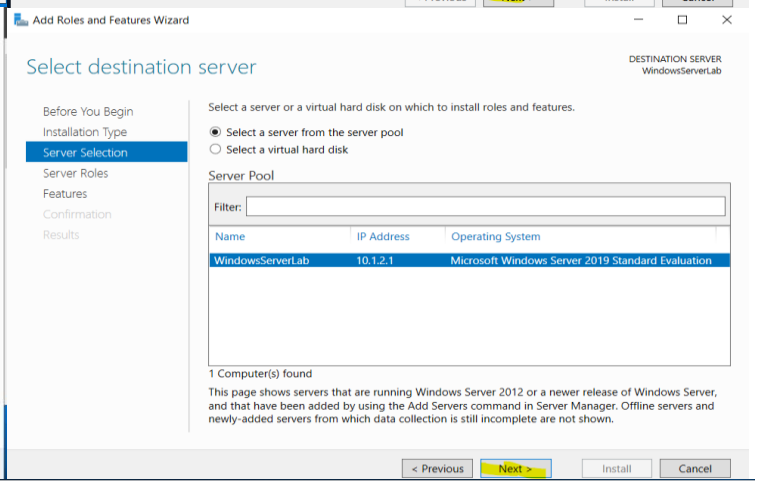
בשלב זה אקים דומיין ואצרף את PC1 ו PC2 לדומיין. לאחר מכן אקים שרת DNS ו IIS.

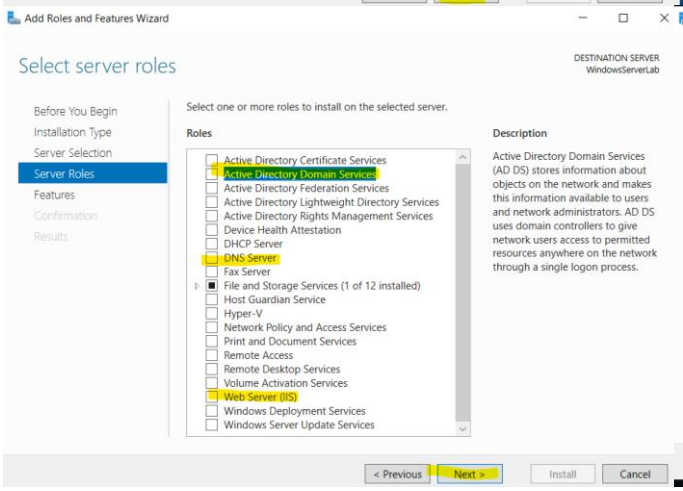
יש לעקוב אחרי השלבים הבאים במכונת WINDOWS SERVER:

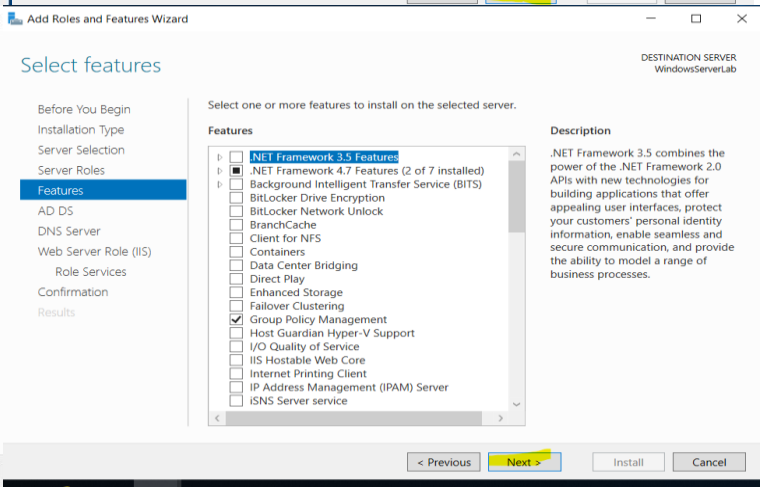




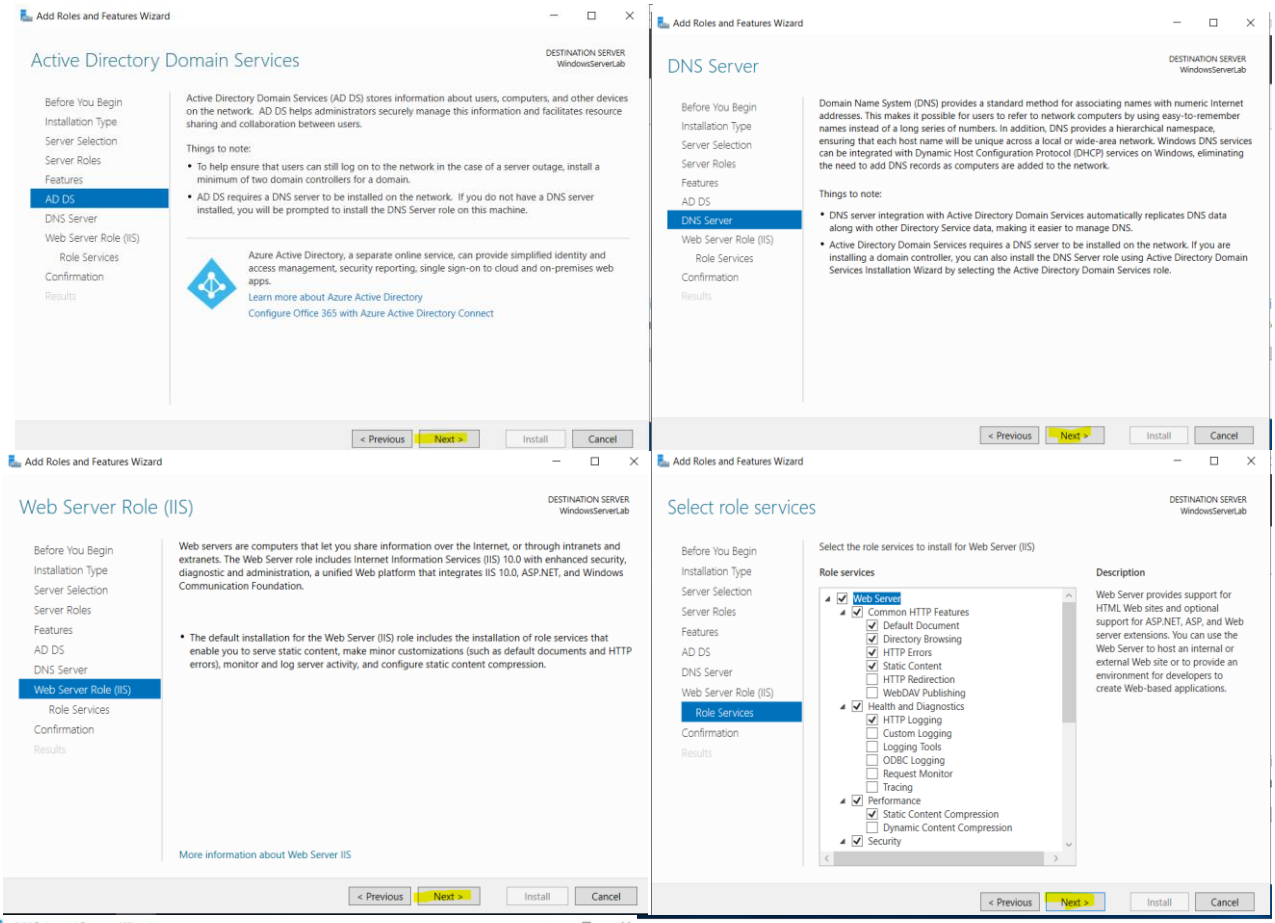




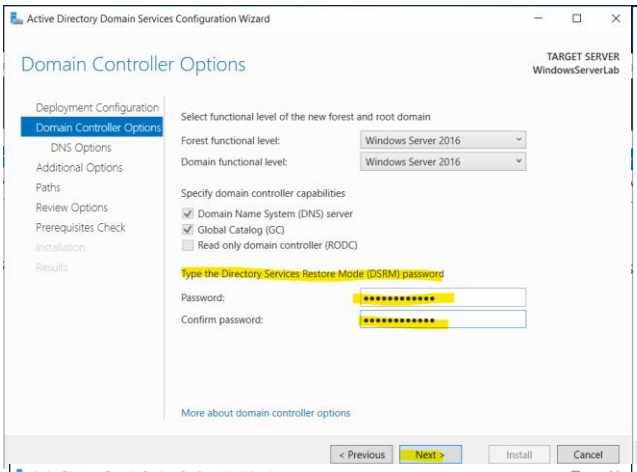


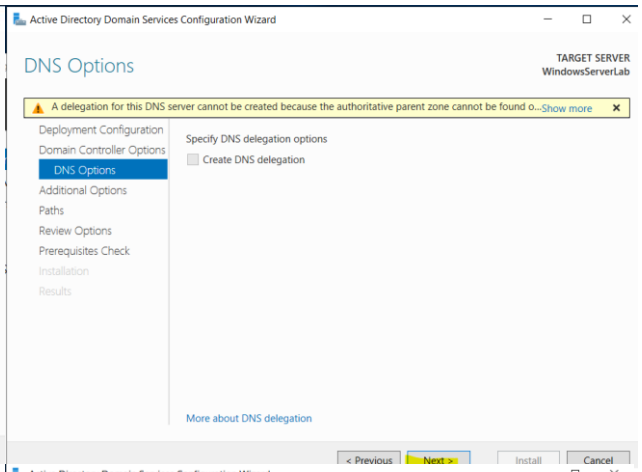


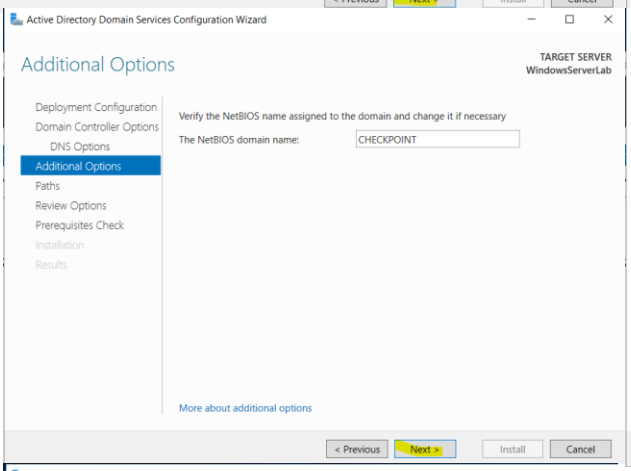
By Elior Sofer

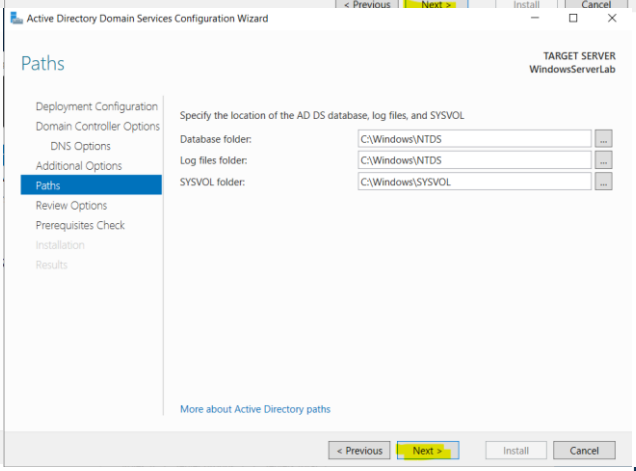


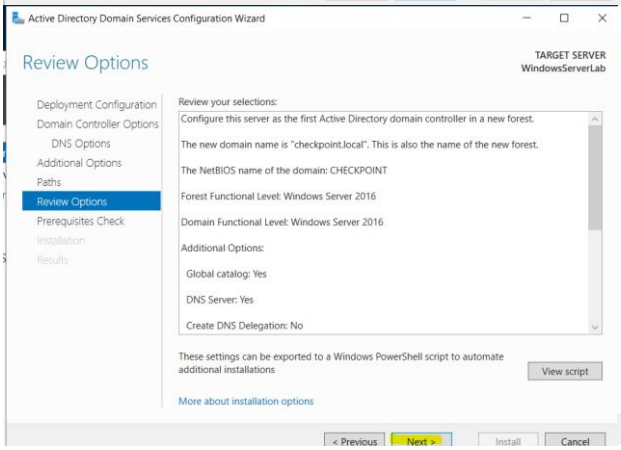
By Elior Sofer

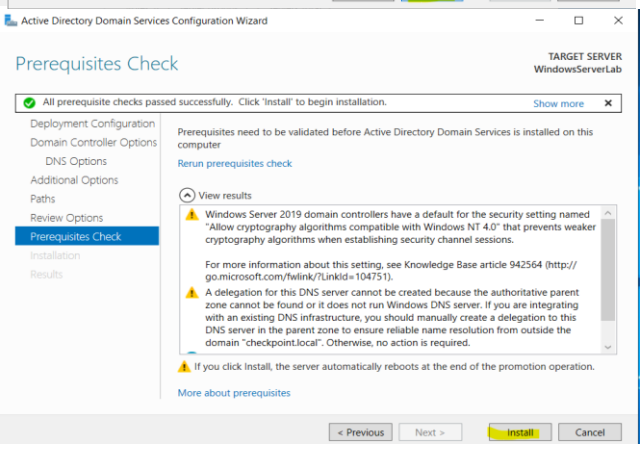










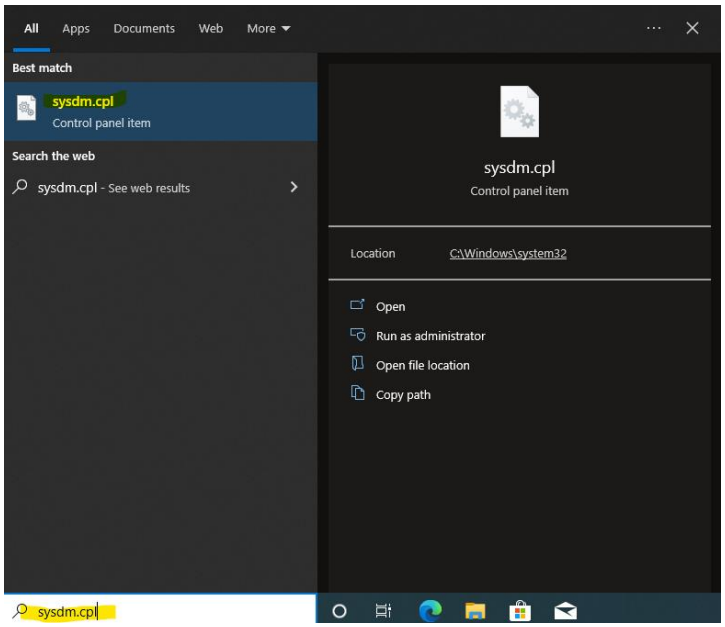


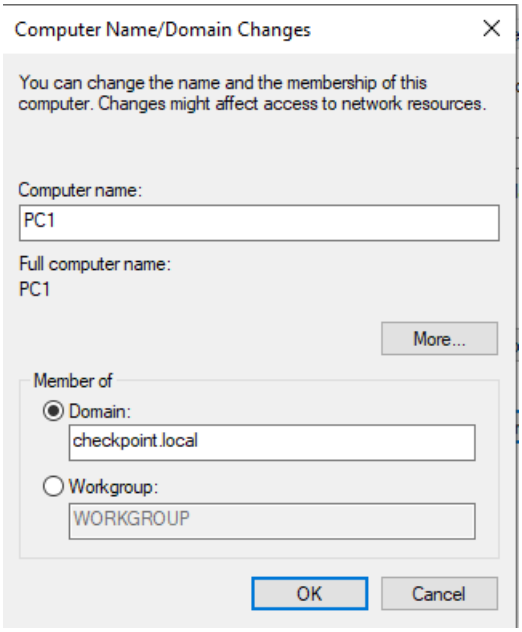
By Elior Sofer

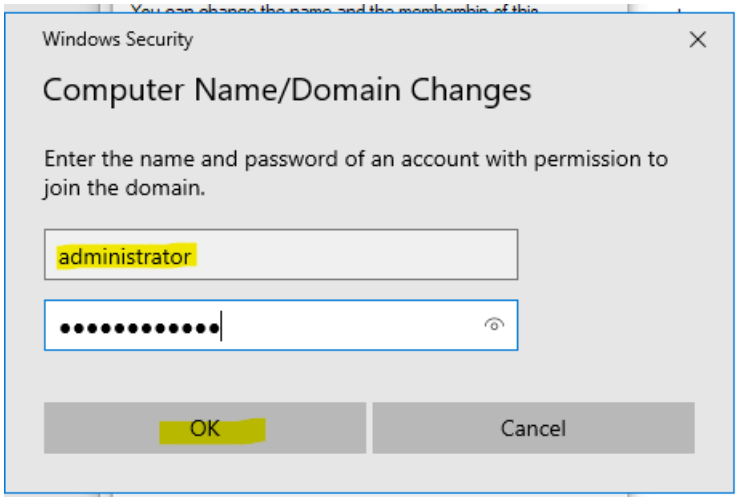
כעת יש להוסיף לדומיין את PC1 ו PC2.

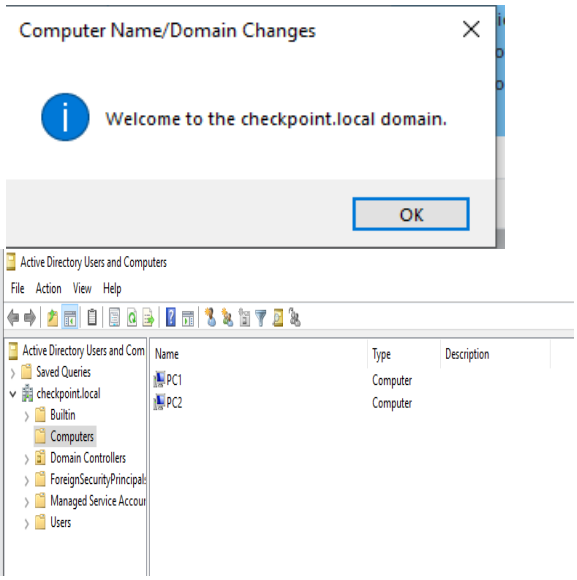
לפי שנוסיף, יש להגדיר פרוטוקולים נוספים בחוק INTERNET ACCESS שהגדרנו ב FW על מנת שנוכל להוסיף את המחשבים לדומיין:

התהליך זהה אחד לאחד בשניהם. אדגים כיצד להוסיף את מכונת PC 1 לדומיין:



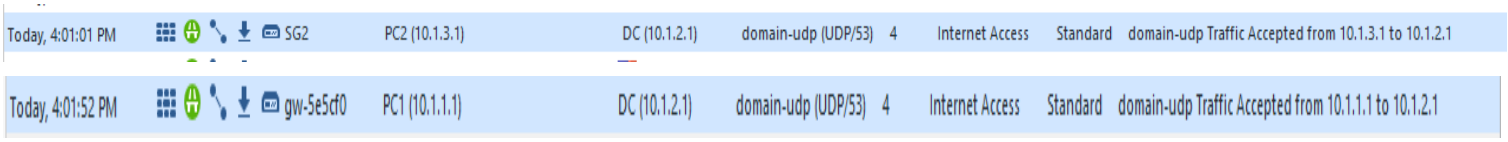






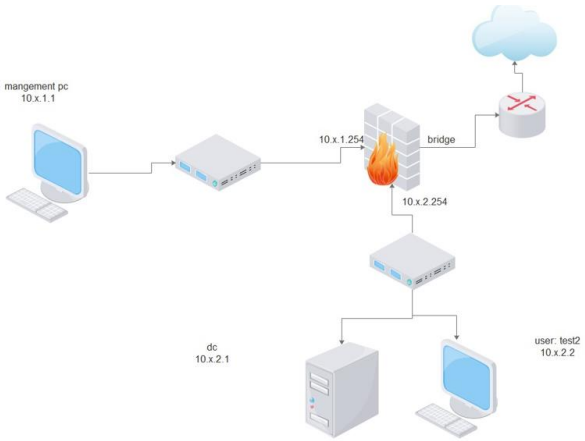
By Elior Sofer

כעת אוכיח עפ"י הלוגים כי שרת הDC שהקמנו משמש כשרת DNS ושרת IIS לעמדות קצה (PC1 וPC2):



חלק ב'

חלק זה מבוסס על הטופולוגיה הבאה:

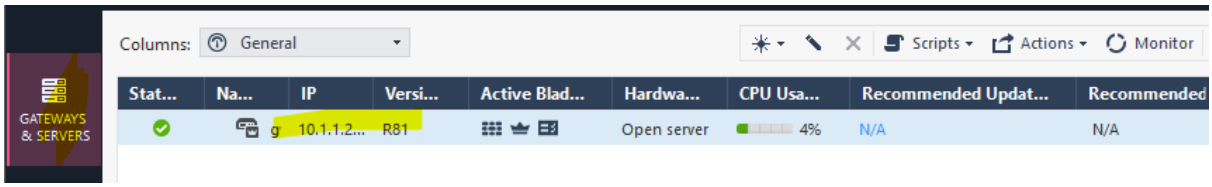


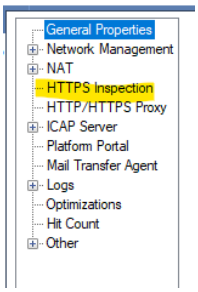
כאמור הקמתי את הסביבה לפי הטופולוגיה הנ"ל עם כל החוקים הבסיסיים.

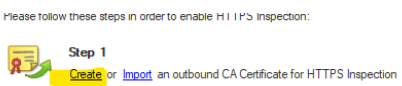
בחלק זה אראה פיצ'רים מתקדמים, כיצד מקנפגים אותם וPOC:

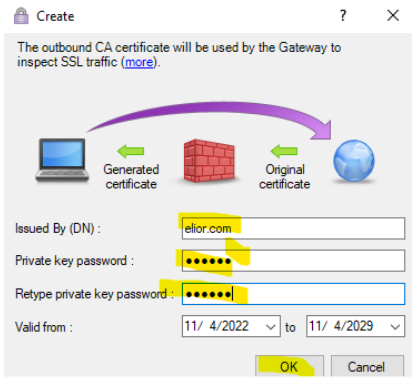
הפעלת HTTPS Inspection:

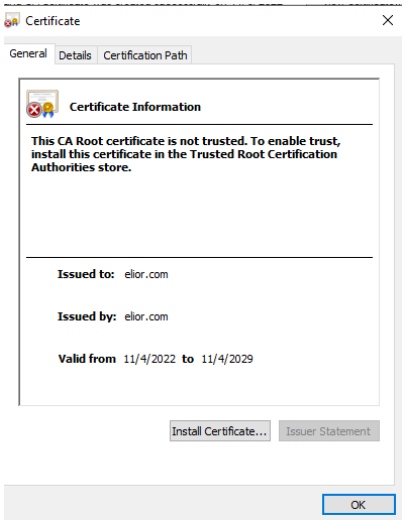
על מנת להפעיל פונקציה זאת יש לעקוב אחרי הצילומי מסך הבאים:

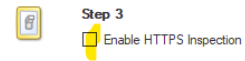


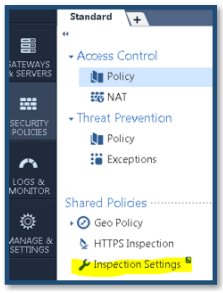


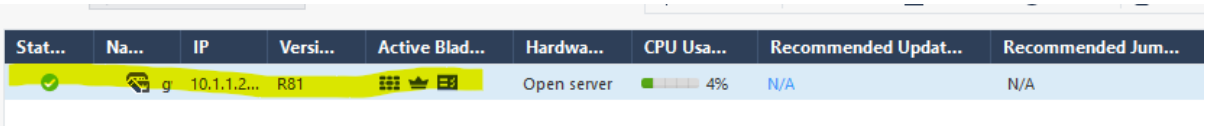


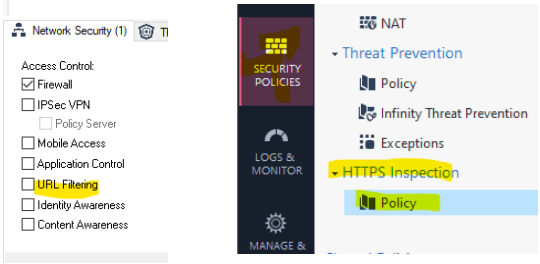


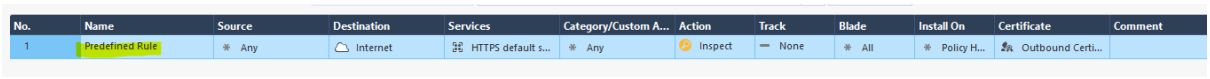


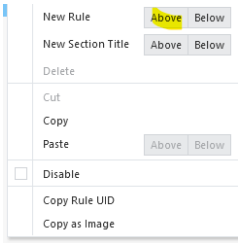


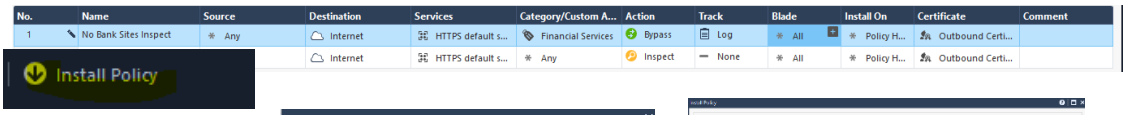


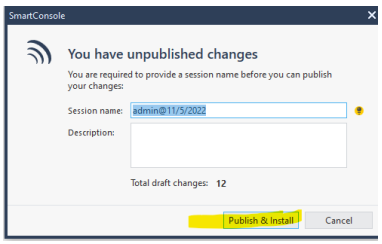


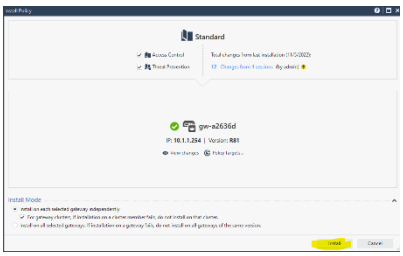






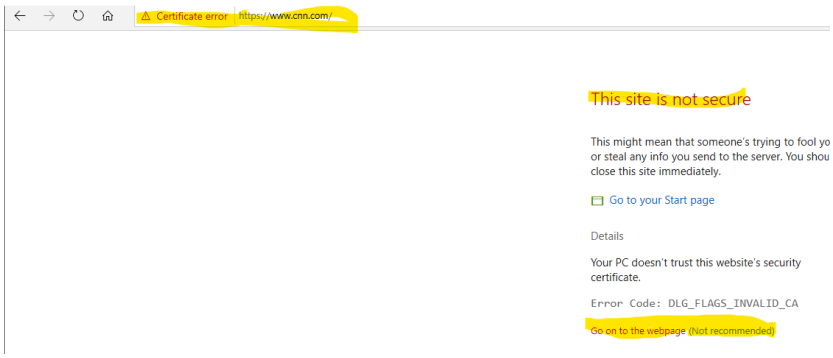


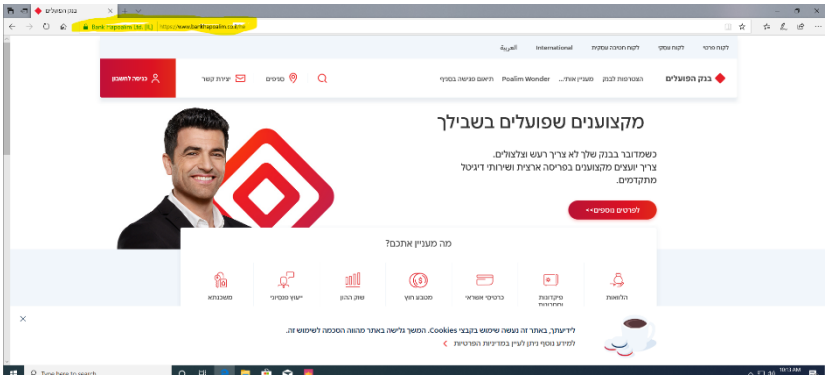




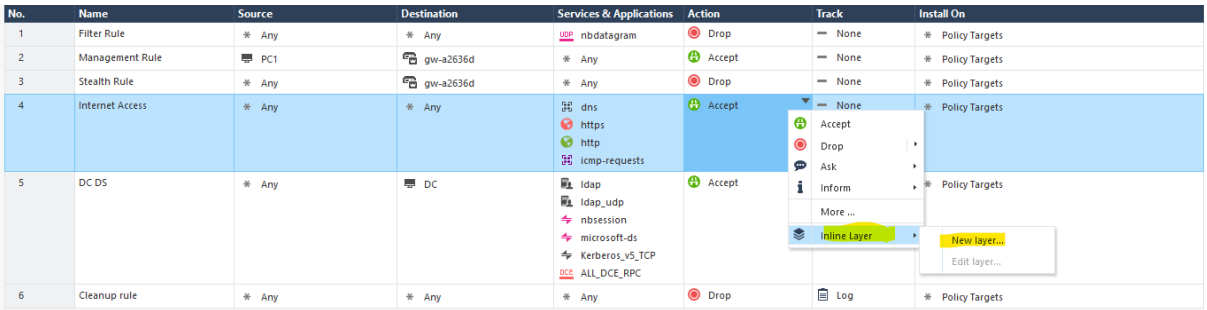
By Elior Sofer

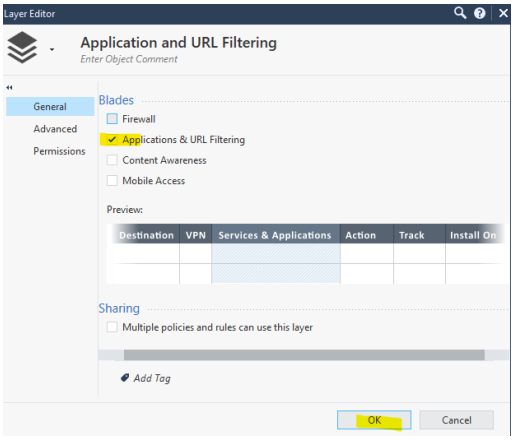
:POC





עכשיו נצטרך על מנת לעבוד עם הפיצ'ר הבא לעשות חוק בשכבה:



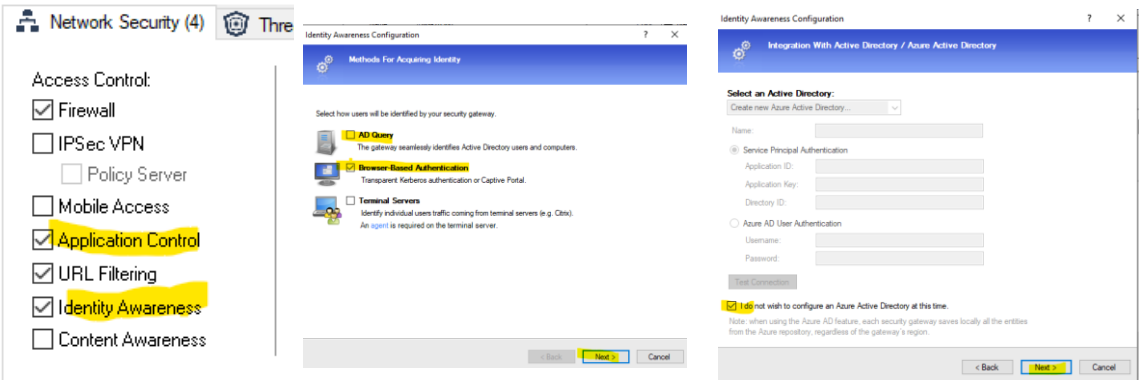


By Elior Sofer

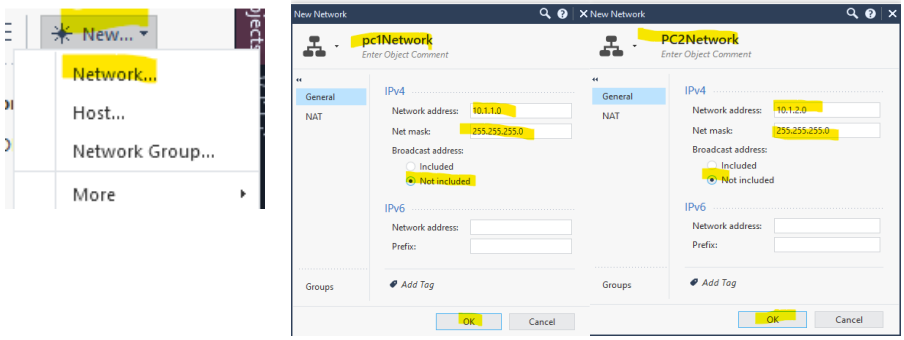
4	Internet Access	Any	Any	dns https http icmp-requests	Application and URL	N/A	Policy Targets
4.1	Cleanup rule	Any	Any	Any	Drop	None	Policy Targets

כעת אדגים את הפיצ'ר user identity:

Stat...	Na...	IP	Versi...	Active Blad...	Hardwa...	CPU Usa...	Recommended Updat...	Recommended Jum...
	g	10.1.1.2...	R81		Open server	3%	N/A	N/A



כעת אגדיר אובייקטים:

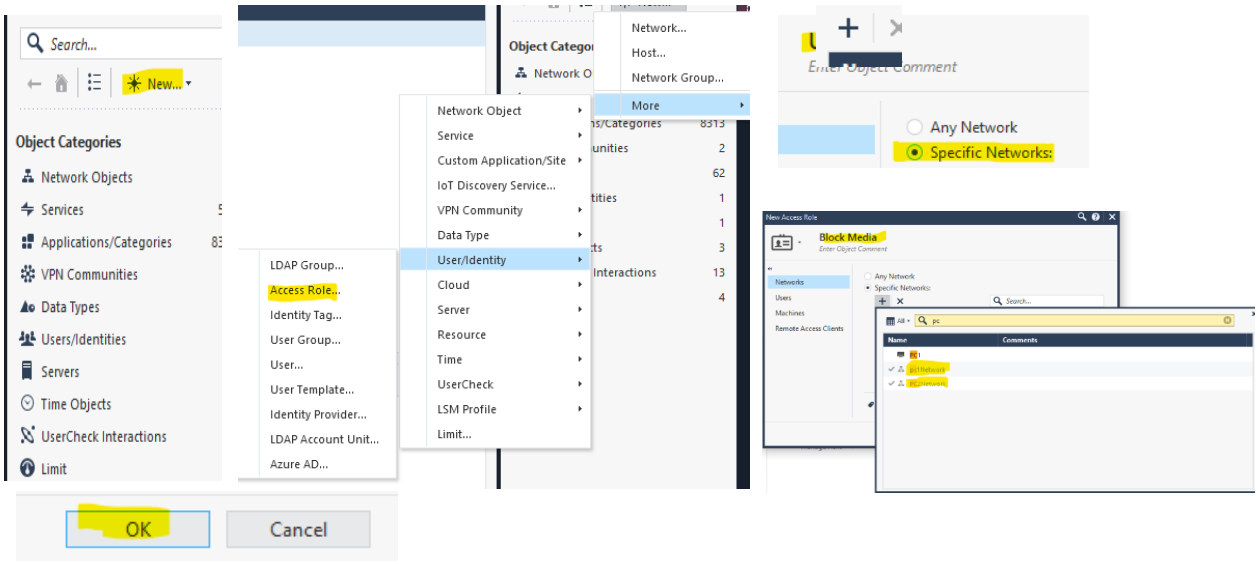


By Elior Sofer

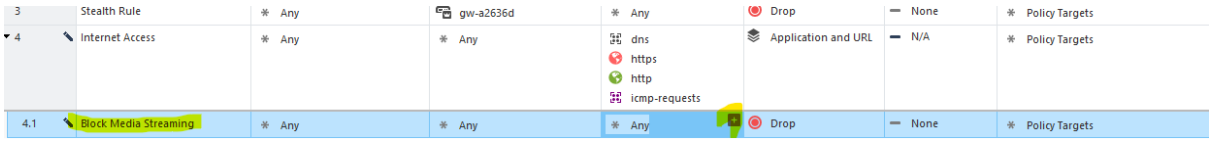
לאחר שהגדרתי את האובייקטים אגדיר את החוקים הבאים:

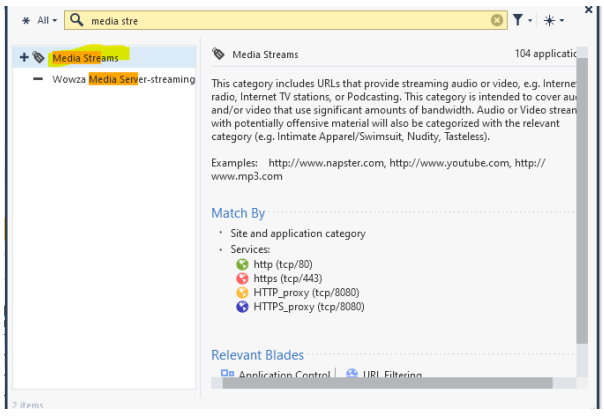
- חוק שחוסם גישה ל- media streaming ו- media sharing לכל משתמשי הרשתות בארגון.
- חוק שמאפשר רק למשתמשים ברשת 10.x.2.0 גישה ל- YouTube.

אדגים יצירת אובייקט Access Role אחד, אבל אותו העיקרון תקף גם לשאר האובייקטים:

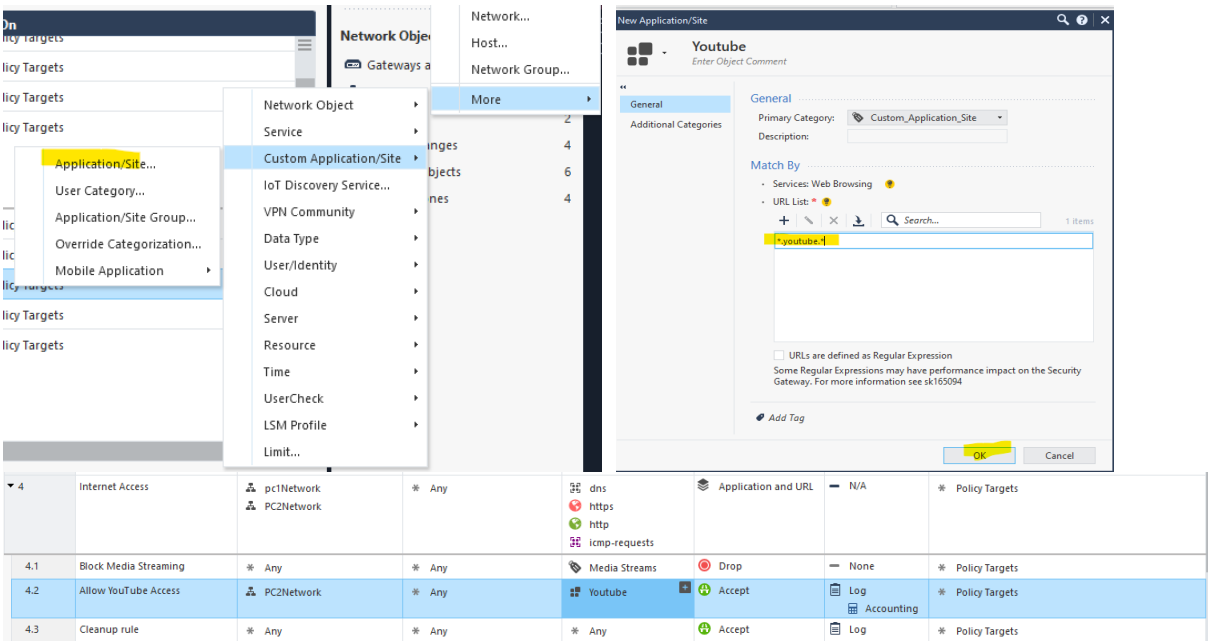


כעת נגדיר את האובייקטים הרלוונטיים לצורך החוקים:

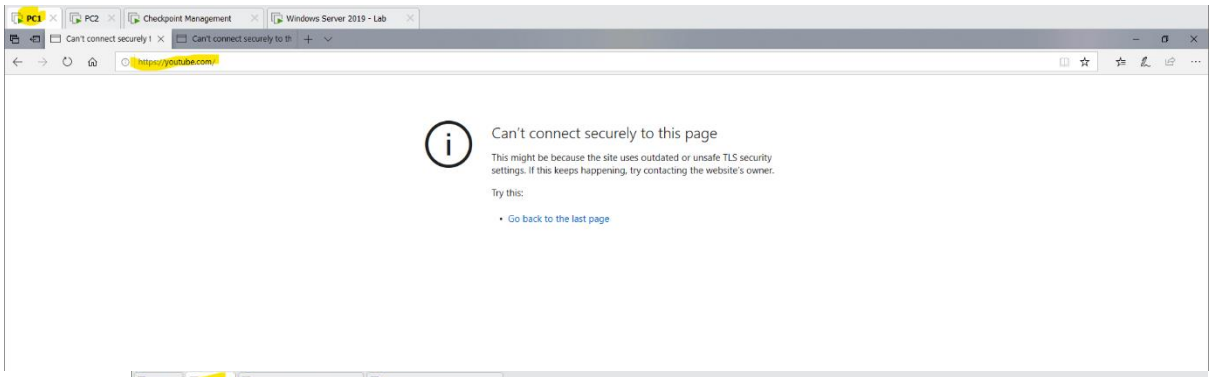


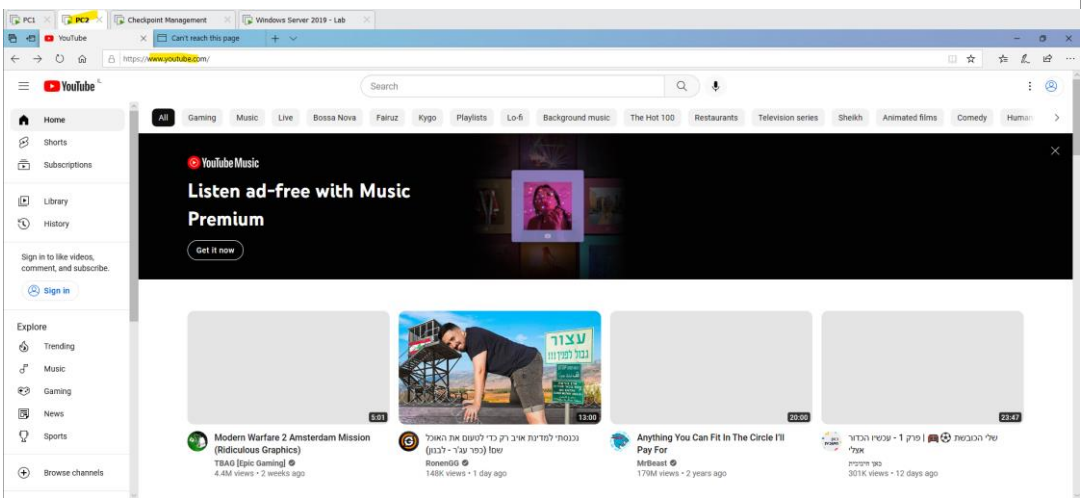


אצור גם אובייקט שמייצג את אתר YOUTUBE:



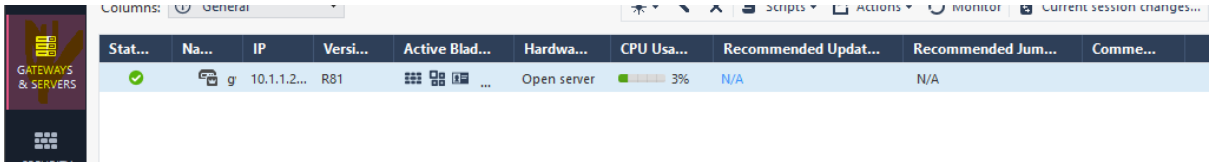
:POC

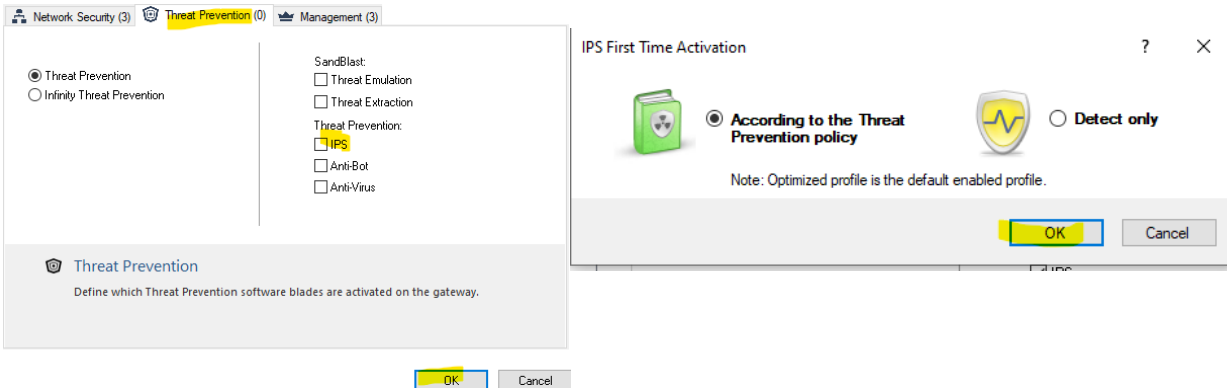


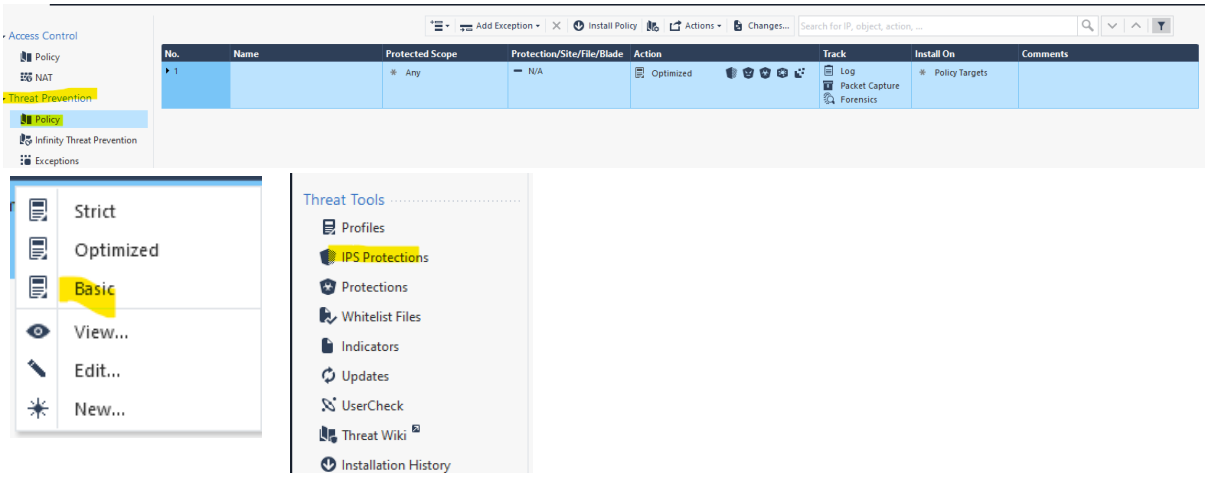


By Elior Sofer

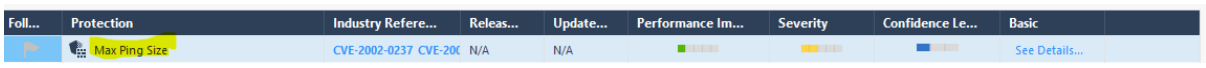
פיצ'ר אחרון שאדגים הוא שימוש ב IP Blade:



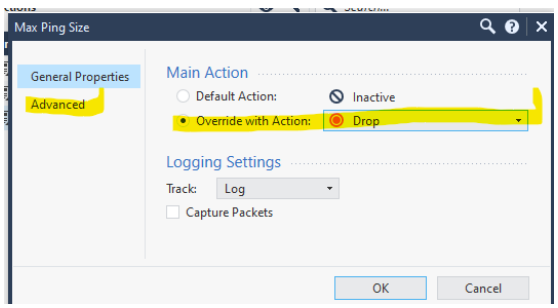


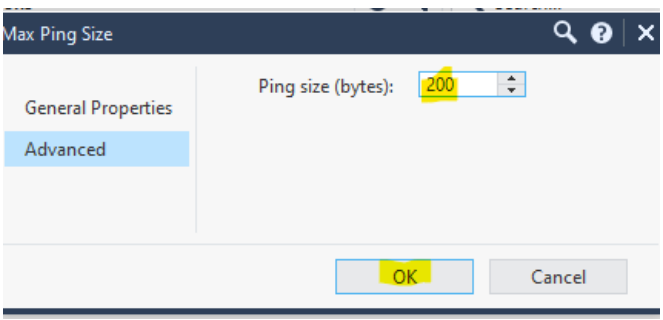


אבחר לשם הדגמה ב :

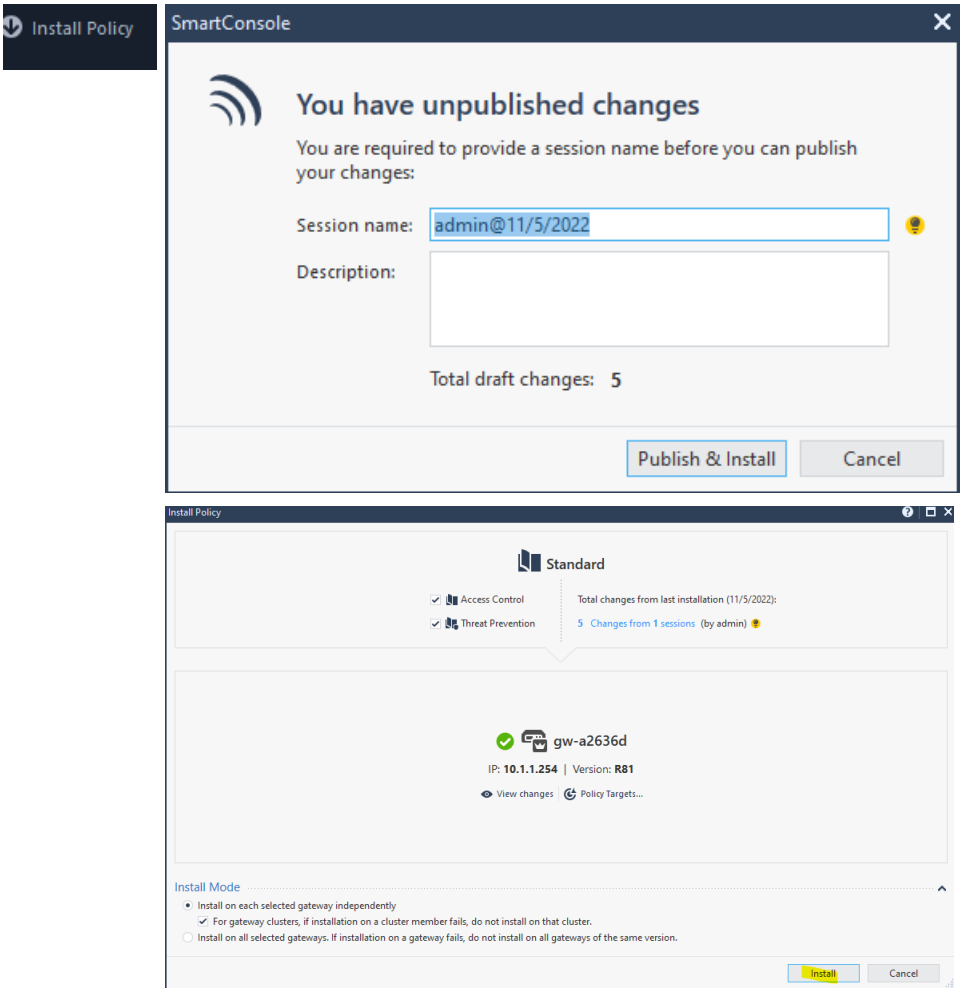


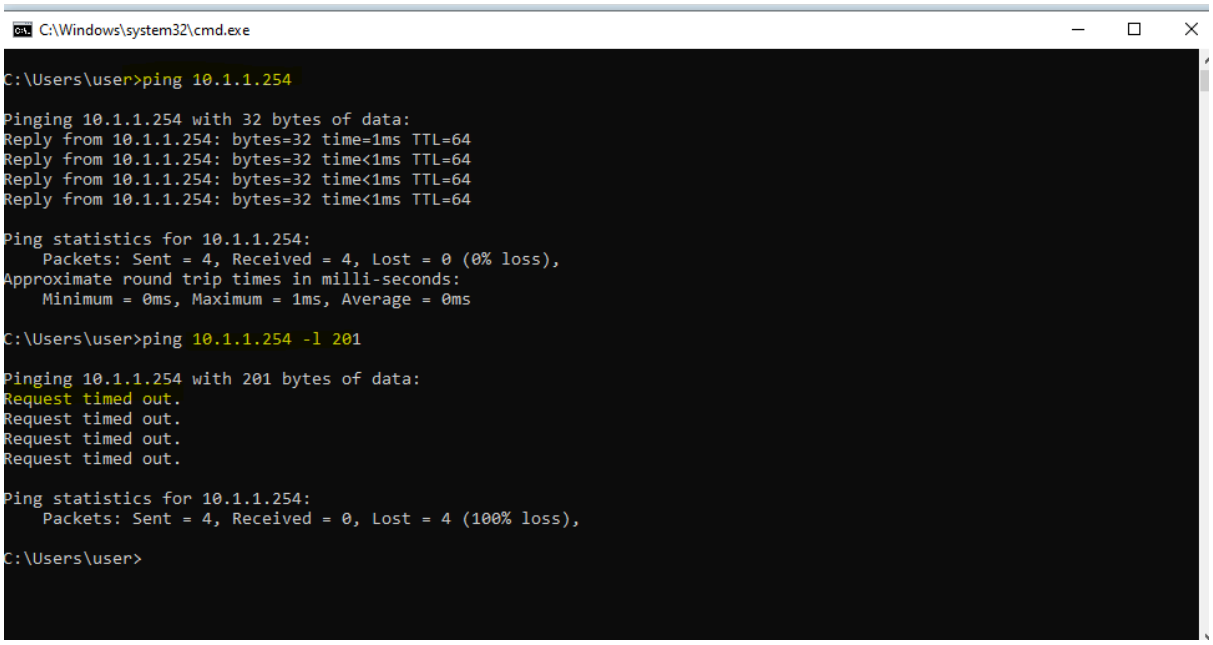
כעת אגדיר שכל פעם ש IPS יפעל בחוק הזה הוא יזרוק את הפקטה, ואגביל את גודל הפקטה עד 200:





By Elior Sofer





By Elior Sofer