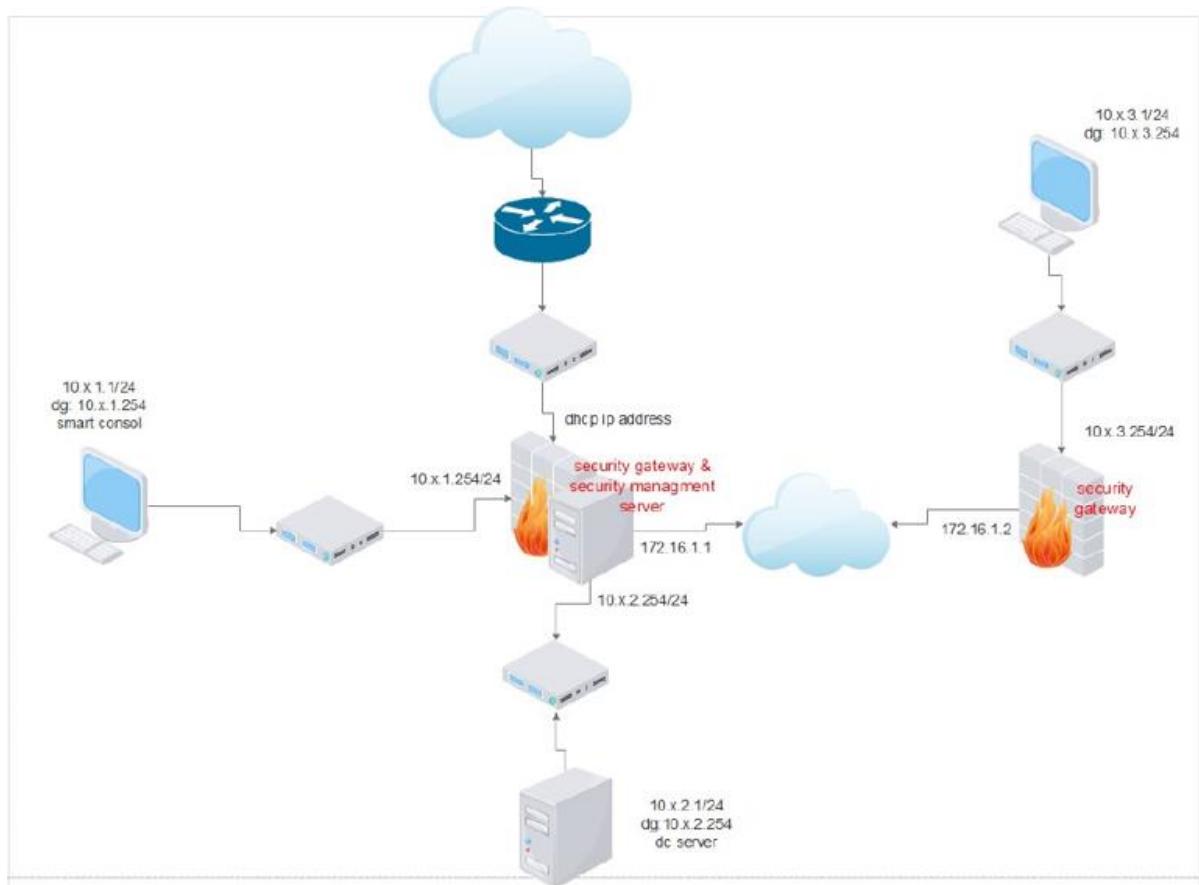


CSP Project

חלק א' - הקמת המעבדה

להלן טופולוגיה הרשת:



הקמת והגדרת מכונה PC1 ו-PC2 WindowsServerLab

ראשית נתחל בהקמת המכונה שתשתמש איתה לניהל את משקי ה-SG (FW) באמצעות ה-

.Console

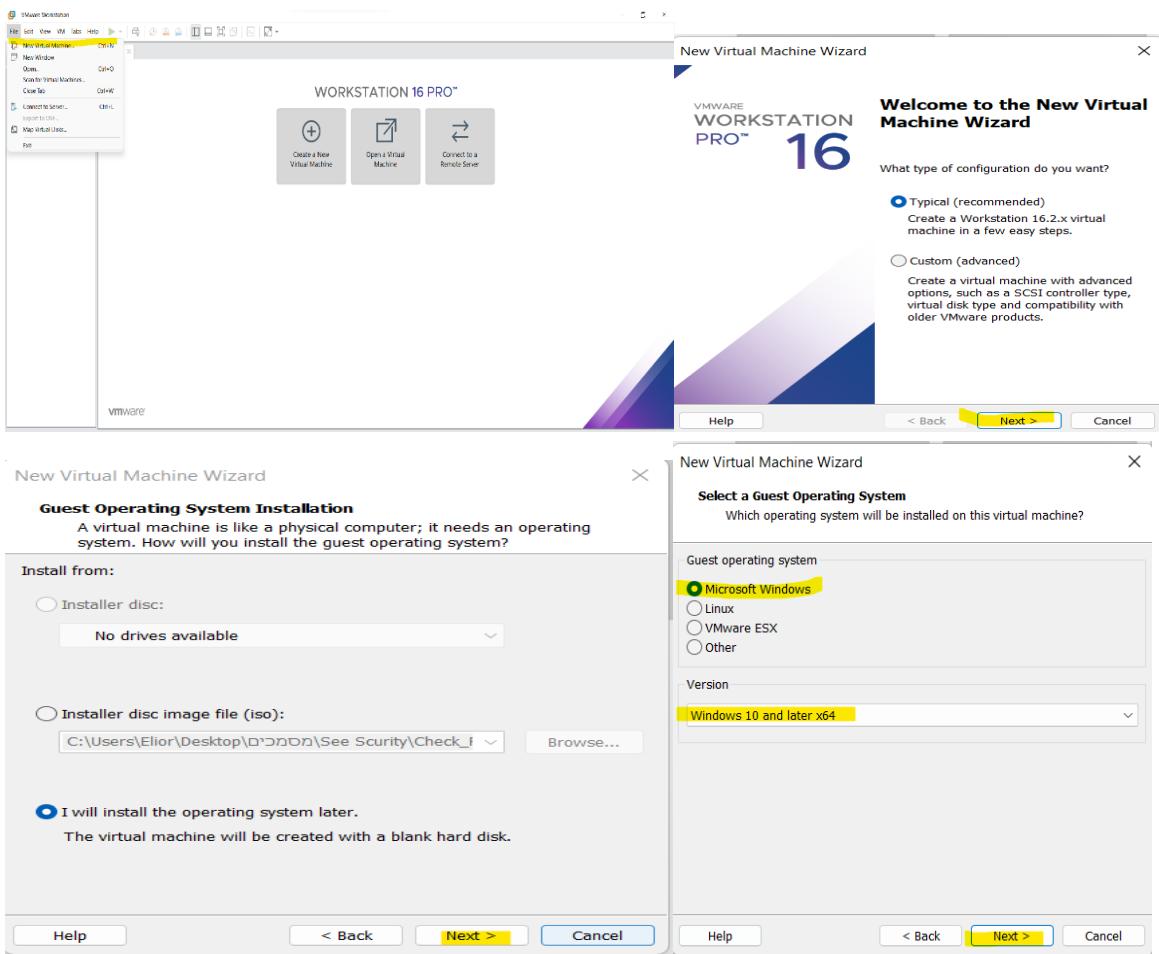
פרטי המכונה:

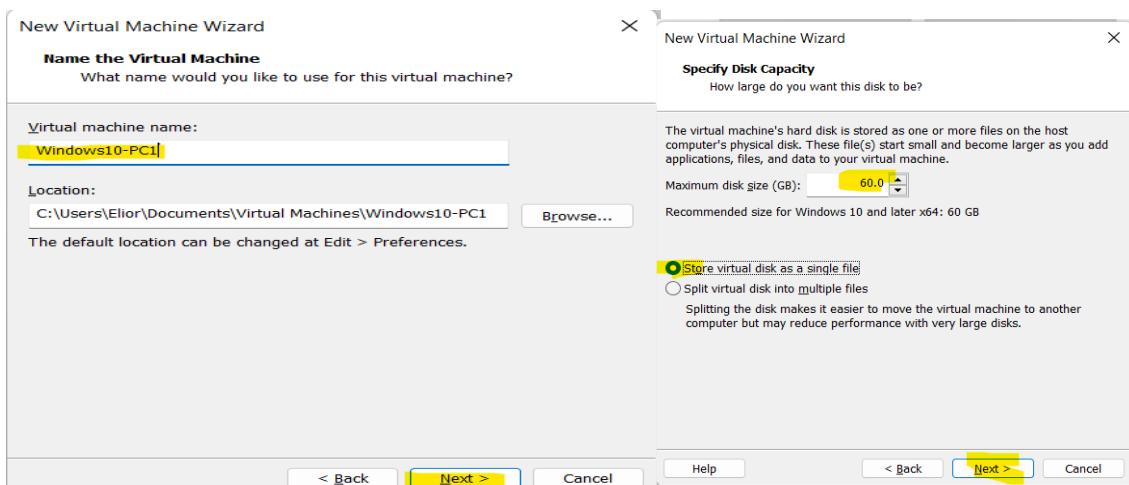
Name: PC1

IP: 10.1.1.1/24

DG: 10.1.1.254

נא לעקוב אחרי השלבים הבאים הדרושים לצורך התקנת המכונה (משמאל לימין):
התחלת זהה לכל אחת מהתיבות קצה **GAIA**. כמו כן במערכת הפעלה
Windows Server יש צורך בחור קובץ ISO שמיועד לה ולכל מכונה יש צורך את
הכתובת IP הרלוונטית לseguemnt שלה.





New Virtual Machine Wizard

Ready to Create Virtual Machine

Click Finish to create the virtual machine. Then you can install Windows 10 and later x64.

The virtual machine will be created with the following settings:

Name:	Windows10-PC1
Location:	C:\Users\Elior\Documents\Virtual Machines\Windows10...
Version:	Workstation 16.2.x
Operating System:	Windows 10 and later x64
Hard Disk:	60 GB
Memory:	2048 MB
Network Adapter:	NAT
Other Devices:	2 CPU cores, CD/DVD, USB Controller, Printer, Sound C...

< Back Cancel

Virtual Machine Settings

Hardware Options

Device	Summary
Memory	2 GB
Processors	2
Hard Disk (NVMe)	60 GB
CD/DVD (SATA)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

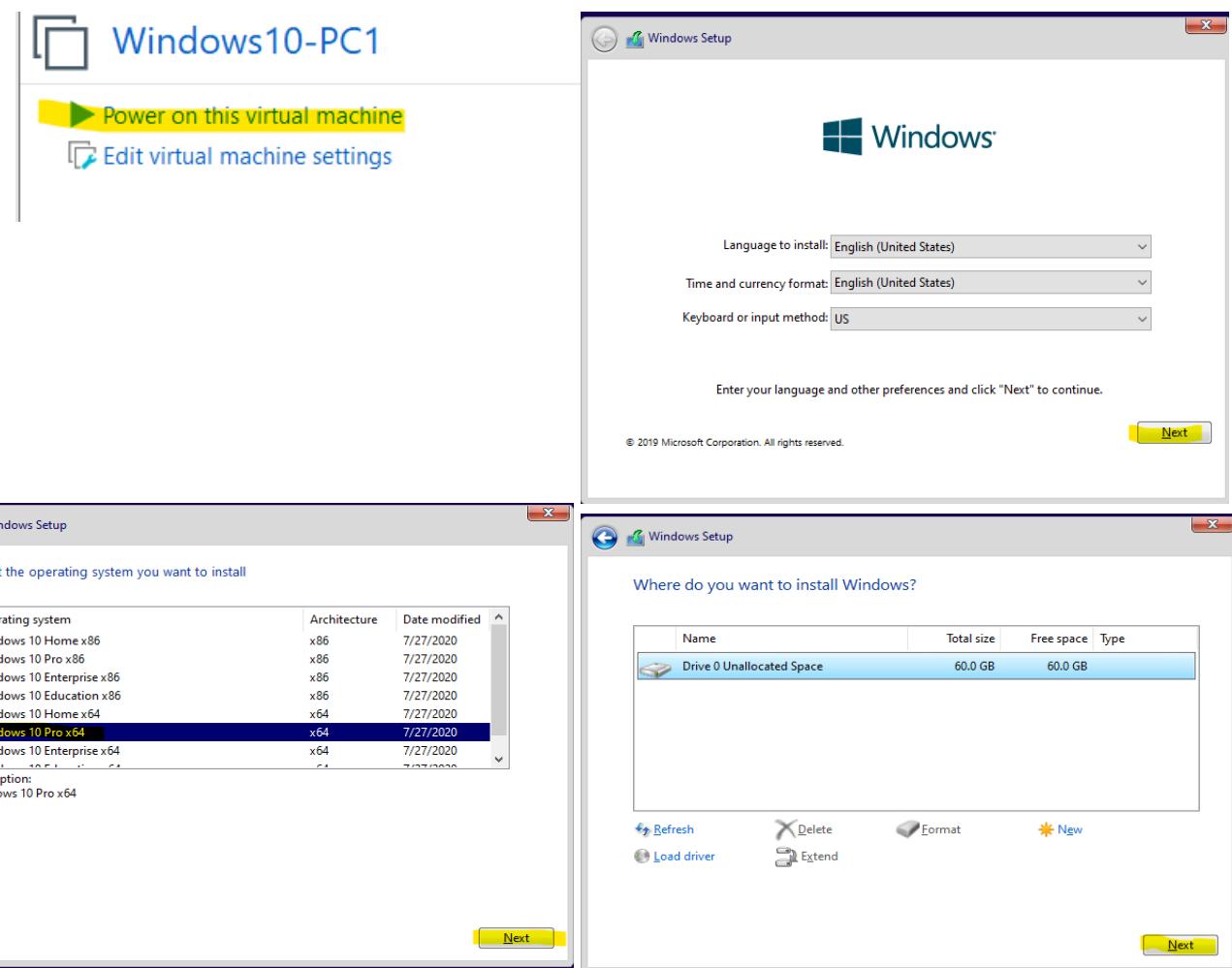
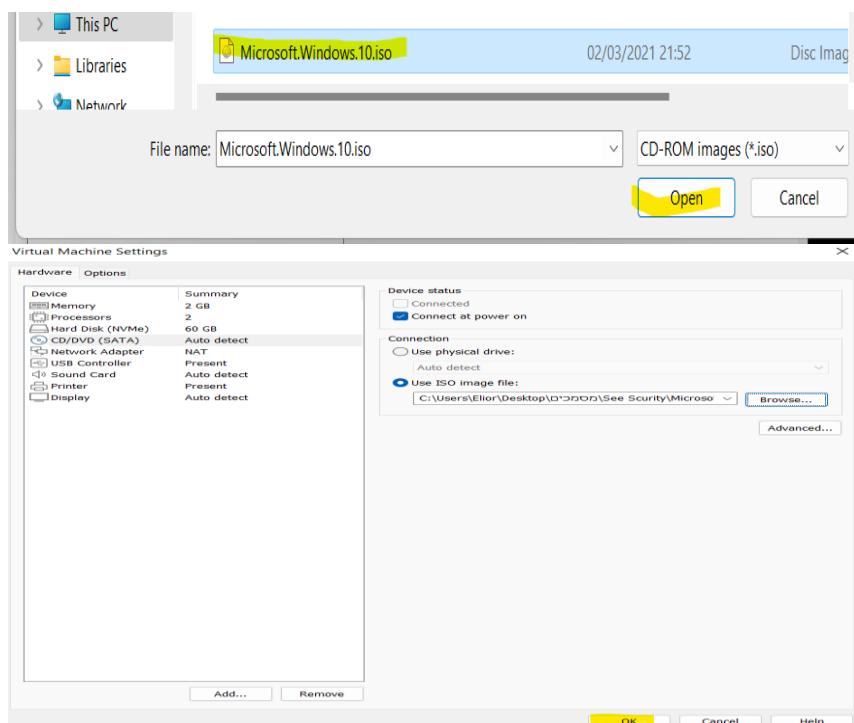
Device status

Connected
 Connect at power on

Connection

Use physical drive:
 Auto detect

Use ISO image file:



By Elior Sofer

Let's add your account

One account connects your device across Microsoft apps and services, like Office, OneDrive, Microsoft Edge, and the Microsoft Store.



Email, phone, or Skype

Create account
Sign in with a security key

Offline account Privacy & Cookies Terms of Use Learn More Next

Sign in to enjoy the full range of Microsoft apps and services



- 1 Sign in and create an account
- 2 Enjoy everything from games to Office to free cloud storage with
- 3 Access the tools you love on all your devices

Limited experience Next

Who's going to use this PC?
What name do you want to use?



User

Or, even better, use an online account Next

Create a super memorable password
Make sure to pick something you'll absolutely remember.



Password

Or, even better, use an online account Next

Let's start with region. Is this right?

U.S. Minor Outlying Islands
U.S. Virgin Islands
Uganda
Ukraine
United Arab Emirates
United Kingdom
United States

Yes

Is this the right keyboard layout?
If you also use another keyboard layout, you can add that next.

Canadian Multilingual Standard (English-India)
Indi
Scottish Gaelic
United Kingdom
United States-Standard

View

How would you like to set up?

Set up for personal use
I'll follow the steps to sign in with a personal Microsoft account.
You'll have full control over this device.

Set up for an organization
I'll gain access to my organization's resources like email, network, apps, and services. Your organization will have full control over this device.

Do more across devices with activity history



If you want timeline and other Windows features to help you continue what you were doing, even when you switch devices, send Microsoft your activity history, which includes info about websites you browse and how you use apps and services. Select [Learn more](#) to find out how Microsoft products and services use this data to personalize experiences while respecting your privacy.

Learn more No Yes

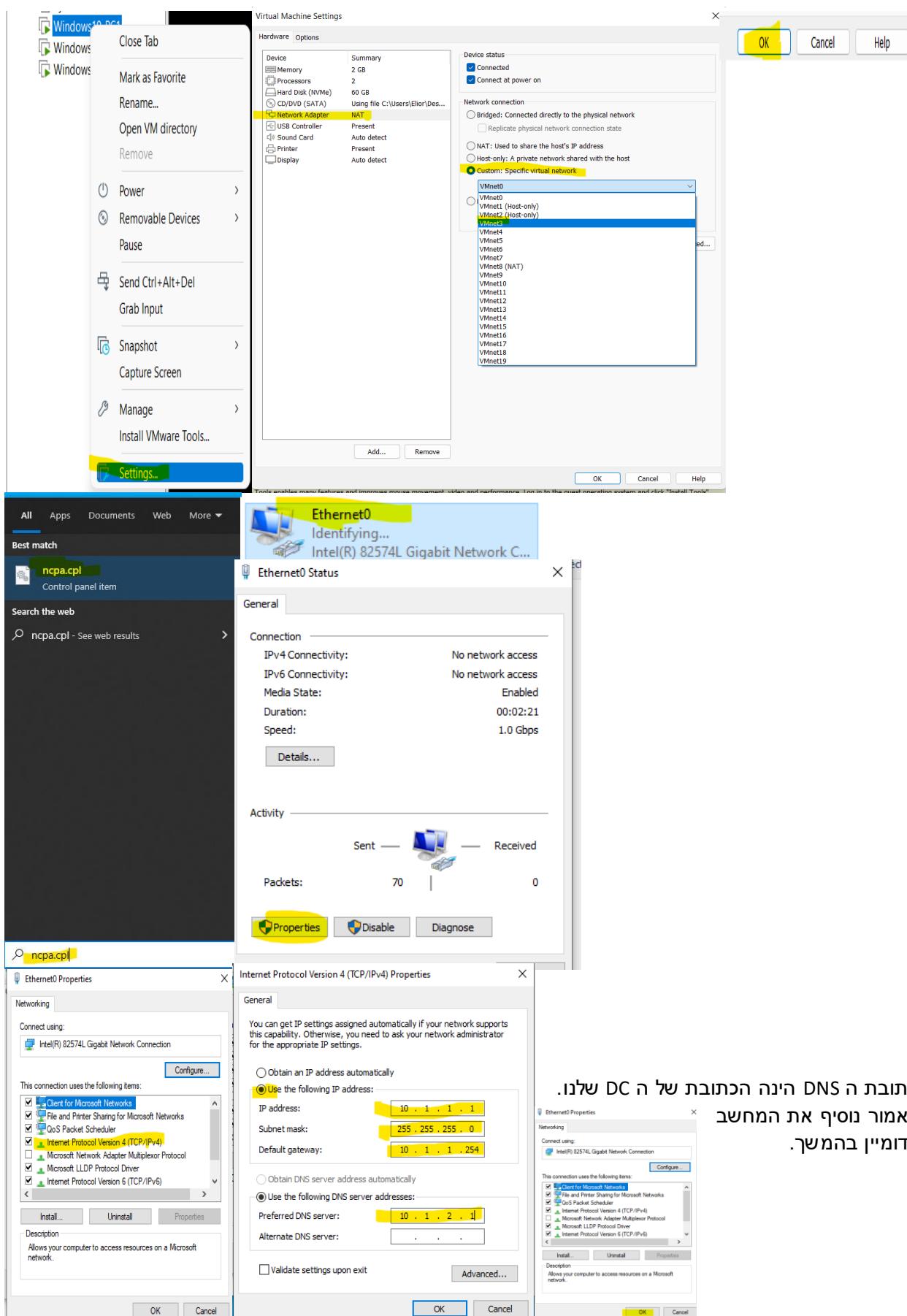
Let Cortana help you get things done
To do this, Cortana needs access to some of your personal information



To let Cortana provide personalized experiences and relevant suggestions, Microsoft collects and uses information including your location and location history, contacts, voice input, speech and handwriting patterns, typing history, search history, calendar details, content and communication history from Microsoft services, messages and apps. In Microsoft Edge, Cortana uses your browsing history. You can always change these choices in the Notebook and disable Cortana in Microsoft Edge.

Learn more Not now Accept

כעת נשאיר את המוכנה **לסגמנט הרלוונטי אליה** ונגדיר לה כתובת IP:



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

כעת סיימנו להגדיר את המוכנה הראשונה.

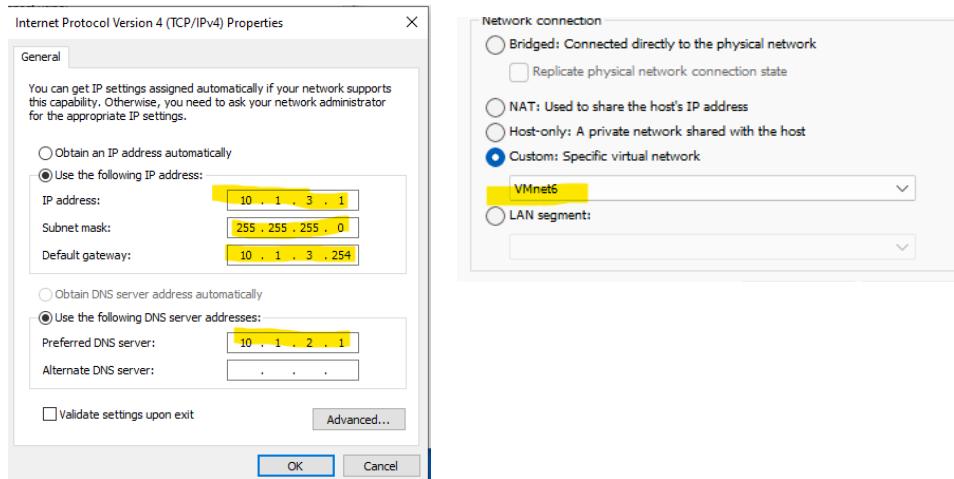
הגדרתי את המוכנה PC2 בדיק כמו שהגדרתי את המוכנה הראשונה, אך שיכתי אותה ל VNET5 והגדרתי אותה לפי הפרטים שלහן:

פרטיה המוכנה:

Name: PC2

IP: 10.1.3.1/24

DG: 10.1.3.254



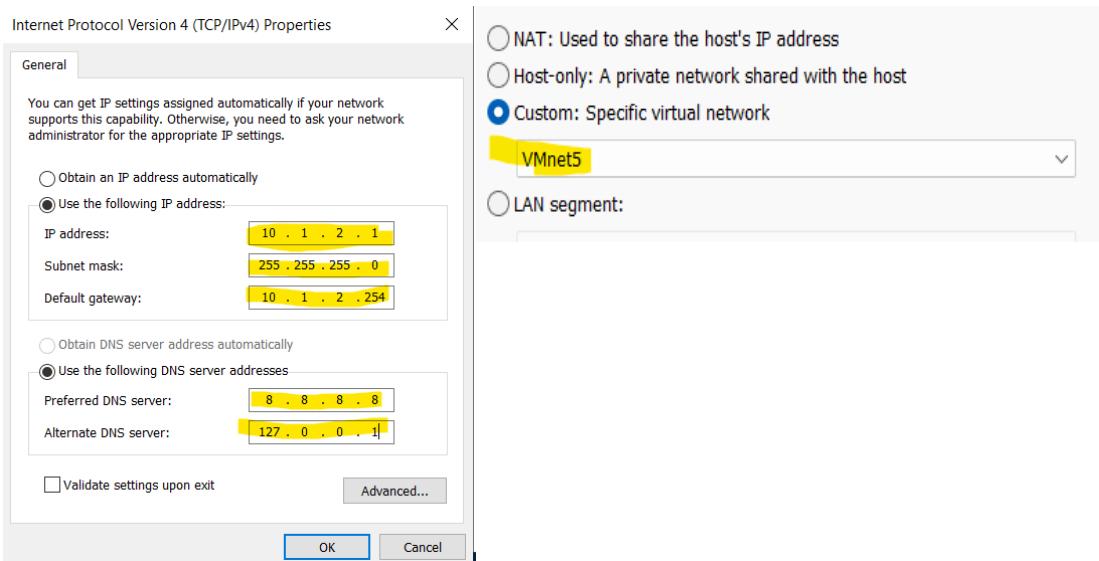
לאחר מכן הגדרתי את המוכנה Windows Server אשר תשתמש אוטומטית בטור DC, שרת DNS ושרת SII. ההגדרה הייתה מאוד דומה להגדרה של המוכנה הראשונה והשנייה. שיכתי אותה ל VNET5 והגדרתי אותה לפי הפרטים שלහן:

פרטיה המוכנה:

Name: WindowsServerLab

IP: 10.1.2.1/24

DG: 10.1.2.254



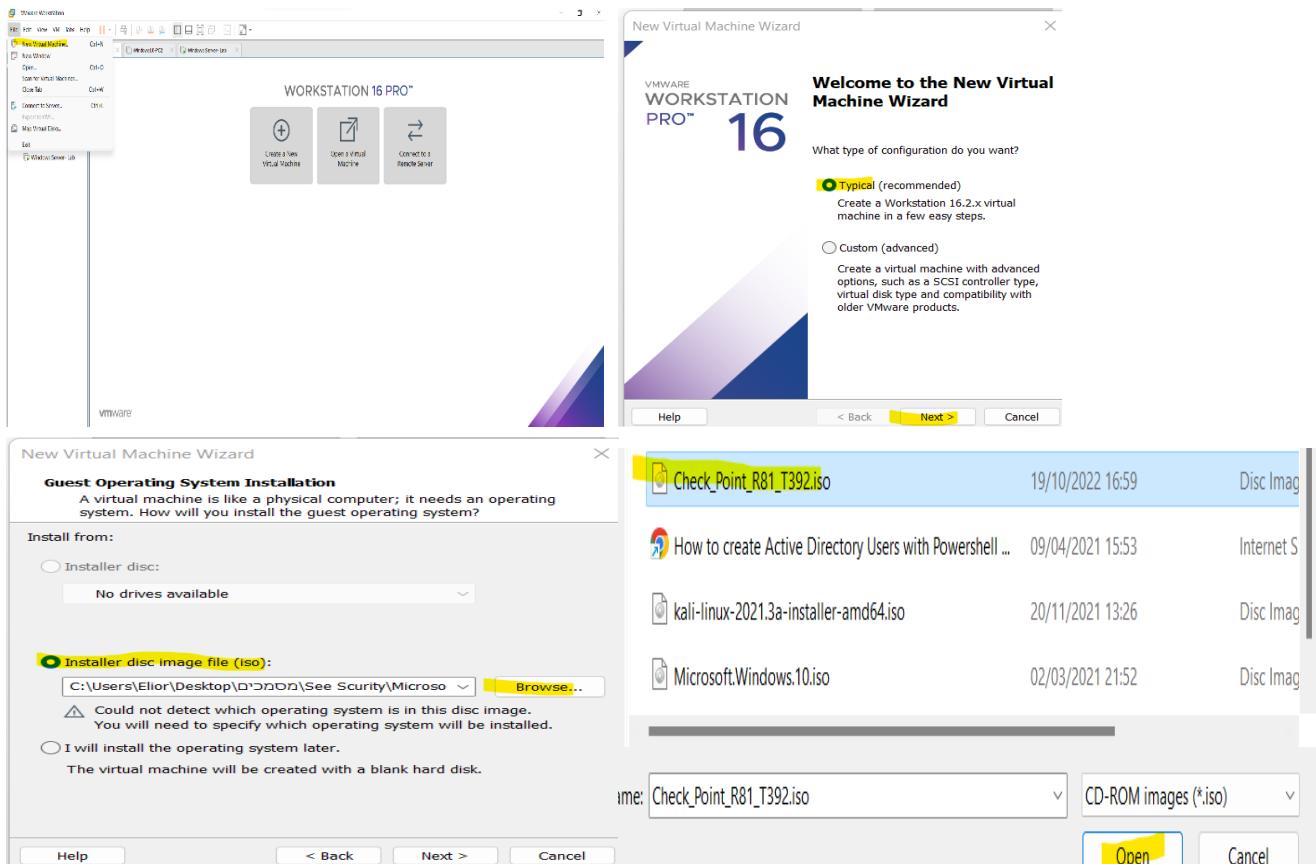
הקמת 2 שרת Security Management Server ו-Security Gateway

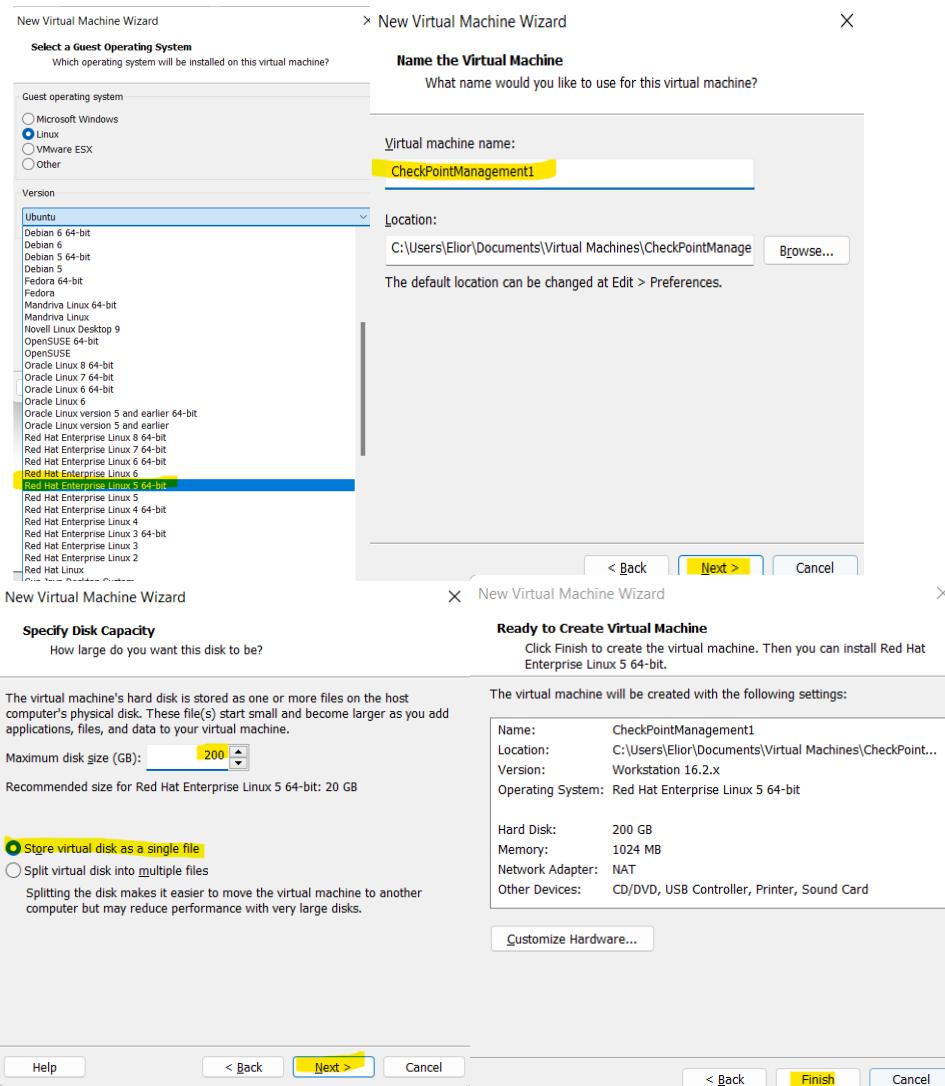
בשלב זה נקיים לפי הטופולוגיה SG (Stand Alone) Security Management server+ SG (Distributed) ובסוגמנט נפרד SG.

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

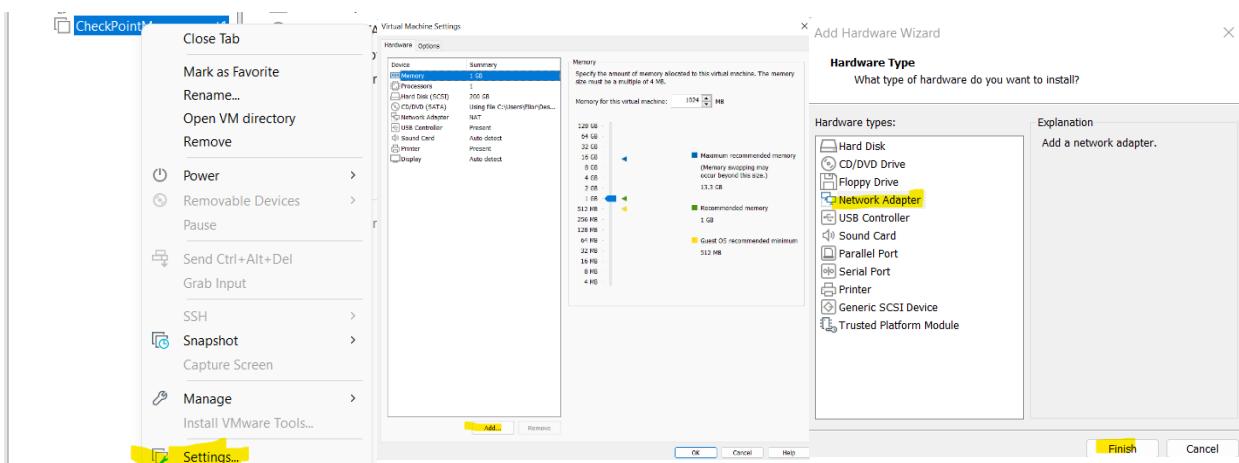
- 10.1.1.254 אשר יתחבר לagemnt של PC1 ויוואו ממשק ניהול.
- 10.2.1.254 אשר יתחבר לagemnt של WindowsServerLab PC2.
- 172.16.1.1 אשר יתחבר לשני, אשר יתחבר לagemnt של PC2.
- אשר יאפשר יציאה החוצה לאינטרנט.

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

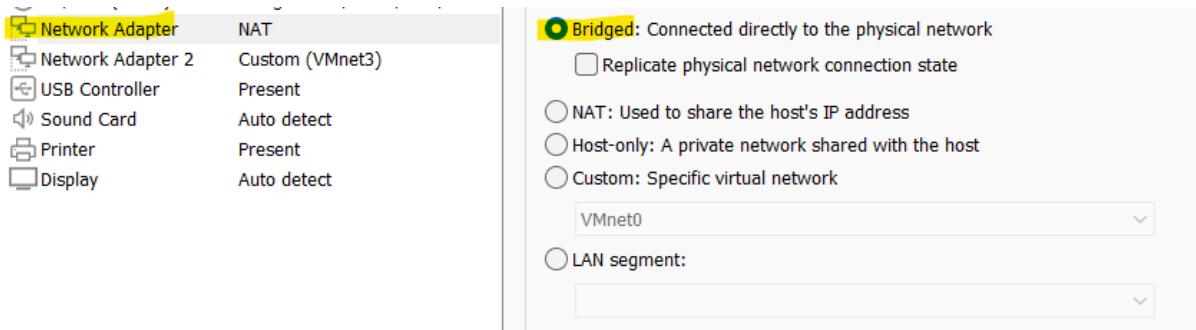




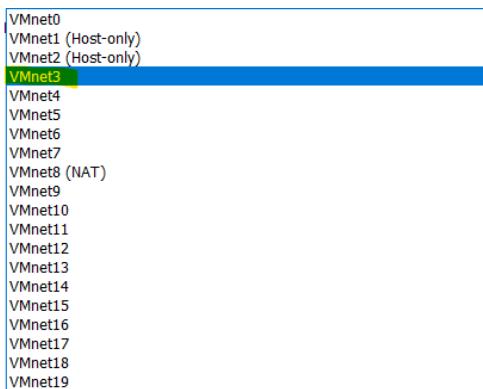
עת Ngidir at 4 hamashkim b'mekoma. Kl rshet lafi h VNET hrloonti la (mbatzim at ha'ula 3 pumim ba'hataema mci'on shi cabr kartis achd shmagiu um mekona shishm otom litzia ha'choza la'intranet-Interface (Bridge Interface):



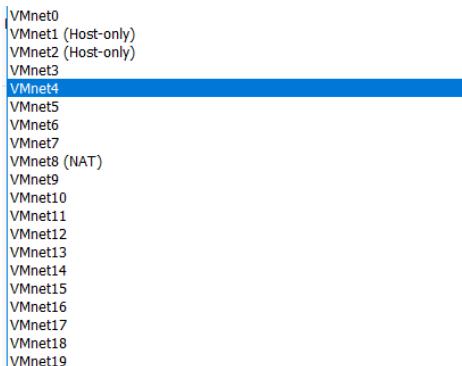
כרטיס הרשת שמשתמש אותו ליציאה החוצה:



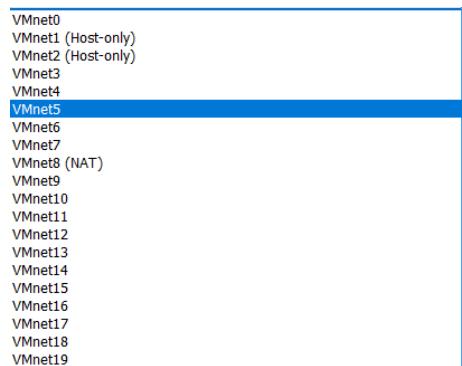
כרטיס הרשת שמשתמש אותו לניהול הממשק:



כרטיס הרשת שמחבר אותו למכונת PC2 ול SG השני:



כרטיס הרשת שמחבר אותו ל Lab WindowsServerLab:

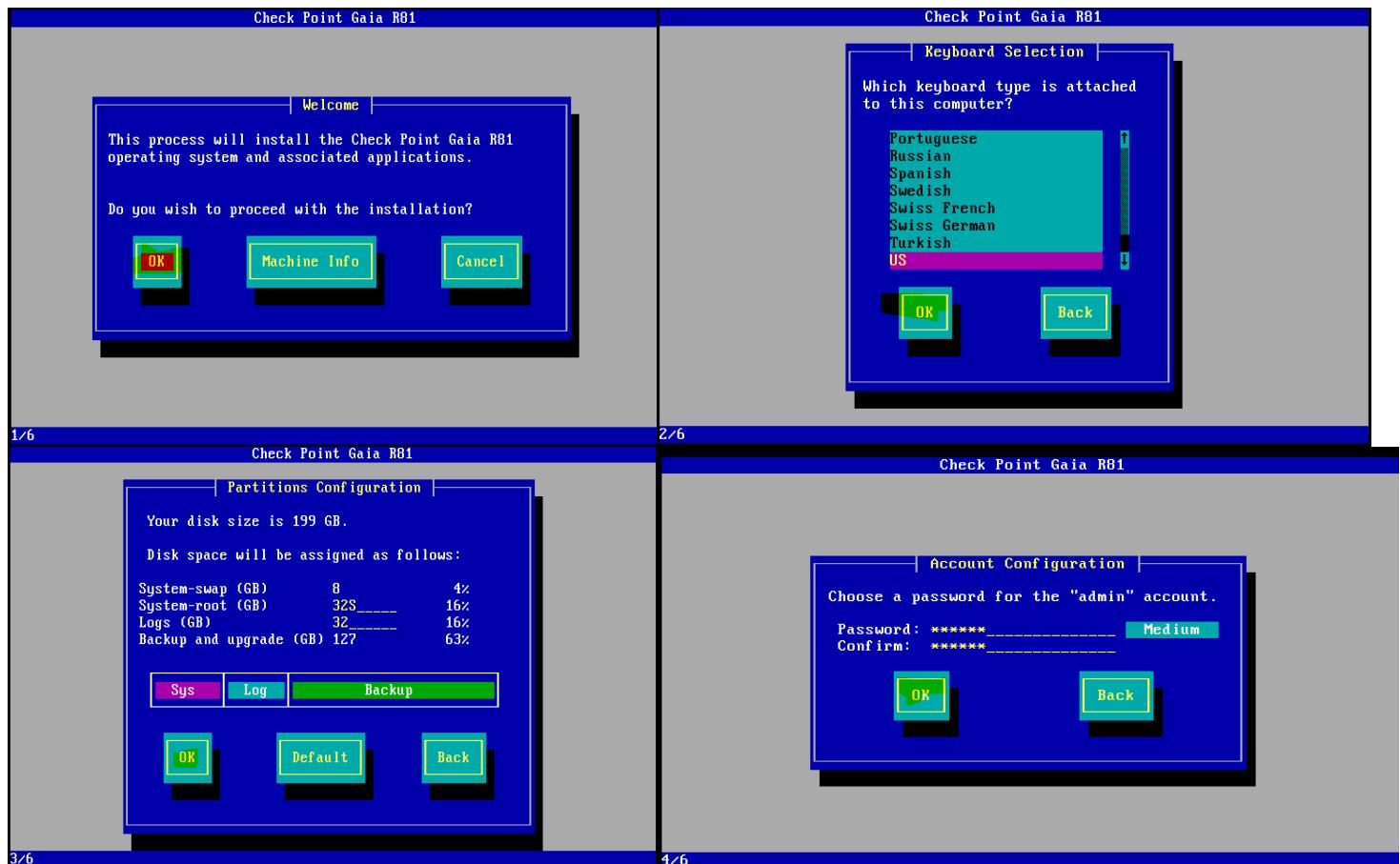


cutet נמשך בתהליך ההתקנה וההגדירה של המכונה:

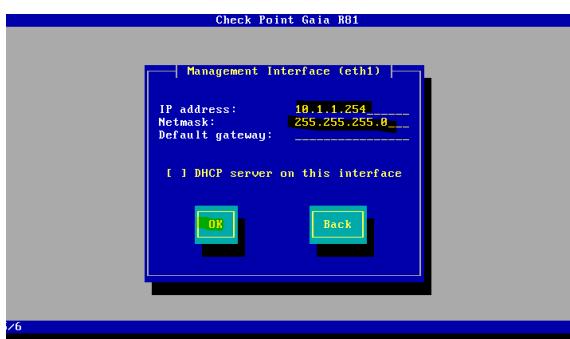
The screenshot shows the 'Virtual Machine Settings' window for a virtual machine named 'CheckPointManagement1'. The 'Hardware' tab is selected. In the 'Processor' section, it shows 1 processor with 4 cores, totaling 4 cores. Under 'Virtualization engine', none of the options (VT-x/EPT, CPU performance counters, or IOMMU) are checked. In the 'Memory' section, the current allocation is 1 GB, which is highlighted in yellow. The 'Memory for this virtual machine' dropdown is set to 8192 MB. A slider below shows the range from 4 MB to 128 GB, with 8 GB currently selected. To the right of the slider, there are three colored boxes: blue for 'Maximum recommended memory' (13.3 GB), green for 'Recommended memory' (1 GB), and yellow for 'Guest OS recommended minimum' (512 MB). The 'Virtual Machine Settings' window has a close button ('X') in the top right corner.

The screenshot shows the 'Welcome to Check Point Gaia R81' screen. It displays the following text:
Install Gaia on this system
Do not install Gaia. Boot from local drive
Install Gaia on a system listed in sk77660
Press [Tab] to edit options

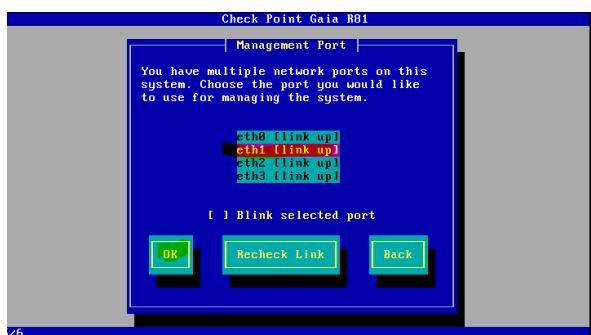
The 'Check Point Software Technologies LTD.' logo is at the bottom left, and the 'GAIA' logo is at the bottom right. The background features a blue and white geometric pattern.

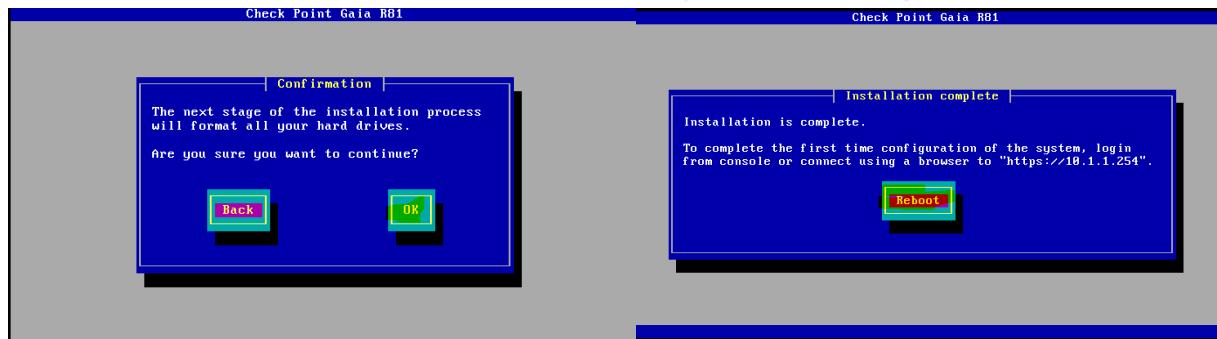
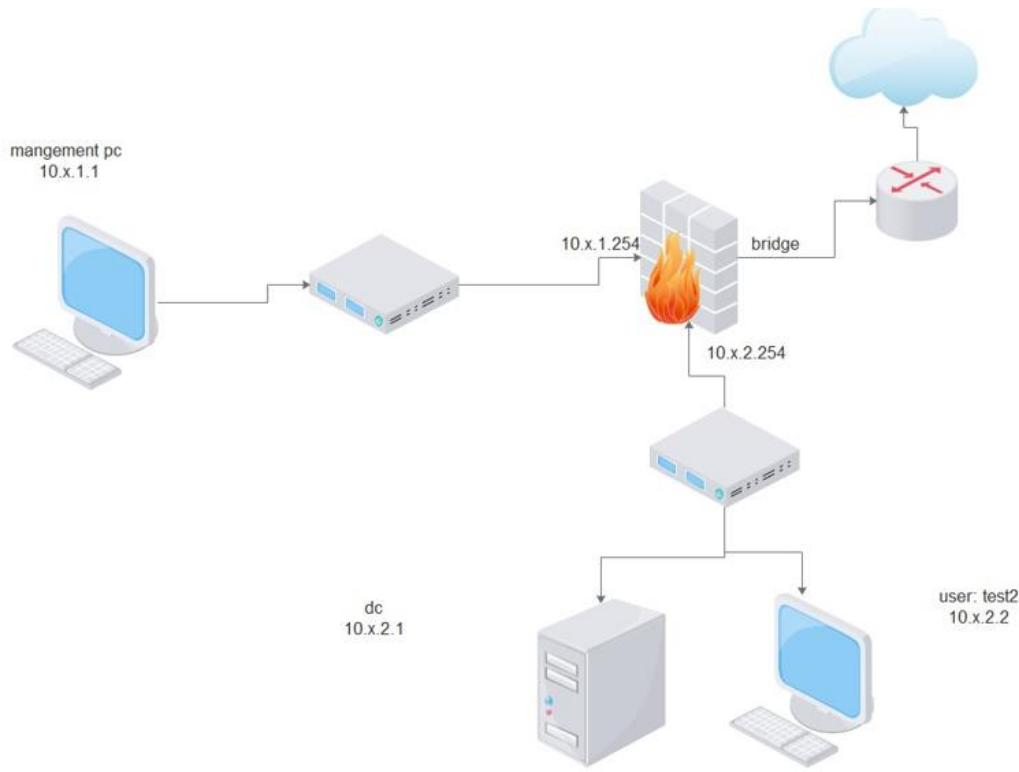


בשלב זה נבחר את הממשק שדרכו נרצה לנהל. במקרה של זה VNET3 והוא נמצא שני. לכן בחרתי ב eth1



כעת אגדייר בשדה הראשון את הכתובת IP של היציאה למשק זה מהמכונה:



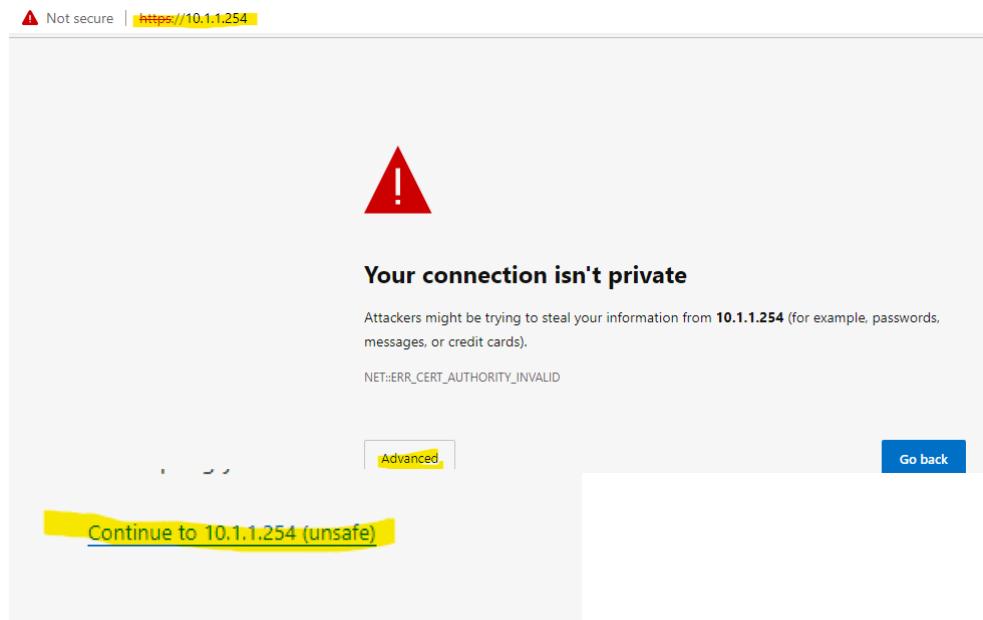


כעת המערכת הפעלה GAIA תעליה. נזין שם משתמש וסיסמה שהגדכנו בתהליך ההתקנה

```
This system is for authorized use only.
login: admin
Password:
In order to configure your system, please access the Web UI and finish the First
Time Wizard.
gw-5e5cf0> _
```

כעת נצטרך להציג את ה SMART CONSOLE דרך הדפסן ב PC1 אשר נמצא במשרket ניהולו:

נכנו דרך PC1 לכתובת של המשרket: <https://10.1.1.254>



כעת נזין את השם משתמש אוisman שהגדרנו בתחילת ההתקנה:

כעת אגדיר תחת Interface את הממשק שモץיא לאינטרנט. במקרה שלי זה eth0

The image shows two adjacent configuration windows from the Check Point software.

Internet Connection: This window allows you to configure an interface to connect to the Internet. It includes fields for selecting the interface (set to eth0), configuring IPv4 (set to Off), and configuring IPv6 (also set to Off). Buttons at the bottom include < Back, Next >, and Cancel.

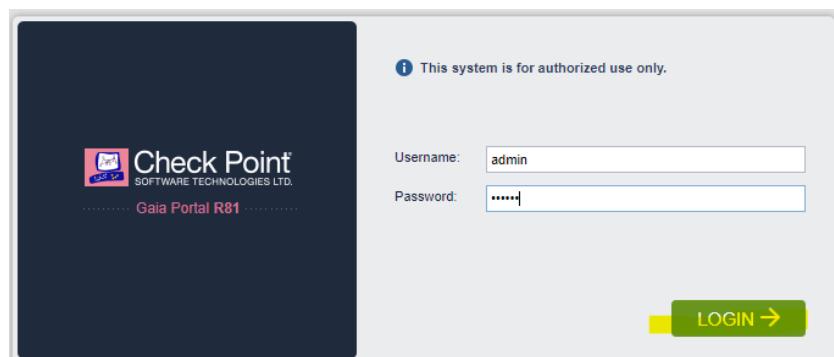
Device Information: This window is for entering device details. It includes fields for Host Name (set to gw-5e5cf0), Domain Name (Optional), Primary DNS Server, Secondary DNS Server, and Tertiary DNS Server. It also includes a section for Proxy Settings with a checkbox for "Use a Proxy server" (unchecked) and fields for Address and Port (set to 8080). Buttons at the bottom include < Back, Next >, and Cancel.

The image shows two adjacent configuration windows from the Check Point software.

Date and Time Settings: This window allows you to set the date and time manually or use Network Time Protocol (NTP). Under "Set time manually:", Date is set to Tuesday, November 01, 2022, Time is 10:58, and Time Zone is Jerusalem, Asia (GMT +2:00). Under "Use Network Time Protocol (NTP):", Primary NTP server is ntp.checkpoint.com, Version is 4, Secondary NTP server is ntp2.checkpoint.com, Version is 4, and Time Zone is Jerusalem, Asia (GMT +2:00). Buttons at the bottom include < Back, Next >, and Cancel.

Installation Type: This window allows you to choose the type of installation. The radio button for "Security Gateway and/or Security Management" is selected, while "Multi-Domain Server" is unselected. Buttons at the bottom include < Back, Next >, and Cancel.

כעת לאחר ההתקנה נתחבר למשק ניהול:



כעת נוצרה להגדר את היציאה החוצה לאינטרנט. נזין את כתובתם של ה DG במחשב שלכם (הפייזי):

Network Management > IPv4 Static Routes

IPv4 Static Routes

Destination Address	Next Hop Type	Rank	Local Scope	Gateways (Priority)	Monitored Protocols	Ping	Comment
Default	Normal	60	N/A	10.1.1.254 (None)	None	No	

Displaying 1 - 1 of 1

Edit Destination Route: Default

Destination: Default
Next Hop Type: Normal
Normal: Accept and forward packets.
Reject: Drop packets, and send unreachable messages.
Black Hole: Drop packets, but don't send unreachable messages.

Rank: Default: 60
Comment:

Add Gateway

Ping: [Add Gateway](#) [Edit](#) [Delete](#)

Gateway	Priority	Monitored Addresses
10.1.1.254	None	None

Add IP Address Gateway

IPv4 Address: 192.168.1.1
Priority: None

Monitored IPs

Add Edit Delete

Monitored Addresses

Force Interface Symmetry:
Monitored IP Fail Condition:

Ok **Cancel**

Edit Destination Route: Default

Destination: Default
Next Hop Type: Normal
Normal: Accept and forward packets.
Reject: Drop packets, and send unreachable messages.
Black Hole: Drop packets, but don't send unreachable messages.

Rank: Default: 60
Comment:

Add Gateway

Ping: [Add Gateway](#) [Edit](#) [Delete](#)

Gateway	Priority	Monitored Addresses
192.168.1.1	None	None

Save **Cancel**

כעת נגדר את הכרטיסי רשות:

The screenshot shows the Winbox interface for managing network interfaces. In the top right, there's a table titled 'Interfaces' with columns: Name, Type, IPv4 Address, Subnet Mask, IPv6 Address, IPv6 Mask Length, Link Status, and Comment. The table lists several interfaces: eth0 (selected and highlighted in yellow), eth1, eth2, eth3, and lo. eth0 has an IP of 10.1.1.254 and is Down. eth1 has an IP of 10.1.1.254 and is Up. eth2 has an IP of 10.1.1.254 and is Down. eth3 has an IP of 10.1.1.254 and is Down. lo has an IP of 127.0.0.1 and is Up.

A detailed configuration dialog for 'Edit eth0' is open in the foreground. It shows the interface is currently Up and set to Ethernet. The 'Enable' checkbox is checked. Under the 'IPv4' tab, the 'Obtain IPv4 address automatically' radio button is selected. If the 'Use the following IPv4 address:' option was chosen, the fields would show an IP of 192.168.1.18 and a subnet mask of 255.255.255.0. There are 'OK' and 'Cancel' buttons at the bottom of the dialog.

ניתן לראות שיש כעת פינガ מהמכונה החוצה לאינטרנט:

```
gw-5e5cf0> ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=52 time=67.3 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=52 time=74.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=52 time=71.2 ms
-
```

בשני הממשקים השניים נctrיך להזין באופן ידני את הכתובות זו:

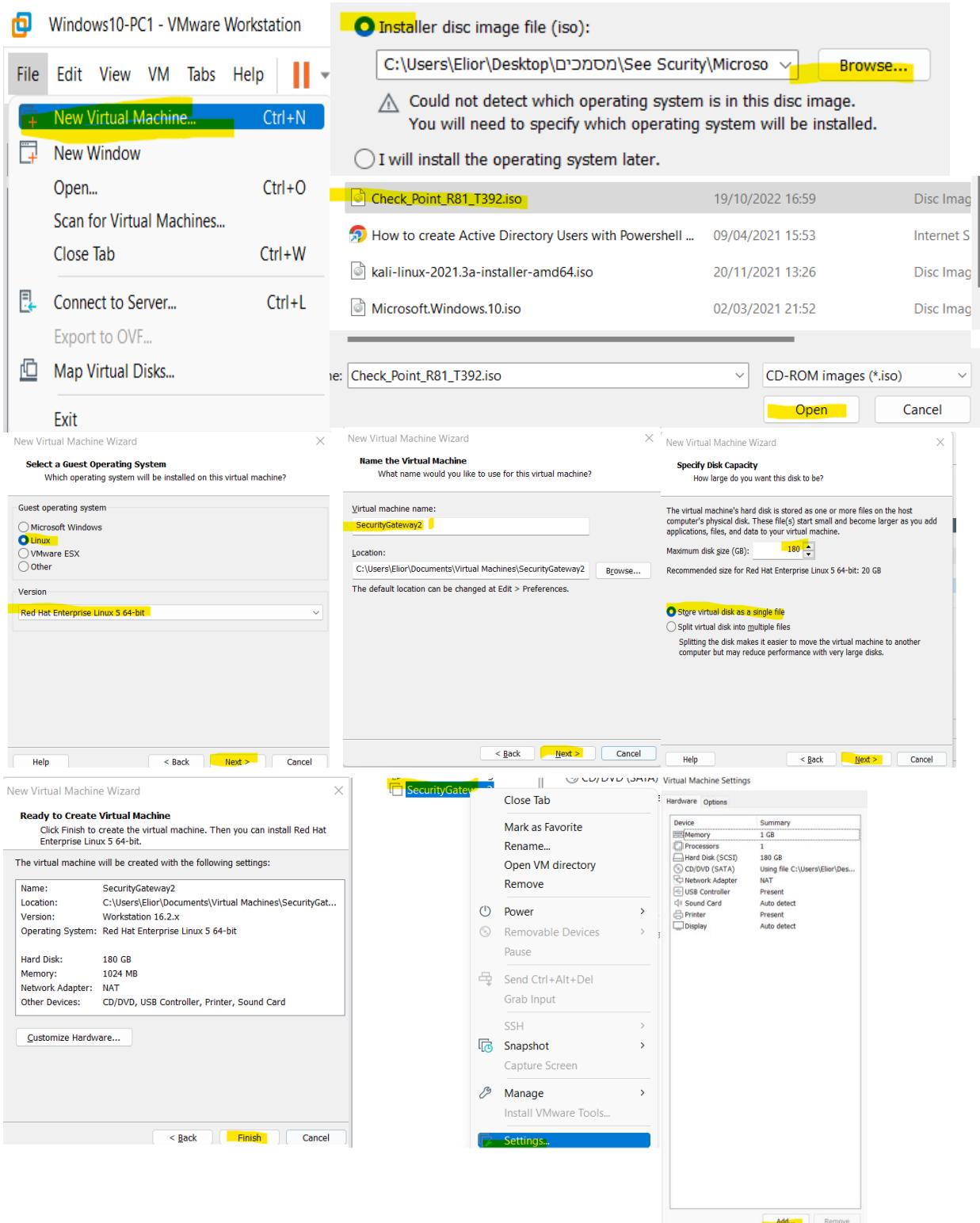
Two configuration dialogs are shown side-by-side. The left dialog is for 'Edit eth2' and the right one is for 'Edit eth3'. Both dialogs have 'Link Status' set to 'Up', 'Type' set to 'Ethernet', and 'Enable' checked. The 'Comment' field for eth2 is 'Second SG and PC2 Interface' and for eth3 it is 'DC Interface'.

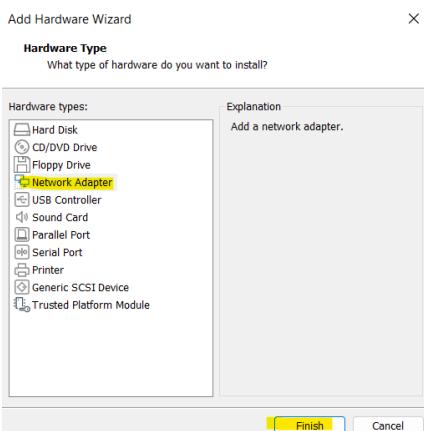
Under the 'IPv4' tab, both dialogs have the 'Obtain IPv4 address automatically' radio button selected. If the 'Use the following IPv4 address:' option was chosen, the fields would show an IP of 172.16.1.1 for eth2 and 10.1.2.254 for eth3, with a subnet mask of 255.255.255.0 in both cases.

At the bottom of each dialog are 'OK' and 'Cancel' buttons.

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

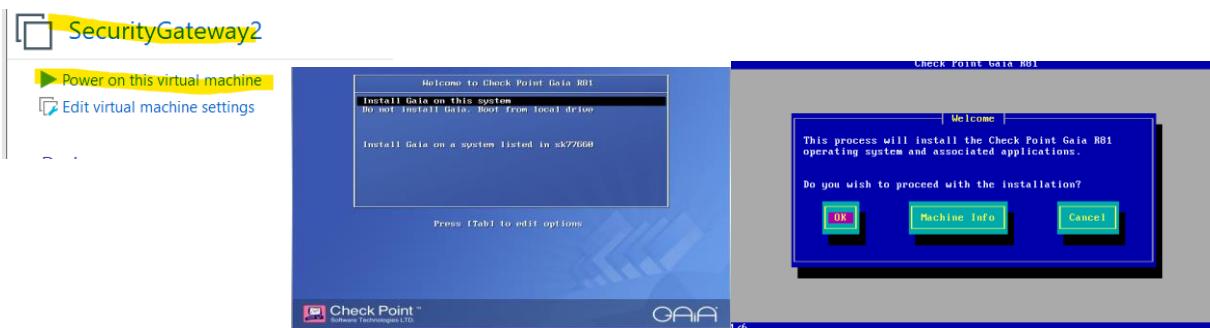
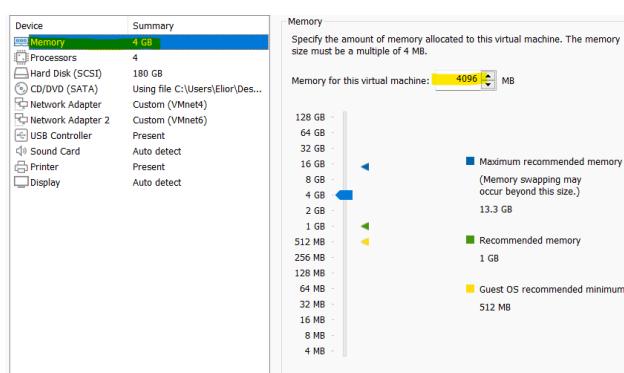
התקנת מכונת SG הנפרדת וחיבורה למשק ניהול

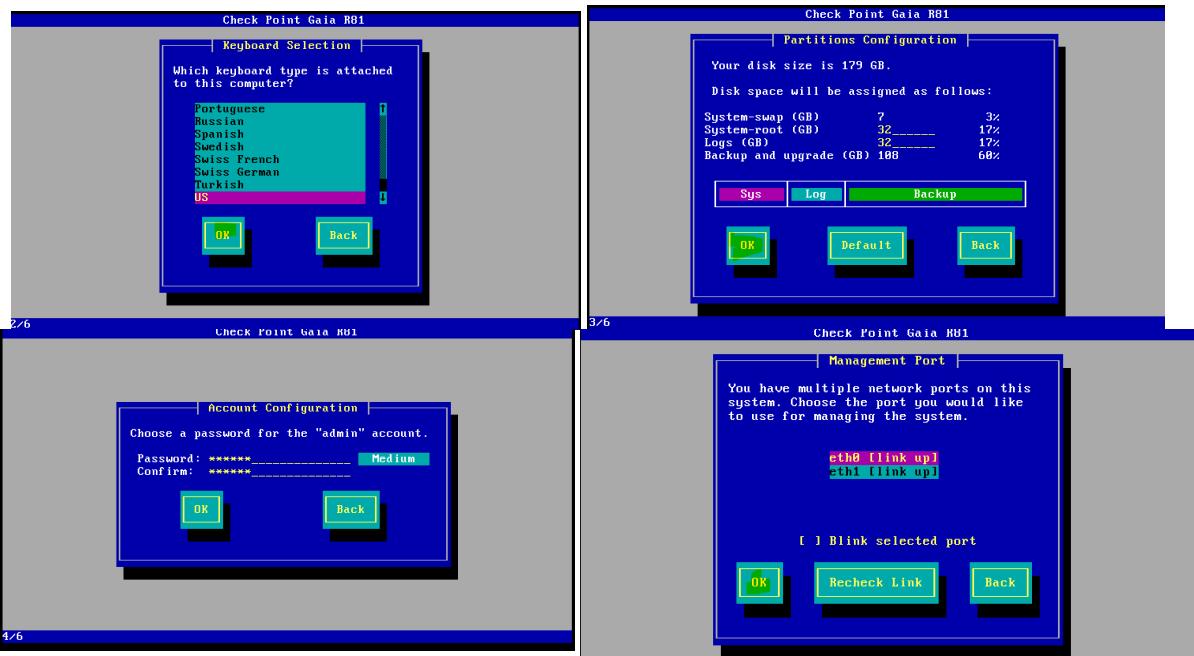




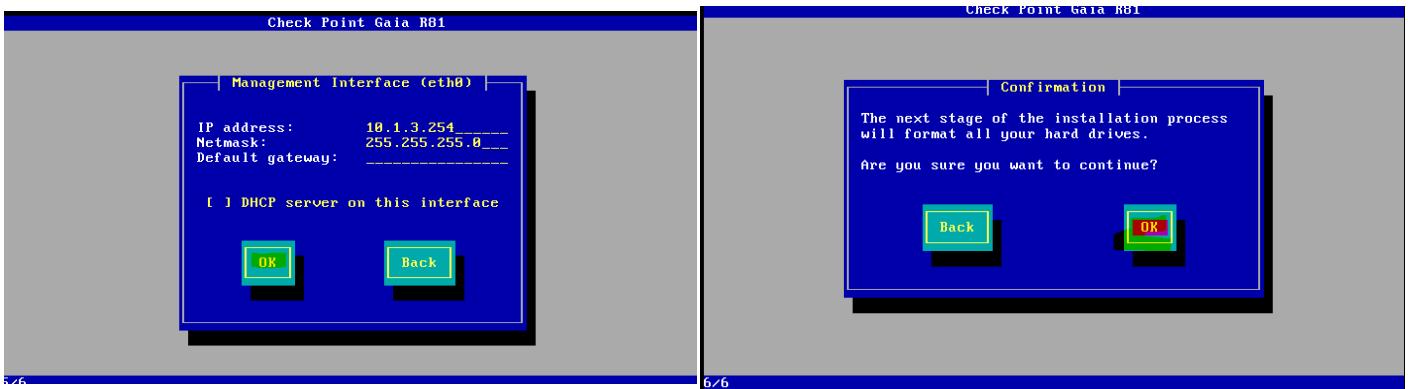
כרטיס הרשת הראשון במכונה יתחבר ל PC2

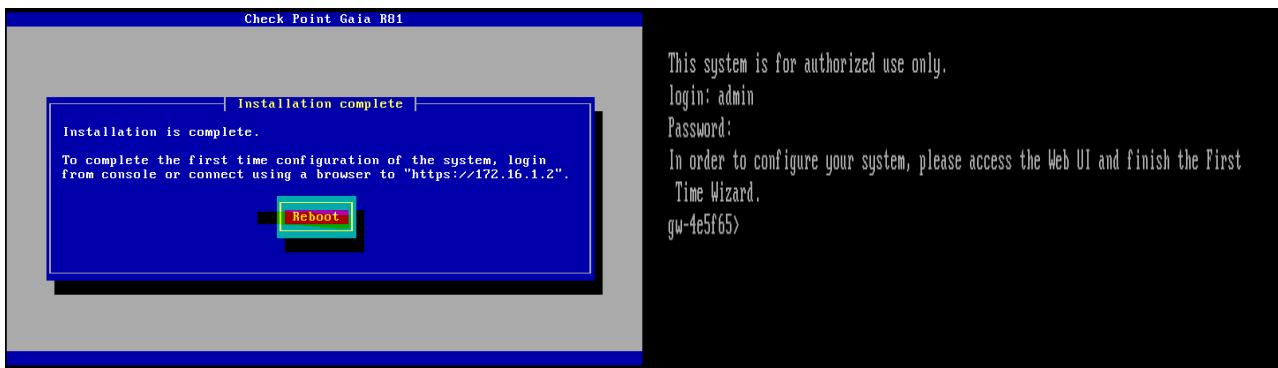
והכרטיס השני יתחבר ל SG1:



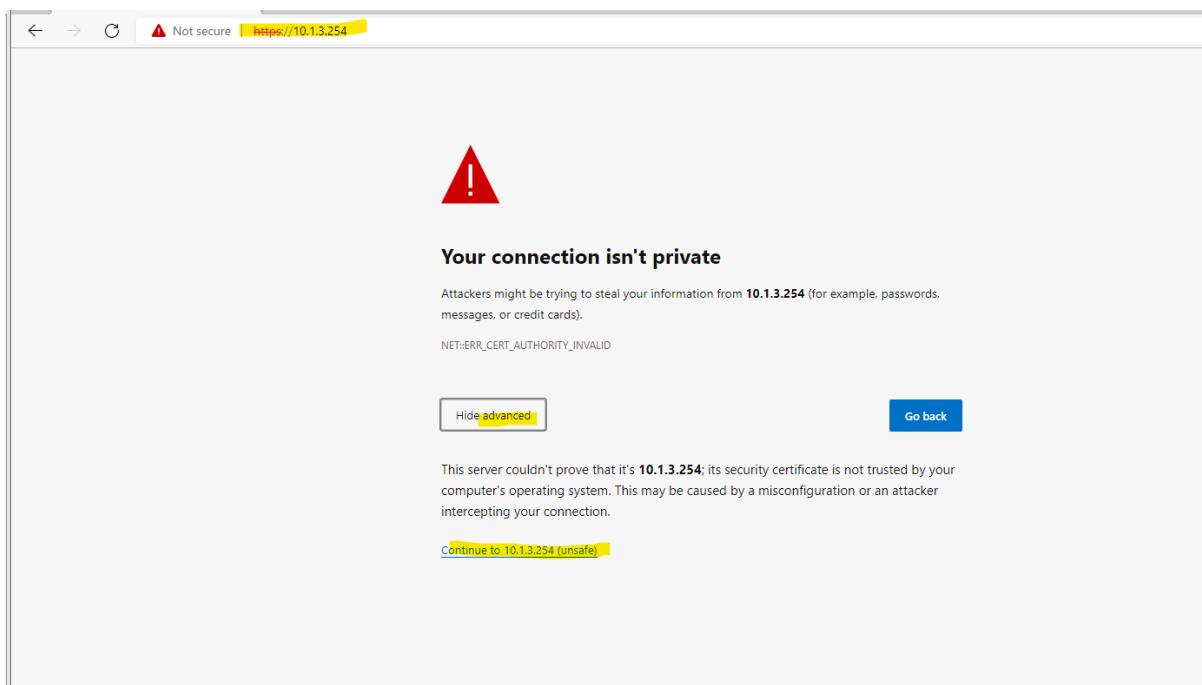


כעת בסדרה הראשון נציג את הכתובת IP של הממשק ניהול לפי טופולוגיה:





כעת יש צורך להגדיר את SG. נכוו לממשק דריך PC2:



Three screenshots illustrating the initial setup process. On the left, the "Gaia Portal R81" interface shows a "Check Point SOFTWARE TECHNOLOGIES LTD." logo and a "Gaia Portal R81" title. In the center, a "R81 First Time Configuration" wizard window is shown, prompting for login with "Username: admin" and "Password:". A green "LOGIN ➔" button is at the bottom. On the right, the "First Time Configuration Wizard" welcome screen is displayed, featuring the Check Point logo, a "vmware" logo, and platform information "Platform: VMware". Navigation buttons "Back", "Next >", and "Cancel" are at the bottom.

Deployment Options

Setup

- Continue with R81 configuration

Installation

- Install from Check Point cloud
- Install from USB device

Recovery

- Import existing snapshot [?](#)

< Back
Next >
Cancel

Management Connection

Interface: **eth0**

Configure IPv4: **Manually**

IPv4 address: **10 . 1 . 3 . 254**

Subnet mask: **255 . 255 . 255 . 0**

Default Gateway: **. . .**

Configure IPv6: **Off**

IPv6 Address:

Mask Length:

Default Gateway:

< Back Next > Cancel

Internet Connection

Configure the interface to connect to the Internet (optional) [?](#)

Interface:	<input type="text" value="eth1"/>
Configure IPv4:	<input type="text" value="Off"/>
IPv4 address:	<input type="text"/>
Subnet mask:	<input type="text"/>
Configure IPv6:	<input type="text" value="Off"/>
IPv6 Address:	<input type="text"/>
Subnet:	<input type="text"/>

[< Back](#) [Next >](#) [Cancel](#)

Device Information

Host Name: SG2

Domain Name:

Primary DNS Server:

Secondary DNS Server:

Tertiary DNS Server:

Proxy Settings

Use a Proxy server

Address:

Port: 8080

Date and Time Settings

 Check Point
SOFTWARE TECHNOLOGIES LTD.

Set time manually:

Date:

Time:

Time Zone:

Use Network Time Protocol (NTP):

Primary NTP server: Version:

Secondary NTP server: Version:

Time Zone:

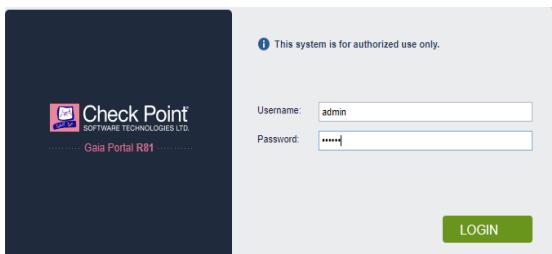
Installation Type

Security Gateway and/or Security Management

Multi-Domain Server

נודא שאנו מורידים את ה V מהאפשרות השנייה!

כעת נצטרך להזין SIC-> תפקידו לחבר בין ה SG הנפרד ל Security Management . נזכיר 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	172.16.1.2	255.255.255.0	-	-	Down	
lo	Loopback	127.0.0.1	255.0.0.0	-	-	Up	

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	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	

התקנת Smart Console

cutת נויריד ונתקן את ה SG אשר למשה מנהל את כל ה SG:

The screenshot shows the Check Point SmartConsole interface. On the left, there's a navigation sidebar with 'Overview' selected. The main area displays 'System Overview' for a 'Check Point Security Gateway | R81'. It shows the kernel version (3.10.0-957.21.3cpx86_64), edition (64-bit), build number (392), system uptime (1 hour 25 minutes), and software updates (no new recommended updates detected). To the right, there's a section titled 'Blades' with icons for Firewall, IPSec VPN, and IPS.

Below the overview, there's a timeline section with a single entry for 'SmartConsole' at '11/1/2022 12:38 PM'. The application section shows 'Application' and '450,720 KB'. At the bottom, there's a 'Check Point SmartConsole' installation window. It has three panels: 'Welcome' (with 'Installation' and 'Finish' steps), 'Installation' (with a progress bar and 'Install' button), and 'Finish' (with a 'Finish' button).

cutת נתחבר למשק ניהול ה SG הראשי (SG1)

The screenshot shows the SmartConsole login screen. It features a 'SmartConsole' logo and the text 'R81'. Below it is a login form with fields for 'admin', 'password', and 'IP address' set to '10.1.1.254'. There are checkboxes for 'Read Only' and 'Demo Mode'. A 'LOGIN →' button is at the bottom. To the right, a message says 'First connection to server 10.1.1.254' and asks to verify the server identity by comparing the displayed fingerprint ('DUST NASH LILA NEWS DARE HEED COVE LOSE BAWL MASS CRAM WEB') with the one in the server. It includes 'BACK' and 'PROCEED' buttons.

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

חוק מס' 1:

מטרת החוק: לזרוק חבילות מיד ולא Log. החוק מצל על ה- Firewall וכן מאיצ' את ביצועיו. בנוסף סינון הרשותות שנכנסות ל- Log הופך אותו לקריא יתירה. מיקום החוק: ראשוני.

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

חוק מס' 2 (התמוךות Stealth Rule)

מטרת החוק: להגן על ה- Security Gateway על-ידי חסימת התקשרות אליו. למורoutes חוק זה, ניתן ליצור קשר עם ה- Security Gateway בזכות חוק מערכת וחוק ניהול. מיקום החוק: בין החוקים הראשונים.

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

חוק מס' 3 (Management Rule)

מטרת החוק: לאפשר ניהול של ה- Security Gateway. מיקום החוק: מעל Stealth Rule.

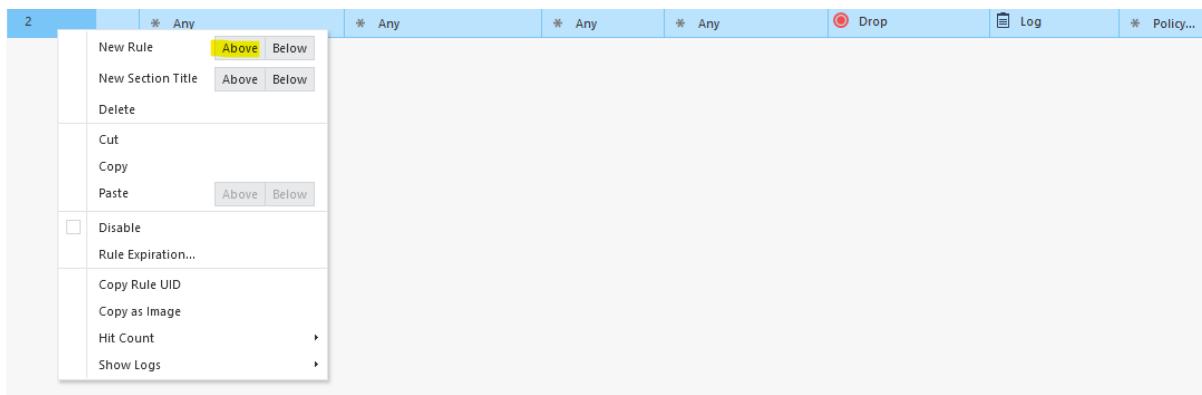
Name	Source	Destination	Services & Application	Action	Track	Install On
Management	windows10	gw-2cef02	https echo-request ssh_version_2	Accept	Log	* Policy Targets

חוק מס' 4 (Cleanup Rule)

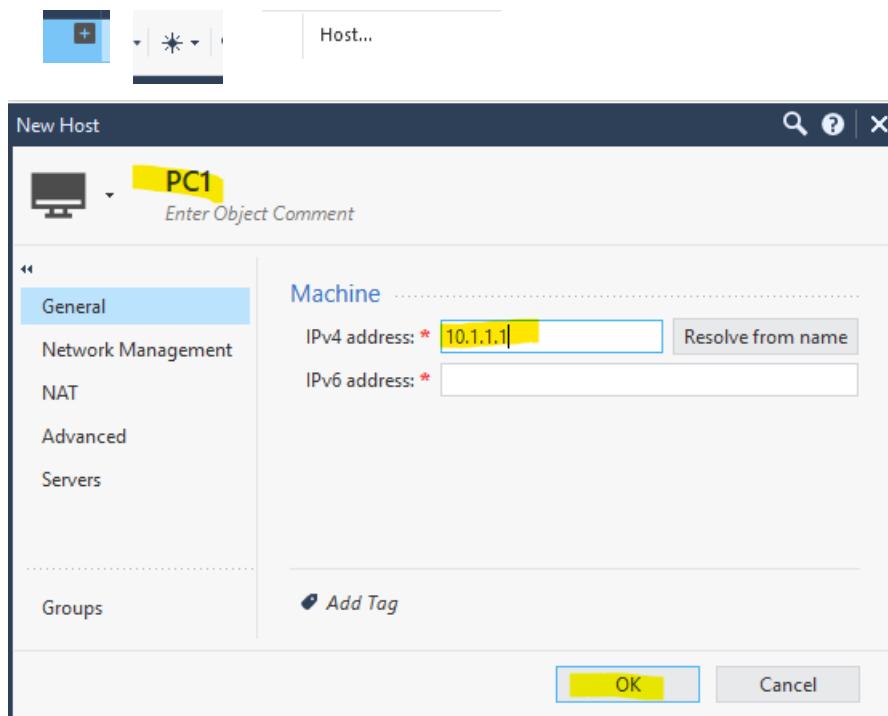
מטרת החוק: ביצוע Log ל Packets שנזרקים כתוצאה מחוסר התאמה לשום חוק אחר. מיקום החוק: תמיד אחרון.

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

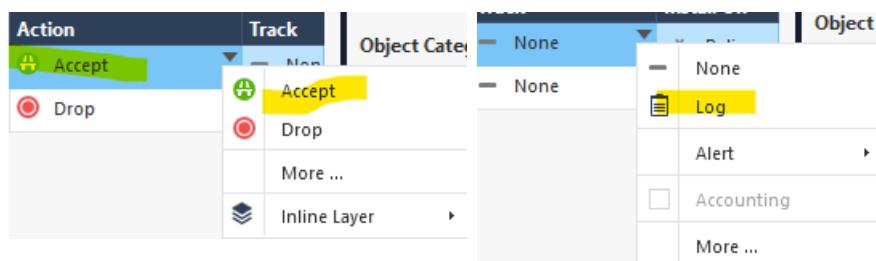
על מנת ליצור חוק יש לעשות את הפעולות הבאות:



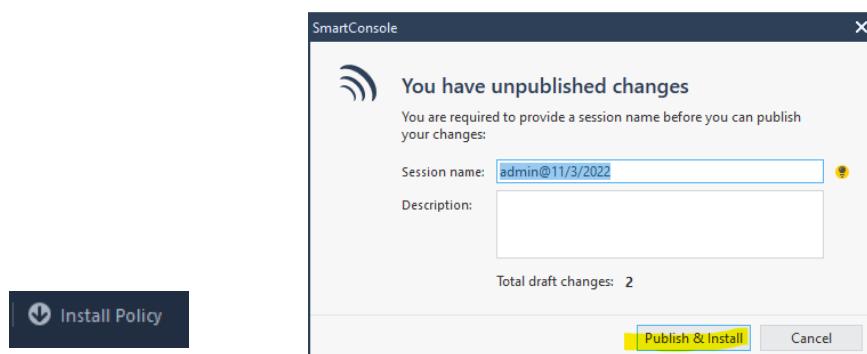
לאחר מכן יש ליצור אובייקט על פי הצורך. לדוגמה בחוק Management Rule ליצור אובייקט ל PC1
וاسم אותו ב :Source



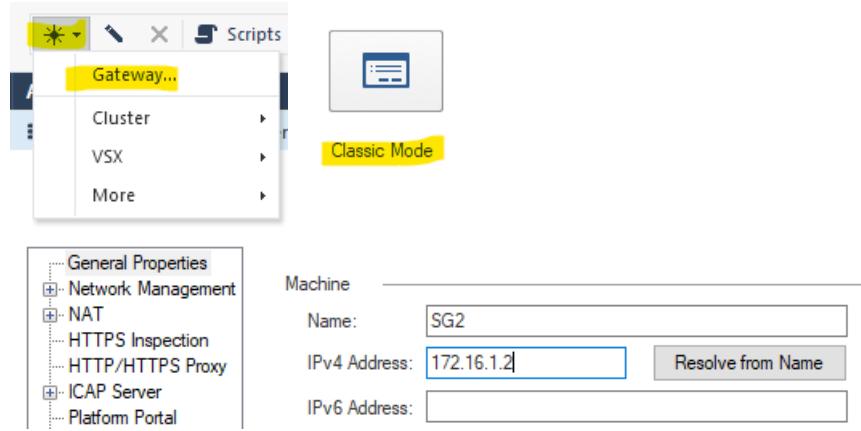
לאן מכאן נשנה את ה ACTION ל **TRACK** ומשנה את ה **LOG** על מנת שנוכל לראות לוגים
שקשורים לחוק



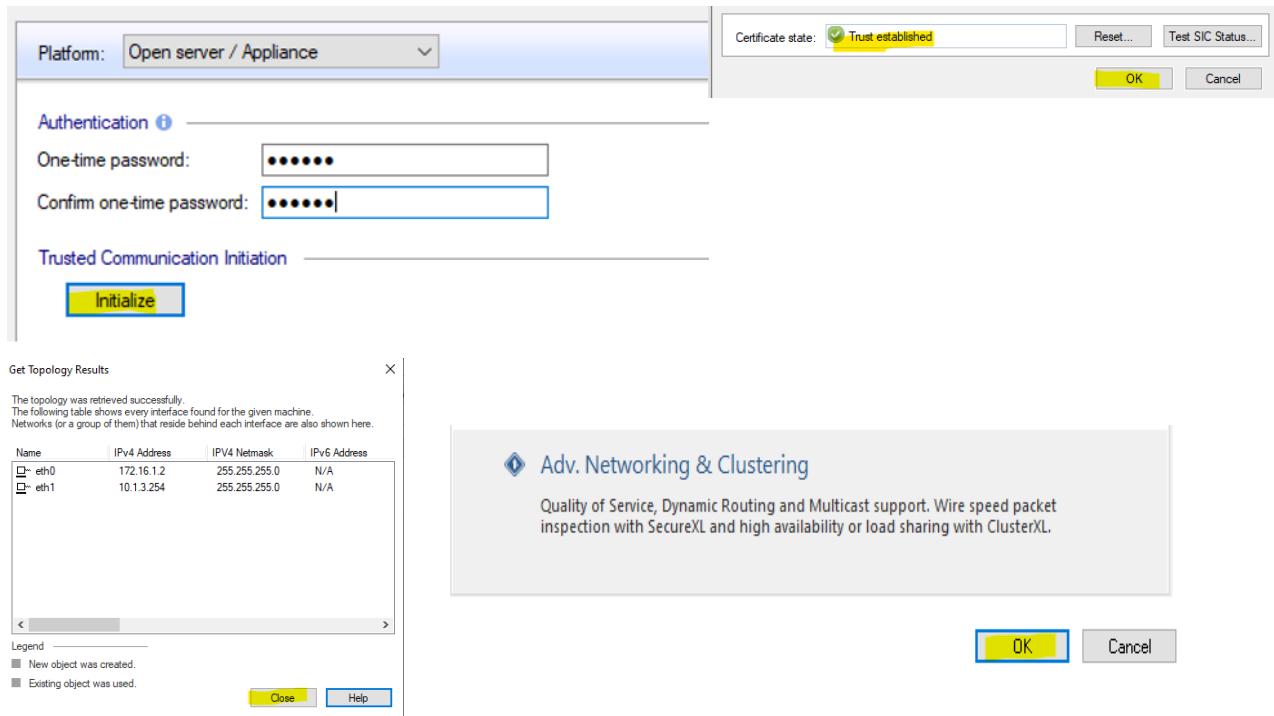
לאחר מכן נגדר את כל שאר החוקים שתיארתי ונלחץ על **Publish & Install Policy** ו**Install Policy** על
מנת להחיל את הפוליסה החדשה.

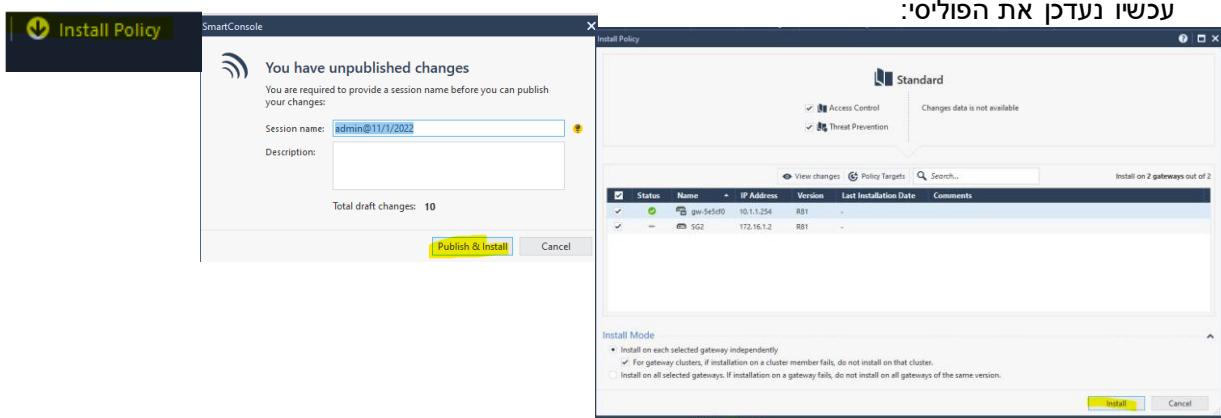


כעת נחבר את SG2 ל Security Management



כעת נזין את ה SIC שהגדרנו קודם לכן:





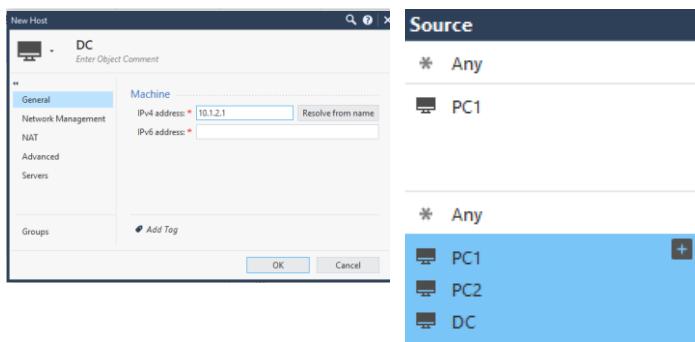
Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updates	Recommended Jumbo	Comments
Green	gw-5e5df0	10.1.1.254	R81	Open server	4%	N/A	N/A	N/A	
Green	SG2	172.16.1.2	R81	Open server	6%	N/A	N/A	N/A	

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

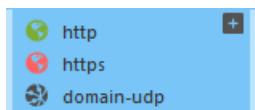
ניתן שם לחוק:

4		Internet Access
---	--	-----------------

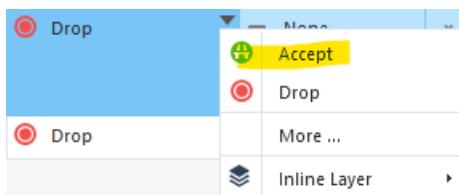
ב Source נשם את האובייקטים PC1 PC2 וניתור גם אובייקט ל DC ונוסיף אותו:



ב Destination לא נגע (נשאר על ANY בשלב זה) ובעומודת Services & Applications נקבע את ה프וטוקולים הנחוצים לגלוש באינטרנט. במקרה זה HTTPS,HTTP,DNS

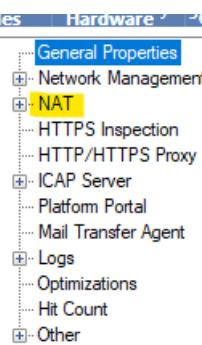


כעת נשנה את ה Action ל Accept

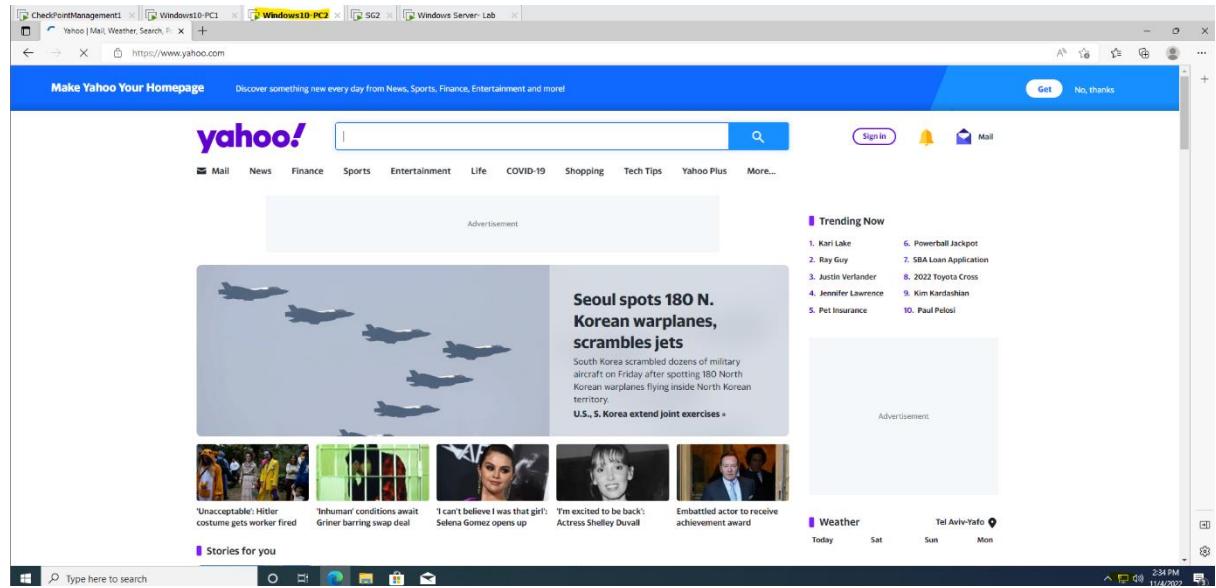
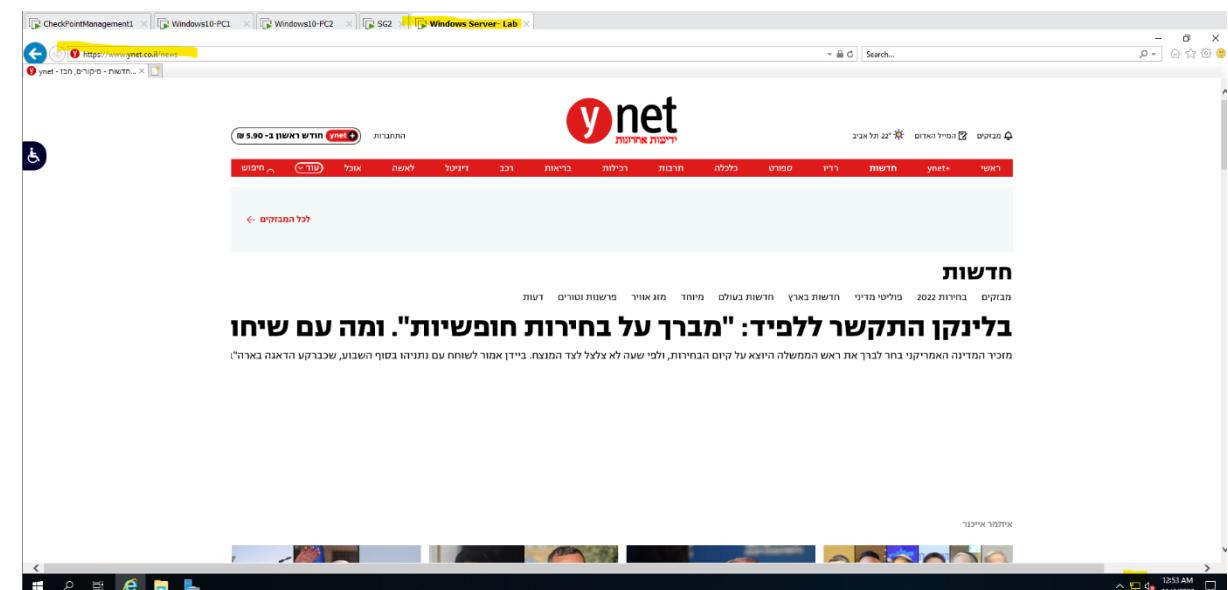
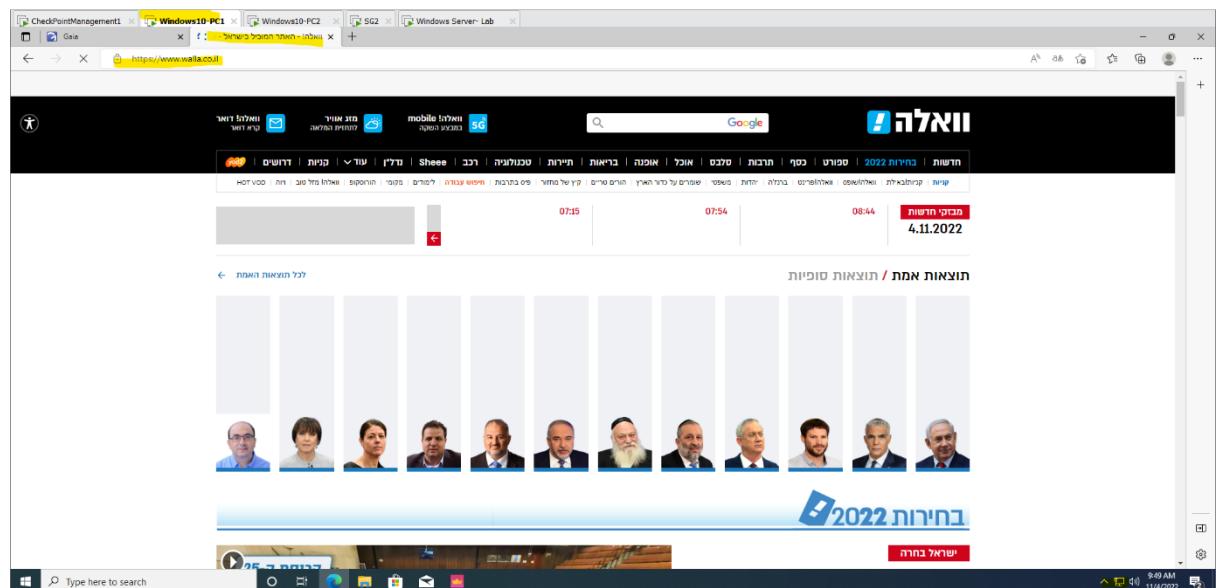


כעת נגדיר NAT לכל אחד מ ה SG:

Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Updates	Recommended Jumbo
✓	gw-5e5cf0	10.1.1.254	R81	Open server	3%	4 updates available	Check_Point_R81_JUMBO,	
✓	SG2	172.16.1.2	R81	Open server	1%	4 updates available	Check_Point_R81_JUMBO,	



כעת נתקן את הפוליסה נראה שהאינטרנט עובד בכל העמדות קצה:



By Elior Sofer

הקמת DC, שרת DNS, IIS והוספה PC2 ו PC1 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:

The screenshot displays the Windows Server 2019 Add Roles and Features Wizard across five windows. The process involves selecting the destination server, choosing roles and features, and then installing them.

- Before You Begin (Step 1):** Shows the 'Before You Begin' screen with 'Installation Type' selected. It includes links for 'Server Selection', 'Server Roles', 'Features', 'Confirmation', and 'Results'.
- Select destination server (Step 2):** Shows the 'Select destination server' screen where 'WindowsServerLab' is chosen as the destination server. It lists one computer found: 'WindowsServerLab' (IP: 10.1.2.1, OS: Microsoft Windows Server 2019 Standard Evaluation).
- Select installation type (Step 3):** Shows the 'Select installation type' screen with 'Role-based or feature-based installation' selected. It includes links for 'Before You Begin', 'Server Selection', 'Server Roles', 'Features', 'Confirmation', and 'Results'.
- Select server roles (Step 4):** Shows the 'Select server roles' screen. Under 'Roles', 'DNS Server' is selected. Under 'Description', it details the Active Directory Domain Services role. It includes links for 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles', 'Features', 'AD DS', 'DNS Server', 'Web Server Role (IIS)', 'Role Services', 'Confirmation', and 'Results'.
- Select features (Step 5):** Shows the 'Select features' screen. Under 'Features', 'NET Framework 3.5 Features' is selected. Under 'Description', it details .NET Framework 3.5. It includes links for 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles', 'Features', 'AD DS', 'DNS Server', 'Web Server Role (IIS)', 'Role Services', 'Confirmation', and 'Results'.

Add Roles and Features Wizard

Active Directory Domain Services

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Web Server Role (IIS)
Role Services
Confirmation
Results

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.

Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.
Learn more about Azure Active Directory
Configure Office 365 with Azure Active Directory Connect

DNS Server

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Web Server Role (IIS)
Role Services
Confirmation
Results

Domain Name System (DNS) provides a standard method for associating names with numeric Internet addresses. This makes it possible for users to refer to network computers by using easy-to-remember names instead of a long series of numbers. In addition, DNS provides a hierarchical namespace, ensuring that each host name will be unique across a local or wide-area network. Windows DNS services can be integrated with Dynamic Host Configuration Protocol (DHCP) services on Windows, eliminating the need to add DNS records as computers are added to the network.

Things to note:

- DNS server integration with Active Directory Domain Services automatically replicates DNS data along with other Directory Service data, making it easier to manage DNS.
- Active Directory Domain Services requires a DNS server to be installed on the network. If you are installing a domain controller, you can also install the DNS Server role using Active Directory Domain Services Installation Wizard by selecting the Active Directory Domain Services role.

Web Server Role (IIS)

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Web Server Role (IIS)
Role Services
Confirmation
Results

Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 10.0 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 10.0, ASP.NET, and Windows Communication Foundation.

The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

More information about Web Server IIS

Select role services

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Web Server Role (IIS)
Role Services
Confirmation
Results

Select the role services to install for Web Server (IIS)

Role services	Description
<input checked="" type="checkbox"/> Web Server	Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.
<input checked="" type="checkbox"/> Common HTTP Features	
<input checked="" type="checkbox"/> Default Document	
<input checked="" type="checkbox"/> Directory Browsing	
<input checked="" type="checkbox"/> HTTP Errors	
<input checked="" type="checkbox"/> Static Content	
<input type="checkbox"/> WebDAV Publishing	
<input checked="" type="checkbox"/> Health and Diagnostics	
<input checked="" type="checkbox"/> HTTP Logging	
<input type="checkbox"/> Custom Logging	
<input type="checkbox"/> Logging Tools	
<input type="checkbox"/> ODBC Logging	
<input type="checkbox"/> Request Monitor	
<input type="checkbox"/> Tracing	
<input checked="" type="checkbox"/> Performance	
<input checked="" type="checkbox"/> Static Content Compression	
<input type="checkbox"/> Dynamic Content Compression	
<input checked="" type="checkbox"/> Security	

Confirm installation selections

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Web Server Role (IIS)
Role Services
Confirmation
Results

To install the following roles, role services, or features on selected server, click Install.

Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Domain Services
DNS Server
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools

Export configuration settings
Specify an alternate source path

Installation progress

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
DNS Server
Web Server Role (IIS)
Role Services
Confirmation
Results

View installation progress

Feature installation
Configuration required. Installation succeeded on WindowsServerLab.

Active Directory Domain Services
Additional steps are required to make this machine a domain controller.
Promote this server to a domain controller

DNS Server
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD Tools
Active Directory Administrative Center

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

Server Manager

Dashboard

Post-deployment Configuration
Configuration required for Active Directory Domain Services at WindowsServerLab.
Promote this server to a domain controller

Feature installation
Configuration required. Installation succeeded on WindowsServerLab.

This local server
Add Roles and Features
Task Details
5 Connect this server to cloud services
More

Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
WindowsServerLab

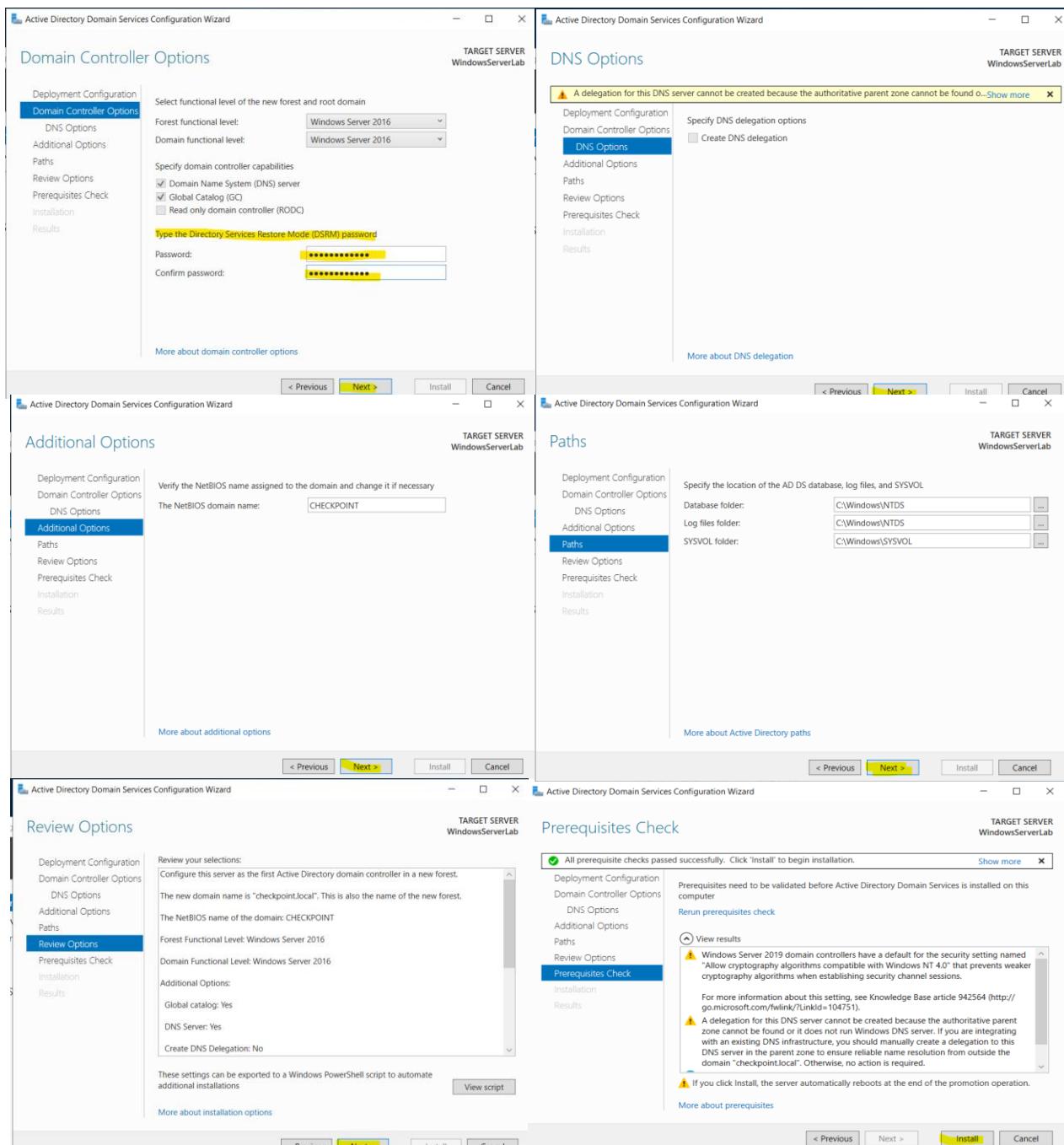
Select the deployment operation

Add a domain controller to an existing domain
 Add a new domain to an existing forest
 Add a new forest

Specify the domain information for this operation
Root domain name:

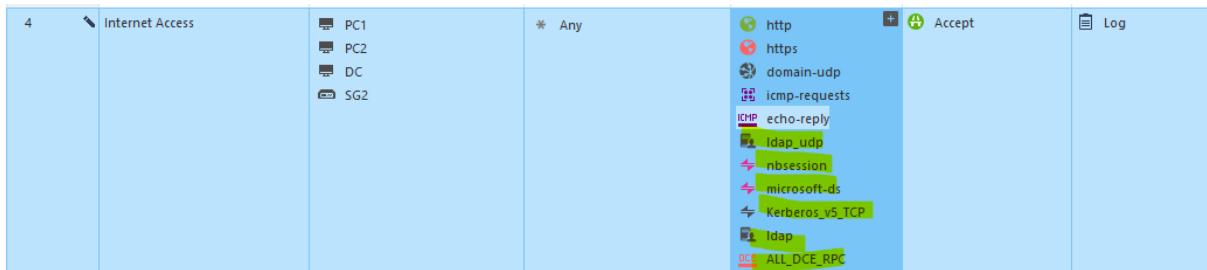
More about deployment configurations

By Elior Sofer



כעת יש להוסיף לדומיין את PC1 ו-PC2.

לפי שנוסיף, יש להגדיר פרוטוקולים נוספים בחולק INTERNET ACCESS שהגדרנו בFW על מנת שנוכל להוסיף את המחשבים לדומיין:



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

The screenshot illustrates the steps to join a computer to a domain:

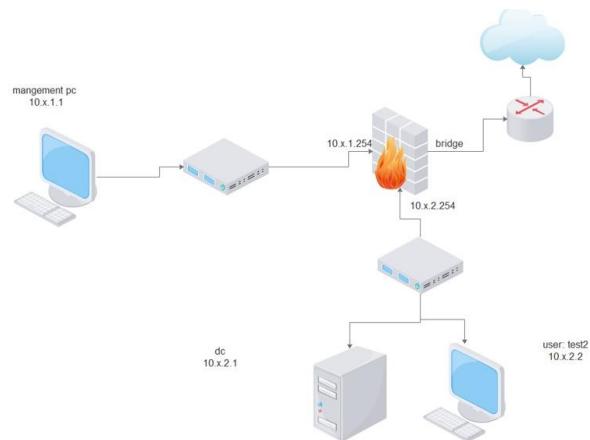
- Windows Search:** Shows the search results for "sysdm.cpl".
- Computer Name/Domain Changes Dialog:** A modal window where the computer name is set to "PC1" and it is joined to the domain "checkpoint.local".
- Windows Security Dialog:** A modal window asking for administrator credentials ("administrator" and password). The "OK" button is highlighted.
- Active Directory Users and Computers:** A screenshot of the ADUC interface showing the "checkpoint.local" domain container with two computer objects: "PC1" and "PC2".

כעת אוכיח עפ"י הלוגים כי שרת DC שהקמנו משמש כשרת DNS ושרת SI לעמדות קצה (PC1 ו PC2):

Today, 4:01:01 PM		SG2	PC2 (10.1.3.1)	DC (10.1.2.1)	domain-udp (UDP/53)	4	Internet Access	Standard	domain-udp Traffic Accepted from 10.1.3.1 to 10.1.2.1
Today, 4:01:52 PM		gw-5e5cf0	PC1 (10.1.1.1)	DC (10.1.2.1)	domain-udp (UDP/53)	4	Internet Access	Standard	domain-udp Traffic Accepted from 10.1.1.1 to 10.1.2.1

חלק ב'

חלק זה מוגש על הטופולוגיה הבאה:



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

בחלק זה אראה כיצד מתקדמיים, כיצד מתקנים אותם וPOC:

הפעלת HTTPS Inspection

על מנת להפעיל פונקציה זאת יש לעקוב אחרי הצלומי מס' הבאים:

Columns: General

Stat...	Na...	IP	Versi...	Active Blad...	Hardwa...	CPU Usa...	Recommended Updat...	Recommended
g	10.1.1.2...	R81		Open server	4%	N/A	N/A	N/A

General Properties

- Network Management
- NAT
- **HTTPS Inspection**
- HTTP/HTTPS Proxy
- ICAP Server
- Platform Portal
- Mail Transfer Agent
- Logs
- Optimizations
- Hit Count
- Other

Please follow these steps in order to enable HTTPS inspection:

Step 1 Create or Import an outbound CA certificate for HTTPS inspection

The outbound CA certificate will be used by the Gateway to inspect SSL traffic (more).

Generated certificate

Original certificate

Issued By (DN) : ellor.com

Private key password :

Retype private key password :

Valid from : 11/4/2022 to 11/4/2029

OK Cancel

Step 3

Enable HTTPS Inspection

The screenshot shows the FortiGate Management Interface. On the left, a 'Certificate' window displays 'Certificate Information' with a warning about a CA Root certificate being untrusted. It lists the 'Issued to' as elior.com, 'Issued by' as elior.com, and 'Valid from' and 'to' as 11/4/2022. Buttons for 'Install Certificate...' and 'Issuer Statement' are at the bottom. An 'OK' button is visible below the certificate window. On the right, the 'Inspection Settings' window is open under 'Standard' mode. The 'Gateways' tab is selected, showing a table with one row for 'firewall1' with IP 10.200.0.254 and 'Recommended Inspection' assigned. A yellow box highlights the 'Recommended Inspection' column.

Stat... Na... IP Versi... Active Blad... Hardwa... CPU Usa... Recommended Updat... Recommended Jum...

g 10.1.1.2... R81

Network Security (1)

- Access Control
 - Firewall
 - IPSec VPN
 - Policy Server
 - Mobile Access
 - Application Control
 - URL Filtering
 - Identity Awareness
 - Content Awareness

NAT

Threat Prevention

HTTPS Inspection

Policy

A table titled 'Predefined Rule' shows one rule: 'No Bank Sites Inspect' with 'Source * Any', 'Destination Internet', 'Services HTTPS default s...', 'Category/Custom A... * Any', 'Action Bypass', 'Track Log', 'Blade * All', 'Install On * Policy H...', 'Certificate Outbound Certi...', and 'Comment'. A yellow box highlights the 'Bypass' action.

New Rule

New Section Title

Delete

Cut

Copy

Paste

Disable

Copy Rule UID

Copy as Image

A table titled 'SmartPolicy' shows two rules: 'No Bank Sites Inspect' and another rule with 'Source * Any', 'Destination Internet', 'Services HTTPS default s...', 'Category/Custom A... * Any', 'Action Inspect', 'Track Log', 'Blade * All', 'Install On * Policy H...', 'Certificate Outbound Certi...', and 'Comment'. A yellow box highlights the 'Inspect' action.

Install Policy

You have unpublished changes

You are required to provide a session name before you can publish your changes:

Session name:

Description:

Total draft changes: 12

Publish & Install

SmartPolicy

Install Policy

Session name: firewall1

Blade: * All

Install On: * Policy H...

Certificate: Outbound Certi...

Action: Inspect

Category: Financial Services

Services: HTTPS default services

Source: * Any

Destination: Internet

Track: Log

Blade: * All

Install On: * Policy H...

Certificate: Outbound Certi...

Action: Bypass

Category: Financial Services

Services: HTTPS default services

Source: * Any

Destination: Internet

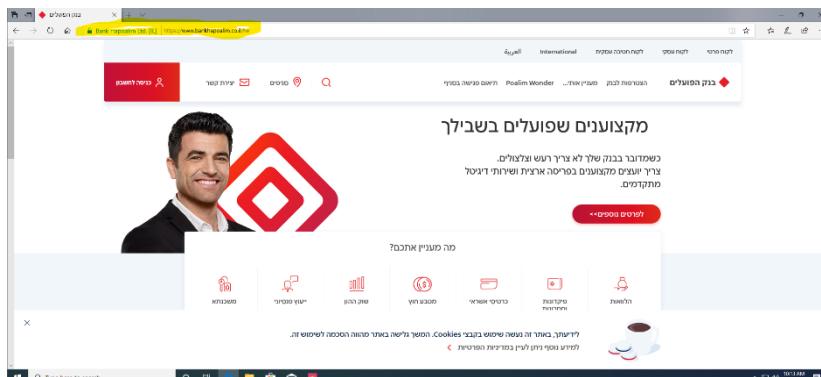
Track: Log

Blade: * All

Install On: * Policy H...

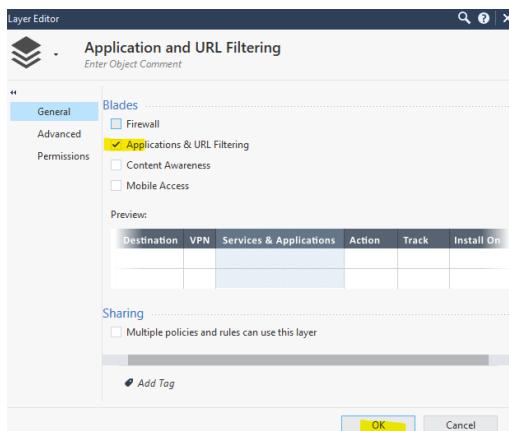
Certificate: Outbound Certi...

:POC



עכשו נctrיך על מנת לעבוד עם הפיצ'ר הבא לעשות חוק בשכבה:

No.	Name	Source	Destination	Services & Applications	Action	Track	Install On
1	Filter Rule	* Any	* Any	nbdatagram	Drop	— None	* Policy Targets
2	Management Rule	PC1	gw-82636d	* Any	Accept	— None	* Policy Targets
3	Stealth Rule	* Any	gw-82636d	* Any	Drop	— None	* Policy Targets
4	Internet Access	* Any	* Any	dns https http icmp-requests	Accept	Accept Drop Ask Inform More ...	* Policy Targets
5	DC DS	* Any	DC	ldap ldap_udp nbession microsoft-ds Kerberos_v5_TCP ALL_DCE_RPC	Accept	Inline Layer	New layer... Edit layer...
6	Cleanup rule	* Any	* Any	* Any	Drop	Log	* Policy Targets



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

cutet adgim at haPicer : user identity



The screenshot shows the 'Identity Awareness Configuration' wizard. Step 1: 'Methods For Acquiring Identity' lists 'AD Query', 'Browser-Based Authentication', and 'Terminal Servers'. Step 2: 'Integration With Active Directory / Azure Active Directory' shows options for 'Select an Active Directory' (Create new Azure Active Directory) and 'Azure AD User Authentication' (Username and Password fields). Step 3: 'Identity Awareness Configuration' shows 'Identity Awareness is Now Active!' with a message: 'Identity Awareness is now enabled on gateway gr-a203fd.' and a list of 'Selected methods for acquiring identity: Browser-Based Authentication'.

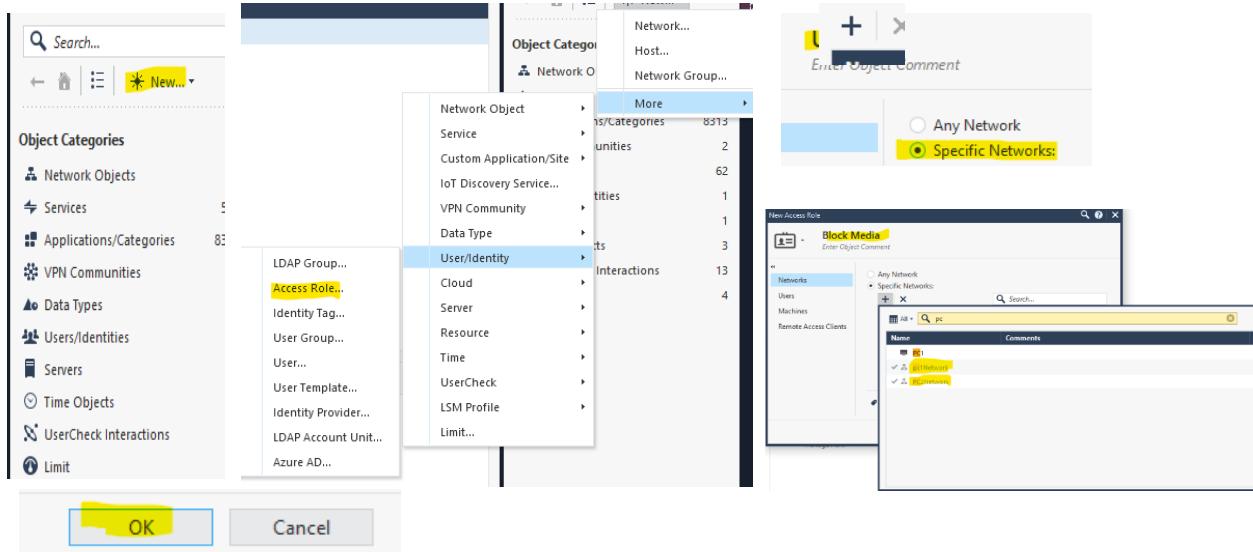
The screenshot shows the 'Identity Awareness Configuration' wizard. Step 1: 'Browser-Based Authentication Settings' shows a table with a row for 'Finance_Users' with 'Any' source and 'http' destination, action 'accept (display captive portal)'. Step 2: 'Identity Awareness Configuration' shows 'Identity Awareness is Now Active!' with a message: 'Identity Awareness is now enabled on gateway gr-a203fd.' and a list of 'Selected methods for acquiring identity: Browser-Based Authentication'.

cutet agdir obikutim:

The screenshot shows the 'New Network' dialog. It contains two network configurations: 'pc1Network' and 'PC2Network'. Both networks have 'IPv4' settings with 'Network address: 10.1.1.0', 'Net mask: 255.255.255.0', and 'Broadcast address: 10.1.1.255'. Under 'IPv6', both have 'Network address:' and 'Prefix:' fields. At the bottom, there are 'OK' and 'Cancel' buttons.

לאחר שהגדרתי את האובייקטים אגדיר את החוקים הבאים:

- חוק שחייב גישה ל- media sharing ו- media streaming לכל משתמש הרשות בארגון.
- חוק שמאפשר רק למשתמשים ברשות 10.x.2.0 גישה ל- YouTube.
- אגדים ייצור אובייקט אחד, אבל אותו העקנון תקף גם לשאר האובייקטים.



כעת נגדיר את האובייקטים הרלוונטיים לצורך החוקים:

	Stealth Rule	*	Any	gw-a2636d	*	Any	Drop	None	*	Policy Targets	
4	Internet Access	*	Any	*	Any	*	dns https http icmp-requests	Application and URL	N/A	*	Policy Targets
4.1	Block Media Streaming	*	Any	*	Any	*	Any	Drop	None	*	Policy Targets

Block Media Streaming Rule Details:

- Match By:**
 - Site and application category
 - Services
- Relevant Blades:** Application Control, URL Filtering

This category includes URLs that provide streaming audio or video, e.g. Internet radio, Internet TV stations, or Podcasting. This category is intended to cover audio and/or video that use significant amounts of bandwidth. Audio or video stream with potentially offensive material will also be categorized with the relevant category (e.g. Intimate Apparel/Swimsuit, Nudity, Tastlessness).

Examples: <http://www.napster.com>, <http://www.youtube.com>, <http://www.mp3.com>

אוצר גם אובייקט שמייצג את אתר YouTube

The screenshot shows the 'Network Object' context menu open, with 'Custom Application/Site...' selected. To the right, a 'New Application/Site' dialog is open for 'Youtube'. It includes fields for 'Primary Category' (set to 'Custom_Application_Site'), 'Description', and 'Match By' (with 'URL List' containing 'youtube.1'). Below the dialog is a table of policy rules:

	Internet Access	Policy Targets
4	pctNetwork PC2Network	* Any dns https http icmp-requests
4.1	Block Media Streaming	* Any Media Streams Drop
4.2	Allow YouTube Access	* Any Youtube Accept
4.3	Cleanup rule	* Any Accept Log

:POC

The top screenshot shows a browser window with the URL <https://www.youtube.com/>. A warning message says: "Can't connect securely to this page. This might be because the site uses outdated or unsafe TLS security settings. If this keeps happening, try contacting the website's owner. Try this: Go back to the last page".

The bottom screenshot shows the same browser window with the YouTube homepage loaded successfully, displaying the "Listen ad-free with Music Premium" offer and various video thumbnails.

By Elior Sofer

פיצ'ר אחרון שאדג'ים הוא שימוש ב IP Blade :

The screenshot shows the FortiGate Management interface. In the top navigation bar, 'Threat Prevention (0)' is highlighted. On the left, under 'Threat Prevention', 'Basic' is selected. In the center, a dialog box titled 'IPS First Time Activation' is open, showing two options: 'According to the Threat Prevention policy' (selected) and 'Detect only'. A note below states: 'Note: Optimized profile is the default enabled profile.' At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

Threat Prevention
Define which Threat Prevention software blades are activated on the gateway.

IPS Protection

No.	Name	Protected Scope	Protection/Site/File/Blade	Action	Track	Install On	Comments
1	*	Any	N/A	Optimized	Log Packet Capture Forensics	Policy Targets	

Threat Tools

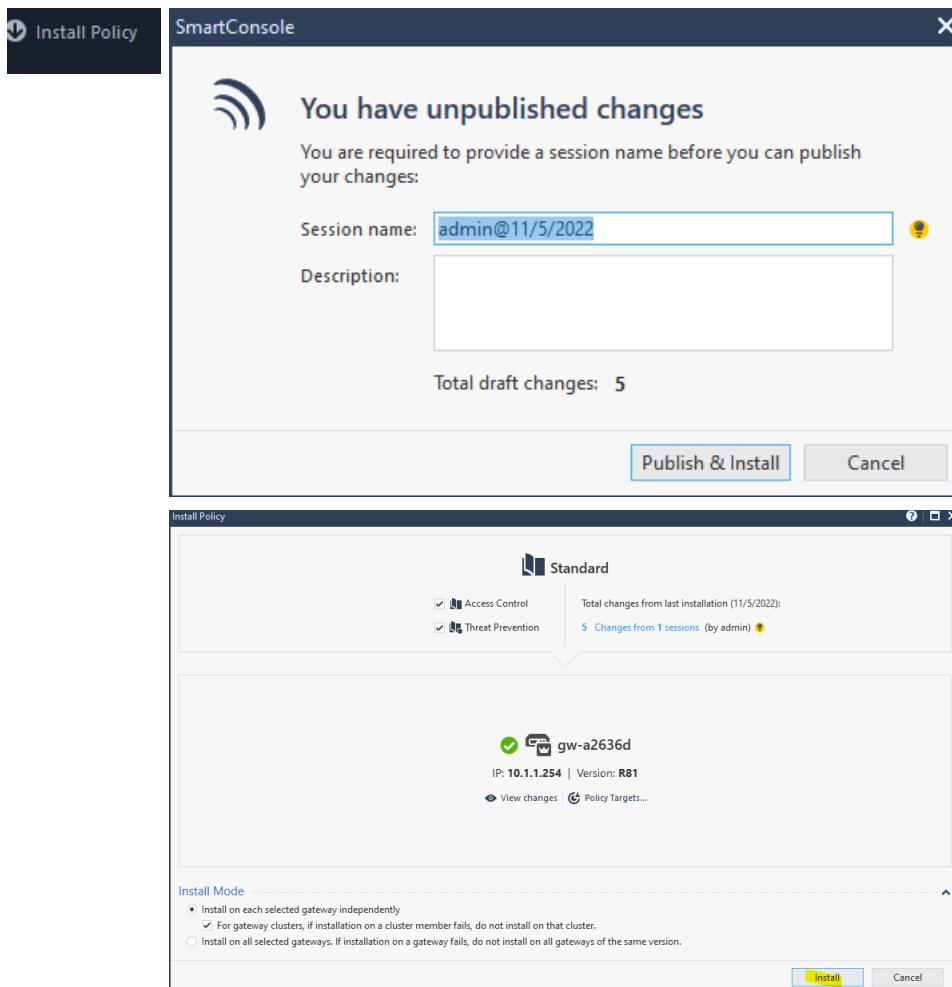
- Profiles
- IPS Protections**
- Protections
- Whitelist Files
- Indicators
- Updates
- UserCheck
- Threat Wiki
- Installation History

אבלר לשם הדגמה ב :

Foll...	Protection	Industry Refer...	Releas...	Update...	Performance Im...	Severity	Confidence Le...	Basic
	Max Ping Size	CVE-2002-0237	CVE-20-	N/A	N/A			See Details...

כעת אגדיר שכל פעם שIPS יפעיל בחוק זהה הוא יזרוק את הפקטה, ואגביל את גודל הפקטה עד 200:

The screenshot shows the configuration of a 'Max Ping Size' rule. On the left, the 'Main Action' section has 'Override with Action:' set to 'Drop'. On the right, the 'General Properties' section shows 'Ping size (bytes):' set to 200. Both sections have 'OK' and 'Cancel' buttons at the bottom.



```
C:\Windows\system32\cmd.exe
C:\Users\user>ping 10.1.1.254
Pinging 10.1.1.254 with 32 bytes of data:
Reply from 10.1.1.254: bytes=32 time=1ms TTL=64
Reply from 10.1.1.254: bytes=32 time<1ms TTL=64
Reply from 10.1.1.254: bytes=32 time<1ms TTL=64
Reply from 10.1.1.254: bytes=32 time<1ms TTL=64

Ping statistics for 10.1.1.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\user>ping 10.1.1.254 -l 201
Pinging 10.1.1.254 with 201 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.1.254:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\user>
```