

# FortiGate Final

שקד אוריאל ברמי

מרצה: יוסף ברוך אל

תאריך הגשה: 05.3.2024



## תוכן עניינים

3.....	יצירת פרופיל חדש – עם הרשות דמות לprofil Super_Admin
7.....	יצירת משתמש חדש – והוסpto לקובוצה שיצרנו
8.....	בדיקות תקינות
10.....	יצירת קבוצה חדשה לIT עם הרשות צפיה בלבד למשתכנים בחרים
12.....	יצירת שלושה משתמשים, וצירופם לקובצת IT
14.....	בדיקות תקינות
17.....	מדיניות סיסמאות
17.....	יצירת מדיניות סיסמאות אחידה לכל המשתמשים
18.....	SSLVPN Tunnel Mode
18.....	הקמת קבוצה בשם LDAP_Sales ויצירת שלושה משתמשים חדשים בתוכה
23.....	הקמת חוק שיאפשר למשתמש VPN להגיע לוינדוס בעזרת RDP
42.....	SSLVPN WEB Mode
42.....	יצירת קבוצה בשם LDAP_HR
44.....	הקמת 3 משתמשים חדשים ולשייך אותם לקובוצה
48.....	יצירת חוק אשר מאפשר למשתמשים אלו להגיע ב RDP ל win10
54.....	VIP
54.....	התקנת SSL בסביבת Envario בשרת DC
61.....	הפצת VIP לוודא שהבתות נגישה מבחן
66.....	IPSEC
66.....	יצירת IPSEC עם חבר בכיתה
71.....	Inspection
71.....	יצירת פרופיל Inspection חדש
77.....	Web-Filter
77.....	יצירת פרופיל Web-Filter
79.....	הקשחה
83.....	DNS-Profile
84.....	הפעלת חסימה לאתרים ודומיינים מסווג C&C
85.....	חסימה של דומיין ספציפי
87.....	Anti-Virus Profile
87.....	יצירת פרופיל חדש
91.....	Profile-IPS
91.....	יצירת פרופיל IPS וחסימת IP שמזהה C&C
94.....	Application-Control
94.....	יצירת פרופיל וחסימת TeamViewer

# ניהול משתמשים

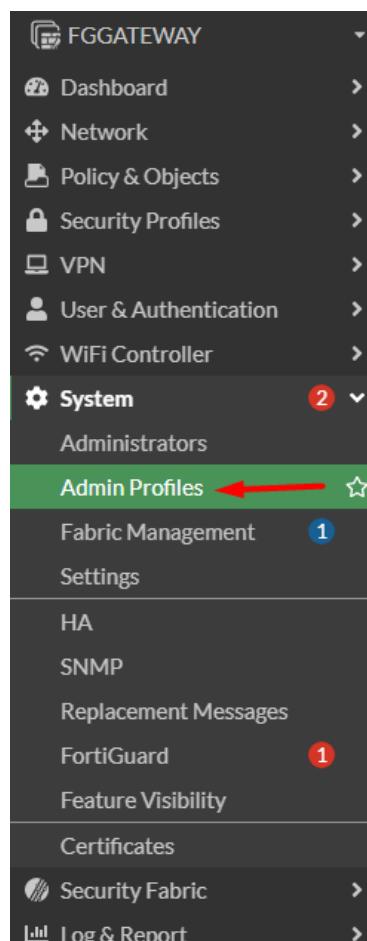
## יצירת פרופיל חדש – עם הרשות דומות לפרופיל Super\_Admin

נכיה שיש לנו צוות עובדים. לכל אחד מהם צריכים להיות הרשות גישה שונות ל-Fortigate. אנו רוצים להקל על ניהול הרשותות ולוזוד שכל מנהל מערכת יוכל לבצע רק את המשימות הדרשיות לו.

במקרה שביקשו מאייתנו, ביקשו שנוצר פרופיל חדש, עם הרשות דומות לפרופיל Super\_Admin.

בעיקרון, פרופיל Super\_Admin יכול לבצע הכל ב-FortiGate.

דבר ראשון שנרצה לראות, זה את הגישות שיש למשתמש Super\_Admin, נכנס ל-LUI של FortiGate, ונלחץ על Admin Profiles, בעט נלחץ על System.



לוחץ על Super\_Admin

The screenshot shows the FG GATEWAY interface with the title bar "FG GATEWAY". The left sidebar contains navigation links: Dashboard, Network, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi Controller, System (selected), Administrators, Admin Profiles (selected), Fabric Management (with 1 notification), Settings, HA, SNMP, Replacement Messages, FortiGuard (with 1 notification), Feature Visibility, Certificates, Security Fabric, and Log & Report. The main content area has a green header with "Create New", "Edit", "Delete", and "Search" buttons. A table titled "Profile Name" lists two entries: "prof\_admin" and "super\_admin", with a red arrow pointing to the "super\_admin" entry.

Profile Name
prof_admin
super_admin

Edit Admin Profile

Name	super_admin
Comments	0/255

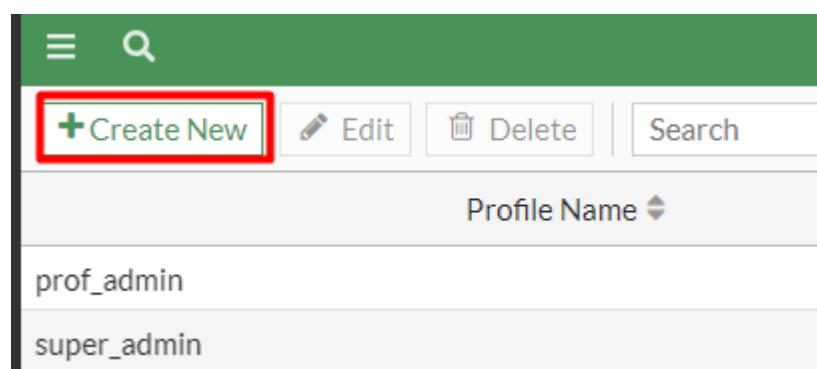
וניתן לראות, שאצל Super\_Admin הכל על Read/Write, מה שהוא יכול לבצע כל שינוי וראות כל הגדרה

Access Permissions

Access Control	Permissions			Set All ▾
Security Fabric	None	Read	Read/Write	
FortiView	None	Read	Read/Write	
User & Device	None	Read	Read/Write	
Firewall	None	Read	Read/Write	Custom
Log & Report	None	Read	Read/Write	Custom
Network	None	Read	Read/Write	Custom
System	None	Read	Read/Write	Custom
Security Profile	None	Read	Read/Write	Custom
VPN	None	Read	Read/Write	
WAN Opt & Cache	None	Read	Read/Write	
WiFi & Switch	None	Read	Read/Write	

Permit usage of CLI diagnostic commands

בעת ניצור פרופיל חדש, נקרא לו ShukiAdminProfile וניתן לו גישת Read/Write על הכל  
בשביל ליצור פרופיל חדש נלחץ על כפתור New Create New



כעת נגדיר לו על הכל Read/Write וביתן לו את השם

New Admin Profile

Name	ShukiAdminProfile
Comments	0/255

Access Permissions

Access Control	Permissions	Action	
Security Fabric	None	Read	<input checked="" type="checkbox"/> Read/Write
FortiView	None	Read	<input checked="" type="checkbox"/> Read/Write
User & Device	None	Read	<input checked="" type="checkbox"/> Read/Write
Firewall	None	Read	<input checked="" type="checkbox"/> Read/Write
Log & Report	None	Read	<input checked="" type="checkbox"/> Read/Write
Network	None	Read	<input checked="" type="checkbox"/> Read/Write
System	None	Read	<input checked="" type="checkbox"/> Read/Write
Security Profile	None	Read	<input checked="" type="checkbox"/> Read/Write
VPN	None	Read	<input checked="" type="checkbox"/> Read/Write
WAN Opt & Cache	None	Read	<input checked="" type="checkbox"/> Read/Write
WiFi & Switch	None	Read	<input checked="" type="checkbox"/> Read/Write

Permit usage of CLI diagnostic commands

Override Idle Timeout

ונלחץ על OK

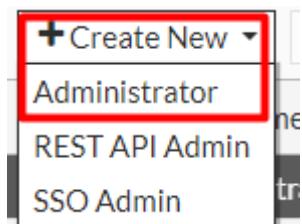
## יצירת משתמש חדש – והוספה לקבוצת שיזרנו

בעת הצורך ליצור משתמש חדש, ונוסיף אותו לקבוצת שיזרנו בסעיף הקודם, משתמש זהה בדרך כלל שיבוא עוזב חדש לארגון שלנו, ונרצה להגביל לו את הגישות.

כמו קודם, נכנס למסך System Ark הפעם נכנס למשתמש Administrators, להלן תמונה אשר מציגה היכן זה נמצא.



לחץ על 'Create New', ולאחר מכן על 'Administrators'.



נתן לו שם, נקבע לו Shaked, על שמי, אחלה שם, נתן לו את ה-profile שיזרנו קודם, וכמו כן נתן לו סיסמה שאבchar.

A screenshot of the 'Create New User' form. The 'Username' field contains 'Shaked' (highlighted with a red box). The 'Type' dropdown is set to 'Local User'. The 'Password' and 'Confirm Password' fields both contain masked text. Below them is a note about password rules: 'Password must conform to the following rules:' followed by '8 Minimum length' and 'Cannot reuse old passwords'. The 'Comments' field has 'Write a comment...' and a character count of '0/255'. The 'Administrator profile' dropdown is set to 'ShukiAdminProfile' (highlighted with a red box). The 'Force Password Change' checkbox is checked.

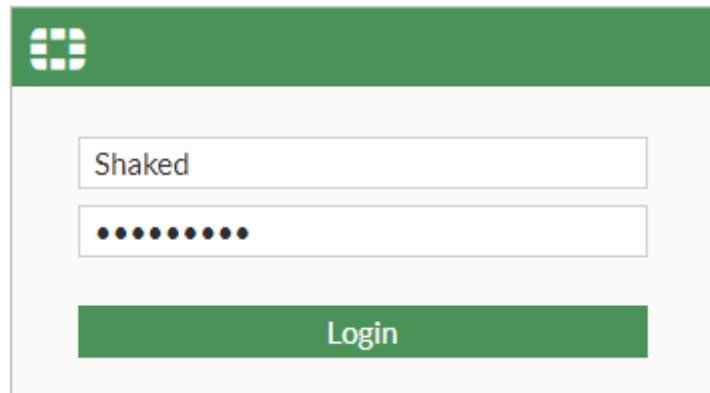
בעת לחץ על Ok

ובעת נתן לראות ברשימת המשתמשים, שהprofile שיזרנו שמו, נמצא.

System Administrator				
Name	Profile	Type	Status	Action
Shaked	ShukiAdminProfile	Local	Disabled	
admin	super_admin	Local	Disabled	
cmtadmin	super_admin	Local	Disabled	

## בדיקות תקינות

בכדי לבדוק את התקינות נתנתק FortiGate, ונכתב את הפרטים שנתנו לו קודם.



כעת ניתן לראות שאנו מחובר דרכו

A screenshot of the FortiExplorer interface. On the left, there's a sidebar with the title "Administrators" and two status indicators: "1 HTTPS" and "0 FortiExplorer". Below this, a list shows a user named "Shaked" followed by "ShukiAdminProfile". A red arrow points from the text "Shaked" to a small blue circular icon with a white number "1" inside, which is positioned next to the "HTTPS" status indicator. At the bottom of the interface is a dark blue footer bar with the text "Download HTTPS CA certificate" and an information icon.

ונitin לראות שיש לי באמת גישה כמו Super\_Admin

The screenshot shows the FortiGate management interface. The left sidebar is titled 'FGGATEWAY' and contains a tree view of configuration sections: Dashboard, Network, Policy & Objects, Security Profiles, VPN, User & Authentication, System (selected), Administrators, Admin Profiles (selected), Fabric Management, Settings, HA, SNMP, Replacement Messages, FortiGuard, Feature Visibility, Certificates, Security Fabric, and Log & Report. A red box highlights the 'System' and 'Admin Profiles' sections. The main content area is titled 'Admin Profiles' and displays a table with three rows:

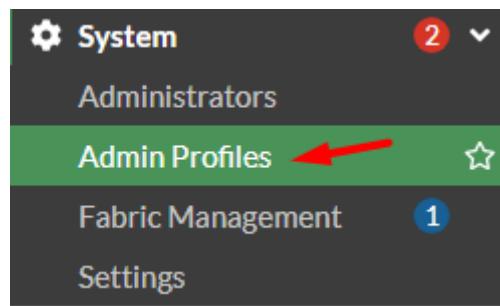
Profile Name	Comments	Ref.
ShukiAdminProfile		1
prof_admin		0
super_admin		3

At the top right of the main window, there are several status icons, including a red box around the 'Shaked' icon.

## יצירת קבוצה חדשה לזו עם הרשות צפיה בלבד לממשקים נבחרים

במקרה זה, ביקשו מאייתנו ליצור קבוצה חדשה, עם הרשות צפיה בלבד לממשקים VIPs וLogs בלבד, אחסום בלבד וInterfaces בלבד.

נחזיר למסך System ונכנס לAdmin Profiles



ונלחץ על Create New

Create New

## ניתן לו שם, נקרא לו IT\_Accounts

New Admin Profile

Name	<input type="text" value="IT_Accounts"/>
Comments	<input type="text" value=""/> 0/255
Access Permissions	
Access Control	Permissions <a href="#">Set All ▾</a>
Security Fabric	<input checked="" type="radio"/> None <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
FortiView	<input checked="" type="radio"/> None <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
User & Device	<input checked="" type="radio"/> None <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
Firewall	<input checked="" type="radio"/> None <input type="button" value="Read"/> <input type="button" value="Read/Write"/> <input type="button" value="Custom"/>
Policy	<input checked="" type="radio"/> None <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
Address	<input checked="" type="radio"/> None <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
Service	<input checked="" type="radio"/> None <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
Schedule	<input checked="" type="radio"/> None <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
Others	<input checked="" type="radio"/> None <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
Log & Report	<input checked="" type="radio"/> None <input type="button" value="Read"/> <input type="button" value="Read/Write"/> <input type="button" value="Custom"/>
Network	<input checked="" type="radio"/> None <input type="button" value="Read"/> <input type="button" value="Read/Write"/> <input type="button" value="Custom"/>
Configuration	<input checked="" type="radio"/> None <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
Packet Capture	<input checked="" type="radio"/> None <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
Router	<input checked="" type="radio"/> None <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
System	<input checked="" type="radio"/> None <input type="button" value="Read"/> <input type="button" value="Read/Write"/> <input type="button" value="Custom"/>
Security Profile	<input checked="" type="radio"/> None <input type="button" value="Read"/> <input type="button" value="Read/Write"/> <input type="button" value="Custom"/>
VPN	<input checked="" type="radio"/> None <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
WAN Opt & Cache	<input checked="" type="radio"/> None <input type="button" value="Read"/> <input type="button" value="Read/Write"/>
WiFi & Switch	<input checked="" type="radio"/> None <input type="button" value="Read"/> <input type="button" value="Read/Write"/>

Permit usage of CLI diagnostic commands

נפעיל את Policy, בכך שונוכל לראות Policies למינויים שהADMINS יצרו.

נפעיל את Address, זה יתאפשר לראות את הIP Virtual.

נפעיל את Log&Reports, זה יתאפשר לראות כל הLogs ב-FortiGate

נפעיל את Network Configuration, זה יאפשר לנו לראות את כל ה-Interfaces ב-FortiGate

## יצירת שלושה משתמשים, וצירופם לקובץ IT

לצורך יצירת שלושה משתמשים, נדרש ללבת ל-**System**, וליצור Administrators חדשים.



בכדי ליצור Administrator חדש, נלחץ על בפחו **Create New Administrator**.



ניתור שלושה משתמשים, בשמות שונים, לראשונה נקרא משה, לשני נקרא עופר, ושלישי נקרא יוסי, כמפורט  
שאთם יכולים נשיר לקובץ שיצרנו קודם.

להלן הגדרות משתמש בשם משה:

The screenshot shows the 'Create New Administrator' form. The fields filled in are:

- Username: Moshe
- Type: Local User (selected from dropdown)
- Password: A series of dots representing a password.
- Confirm Password: A series of dots representing a password.
- Comments: Write a comment... (empty)
- Administrator profile: IT\_Accounts (selected from dropdown)
- Force Password Change: Off (checkbox)
- Other options (disabled): Two-factor Authentication, Restrict login to trusted hosts, Restrict admin to guest account provisioning only.

להלן הגדרות משתמש בשם עופר:

The screenshot shows the 'Add User' dialog box. The 'Username' field is set to 'Ofer'. Under the 'Type' section, 'Local User' is selected. The 'Password' and 'Confirm Password' fields both contain '\*\*\*\*\*'. Below the password fields, a note says 'Password must conform to the following rules:' followed by two radio buttons: 'Minimum length' (selected) and 'Cannot reuse old passwords'. In the 'Comments' section, there is a text input field with 'Write a comment...' and a character count of '0/255'. The 'Administrator profile' dropdown is set to 'IT\_Accounts'. Below this, the 'Force Password Change' checkbox is checked. At the bottom, there are three radio buttons for account restrictions: 'Two-factor Authentication' (unchecked), 'Restrict login to trusted hosts' (unchecked), and 'Restrict admin to guest account provisioning only' (unchecked).

להלן הגדרות משתמש בשם יוסי:

The screenshot shows the 'Add User' dialog box. The 'Username' field is set to 'Yossi'. Under the 'Type' section, 'Local User' is selected. The 'Password' and 'Confirm Password' fields both contain '\*\*\*\*\*'. Below the password fields, a note says 'Password must conform to the following rules:' followed by two radio buttons: 'Minimum length' (selected) and 'Cannot reuse old passwords'. In the 'Comments' section, there is a text input field with 'Write a comment...' and a character count of '0/255'. The 'Administrator profile' dropdown is set to 'IT\_Accounts'. Below this, the 'Force Password Change' checkbox is checked. At the bottom, there are three radio buttons for account restrictions: 'Two-factor Authentication' (unchecked), 'Restrict login to trusted hosts' (unchecked), and 'Restrict admin to guest account provisioning only' (unchecked).

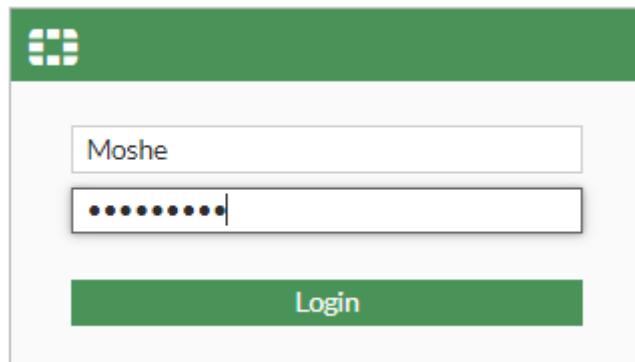
ולהן כל המשתמשים שלנו

System Administrator 4			
Moshe		IT_Accounts	Local
Ofer		IT_Accounts	Local
Shaked		ShukiAdminProfile	Local
Yossi		IT_Accounts	Local

## בדיקות תקינות

כעת נתחבר מכל המשתמשים שיצרנו ללו, ונראה באמת, שהגישות שננתנו להם, אלה הגישות שיופיעו להם, ובמובן, שיתחברו בראו.

להלן הכניסה למשתמש משה:



כעת ניתן לראות שאנו מתחברים דרך משה, שנאנחנו רק יכולים לצפות במידע ולא לעורר אותו, אלה הגישות שננתנו.

The screenshot shows the FortiGate Management Interface. On the left is a navigation sidebar with options like Dashboard, Network, Policy & Objects, Firewall Policy, Addresses, Internet Service Database, Virtual IPs, Log & Report, and FMC. The main pane displays network configuration details for a device named 'FortiGate VM64-AZURE'. It lists various interface types: 802.3ad Aggregate, Physical Interface (port1, port2), and Tunnel Interface (natroot). Each interface entry includes its type, members, IP/Netmask, administrative access (e.g., SSH, FMC Access, FNG Access), DHCP clients, DHCP ranges, and reference count. At the bottom of the interface list, there is a note about security rating issues and an update timestamp.

להלן הכניסה למשתמש עופר:

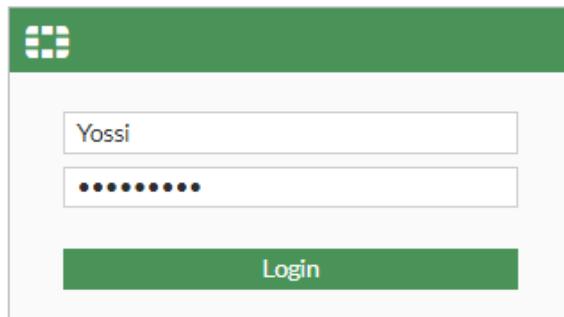
The image shows a login interface with a green header containing a grid icon. The main area has two input fields: the top one is labeled 'Ofer' and the bottom one contains several dots ('••••••••'). Below the fields is a large green 'Login' button.

בעת ניתן לראות שאנו מחוברים דרך עופר, שאנו רק יכולים לצפות במידע ולא לעורו אותו, אלה הגישות שנתקנו.

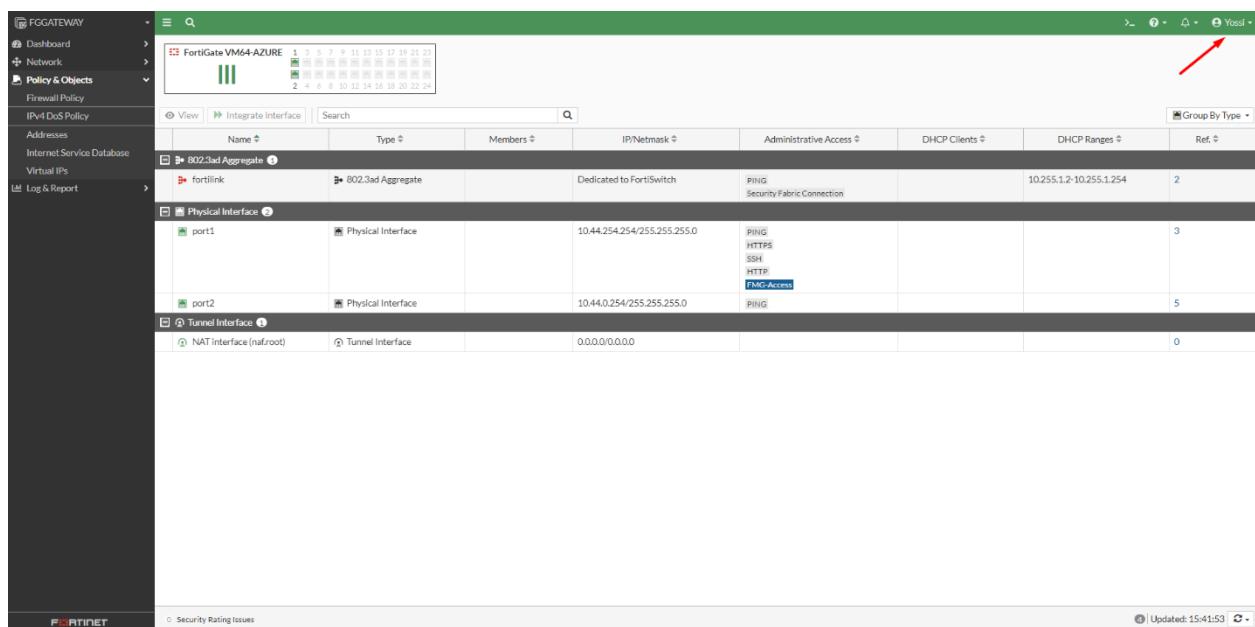
The screenshot shows the FortiGate Management Interface. The left sidebar lists navigation options: Dashboard, Network, Policy & Objects, Firewall Policy, IPv4 DoS Policy, Addresses, Internet Service Database, Virtual IPs, and Log & Report. The main content area displays network interface configurations for the FortiGate VM64-AZURE. A red arrow points to the search bar at the top right of the interface table. The table columns include Name, Type, Members, IP/Netmask, Administrative Access, DHCP Clients, DHCP Ranges, and Ref. The table shows the following entries:

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-10.255.1.254	2
port1	Physical Interface		10.44.254.254/255.255.255.0	PING HTTPS SSH HTTP FortiAccess			3
port2	Physical Interface		10.44.0.254/255.255.255.0	PING			5
NAT interface (naf.root)	Tunnel Interface		0.0.0.0/0.0.0				0

להלן הרכישה למשתמש יוסי:



כעת ניתן לראות שאנו מחוברים דרך יוסי, שאנו רוק נוכלם לצפות במידע ולא לעורר אותו, ואלה הגישות שנתקנו.



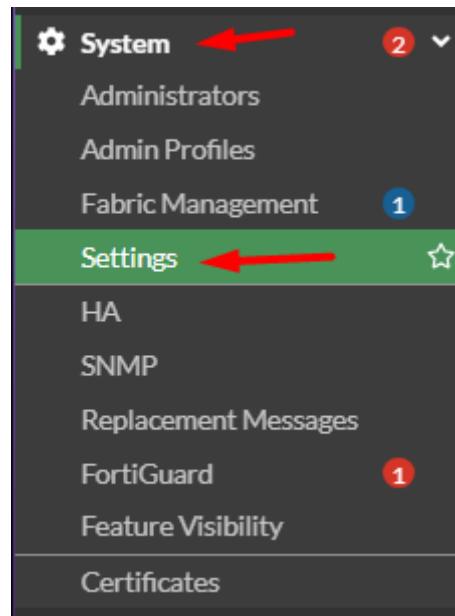
The screenshot shows the FortiGate Management interface. On the left is a navigation sidebar with options like Dashboard, Network, Policy & Objects, Firewall Policy, Addresses, Internet Service Database, Virtual IPs, and Log & Report. The main area displays network interface configurations for a FortiGate VM64-AZURE. The interface table includes columns for Name, Type, Members, IP/Netmask, Administrative Access, DHCP Clients, DHCP Ranges, and Ref. The table lists an 802.3ad Aggregate named 'fortilink' with two members: 'port1' and 'port2'. Both ports are Physical Interfaces with IP ranges 10.44.254.254/255.255.255.0 and 10.44.0.254/255.255.255.0 respectively. Under 'Administrative Access', 'port1' has PING, HTTPS, SSH, HTTP, and FMC-Access listed, while 'port2' only has PING. The 'Tunnel Interface' section shows a NAT Interface (natroot) with an IP range of 0.0.0.0/0.0.0. At the bottom, there are status indicators for Security Rating Issues and a timestamp of Updated: 15:41:53.

# מדיניות סיסמאות

יצירת מדיניות סיסמאות אחידה לכל המשתמשים

מדיניות סיסמאות אחידה לכל המשתמשים נועדה לשפר את האבטחה של מערכות מידע. היא מבטיחה שבכל הסיסמאות יהיו חזקות וקשות לנחש, ומקשה על אנשים שלא אמורים להכנס, להכנס להגדרות הארגון.

לצורך זה נכנס לSystem, Settings, Password Policy, שם יהיה לנו



נעשו 8 תווים לפחות, עם 2 סמלים מיוחדים, 2 אותיות גדולות, אחת קטנה, ומספר אחד לפחות.

A screenshot of the FortiGate Password Policy configuration screen. It shows the following settings:

- Password scope: Admin (selected)
- Minimum length: 8 (highlighted with a red box)
- Minimum number of new characters: 0
- Character requirements:
  - Upper case: 2
  - Lower case: 1
  - Numbers (0-9): 1
  - Special: 2
- Allow password reuse: Off
- Password expiration: Off

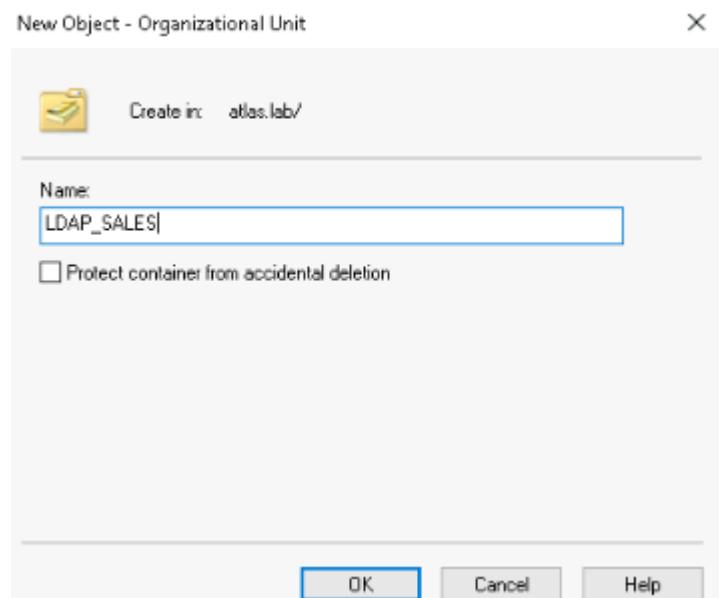
Below the form is a green 'Apply' button and the text 'לאחר ששמננו את ההגדרות הללו, נלחץ על בפטור Apply'.

# SSLVPN Tunnel Mode

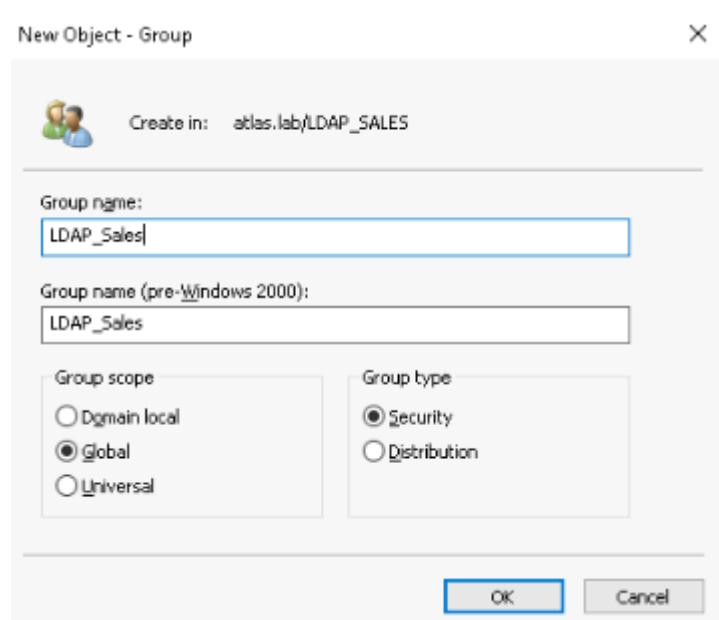
SSLVPN Tunnel בעצם נותן לך גישה מאובטחת לרשת פרטית דרך האינטרנט. הוא פתרון עבור אנשים שצוצים לעבוד מהבית או מכל מקום אחר מחוץ למקום העבודה.

## הקמת קבוצה בשם LDAP\_Sales ויצירת שלושה משתמשים חדשים בתוכה

לצורך הקמת הקבוצה, נצטרך להכנס אל Active Directory Users And Computers  
וניצור יחידה ארגונית חדשה בשם שריצינו



וניצור קבוצה בתוכו בשם שריצינו



כעת ביצור שלושה משתמשים

ראשון נקרא שוקי

New Object - User

Create in: atlas.lab/LDAP\_SALES

Password:  Confirm password:

User must change password at next logon  
 User cannot change password  
 Password never expires  
 Account is disabled

< Back **Next >** Cancel

New Object - User

Create in: atlas.lab/LDAP\_SALES

First name: Shuki Initials:   
Last name:   
Full name: Shuki

User logon name:  
Shuki  @atlas.lab

User logon name (pre-Windows 2000):  
ATLAS\  Shuki

< Back **Next >** Cancel

לשבי נקרא מוקי

New Object - User X

Create in: atlas.lab/LDAP\_SALES

First name: Muki Initials:

Last name:

Full name: Muki

User logon name:  
Muki  @atlas.lab

User logon name (pre-Windows 2000):  
ATLAS\  Muki

New Object - User X

Create in: atlas.lab/LDAP\_SALES

Password:

Confirm password:

User must change password at next logon  
 User cannot change password  
 Password never expires  
 Account is disabled

לשלישי נקרא בוקי

New Object - User

Create in: atlas.lab/LDAP\_SALES

First name:	Buki	Initials:	
Last name:			
Full name:	Buki		
User logon name:	Buki	@atlas.lab	▼
User logon name (pre-Windows 2000):	ATLAS\	Buki	

< Back    Next >    Cancel

New Object - User

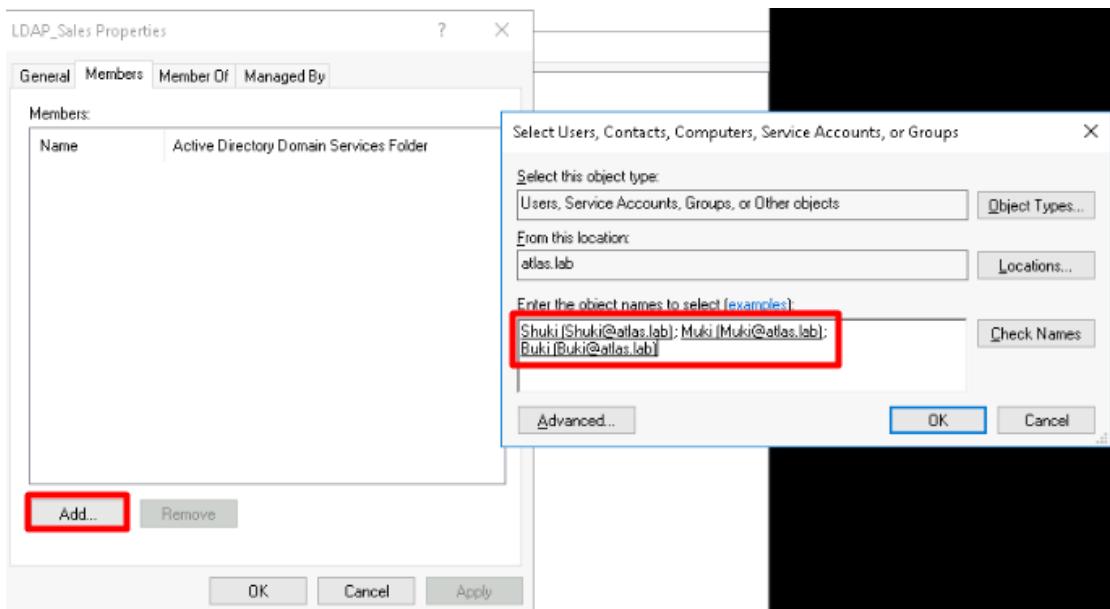
Create in: atlas.lab/LDAP\_SALES

Password:	*****
Confirm password:	*****

User must change password at next logon  
 User cannot change password  
 Password never expires  
 Account is disabled

< Back    Next >    Cancel

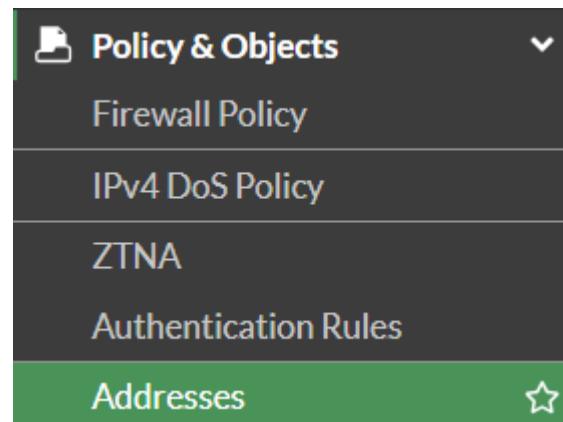
כעת נשים את כל המשתמשים בתוך הקבוצה



## הקמת חוק שיאפשר למשתמש מVPN להגיע לווינדוס בעזרת RDP

דבר ראשון שנעשה, זה יצירת טווח IP חדש, לטובת שימוש Tunnel

Addresses נכנס ל对着 Objects & Policy



לחץ על New Create, וגעשה



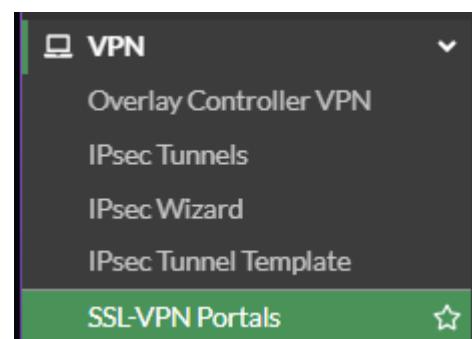
חשוב מאד, שלפנינו זה, לבדוק מה הכתובות הפרטיות שאנו עובדים איתם, להלן הכתובות בסירין Envario



כעת ניתן את הטווח החדש על פי הכתובות הפרטיות שלנו

Name	PC_Address_Tunnel
Color	<input type="button" value="Change"/>
Type	Subnet
IP/Netmask	10.44.1.0/24
Interface	port2
Static route configuration	<input checked="" type="checkbox"/>
Comments	Write a comment... 0/255

כעת בשייל להפעיל את הטווח, נצורך לשים אותו בתא Tunnel Access  
ונבנש לVPN, ועוד למשתמש portals



לחץ פעמיים על זה

tunnel-access

## נלחץ על Routing Address Override, ונבחר בטווח שלינו

Name: tunnel-access

Limit Users to One SSL-VPN Connection at a Time:

Tunnel Mode:

Split tunneling:

- Disabled: All client traffic will be directed over the SSL-VPN tunnel.
- Enabled Based on Policy Destination: Only client traffic in which the destination matches the destination of the configured firewall policies will be directed over the SSL-VPN tunnel.
- Enabled for Trusted Destinations: Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.

Routing Address Override:  +

Source IP Pools:  +

לאחר שבחרנו, נלחץ OK

Name: tunnel-access

Limit Users to One SSL-VPN Connection at a Time:

Tunnel Mode:

Split tunneling:

- Disabled: All client traffic will be directed over the SSL-VPN tunnel.
- Enabled Based on Policy Destination: Only client traffic in which the destination matches the destination of the configured firewall policies will be directed over the SSL-VPN tunnel.
- Enabled for Trusted Destinations: Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.

Routing Address Override:  +

Source IP Pools:  +

Tunnel Mode Client Options:

- Allow client to save password:
- Allow client to connect automatically:
- Allow client to keep connections alive:
- DNS Split Tunneling:

Host Check

Restrict to Specific OS Versions

Web Mode

FortiClient Download

Download Method:  Direct  SSL-VPN Proxy

Customize Download Location:

OK Cancel

בכדי שנוכל לסנכרן בין AD לבין הפורטי, נעשה Portal חדש

New SSL-VPN Portal

Name: AD-Portal

Limit Users to One SSL-VPN Connection at a Time:

Tunnel Mode:

Split tunneling:  Disabled  
All client traffic will be directed over the SSL-VPN tunnel.

Enabled Based on Policy Destination  
Only client traffic in which the destination matches the destination of the configured firewall policies will be directed over the SSL-VPN tunnel.

Enabled for Trusted Destinations  
Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.

Routing Address Override:

Source IP Pools:

Tunnel Mode Client Options:

Allow client to save password:

Allow client to connect automatically:

Allow client to keep connections alive:

DNS Split Tunneling:

Host Check:

Restrict to Specific OS Versions:

Web Mode:

Portal Message: SSL-VPN Portal

Theme: Neutrino

Show Session Information:

Show Connection Launcher:

Show Login History:

User Bookmarks:

Rewrite Content IP/UI:

RDP/VNC clipboard:

Predefined Bookmarks:

צרנו Routing Address Override

להלן הגדירות ששמנו

EDIT ADDRESS

Name: AD\_Atlas

Type: Subnet

IP/Netmask: 10.44.11.0 255.255.255.0

Interface: any

Static route configuration:

Comments: Write a comment... 0/255

নির্মাণ পদ্ধতি নথি সূচী

FortiLdap Properties

?

X

Member Of	Dial-in	Environment	Sessions		
Remote control	Remote Desktop Services Profile	COM+			
General	Address	Account	Profile	Telephones	Organization

FortiLdap

First name: FortiLdap Initials:

Last name:

Display name: FortiLdap

Description:

Office:

Telephone number:

E-mail:

Web page:

OK Cancel Apply Help

נתן לפורטי את הפרטים LDAP

The screenshot shows the 'User & Authentication' section of the FortiGate interface. A red arrow points to the 'LDAP Servers' button in the navigation bar.

Name	LDAP_AtlasLab
Server IP/Name	10.44.11.200
Server Port	389
Common Name Identifier	sAMAccountName
Distinguished Name	dc=atlas,dc=lab
Exchange server	<input type="checkbox"/>
Bind Type	Simple    Anonymous <b>Regular</b>
Username	FortiLdap
Password	••••••••••
Secure Connection	<input type="checkbox"/>
Connection status	Successful
<b>Test Connectivity</b>	
<b>Test User Credentials</b>	

כעת ניצור User Definition

The screenshot shows the 'User & Authentication' section with 'User Definition' selected. A navigation bar at the top indicates the steps: 1 User Type, 2 LDAP Server, 3 Remote Users. Below this, a list of user types is shown, with 'Remote LDAP User' selected and highlighted in green.

Local User
Remote RADIUS User
Remote TACACS+ User
<b>Remote LDAP User</b>
FSSO
FortiNAC User

נבחר בסרבר שלנו

The screenshot shows the 'User Type' step selected. It displays 'LDAP Server' and a dropdown menu showing 'LDAP\_AtlasLab' as the selected option.

כעת נבחר בהכל ונעביר לשרת

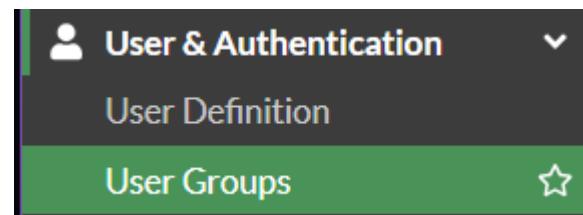
The screenshot shows a user interface for managing LDAP users. At the top, there are navigation links: 'User Type' (checked), 'LDAP Server' (checked), and 'Remote Users' (selected). Below these are buttons for 'Show subtree' (unchecked) and a dropdown menu for 'dc=atlas,dc=lab'. A 'Custom LDAP filter' input field contains '(objectClass=\*)' with an 'Apply' button. There is also a 'Hide unselectable entries' checkbox.

The main area is a table listing users:

ID	Name
Shuki	Shuki
Muki	Muki
krbtgt	krbtgt
hr3	hr3
hr2	hr2
hr1	hr1
Guest	Guest
FortiLdap	FortiLdap
DefaultAccount	DefaultAccount
Buki	Buki
atlasadmin	atlasadmin

At the top right of the table, there are buttons for 'Add All Results', 'Search' (with a magnifying glass icon), and tabs for 'Users' (selected), 'Custom', and 'Selected (11)'. A red arrow points from the 'Selected (11)' tab to the 'Submit' button at the bottom right of the page. The bottom right also has 'Back' and 'Cancel' buttons.

כעת נעשו קבוצה חדשה שתתחבר לרשות



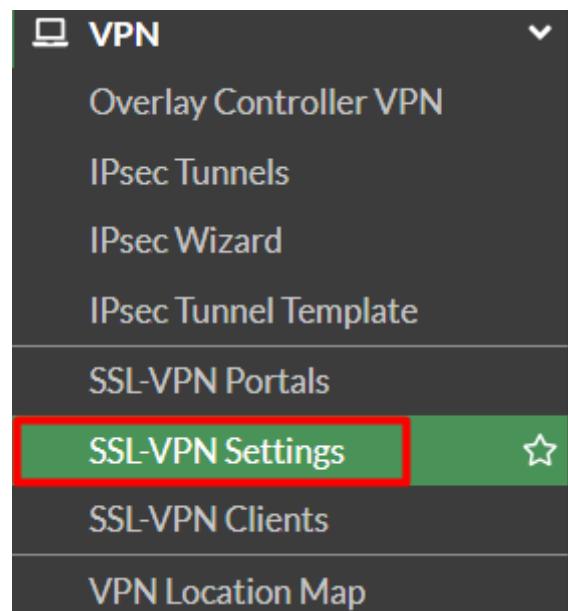
ולהן המשתמשים בטור קבוצה חדשה

Name	LDAP_SALES
Type	Firewall
	Fortinet Single Sign-On (FSSO)
	RADIUS Single Sign-On (RSSO)
	Guest
Members	Buki Muki Shuki

**Remote Groups**

		Add	Edit	Delete
Remote Server	Group Name			
LDAP_AtlasLab		1		

כעת מה שנעשה, זה הגדרות SSLVPN  
בשביל להכנס להגדרות אלו, נכנס אל VPN, ואז אל Settings SSL-VPN



אנו נרצה שייזן מפорт 10443, מפורט 10443, ושישתמש בתעודה שmagua לנו מראש ב-Port1 Interface

**Connection Settings**

- Enable SSL-VPN:
- Listen on Interface(s): port1
- Listen on Port: 10443
- Web mode access will be listening at <https://10.44.254.254:10443>
- Server Certificate: Fortinet\_Factory
- You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). Let's Encrypt can be used to easily generate a trusted certificate if you do not have one.
- Redirect HTTP to SSL-VPN:
- Restrict Access: Allow access from any host
- Idle Logout:
- Inactive For: 300 Seconds
- Require Client Certificate:

כעת נגדיר את הגדרות הקלינט, אם נגלה מטה באותו עמוד שבו אנו נמצא נראת חלונית כזו

Authentication/Portal Mapping ?

<span style="color: green;">+</span> Create New <span style="color: #0070C0;">Edit</span> <span style="color: #0070C0;">Delete</span> <span style="color: #0070C0;">Send SSL-VPN Configuration</span>	
Users/Groups <span style="color: #0070C0;">▼</span>	Portal <span style="color: #0070C0;">▼</span>
All Other Users/Groups	<span style="color: orange;">⚠</span> Not Set
1	

מה שנעשה, זה נלחץ על הכפתור New

ונלחץ על Users/Groups

Users/Groups + ←

Portal ▼

OK Cancel

ונבחר בקובץ שיצרנו קודם, ובעת אנחנו צריכים לבחור Portal, אנו נבחר ב Tunnel

Portal

Search

full-access

tunnel-access

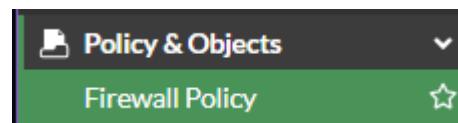
web-access

ככה זה אמרו להראות בסוף

Users/Groups		Portal
LDAP_SALES		tunnel-access
All Other Users/Groups		tunnel-access

## כעת נגידיר Policy חדש ב firewall

## כלך אל Firewall Policy וນבחר בעז Policy&Objects



## ונלחץ על Create New



ונתן לו את ההגדרות הללו, בשבייל לחתת גישה לKDP.

Name	<input type="text" value="SSLVPN_TUNNEL"/>
Incoming Interface	<input type="text" value="SSL-VPN tunnel interface (ssl.root)"/>
Outgoing Interface	<input type="text" value="port2"/>
Source	<input type="text" value="SSLVPN_TUNNEL_ADDR1"/> <span style="color: red;">X</span> <input type="text" value="LDAP_Sales"/> <span style="color: red;">X</span> <span style="color: green;">+</span> <span style="color: green;">+</span>
IP/MAC Based Access Control	<input type="text" value="PC_Address_Tunnel"/> <span style="color: red;">X</span> <span style="color: green;">+</span>
Destination	<input type="text" value="always"/> <span style="color: red;">X</span>
Schedule	<input type="text" value="ALL"/> <span style="color: red;">X</span> <span style="color: green;">+</span>
Service	
Action	<span style="color: green; font-size: 2em;">✓</span> <span style="color: green;">ACCEPT</span> <span style="color: red;">✗</span> <span style="color: red;">DENY</span>
Inspection Mode	<span style="background-color: green; color: white; padding: 2px 10px; border-radius: 5px;">Flow-based</span> <span style="border: 1px solid #ccc; padding: 2px 10px; margin-left: 10px;">Proxy-based</span>

כעת נצורך להורד FortiClient, בכך לבצע את ההתחברות

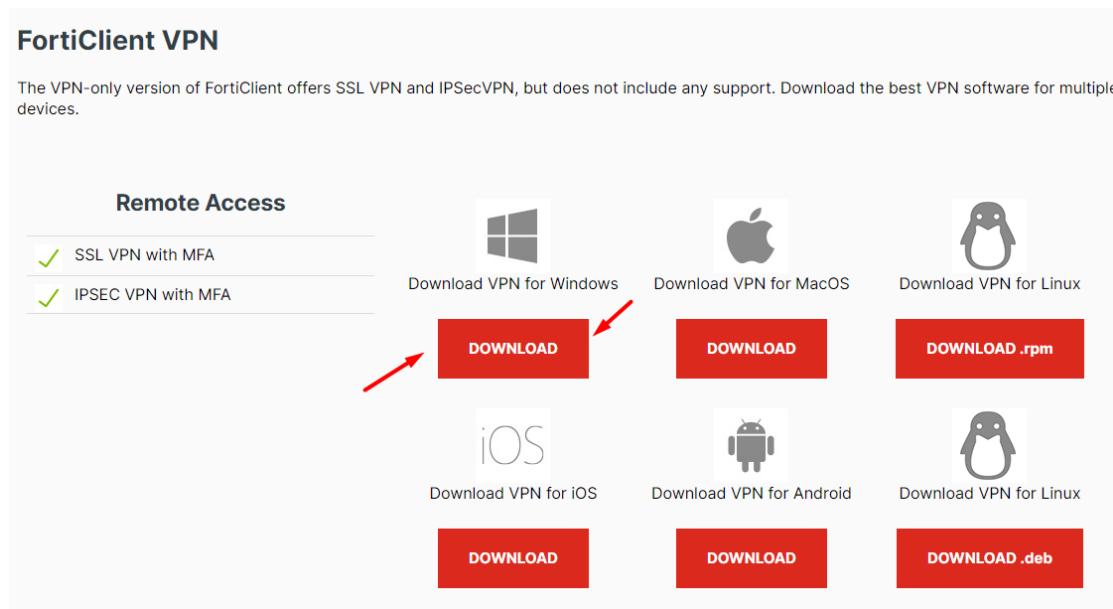
נכנס לאתר שלהם, הקישור נמצא פה

<https://www.fortinet.com/support/product-downloads>

ונליץ על הורדה על FortiClient VPN

## FortiClient VPN

The VPN-only version of FortiClient offers SSL VPN and IPSecVPN, but does not include any support. Download the best VPN software for multiple devices.

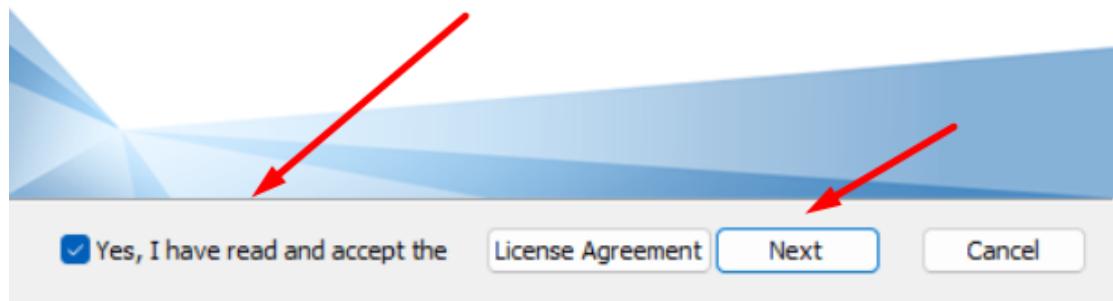


נקרא את התנאים, ונעשה Next

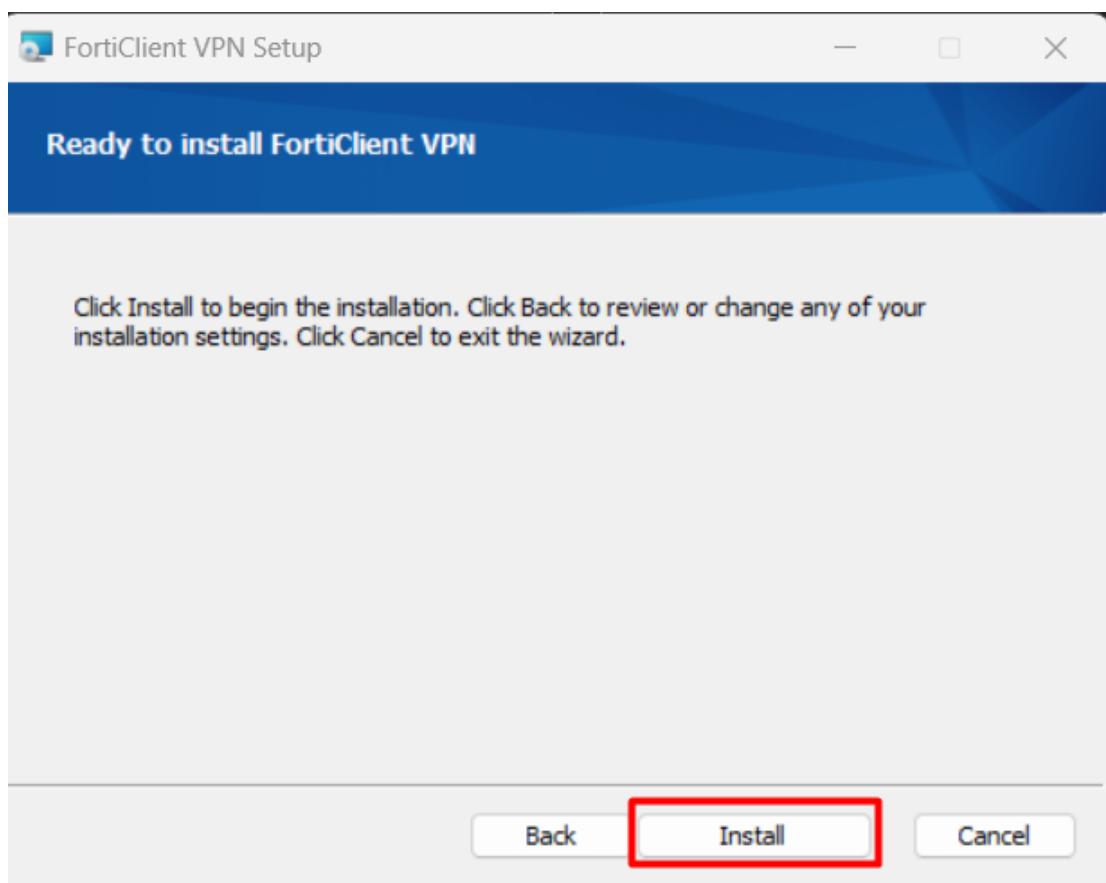


## Welcome to the FortiClient VPN Setup Wizard

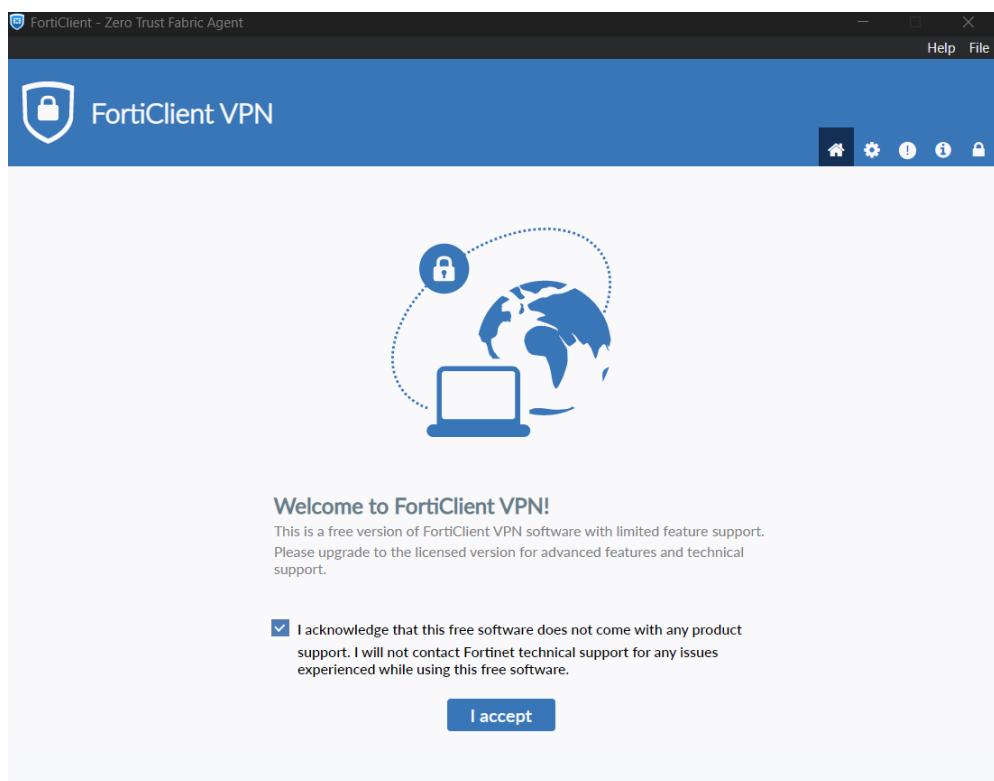
The Setup Wizard will install FortiClient VPN on your computer. Click Next to continue or Cancel to exit the Setup Wizard.



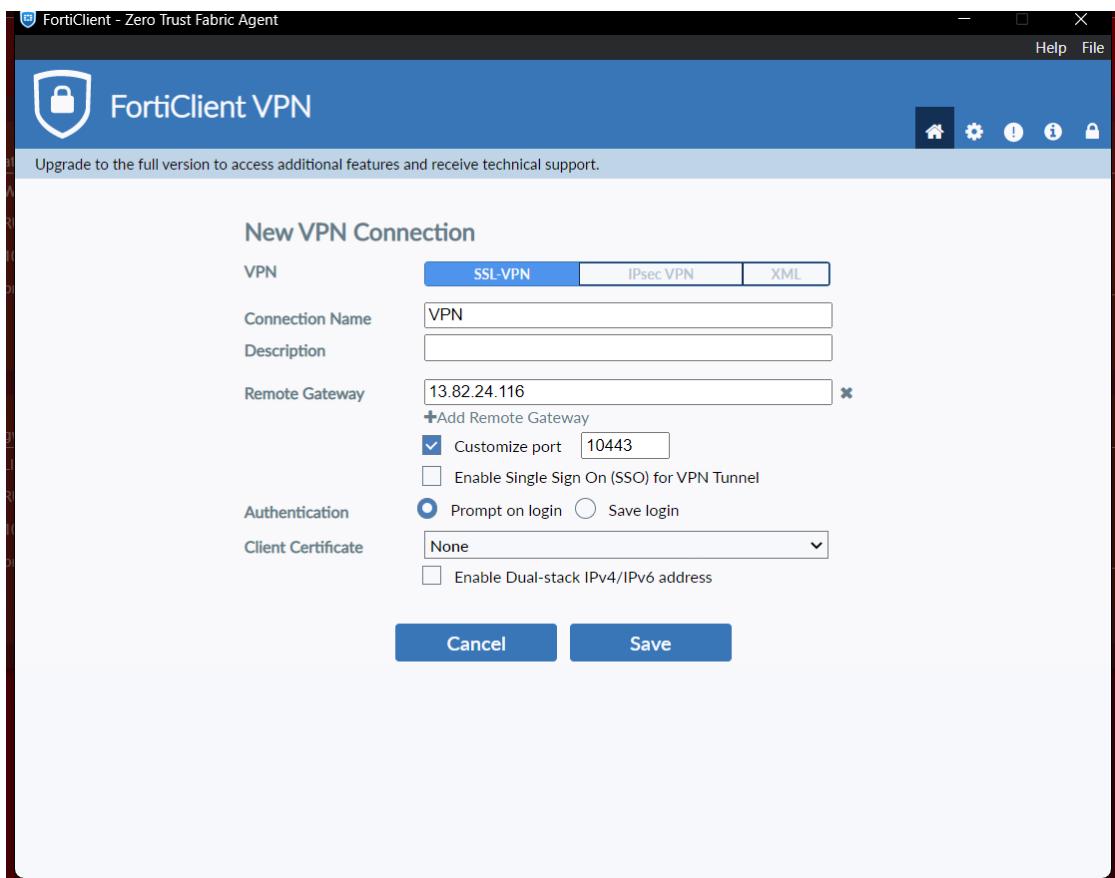
Install נלחץ



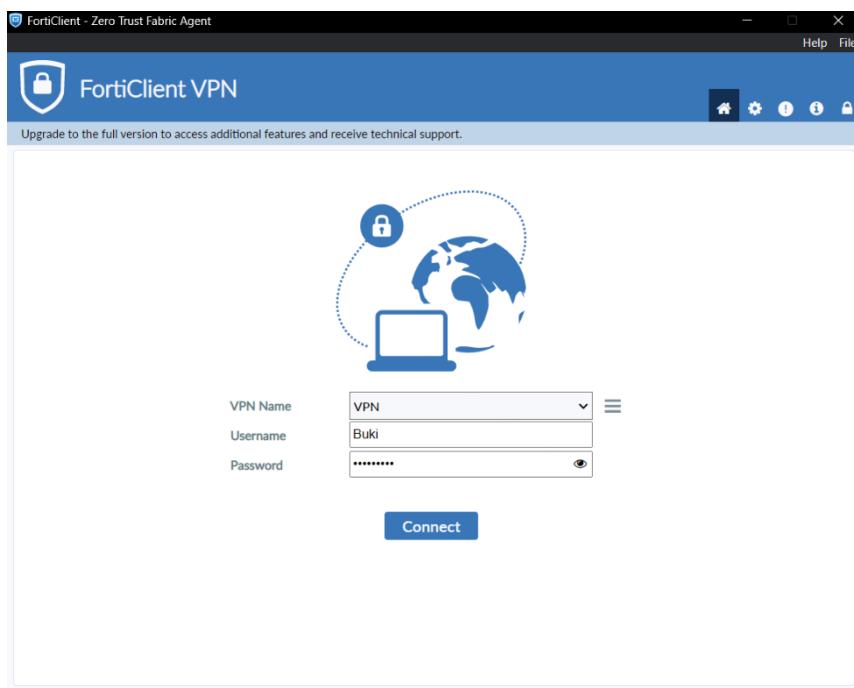
לכונס ל-FortiClient



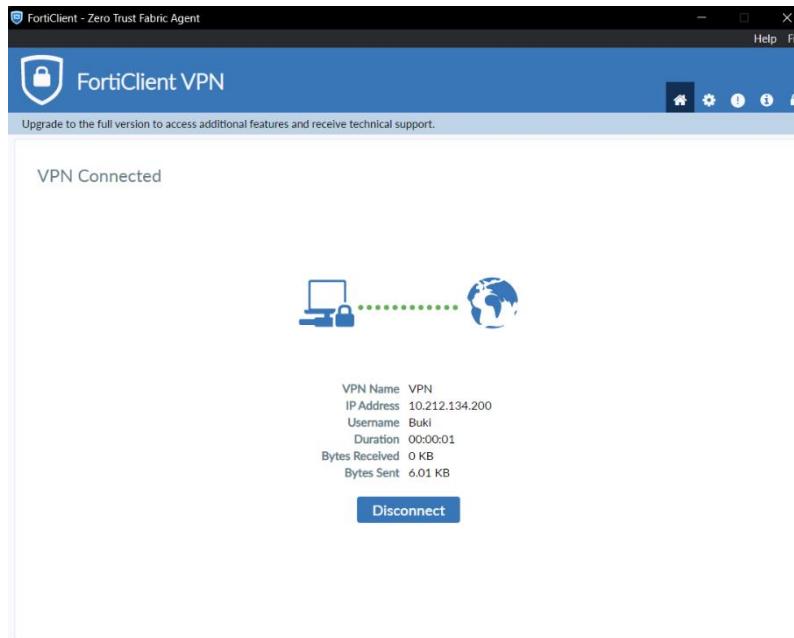
כעת נגדיר את החיבור VPN



ונכנתו את הפרטים לחיבור

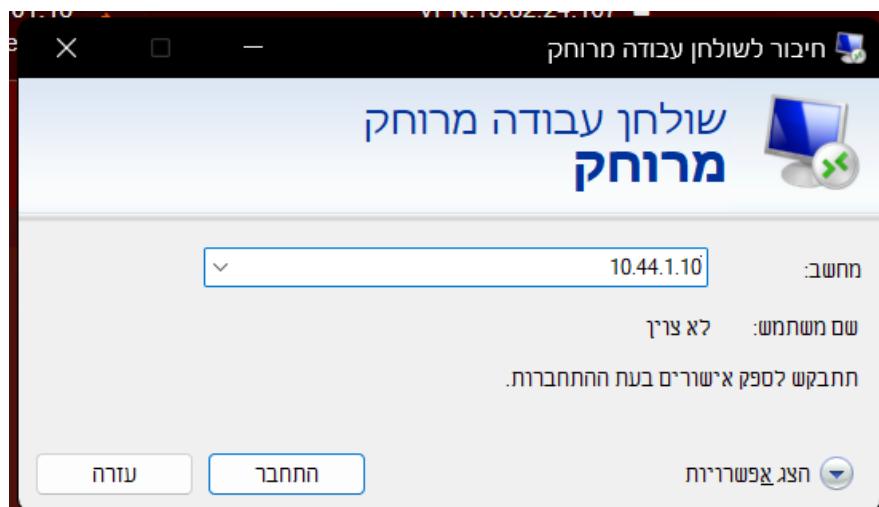


ובעת יש לנו חיבור

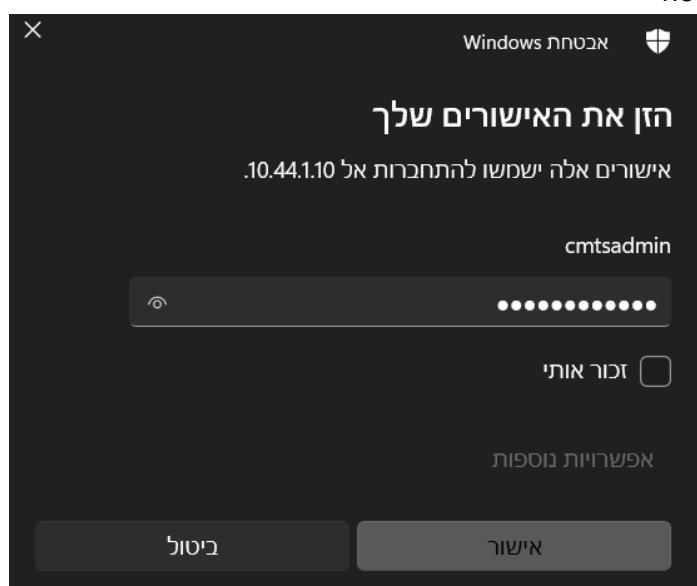


כעת נתחבר דרך RDP למחשב

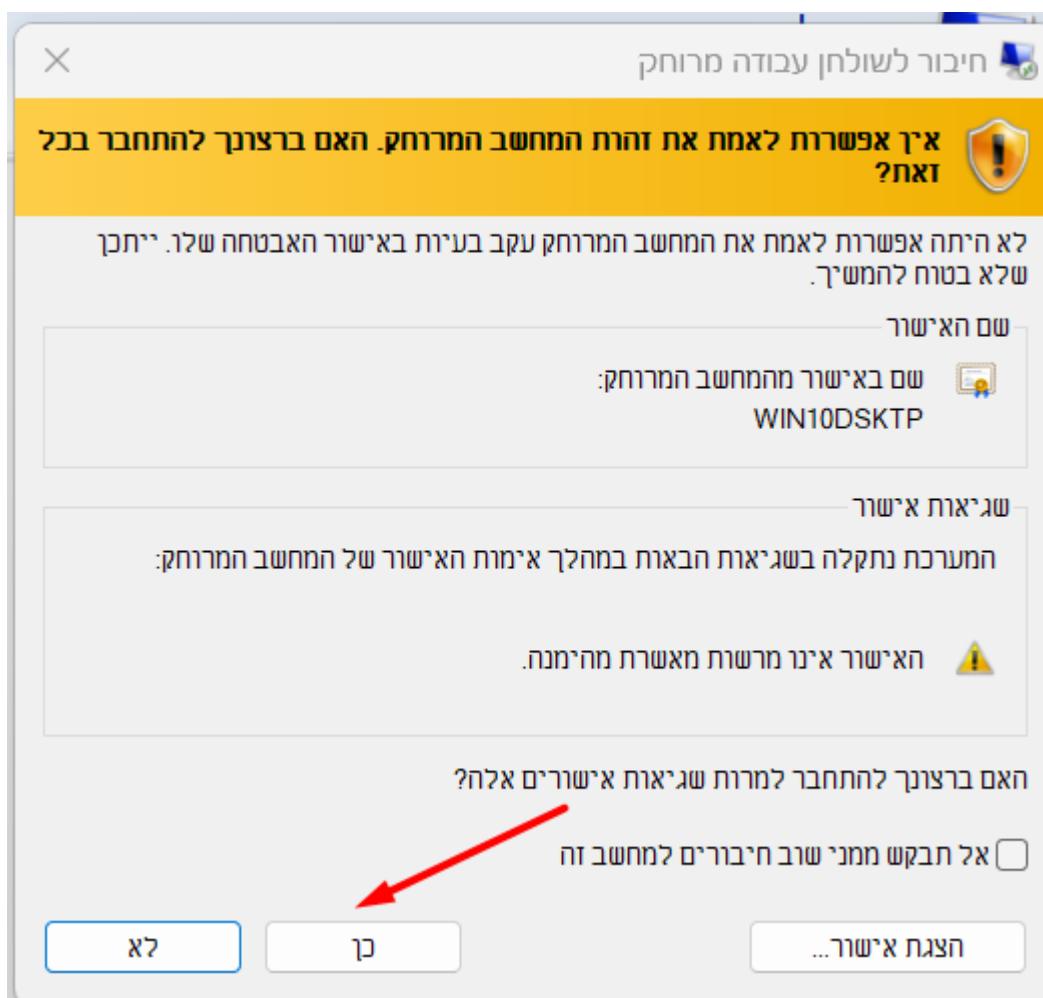
כעת נכתוב את הכתובת של המחשב



נכתב את הפרטី בכניסה



נלחץ על כן ונאשר את החיבור לשולחן העבודה מרוחק



לאחר שנלחץ על כפטור כן, נתחבר לוינטוס 10, באמצעות RDP.

ונראה, שאנו מחברים לשולחן העבודה מרוחק.

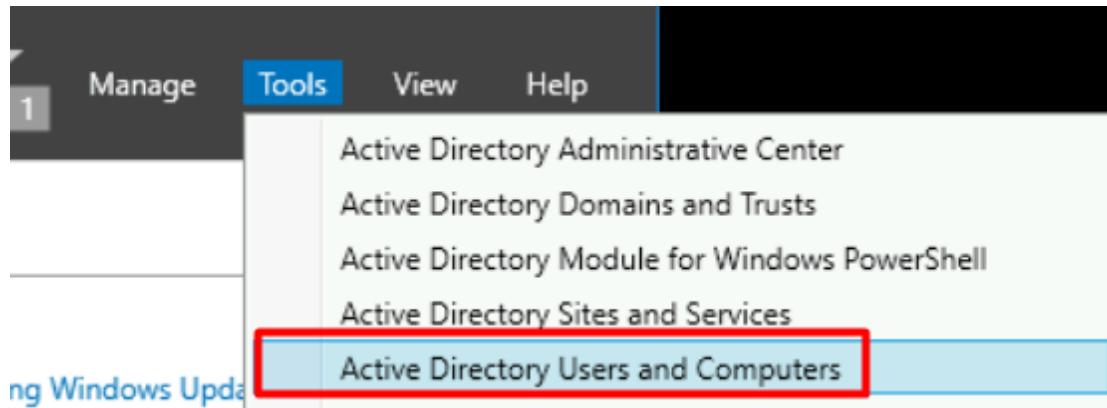


# SSLVPN WEB Mode

יצירת קבוצה בשם HR

לצורך יצירת קבוצה נוצרך לעשות יחידה ארגונית חדשה

לצורך יצירת יחידה ארגונית נוצרך להכנס אל Users and Computers



כעת בפתור ימכו על החוון Domain ונעשה יחידה ארגונית חדשה

A screenshot of the 'Active Directory Users and Computers' interface. The left pane shows a tree view of the domain structure under 'atlas.lab'. The right pane displays a list of objects: 'Container' (Default container for up..., Default container for do..., Default container for sec..., Default container for ma..., Default container for up...). A context menu is open at the bottom of the list, with 'New' selected (highlighted by a red box). A secondary context menu is open under 'New', with 'Organizational Unit' selected (highlighted by a red box). At the bottom of the screen, there is a status bar with the text 'Creates a new item in this container.'

כעת ניתן לה את השם שרצינו, נלחץ על Ok

## New Object - Organizational Unit

X



Create in: atlas.lab/

Name:

LDAP\_HR

Protect container from accidental deletion

OK

Cancel

Help

וכמובן ניצור גם Group

## New Object - Group

X



Create in: atlas.lab/LDAP\_HR

Group name:

LDAP\_HR

Group name (pre-Windows 2000):

LDAP\_HR

Group scope

- Domain local
- Global
- Universal

Group type

- Security
- Distribution

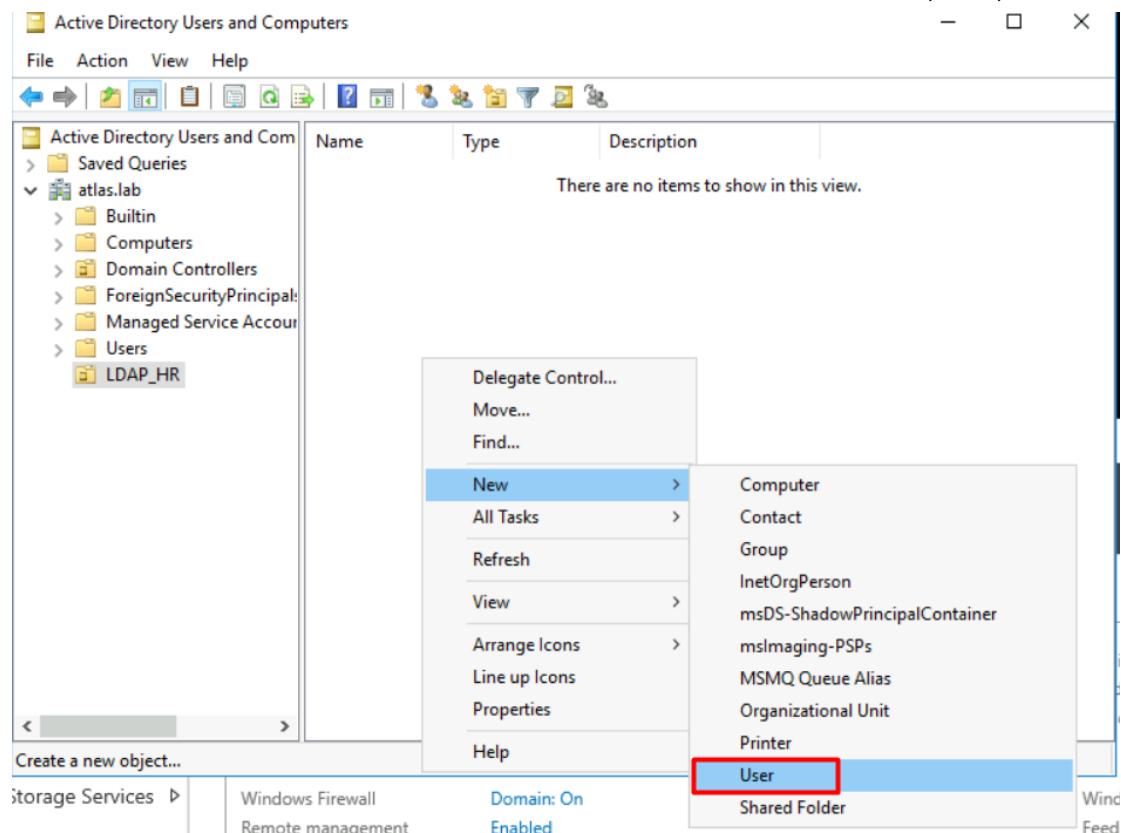
OK

Cancel

### הקמת 3 משתמשים חדשים ולשייר אותם לקבוצה

לצורך הקמת משתמשים, נלך ליחידה ארגונית, וביצור משתמשים בפנים

כפטור ימנו, New, ואז ניצור User חדש



נתן לו את השם, ואז נלחץ על Ok

The screenshot shows the 'New Object - User' dialog box. It has a header 'New Object - User' and a close button 'X'. Below the header, there is a user icon and the text 'Create in: atlas.lab/LDAP\_HR'. The form contains several input fields:

- First name: hr1
- Initials: (empty)
- Last name: (empty)
- Full name: hr1
- User logon name:  
Input field: hr1  
Dropdown: @atlas.lab
- User logon name (pre-Windows 2000):  
Input field: ATLAS\  
Input field: hr1

At the bottom of the dialog are buttons for '< Back', 'Next >', and 'Cancel'.

ובעניך לו סיסמה

New Object - User X

Create in: atlas.lab/LDAP\_HR

Password:  ······

Confirm password:  ······

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

יצור עוד משתמש

New Object - User X

Create in: atlas.lab/LDAP\_HR

First name:  Initials:

Last name:

Full name:

User logon name:  
 @atlas.lab ▼

User logon name (pre-Windows 2000):

< Back Next > Cancel

ונכון גם לו סיסמה

New Object - User X

Create in: atlas.lab/LDAP\_HR

Password:  Confirm password:

User must change password at next logon  
 User cannot change password  
 Password never expires  
 Account is disabled

< Back Next > Cancel

יצור משתמש אחרון

New Object - User X

Create in: atlas.lab/LDAP\_HR

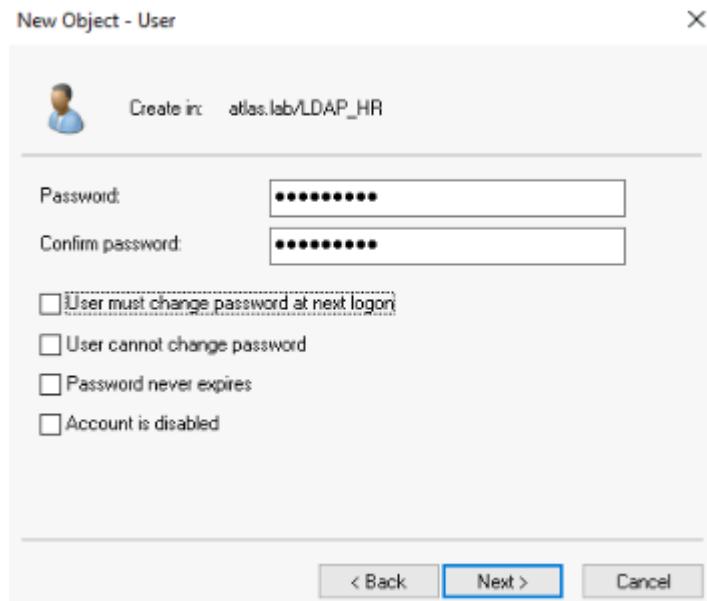
First name: hr3 Initials:   
Last name:   
Full name: hr3

User logon name:

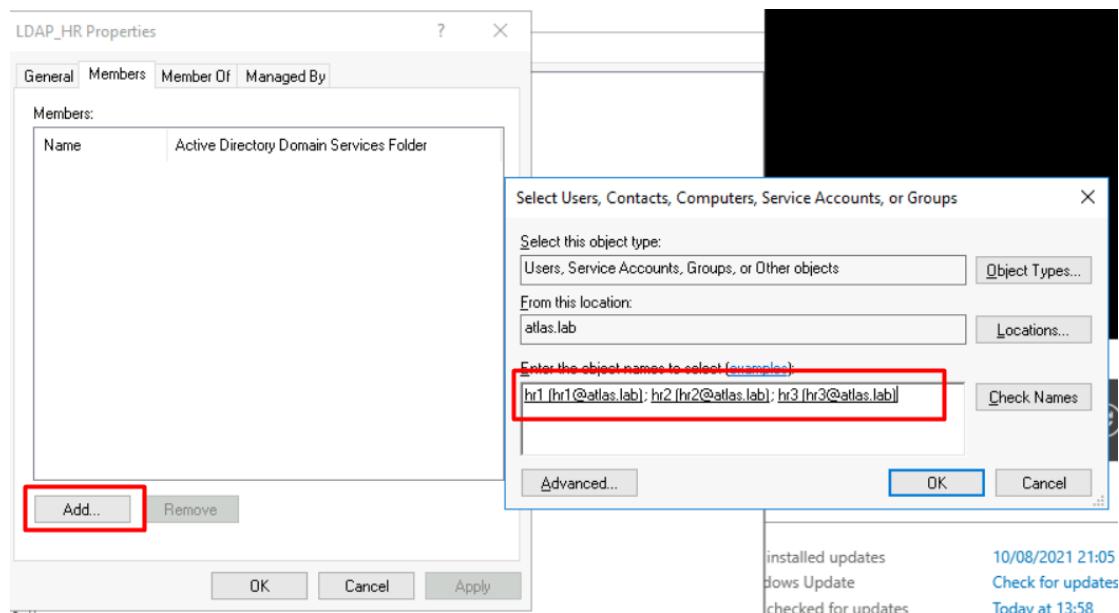
User logon name (pre-Windows 2000):

< Back Next > Cancel

נעניך גם לו סיסמה



שים את כל המשתמשים בתוך הgrp



## יצירת חוק אשר מאפשר למשתמשים אלו להגעה לרDP ב-Win10

בשלב הקודם כבר שינוינו את ההגדאות SSLVPN בכך שוכפל לבצע חיבור, להלן ההגדאות

Connection Settings ⓘ

Enable SSL-VPN

Listen on Interface(s)  port1

Listen on Port

Web mode access will be listening at <https://10.44.254.254:10443>

Server Certificate

You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). Let's Encrypt can be used to easily generate a trusted certificate if you do not have one.

Redirect HTTP to SSL-VPN

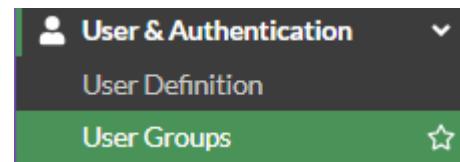
Restrict Access  Allow access from any host  Limit access to specific hosts

Idle Logout

Inactive For  Seconds

Require Client Certificate

כעת אצור קבוצה לפורטי שאוכל להגדיר בPolicy בקלות



כעת אוסיף את כל המשתמשים בקבוצה זהה

The main configuration screen shows a group named 'LDAP\_HR' with type 'Firewall' and members 'hr1', 'hr2', and 'hr3'. Below this is a 'Remote Groups' table:

Remote Server	Group Name
LDAP_AtlasLab	

A small number '1' is visible in the bottom right corner of the table.

כעת אחזר לVPN ssl

#### Authentication/Portal Mapping i

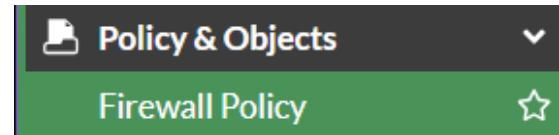
The table lists authentication mappings:

Users/Groups	Portal
LDAP_SALES	tunnel-access
LDAP_HR	web-access
All Other Users/Groups	tunnel-access

A small number '3' is visible in the bottom right corner of the table.

בנעת ניצור Policy חדש בwall

וכנס אל Policy&Objects ואז אל



ונלחץ על Create New



ונשים את הגדרות אלו

This screenshot shows the same configuration dialog as above, but with more detailed settings visible. The 'Source' field lists 'SSLVPN\_TUNNEL\_ADDR1' and 'LDAP\_HR' with a '+' button to add more. The 'Destination' field lists 'PC\_Address\_Tunnel' with a '+' button. The 'Service' field lists 'ALL' with a '+' button. The 'Action' field has 'ACCEPT' checked and 'DENY' available. The 'Inspection Mode' tab is set to 'Flow-based'.

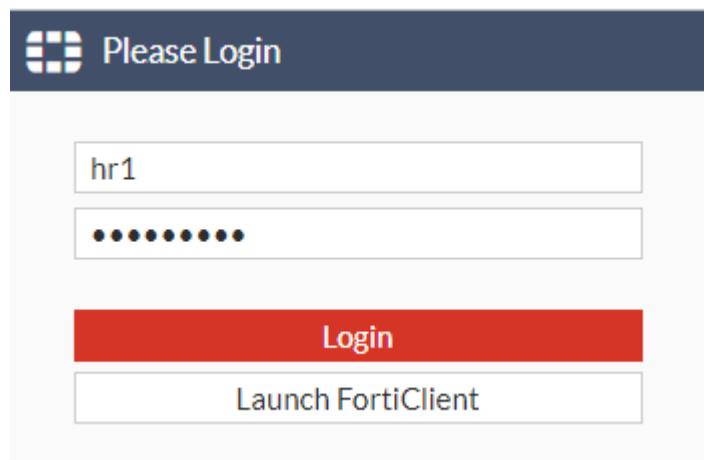
New Bookmark

Name	Webaccess
Type	RDP ▾
Host	10.44.1.10
Port	3389
Description	
Single Sign-On	Disable SSL-VPN Login
Username	
Password	
Color depth	8 Bit 16 Bit <b>32 Bit</b>
Screen width	0 ▾
Screen height	0
Keyboard layout	English, United States. ▾
Security	Allow the server to choose the type ▾
Restricted admin mode	<input checked="" type="checkbox"/>
<b>OK</b> <b>Cancel</b>	

ובעת נתחבר למשתמש HR דרך FortiClient  
נכנס לכתובת הn"ל בעזרת הפורט שצינו קודם (10443)

13.82.24.116:10443/remote/login

ונתחבר אל משתמש HR שלו



לאחר שנשים את הפרטים נראה מסך זה, נבחר את המחשב

## SSL-VPN Portal

[Download FortiClient ▾](#)

### Bookmarks



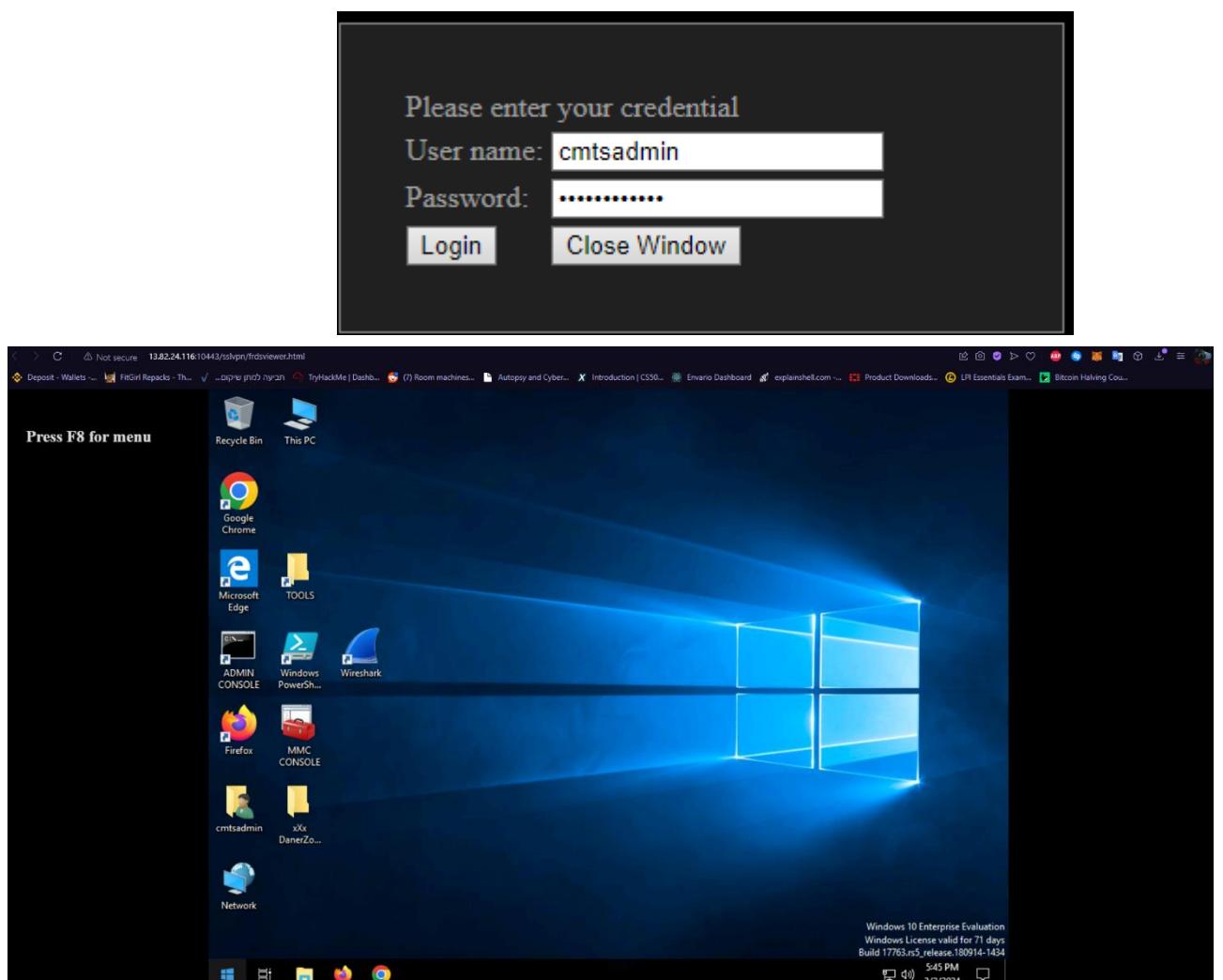
Webaccess

[Quick Connection](#)

[+ New Bookmark](#)

### History

ולהן יש לנו חיבור מוצלח של RDP



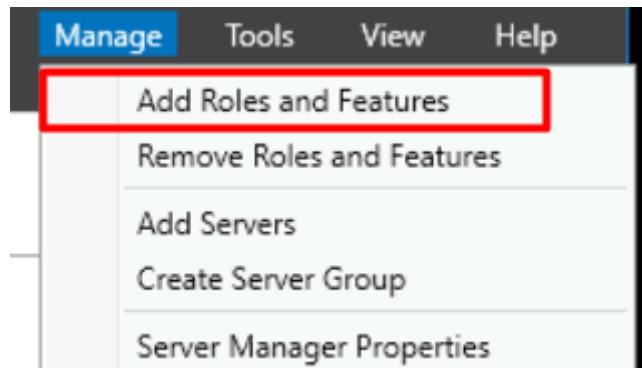
# VIP

## התקנת IIS בסביבת Envario בשרת ה-DC

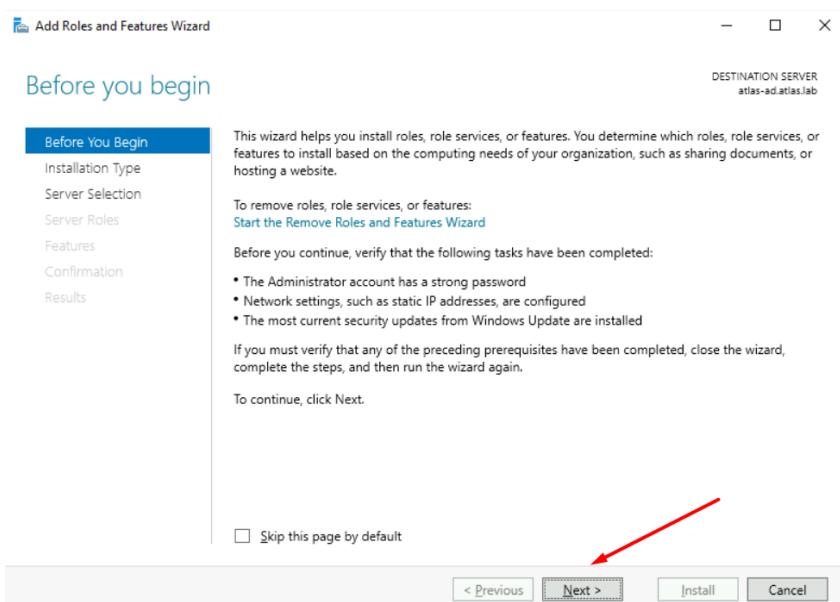
בתובת IP וירטואלית היא בתובת IP שאינה קשורה ישירות למכשיר פיזי. היא משמשת במסגרו עבור בתובת ה-IP האמיתית של המשתמש, ומאפשרת לו גישה לפורטל החברה בצורה מאובטחת ופרטית יותר על ניהול משתמשים, מחשבים, מסאים ואפליקציות ברשות.

כעת נלך להתקין רול IIS באשר DC שלנו, להלן השלבים להתקנת IIS:

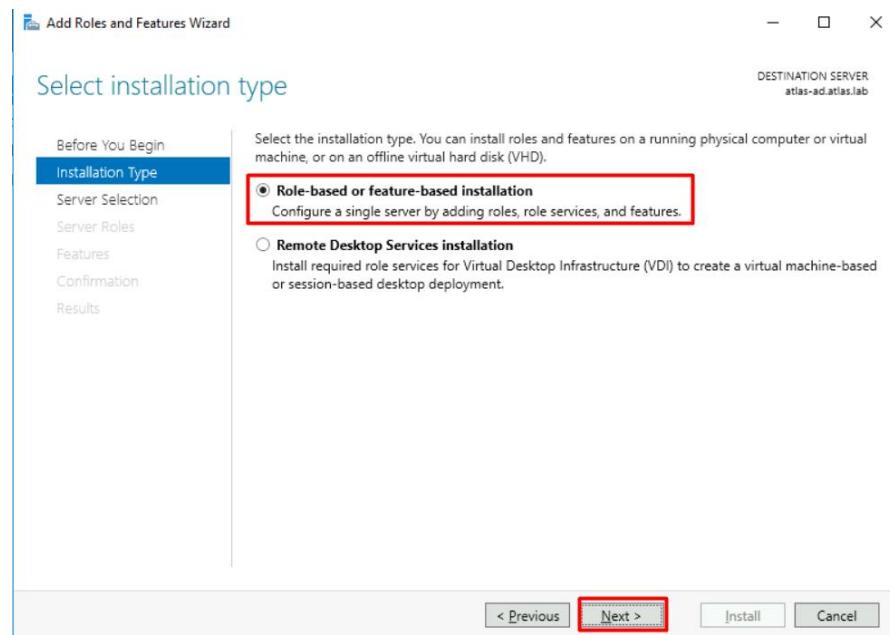
בכדי להוריד IIS ROLE נתחבר לשרת, ונלחץ על Add Roles And Features



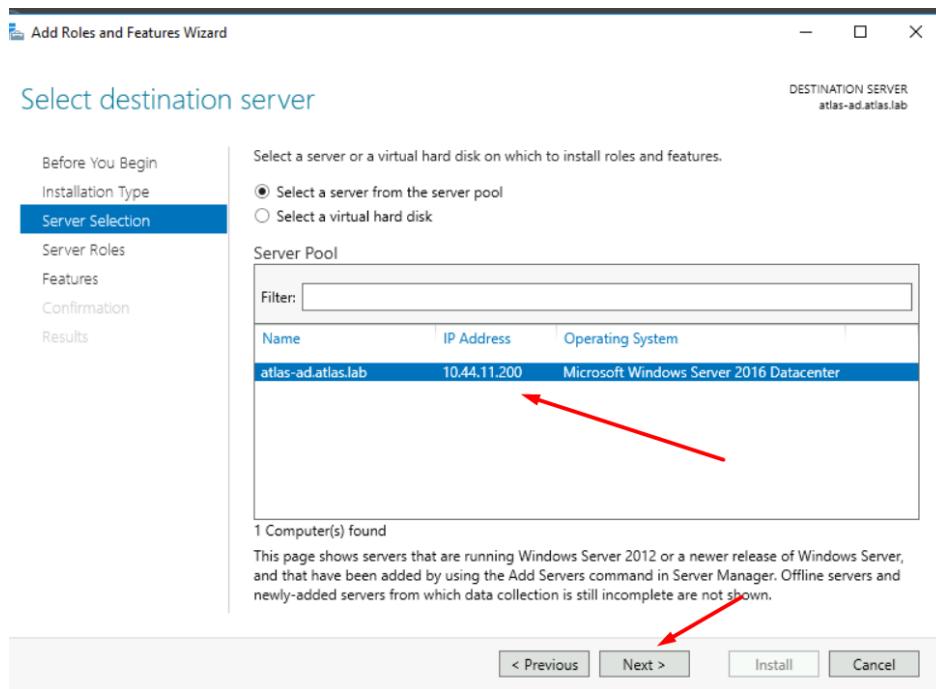
לאחר מכן נלחץ על Next



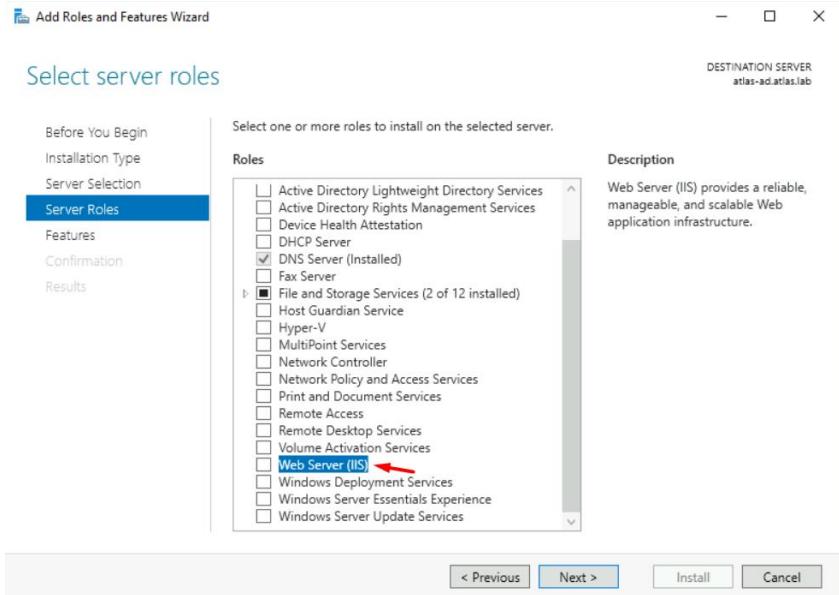
לחץ על Next , ונעשה Next



נבחר את הSERVER שלנו, ונעשה Next

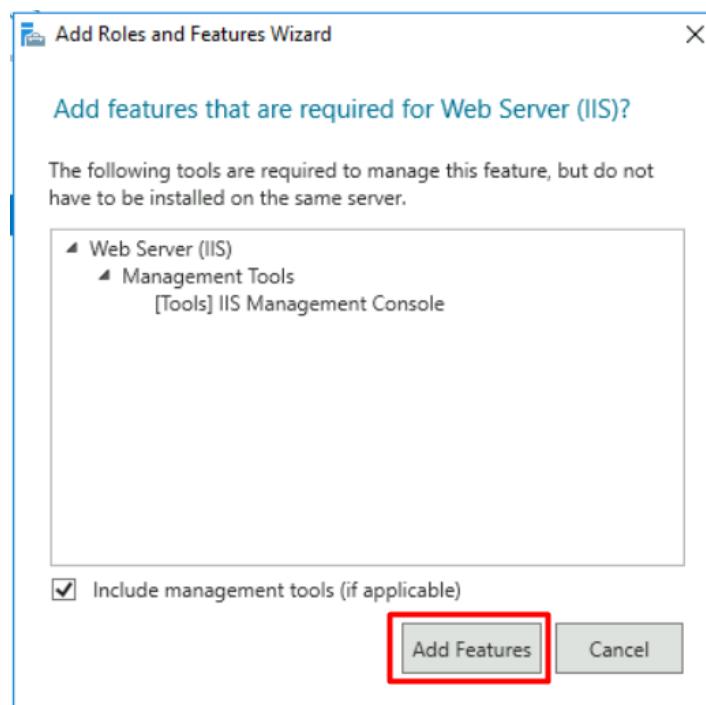


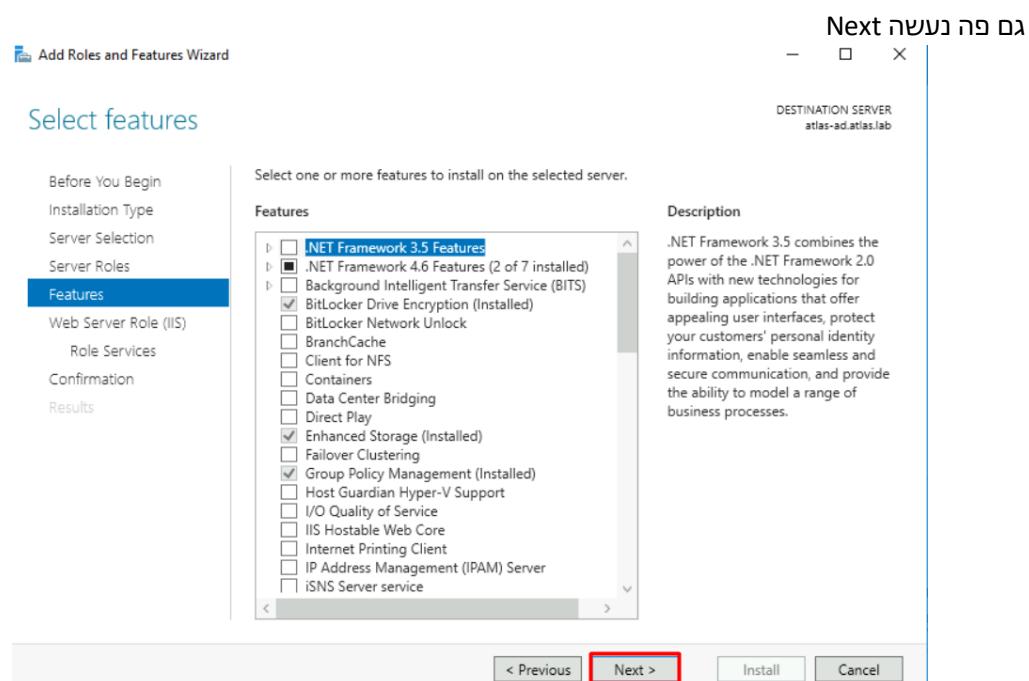
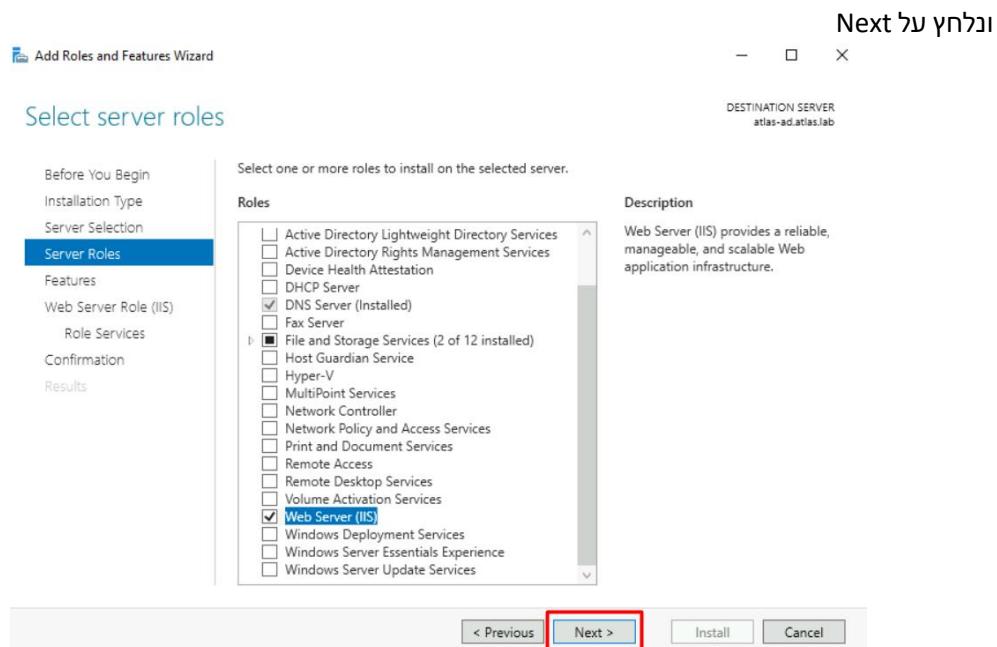
## בונט נלחץ על IIS



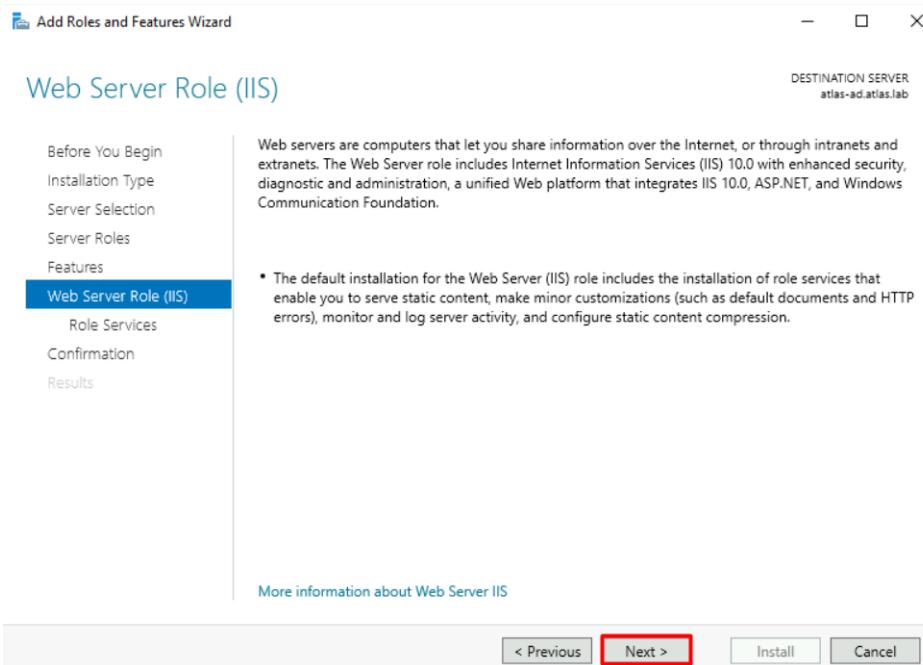
יפתח לנו החלוןית זו, שתשאל אותנו האם להוסיף Features ל-IIS, בМОון שנענשה

## Add Features

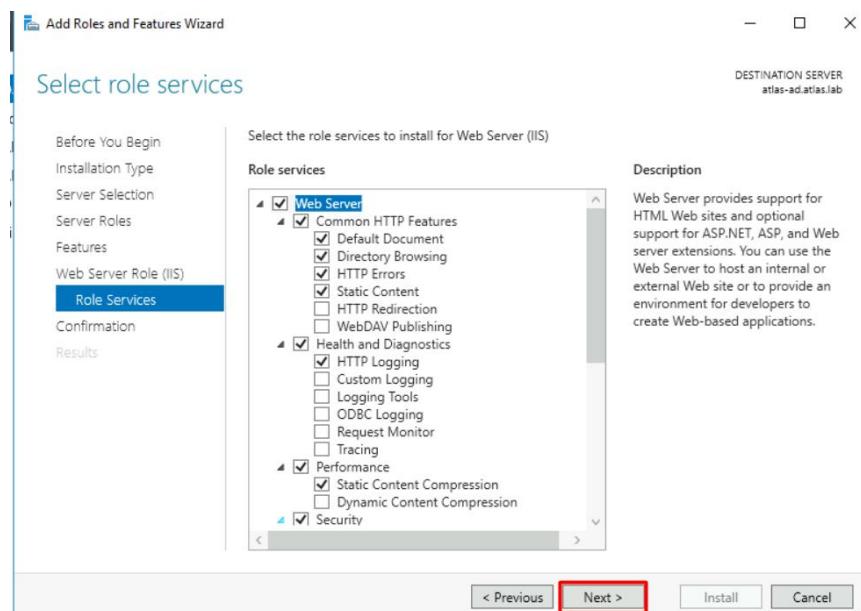




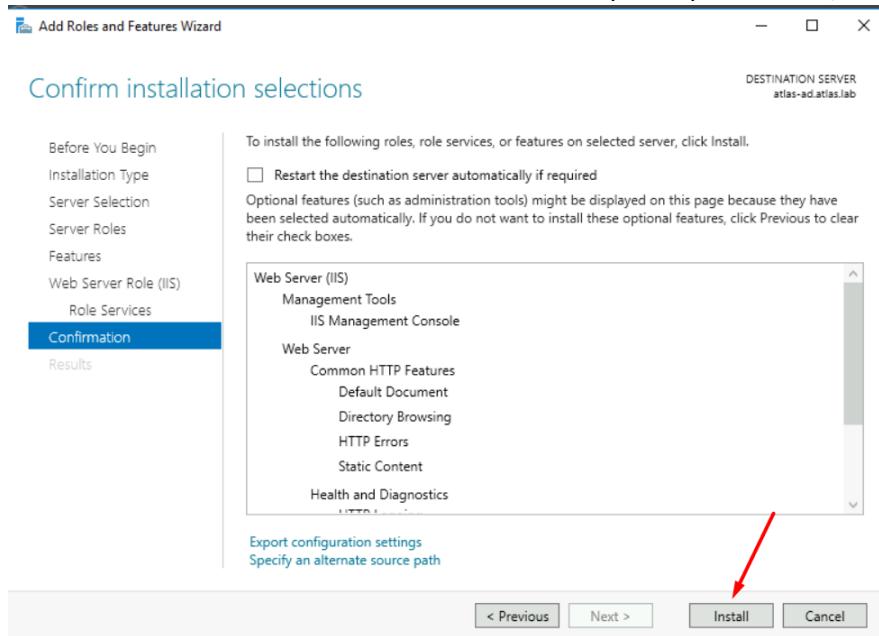
גם פה נעשה Next



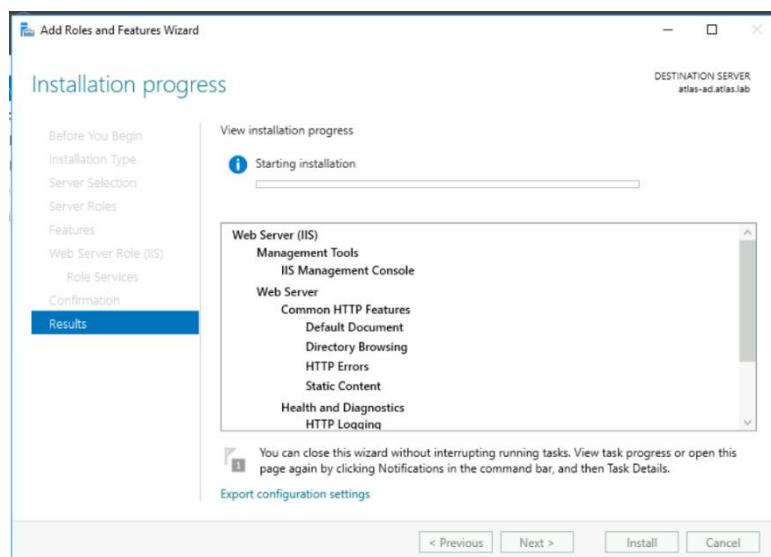
נלחץ Next שוב



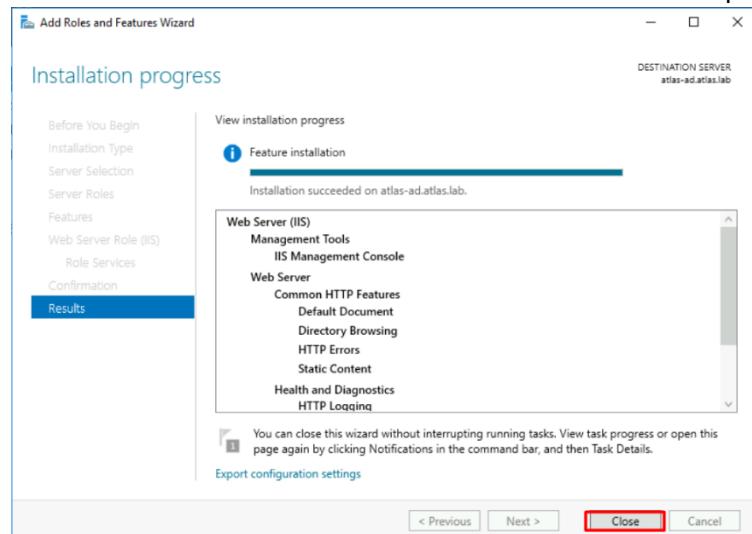
לחץ על Install, ונתuil בהליך ההתקנה



ונמתיו לסיום הליך ההתקנה



לאחר שסימנו, נלחץ Close



ניתן לעשות כל מה שעשינו פה ב-GUI, בעזרת PowerShell בלבד באמצעות הפקודה הנ"ל

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\atlasadmin> Install-WindowsFeature -Name Web-server -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
----- -----           -----          -----
True   No            NoChangeNeeded {}

PS C:\Users\atlasadmin>
```

## הפעלת VIP לoddא שהבהתובות נגישה מבחן

דבר ראשון אשר נעשה זה ליצור VIP חדש בשבייל RDP

The screenshot shows a software interface for managing network policies and objects. The left sidebar lists various policy types: Firewall Policy, IPv4 DoS Policy, ZTNA, Authentication Rules, Addresses, Internet Service Database, Services, Schedules, and **Virtual IPs**. A green bar at the bottom indicates the current selection. A "Create New" button is located in the bottom right corner of the main pane.

**Virtual IP Configuration:**

- VIP type:** IPv4
- Name:** RDP\_VIP\_Project
- Comments:** Write a comment... 0/255
- Color:** Change

**Network Configuration:**

- Interface:** any
- Type:** Static NAT (selected)
- External IP address/range:** 10.44.254.254
- Map to:** 10.44.11.200

**Optional Filters:** Port Forwarding (selected)

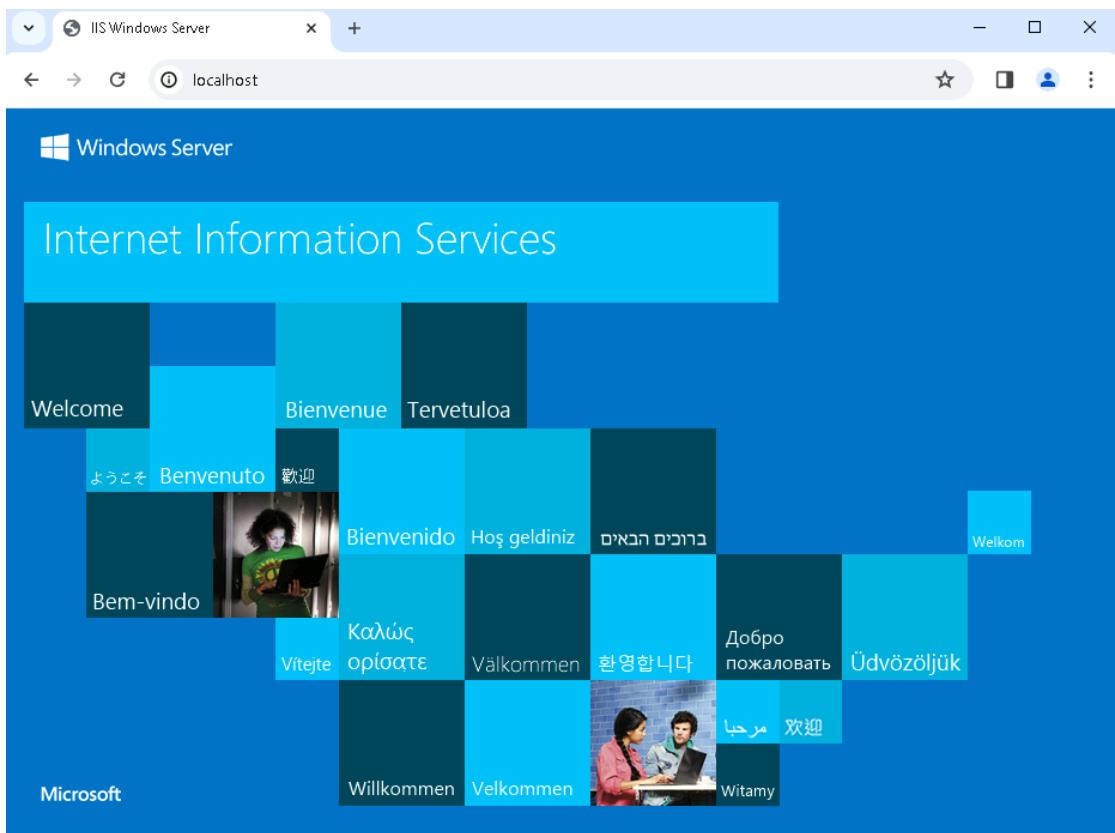
- Protocol:** TCP (selected)
- Port Mapping Type:** One to one (selected)
- External service port:** 54321
- Map to IPv4 port:** 3389

**Buttons at the bottom:** OK (green), Cancel

בעת ניצור Policy חדש בwallfire, לאחר שאמ לא ניצור, כלום לא יעבד לנו

The screenshot shows the 'Policy & Objects' interface with the 'Firewall Policy' tab selected. A green button labeled 'Create New' is visible. The main configuration area includes fields for Name (RDP\_VIP\_PROJECT\_POLICY), Incoming Interface (port1), Outgoing Interface (port2), Source (all), Destination (RDP\_VIP\_Project), Schedule (always), Service (ALL), Action (ACCEPT), and Inspection Mode (Flow-based). Below this, under 'Firewall/Network Options', there is a NAT toggle switch and a Protocol Options dropdown set to 'PROT default'.

כעת.Services נראות localhost בכתובת לדפסן ומכתוב IIS



WEBSERV� חדש בшибיל ניצור VIP כעת

**Policy & Objects**

- Firewall Policy
- IPv4 DoS Policy
- ZTNA
- Authentication Rules
- Addresses
- Internet Service Database
- Services
- Schedules
- Virtual IPs**

**Create New**

---

VIP type: IPv4

Name: WEBSERV

Comments: Write a comment... 0/255

Color: #ccc Change

**Network**

Interface: any

Type: Static NAT FQDN

External IP address/range: 10.44.254.254

Map to: 10.44.11.200

**Optional Filters**

**Port Forwarding**

Protocol: TCP UDP SCTP ICMP

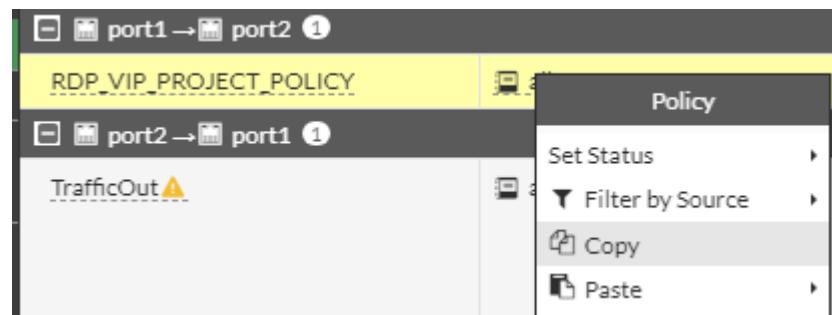
Port Mapping Type: One to one Many to many

External service port: 8080

Map to IPv4 port: 80

**OK** **Cancel**

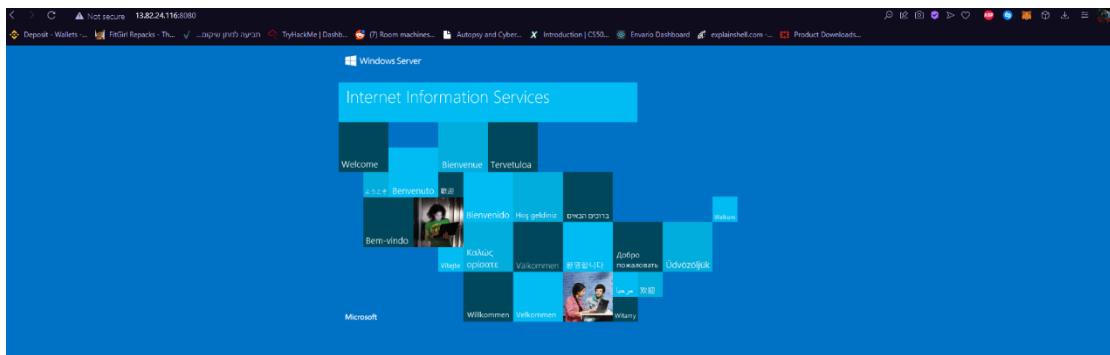
נתוך את ה Policy שיצרנו קודם



ונשנה יעד ושרות

WEBSERV ROLE	all	RDP_VIP_Project	always	RDP	✓ ACCEPT	✗ Disabled	SSL no-inspection	UTM	0 B
WEBSERV ROLE	all	WEBSERV	always	HTTP	✓ ACCEPT	✗ Disabled	SSL no-inspection	UTM	0 B

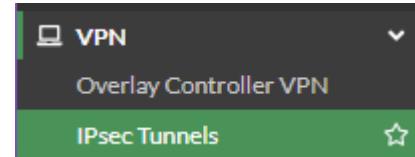
ובכשיו שנכנס לכתובת תחת הפורט 8080 יעבוד לנו



# IPSEC

יצירת IPSEC עם חבר בכיתה

בכדי ליזור Tunnel נכל לפה



לאחר מכן ניצור חדש



נתן לו שם, אנו אהיה TLV

1 VPN Setup > 2 Authentication > 3 Policy & Routing > 4 Review Settings

Name	TLV_TO_NYC
Template type	Site to Site Hub-and-Spoke Remote Access Custom
NAT configuration	No NAT between sites This site is behind NAT The remote site is behind NAT
Remote device type	FortiGate Cisco

כעת נשים את הכתובת החיצונית של רון יעקב וידן

VPN Creation Wizard

✓ VPN Setup > 2 Authentication > 3 Policy & Routing > 4 Review Settings

Remote device	IP Address Dynamic DNS
Remote IP address	13.82.95.242
Outgoing Interface	port1
Authentication method	Pre-shared Key Signature
Pre-shared key	*****

Site to Site - FortiGate

This FortiGate      Internet      Remote FortiGate

כעת נשים את הכתובות של רון ושל רון

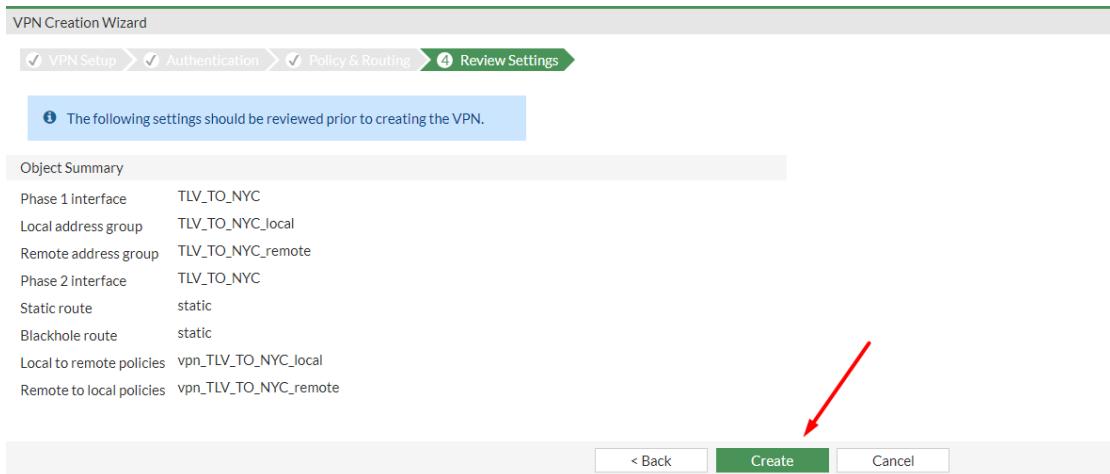
VPN Creation Wizard

✓ VPN Setup > ✓ Authentication > 3 Policy & Routing > 4 Review Settings

Local interface	port2
Local subnets	10.44.11.0/24 10.44.1.0/24
Remote Subnets	10.244.11.0/24 10.244.1.0/24
Internet Access	None Share Local Use Remote

Site to Site - FortiGate

This FortiGate      Internet      Remote FortiGate



### כעת נבצע חיפוש של IPSEC MONITOR

ונפעיל את ה ipsec

Name	Remote Gateway	Peer ID	Incoming Data	Outgoing Data
Site to Site - FortiGate 1	TLV_TO_NYC	13.82.95.242	0 B	0 B

כעת אגדיר Firewall Policy חדש אשר נוון לIPSEC לעשות אליו רק פינג

נלחץ על ALL ונשנה אל PING, שעובד ב ICMP

TLV_TO_NYC → port2 1	vpn_TLV_TO_NYC_remote_0	TLV_TO_NYC_remote	TLV_TO_NYC_local	always	<input checked="" type="checkbox"/> ALL	<input checked="" type="checkbox"/> ACCEPT	<input type="checkbox"/> Disabled	<input type="checkbox"/> no-inspection	<input type="checkbox"/> UTM	0 B
----------------------	-------------------------	-------------------	------------------	--------	---	--	-----------------------------------	--	------------------------------	-----

כעת נראה שבמוקם ALL יש אך ורק RDP

TLV_TO_NYC → port2 1	vpn_TLV_TO_NYC_remote_0	TLV_TO_NYC_remote	TLV_TO_NYC_local	always	<input type="checkbox"/> PING	<input checked="" type="checkbox"/> ACCEPT	<input type="checkbox"/> Disabled	<input type="checkbox"/> no-inspection	<input type="checkbox"/> UTM	0 B
----------------------	-------------------------	-------------------	------------------	--------	-------------------------------	--	-----------------------------------	--	------------------------------	-----

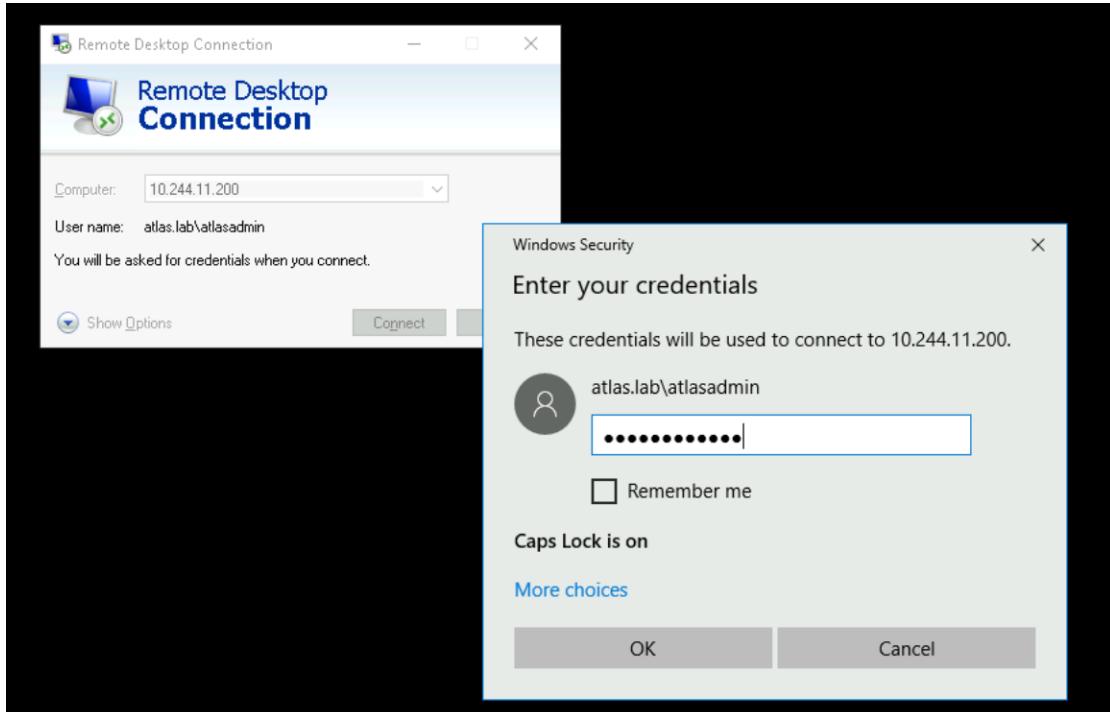
כעת ננסה לעשות לאטלאס של רון פינג (הוא בניו יורק)

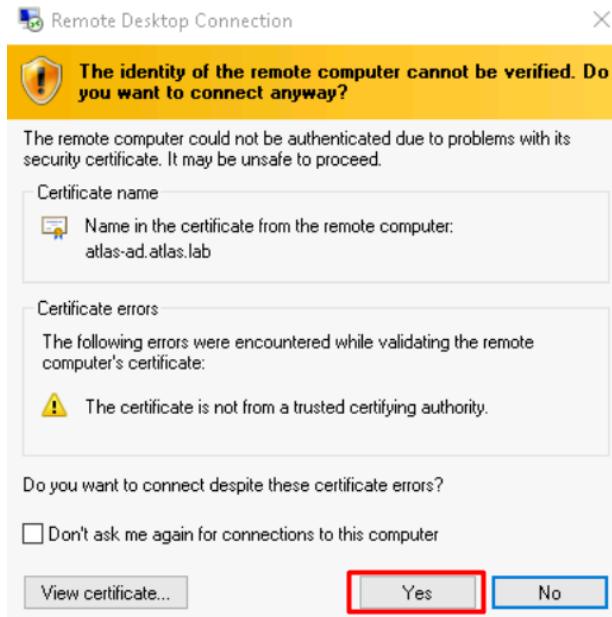
```
C:\Users\atlasadmin>ping 10.244.11.200
```

```
Pinging 10.244.11.200 with 32 bytes of data:  
Request timed out.
```

ולא עובד

כעת ננסה לעשות לו RDP





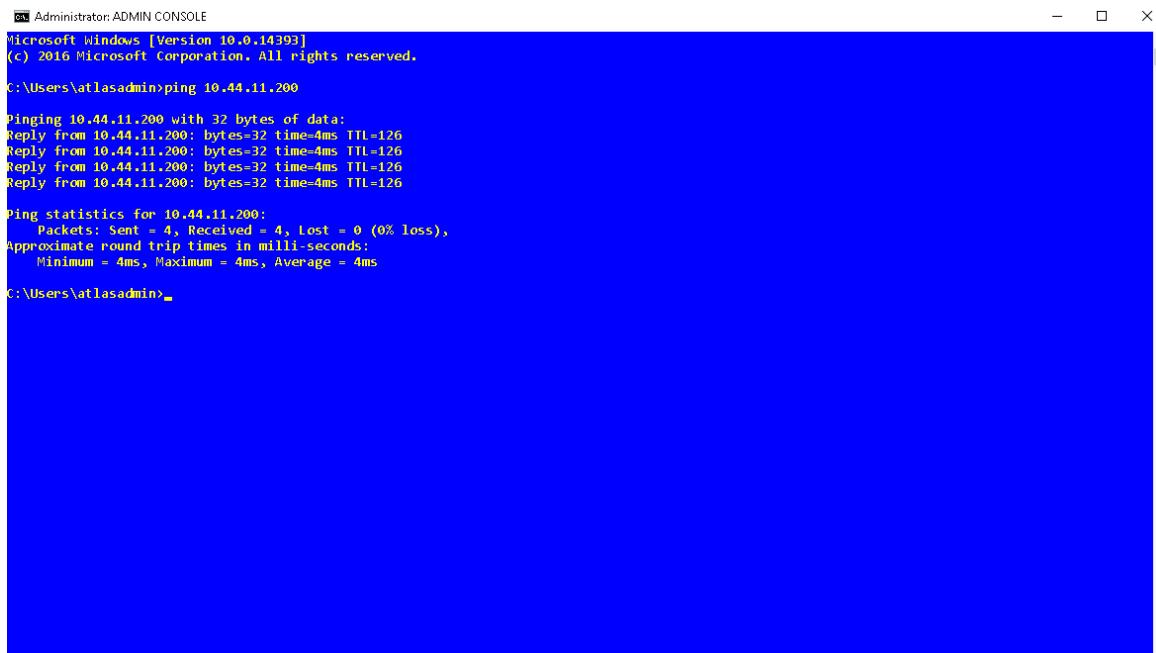
ນາສເຣ ຄົກທິບອຣ

ອັນຂໍມ ບັນນິມ



בעת נראה מה קורה אצל רון במערכות, הוא יצטרך לעשות לו פינג, אך לא להצליח לעשות לו Ping, מאחר ובყע Policy של Fortigate, הגדרנו אף ורק RDP

להלן תמונה של רון עושים לו פינג:



```
Administrator: ADMIN CONSOLE
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

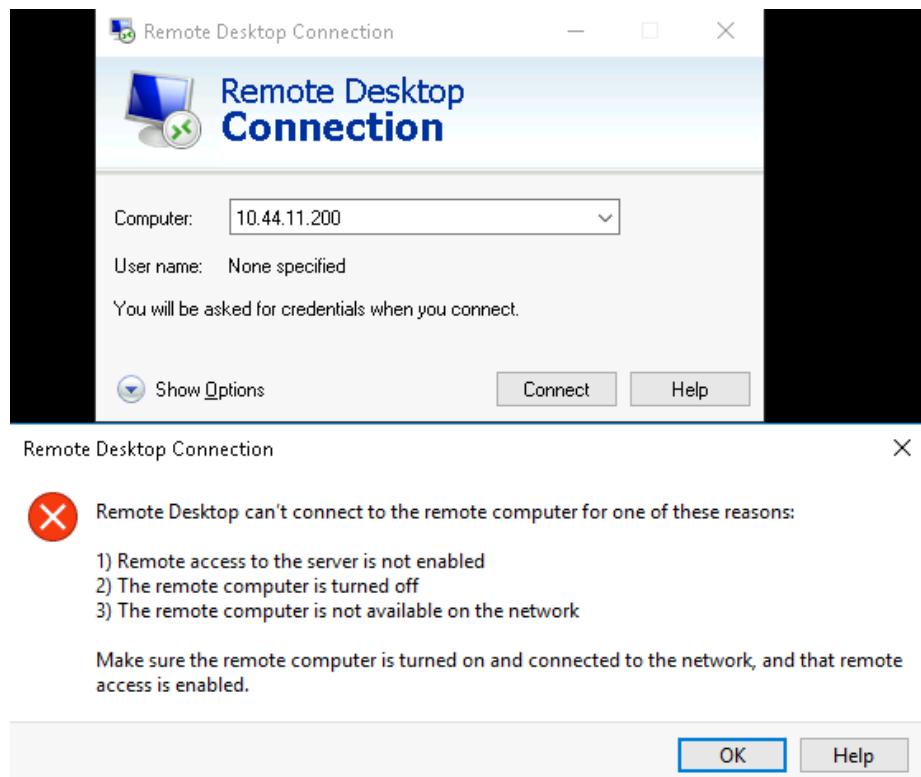
C:\Users\atlasadmin>ping 10.44.11.200

Pinging 10.44.11.200 with 32 bytes of data:
Reply from 10.44.11.200: bytes=32 time=4ms TTL=126

Ping statistics for 10.44.11.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 4ms, Average = 4ms

C:\Users\atlasadmin>
```

ולהן הוכחה שRDP לא צלח לו



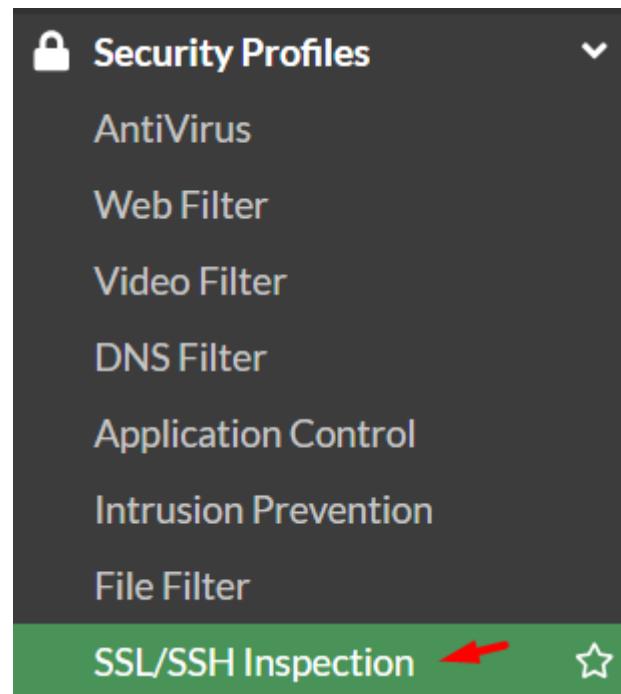
# Inspection

מה זה ?Inspection

Inspection או בעברית בדיקה, בעצם זו אופציה בـFortiGate, שיתן לנו לחת את התוכן המוצפן, יעשה לו Decrypt, ובעצם יבדוק את התוכן, בכך למנוע פישינג, וירוסים ועוד הרבה התקפות אופציונליות.

## יצירת פרוfil Inspection חדש

בכדי להתחיל, נכנס לתפריט הנ"ל בـFortiGate



ולחץ Create New

**+ Create New**

## כעת נשים את הגדרות אלו

New SSL/SSH Inspection Profile

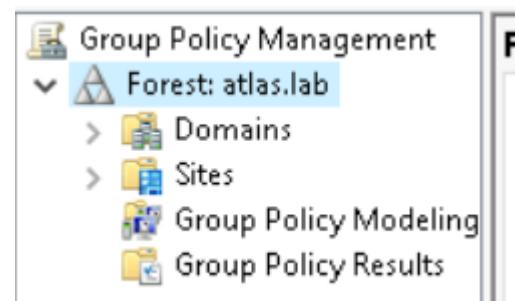
Name	Office_To_Internet_Inspection
Comments	Project
SSL Inspection Options	
Enable SSL inspection of	Multiple Clients Connecting to Multiple Servers Protecting SSL Server
Inspection method	SSL Certificate Inspection <b>Full SSL Inspection</b>
CA certificate	Fortinet_CA_SSL <input type="button" value="Download"/>
Blocked certificates	<input type="button" value="View Blocked Certificates"/>
Untrusted SSL certificates	<input type="button" value="View Trusted CAs List"/>
Server certificate SNI check	<input type="button" value="Enable"/> <input type="button" value="Strict"/> <input type="button" value="Disable"/>
Enforce SSL cipher compliance	<input type="radio"/>
Enforce SSL negotiation compliance	<input type="radio"/>
RPC over HTTPS	<input type="radio"/>
Protocol Port Mapping	
Inspect all ports	<input type="radio"/>
HTTPS	443
SMTSP	465
POP3S	995
IMAPS	993
FTPS	990
DNS over TLS	853

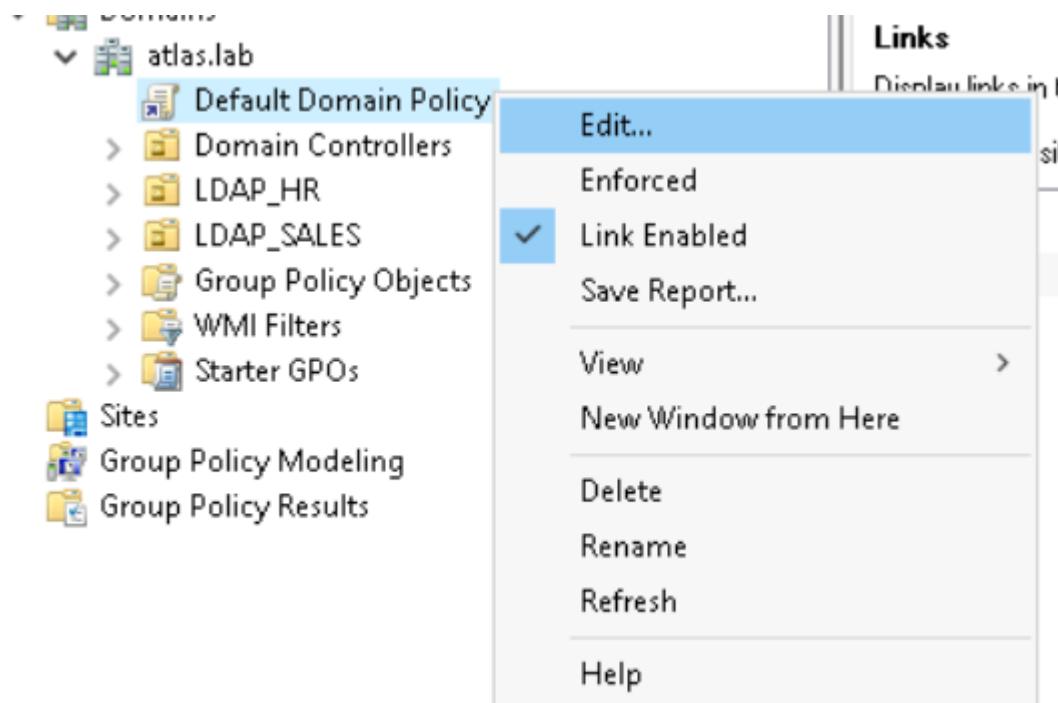
## כעת נלך לTrafficOut SSL ונסנה את הPolicy בFireWall

TrafficOut	port2	port1	all	all	always	ALL	ACCEPT	Enabled	AV default	WEB default	IPS default	UTM	1.98 MB
													<b>SSL Office_To_Internet_Inspection</b>

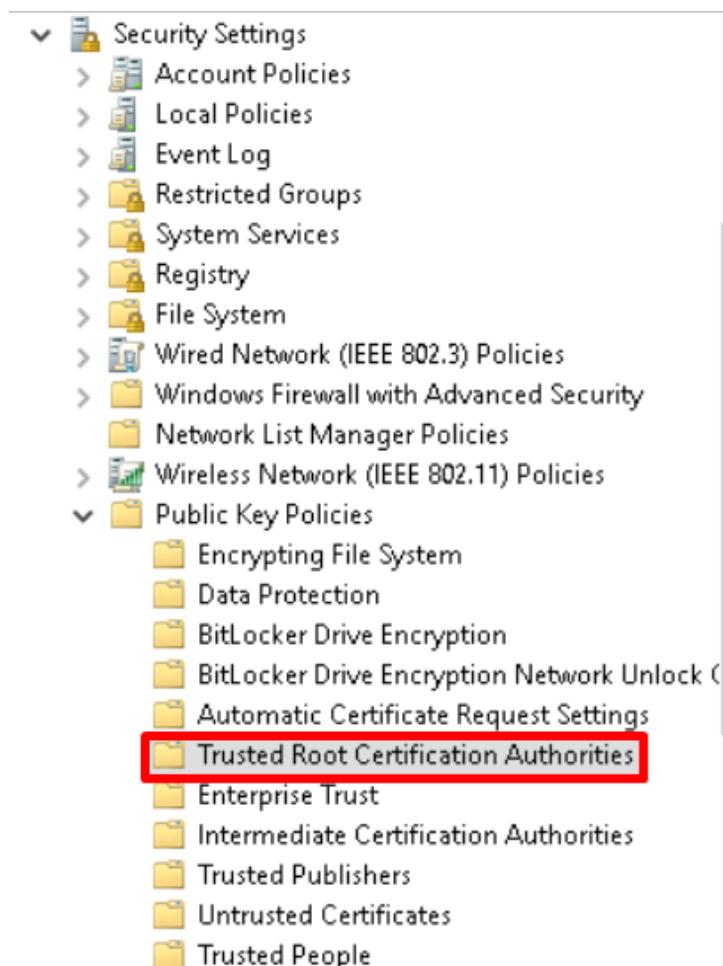
כעת צריך להוריד את התעודה של Fortinet על המכונת

נכנו לPolicy Group

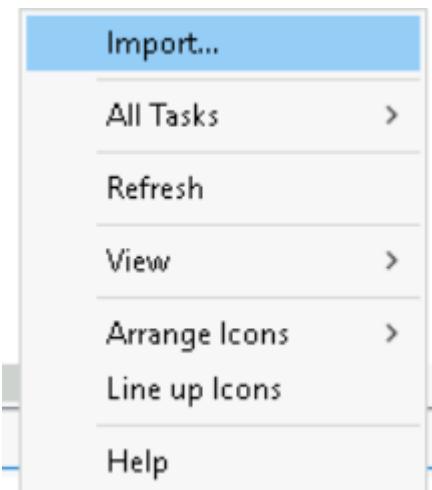




נכנו אל תקיה זו



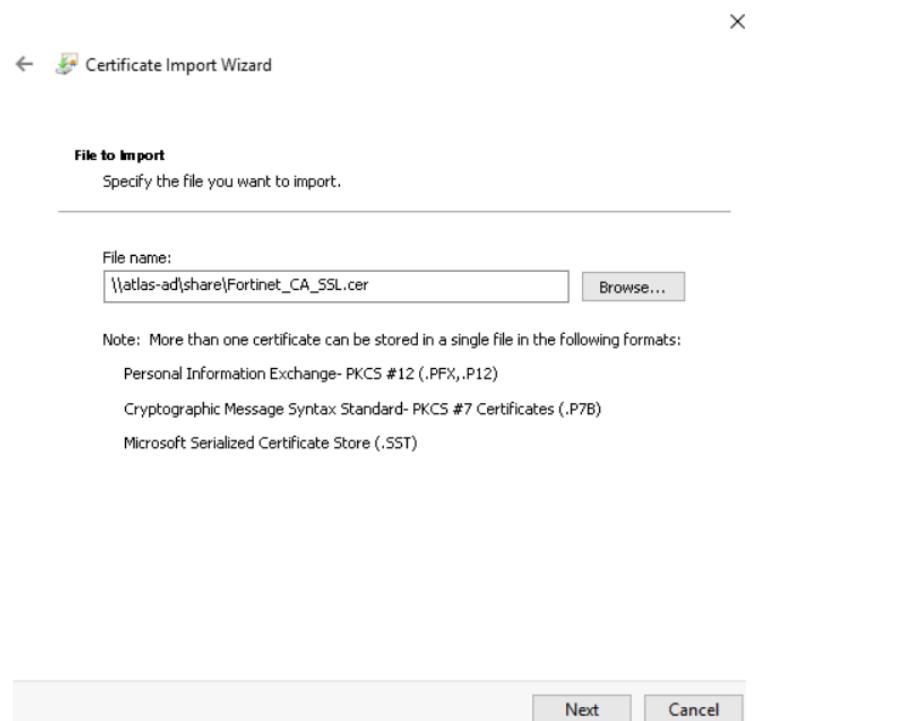
## וילוח IMPORT

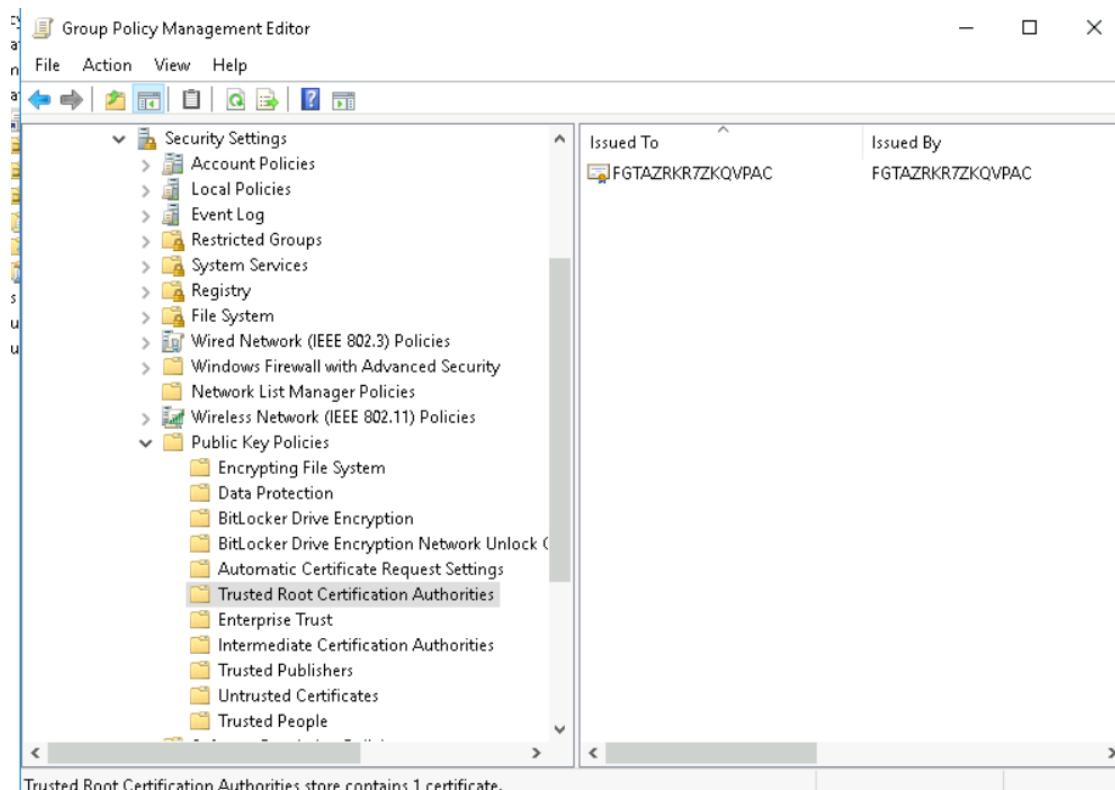


נשים את התעודה בתיקייה משותפת

This PC > Windows (C:) > share				
Name	Date modified	Type	Size	
Fortinet_CA_SSL.cer	26/02/2024 19:30	Security Certificate	2 KB	

נבחר בתעודה





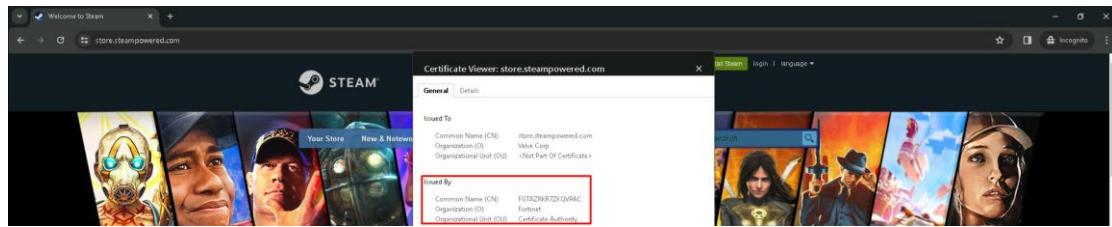
כעת הוא נמצא, כעת נלך למחשב השני, נעדכן GPO, ונראה שיש תעודת.

```
cmd. Command Prompt - gpupdate /force
Microsoft Windows [Version 10.0.17763.1613]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\cmtsadmin>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
```

ובכדי לבדוק שיש inspection, נכנס לדף דפן, ונראה איזו תעודת אנו מקבל, כMOVED שמכנס מגילשה בסתר, כדי למנוע מצב שבו יהיה עדין מטמון.



כעת נכנס לאתר כביכול זדוני, אך לא באמת, סתם בדיקה.

ונראה שתהאטר נחסם



 FortiGuard Intrusion Prevention -  
Access Blocked

Web Page Blocked  
You have tried to access a web page that is in violation of your Internet usage policy.  
Category: Malicious Websites  
URL: https://secure.eicar.org/eicar.com  
To have the rating of this web page re-evaluated [please click here](#)

ונראה בלוג שלא נותן לי להכנס גם

2024/02/26 13:43:03	10.44.11.200	Blocked	https://secure.eicar.org/eicar.com	Malicious Websites	713B / 0B	
---------------------	--------------	---------	------------------------------------	--------------------	-----------	---

# Web-Filter

## יצירת פרופיל Web-Filter

WEB FILTER ב-FORTIGATE הוא כלי המאפשר לך לשלוט בגישה לאטרי אינטרנט ברשותך. הוא מספק הגנה מפני תוכן לא הולם, התקפות זדוניות, ועוד.

בשביל ליצור חדש נלחץ על Security Profiles ושם נלחץ על Web Filter



כעת נלחץ על Create New



אך לפני שניצור, הונחנו להשתמש ב-proxy-based, אך נרצה להבין בעצמו מה זה.

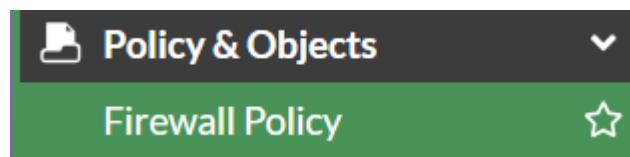
Proxy-Based הוא שיטת בדיקה של פאקטות ב-FortiGate. בשיטה זו, ה-FortiGate פועל כמתוך בין המחשב שלך לבין האתר האינטרנט שאתה מבקר בהם. כלומר, כל התעבורה שלך עוברת דרך ה-FortiGate לפני שהיא מגיעה אליך.

היתרון של Proxy-Based הוא שהוא-FortiGate יכול לבצע בדיקה יסודית מאוד של הפאקטות. זה כולל סריקה לאייתור וירוסים, תוכנות זדוניות, תוכן לא הולם ועוד. כתוצאה לכך, מספק רמת אבטחה גבוהה יותר מאשר שיטות בדיקה אחרות.

כעת ניצור לפי ההנחיות שהתבקשנו, בשם, ו-

Name	Office_Web_Filter
Comments	Write a comment...
Feature set	Flow-based <b>Proxy-based</b>

לפני שנטחיל בביצוע ה Krishot, נצטרך לשנות הגדרות ב Firewall Policy



TrafficOut	all	all	always	ALL	ACCEPT	Enabled	AV default WEB default IPS default SSL Office_To_Internet_Inspection	UTM	20.50 MB
port2→port1									

כעת נצטרך לשנות את ה Web Filter

TrafficOut	all	all	always	ALL	ACCEPT	Enabled	AV default WEB Office_Web_Filter IPS default SSL Office_To_Internet_Inspection	UTM	20.52 MB
port2→port1									

וכעת נוכל להתקדם לה Krishot

## הकשהה

cutet נבצע הקשהות

דבר ראשון שנבעצע, זה חסימה של אתרים בקטגורית חיפוש עבודה

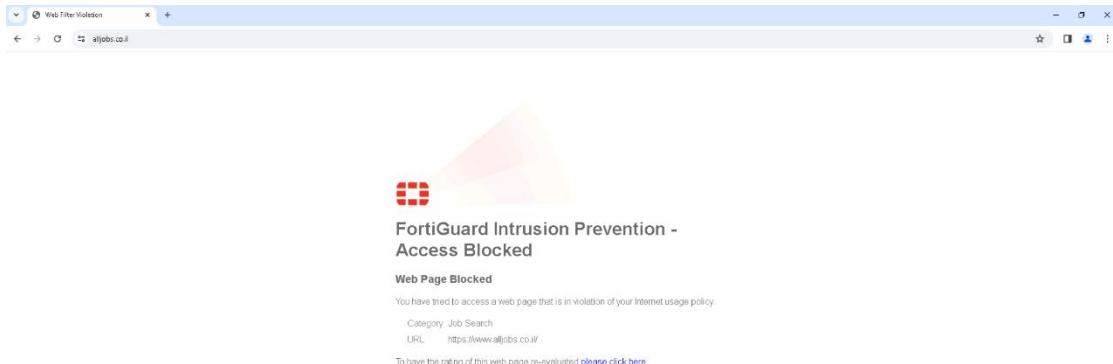
FortiGuard Category Based Filter

Name	Action
Entertainment	Allow
Arts and Culture	Allow
Education	Allow
Health and Wellness	Allow
Job Search	Allow
Medicine	Allow
News and Media	Allow
Social Networking	Allow
Political Organizations	Allow

55% 93

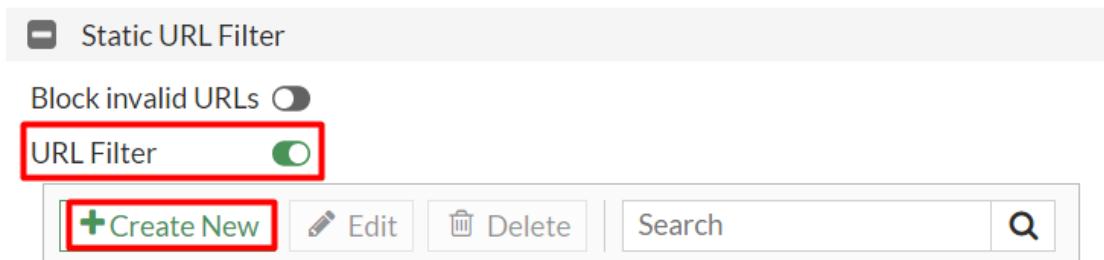
Job Search Block

cutet ננסה להכנס לאתר חיפוש העבודות הפופולרי הישראלי AllJobs



כעת נמנע גישה לReddit.Com

כעת מה שנctrar לעשות, זה הפעלת URL Filter



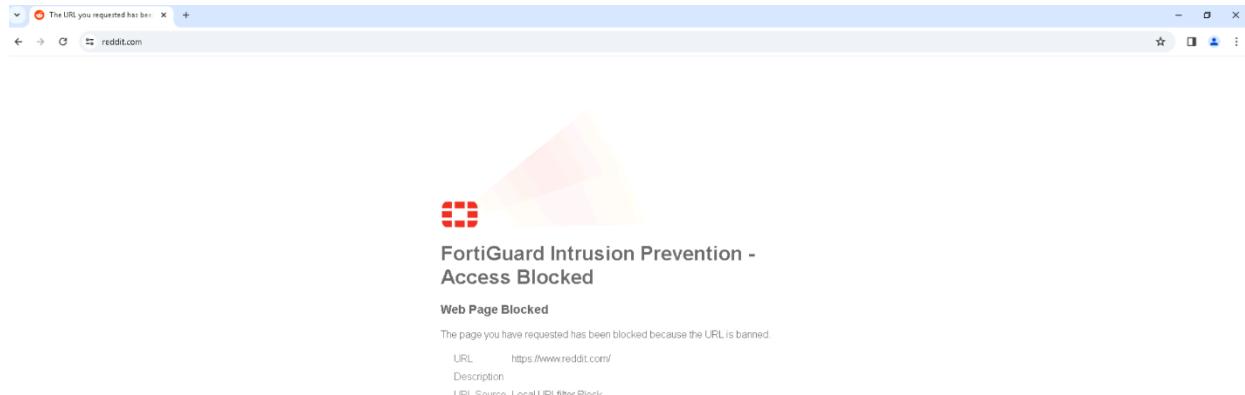
וניצור Filter חדש של כל הדומיין של Reddit

New URL Filter

URL	*.Reddit.com
Type	Simple Regular Expression Wildcard
Action	Exempt Block Allow Monitor
Status	Enable Disable

OK Cancel

ונראה שלא נכנס לנו לרדיט



יצירת מצב שמשתמשים מסוימים יכולים להכנס לשופינג, ואחרים לא.

FortiGuard Category Based Filter

Allow	Monitor	Block	Warning	Authenticate
Name	Action			
News and Media			<input checked="" type="checkbox"/>	Allow
Social Networking			<input checked="" type="checkbox"/>	Allow
Political Organizations			<input checked="" type="checkbox"/>	Allow
Reference			<input checked="" type="checkbox"/>	Allow
Global Religion			<input checked="" type="checkbox"/>	Allow
Shopping			<input checked="" type="checkbox"/>	Allow
Society and Lifestyles			<input checked="" type="checkbox"/>	Allow
Sports			<input checked="" type="checkbox"/>	Allow
Travel			<input checked="" type="checkbox"/>	Allow
Personal Vehicles			<input checked="" type="checkbox"/>	Allow

61% 93

ניתן לHR את האופציה להכנס, אחרים לא.

Edit Filter

Warning Interval	0	hour(s)	5	minute(s)	0	second(s)
Selected User Groups	LDAP_HR					
<button>OK</button> <button>Cancel</button>						

כעת נכנס לאתר Asos ונראה שהוא מבקש מייתנו להתחבר



## FortiGuard Intrusion Prevention - Access Blocked

### Web Page Blocked

You have tried to access a web page which is in violation of your Internet usage policy.

Category Shopping  
URL https://www.asos.com/

To have the rating of this web page re-evaluated [please click here](#).

[Proceed](#) [Go Back](#)



## FortiGuard Intrusion Prevention - Access Blocked

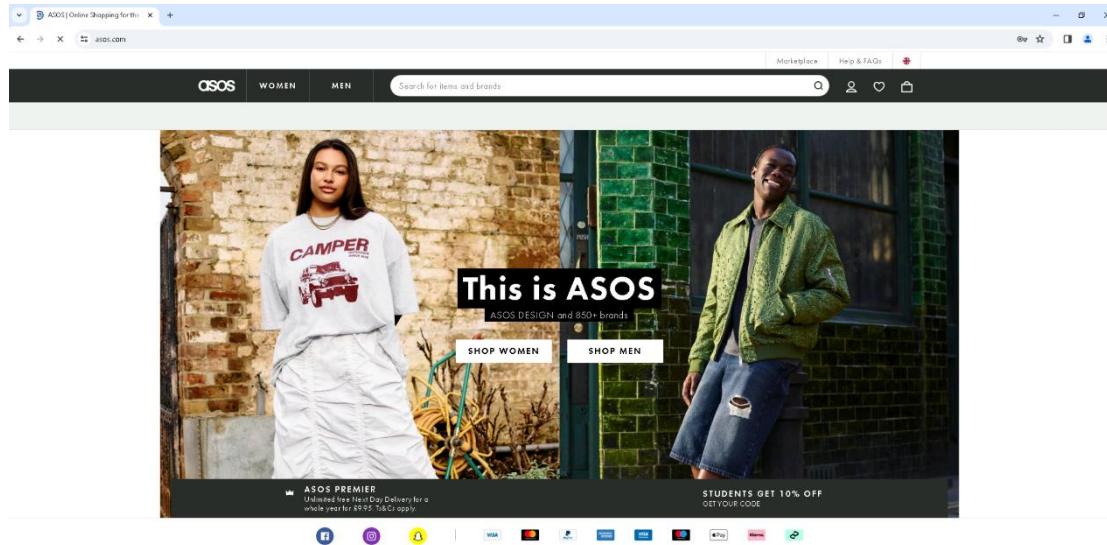
### Web Filter Block Override

Please contact your administrator to gain access to the web page.

Username:

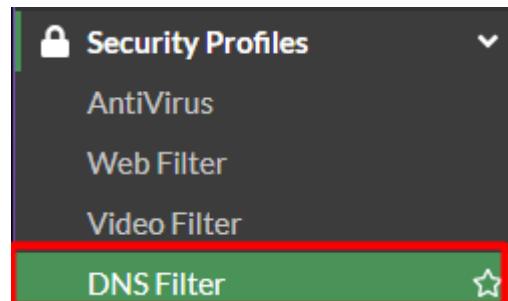
Password:

ונראה ישיר שאנו חסן בדף



# DNS-Profile

דבר ראשון שנעשה, הוא יצירתו של פרופיל פילטר חדש DNS Filter זה נוצר אל Security Profiles



לחץ על Create New

Create New

ונתן לו את השם הנדרש מאייתנו בהנחיות הפרויקט

Name	Office_DNS_Filter
Comments	Comments 0/255
Redirect botnet C&C requests to Block Portal	<input checked="" type="checkbox"/>
Enforce 'Safe Search' on Google, Bing, YouTube	<input checked="" type="checkbox"/>

## הפעלת חסימה לאתרים ודומיינים מסווג C&C

נתחיל מההסבר מה אלה בקשות C&C

בוטנט C&C, זה בעצם מרכז של מוחשבים נגועים בתוכנות זדונית, המרכז מבנה שני רכיבים עיקריים, השרת, והבוטים. שרת C&C יכול לשמש את התקוף למטרות זדוניות רבות כגון גניבת נתונים, הפצת תוכנות זדוניות נוספות, ועוד.

בכדי לחסום בקשות C&C נדרש להפעיל את אופציה זו

Name	Office_DNS_Filter
Comments	Comments 0/255
Redirect botnet C&C requests to Block Portal	<input checked="" type="checkbox"/>
Enforce 'Safe Search' on Google, Bing, YouTube	<input type="checkbox"/>

כעת נבצע חסימה לדומיין ספציפי, נתחל בעמוד הבא למען הסדר הטוב.

## חסימה של דומיין ספציפי

ובצע חסימה לYouTube

נפעיל את Domain Filter

Domain Filter <input checked="" type="checkbox"/>			
<a href="#">+Create New</a>		<a href="#">Edit</a>	<a href="#">Delete</a>
Domain	Type	Action	Status
No results			
0			

ונלחץ על Create New

[+Create New](#)

ובצע חסימה לכל הכתובות השיכות לYouTube

Create Domain Filter

Domain	<input type="text" value=".youtube.com"/>
Type	<input type="radio"/> Simple <input type="radio"/> Reg. Expression <input checked="" type="radio"/> Wildcard
Action	<input checked="" type="radio"/> Redirect to Block Portal <input type="radio"/> Allow <input type="radio"/> Monitor
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

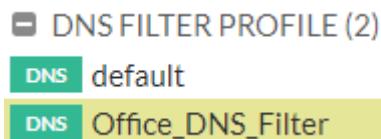
כעת בשביל להחיל את ההגדרות שביצענו, ניתן את dns filter אל TrafficOut

על רק את Firewall Policy



על רק אל dns filter, וניתן לו את dns filter

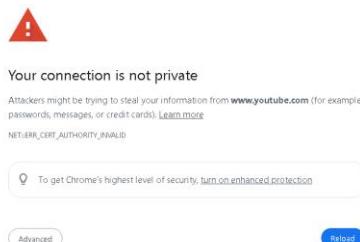
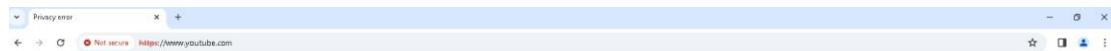
TrafficOut	all	all	always	ALL	ACCEPT	Enabled	AV default	WEB Office_Web_Filter	IPS default	SSL Office_To_Internet_Inspection	UTM	151.43 kB



TrafficOut	all	all	always	ALL	ACCEPT	Enabled	AV default	WEB Office_Web_Filter	DNS Office_DNS_Filter	IPS default	SSL Office_To_Internet_Inspection	UTM	151.43 kB

כעת נודא שהכל עובד

כעת שנכננו ליטוב, זה לא יכנס לנו



ושננסה לעשות פינג לאתר C&C הוא יפנה אותנו לכתובת הדיפולית של פורטי

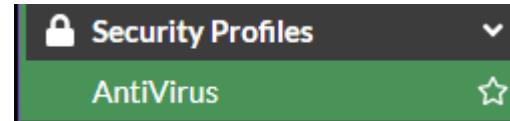
```
Pinging CATSDEGREE.COM [208.91.112.55] with 32 bytes of data:  
Reply from 208.91.112.55: bytes=32 time=3ms TTL=54  
Reply from 208.91.112.55: bytes=32 time=3ms TTL=54  
Reply from 208.91.112.55: bytes=32 time=3ms TTL=54  
Reply from 208.91.112.55: bytes=32 time=3ms TTL=54
```



# Anti-Virus Profile

יצירת פרופיל חדש

נplr אל Security Profiles ואז אל AntiVirus



לאחר מכן נלחץ על Create New

Create New

וניתן לו את השם שנדרש מאיינו, בנוסף לזה עשיית שיחסום כל מה שנראה כמו וירוס, ושיסתכל על כל ה프וטוקולים שהוא מציע

Name	Office_AV_Profile
Comments	Write a comment... 0/255
AntiVirus scan	<input checked="" type="checkbox"/> Block <input type="checkbox"/> Monitor
Feature set	<input checked="" type="radio"/> Flow-based <input type="radio"/> Proxy-based
Inspected Protocols	
HTTP	<input checked="" type="checkbox"/>
SMTP	<input checked="" type="checkbox"/>
POP3	<input checked="" type="checkbox"/>
IMAP	<input checked="" type="checkbox"/>
FTP	<input checked="" type="checkbox"/>
CIFS	<input checked="" type="checkbox"/>

כעת הכתני קובץ לינקם PDF בדרכיב, שאוכל לבדוק אותו ב-RDP

<https://wildfire.paloaltonetworks.com/publicapi/test/apk>

<https://wildfire.paloaltonetworks.com/publicapi/test/macos>

<http://wildfire.paloaltonetworks.com/publicapi/test/apk>

<http://wildfire.paloaltonetworks.com/publicapi/test/macos>



## High Security Alert

You are not permitted to download the file "wildfire-test-apk-file.apk" because it is infected with the virus "Android/PaloAlto\_Test\_Apk\_File".

URL <https://wildfire.paloaltonetworks.com/publicapi/test/apk>

Quarantined File Name [disabled]

Reference URL [http://www.fortinet.com/v?vn=Android%2FPaloAlto\\_Test\\_Apk\\_File](http://www.fortinet.com/v?vn=Android%2FPaloAlto_Test_Apk_File)



## High Security Alert

You are not permitted to download the file "wildfire-test-apk-file.apk" because it is infected with the virus "Android/PaloAlto\_Test\_Apk\_File".

URL <http://wildfire.paloaltonetworks.com/publicapi/test/apk>

Quarantined File Name [disabled]

Reference URL [http://www.fortinet.com/v?vn=Android%2FPaloAlto\\_Test\\_Apk\\_File](http://www.fortinet.com/v?vn=Android%2FPaloAlto_Test_Apk_File)

כעת נמшир בקובץ MACOS גם בזקוק <http://wildfire.paloaltonetworks.com/publicapi/test/macos>



## High Security Alert

You are not permitted to download the file "wildfire-test-macos-file" because it is infected with the virus "Riskware/WildFireTestFile".

URL

<https://wildfire.paloaltonetworks.com/publicapi/test/macos>

Quarantined File Name [disabled]

Reference URL

[http://www.fortinet.com/ve?  
vn=Riskware%2FWildFireTestFile](http://www.fortinet.com/ve?vn=Riskware%2FWildFireTestFile)



## High Security Alert

You are not permitted to download the file "wildfire-test-macos-file" because it is infected with the virus "Riskware/WildFireTestFile".

URL

<http://wildfire.paloaltonetworks.com/publicapi/test/macos>

Quarantined File Name [disabled]

Reference URL

[http://www.fortinet.com/ve?  
vn=Riskware%2FWildFireTestFile](http://www.fortinet.com/ve?vn=Riskware%2FWildFireTestFile)

## כעת נבדוק בלוגים

Date/Time	Action	Service	Source	File Name	Virus/Botnet	User	Details	Action
2024/02/26 17:23:42	Blocked	HTTP	10.44.11.200	wildfire-test-macos-file	Riskware/WildFire...		URL: http://wildfire.paloaltonetworks.com/publicapi/test/macos	Blocked
2024/02/26 17:23:38	Blocked	HTTP	10.44.11.200	wildfire-test-macos-file	Riskware/WildFire...		URL: http://wildfire.paloaltonetworks.com/publicapi/test/macos	Blocked
2024/02/26 17:23:34	Blocked	HTTP	10.44.11.200	wildfire-test-apk-file.apk	Android/PaloAlto_T...		URL: http://wildfire.paloaltonetworks.com/publicapi/test/apk	Blocked
2024/02/26 17:23:29	Blocked	HTTPS	10.44.11.200	wildfire-test-apk-file.apk	Android/PaloAlto_T...		URL: https://wildfire.paloaltonetworks.com/publicapi/test/apk	Blocked

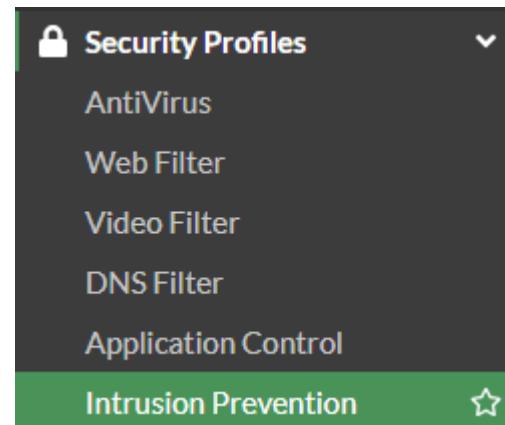
ונראה שהכל נחסם כראוי

# IPS-Profile

IPS או Intrusion prevention היא מערכת אבטחה שטטרתית לזיהות ולמנוע התקפות רשות על התקני רשת שלך. היא עשויה זאת על ידי ניתוח תעבורת רשת וחיפוש אחר דפוסים חדשניים שעשוים להציג על התקפה.

## יצירת פרופיל IPS וחסימת IP שמזההים כBotnet & C&C

כעת נוצר פרופיל IPS לפי דרישות הפרויקט, נכנו אל Security Profiles ואז אל Prevention



ונלץ על התקפה.

Create New

+ Create New

Name	Office_IPS_Profile
Comments	Write a comment... 0/255
Block malicious URLs	<input checked="" type="checkbox"/>

IPS Signatures and Filters

<a href="#">+ Create New</a>	<a href="#">Edit</a>	<a href="#">Delete</a>	
Details	Exempt IPs	Action	Packet Logging
No results			
0			

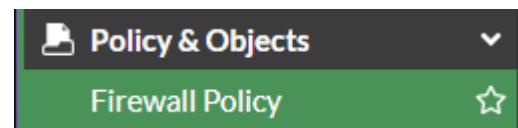
Botnet C&C

Scan Outgoing Connections to Botnet Sites [Disable](#) [Block](#) [Monitor](#)

1833 IP Addresses in botnet package.

כעת בשביל להחיל את כל ההגדרות הללו

ນלך אל Firewall Policy



TrafficOut	all	all	always	ALL	ACCEPT	Enabled	AV default	WEB Office_Web_Filter	DNS Office_DNS_Filter	IPS default	SSL Office_To_Internet_Inspection	UTM	11.74 MB

ונבחר בפרופיל IPS שלנו

#### IPS SENSOR (9)

- IPS all\_default
- IPS all\_default\_pass
- IPS default
- IPS high\_security
- IPS Office\_IPS\_Profile
- IPS protect\_client
- IPS protect\_email\_server
- IPS protect\_http\_server
- IPS wifi-default

## כעת נלך לסתם כתובות מתחום Botnet Packages ונכנסו לו לאתר

The screenshot shows a web-based interface for managing network security policies. On the left, there's a sidebar with sections for 'Name' (Office\_IPS\_Profile), 'Comments' (Write a comment...), and 'Block malicious URLs'. Below these are sections for 'IPS Signatures and Filters' (with 'Create New', 'Edit', and 'Delete' buttons) and 'Botnet C&C' (with 'Scan Outgoing Connections to Botnet Sites', 'Disable', 'Block', and 'Monitor' buttons). A message '1833 IP Addresses in botnet package.' is displayed. On the right, a large table lists various IP addresses, their ports, protocols, and associated names. One row, '5.42.65.1', is highlighted with a red border.

IP	Port	Protocol	Name
1.195.16.247	18,186	TCP	KillNet
1.196.159.155	18,186	TCP	KillNet
1.198.98.106	18,186	TCP	KillNet
1.221.173.148	4,145	TCP	KillNet
3.112.165.123	80	TCP	FormBook
3.141.13.98	5,678	TCP	KillNet
5.2.69.14	443	TCP	Volexity
5.2.200.203	1,080	TCP	KillNet
5.8.18.240	80	TCP	BloodyGang
5.8.33.147	80	TCP	R1Soft.SBM.Exploit
5.17.89.13	4,145	TCP	KillNet
5.42.64.13	80	TCP	Raccoon
5.42.65.1	80	TCP	Amadey

ונראה שלא עובד



ונראה גם בלוג, שלא עובד

The screenshot shows a network log viewer with tabs for 'Summary' and 'Logs'. The 'Logs' tab is selected. The log table has columns for Date/Time, Severity, Source, Protocol, User, Action, Count, and Attack Name. Two entries are listed:

Date/Time	Severity	Source	Protocol	User	Action	Count	Attack Name
2024/02/26 17:41:20	██████	10.44.11.200	6		dropped		Amadey
2024/02/26 17:41:20	██████	10.44.11.200	6		dropped		Amadey

# Application-Control

Application Control נועד למטרה להגן על הרשת מפני איומים מתקדמים המנצלים יישומים פגיעים. מערכת זו מאפשרת לך להציג בקלות כלים מפורטים שיאפשרו או יחסמו תובורה עבור יישומים ספציפיים, תוך ניתוח מיידי של פעילותם לזרחי התנהלות חשודה.

יצירת פרופיל וחסימת TeamViewer

בכדי ליצור פרופיל App Control נכנס אל Security Profiles ואז אל



ואז נלחץ Create New



נקרא לו בשם המתבקש בפרויקט

Name

כעת נשים את TeamViewer

ולך אל "Application and Filter Overrides"

Create New

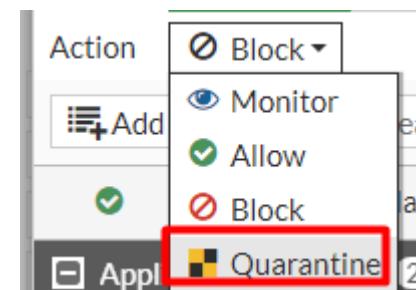
Application and Filter Overrides			
<a href="#">Create New</a> <a href="#">Edit</a> <a href="#">Delete</a>			
Priority	Details	Type	Action
No results			
0			

## כעת נסיף את TeamViewer

Selected 0 All Cloud

	Name	Category	Technology	Popularity	Risk
<b>Application Signature 3/2413</b>					
	Teamviewer	Remote.Access	Client-Server	★★★★★	██████
	Teamviewer_CallReceive	Remote.Access	Client-Server	★★★★★	██████
	Teamviewer_CallRequest	Remote.Access	Client-Server	★★★★★	██████

כעת נעביר מה שזה יעשה, זה ינתק לעובד את הגישה לרשות לגמרי



וhtonksh מאייתנו לשים ליוםים בידוד

Action Quarantine (Expires 2 Day(s))

כעת נלך אל FireWall Policy

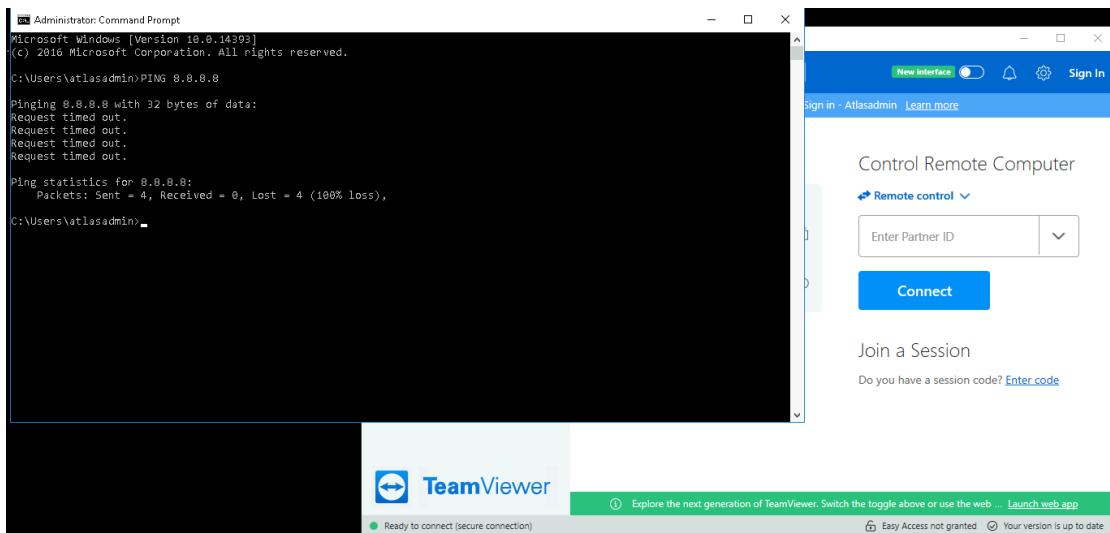


נשים את הprofil שיצרנו

### APPLICATION CONTROL (4)

- APP block-high-risk
- APP default
- APP **Office\_Application\_Control** (highlighted with a red box)
- APP wifi-default

כעת לאחר שנפתח TeamViewer, לא יהיה לנו אינטרנט



ונitinן לראות גם בלוג, שנחסמנו

Date/Time	Source	Destination	Application Name	Action	Application User	Application Details
2024/02/26 17:53:03	10.44.11.200	20.49.104.23 (waws-prod-blu-231-e73a.eastus.cloudapp.azure.com)	TeamViewer	Block		
2024/02/26 17:53:03	10.44.11.200	20.49.104.23 (waws-prod-blu-231-e73a.eastus.cloudapp.azure.com)	TeamViewer	Block		

נכנו אל Dashboard לאחר מכן אל Users & Devices

Dashboard

Status

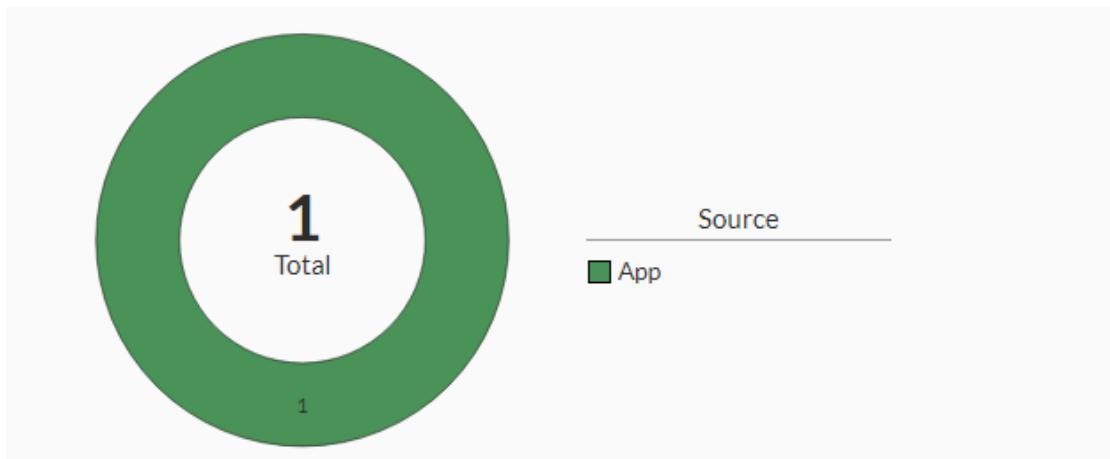
Security

Network

Users & Devices

ואם נכנו אל Quarantine

Quarantine



וניתן לראות מפה לכמה זמן נחסמנו

Quarantine

Source

App

No results

Create New | Delete | Remove All | Search |  q

Details	Device	Source	Expires	Description
Banned IP	10.44.11.200	App	1 day(s) and 23 hour(s)	