



FORTINET



FULL NAME: ALEXANDER CHAIT

TZ:

EDUCATOR: YOSSI BARUCH-EL

DATE:

03.01.2024

קורס למחנכים בסיבר

CSPP

מבואות סיבר

ניהול רשתות ובקר SOC

FortiGate Project

Tables Of Content

You can click on the desired number to get to its corresponding page

<u>User Management</u>	1
<u>Password Policy</u>	8
<u>VPN Configuration</u>	9
<u>VIP Configuration</u>	25
<u>IP-Sec</u>	28
<u>Inspection</u>	35
<u>Web-Filter</u>	38
<u>DNS-Filter</u>	44
<u>Antivirus-Profile</u>	46
<u>IPS-Profile</u>	48
<u>Application Control</u>	51

Part 1: User Management

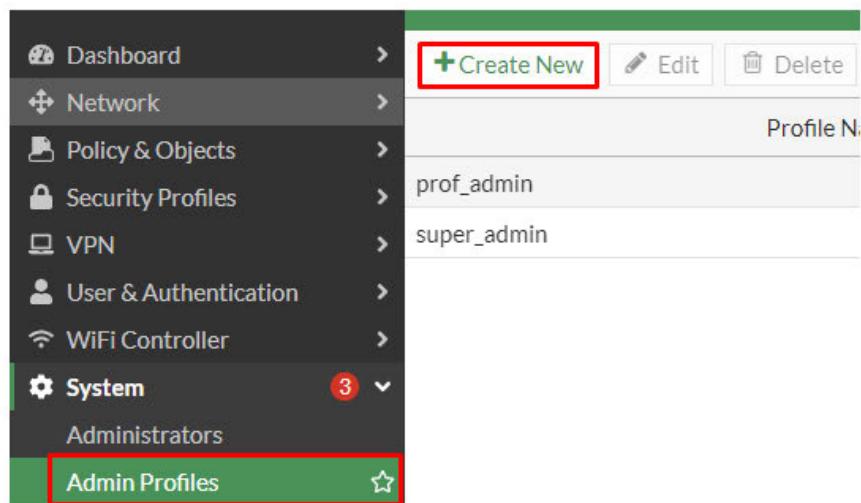
User management in FortiGate involves verifying user identities, defining access policies, enforcing security measures, monitoring user activity, and centralized administration.

It ensures secure and controlled access to network resources for authorized users.

In order to connect to the FortiGate dash board I'll enter the WAN IP

I'll start by creating a new profile named Bozo_Admin, this profile will have super_admin level permissions

I'll go in to System & Admin Profiles and click Create New



I'll give Bozo_Admin super_admin permissions

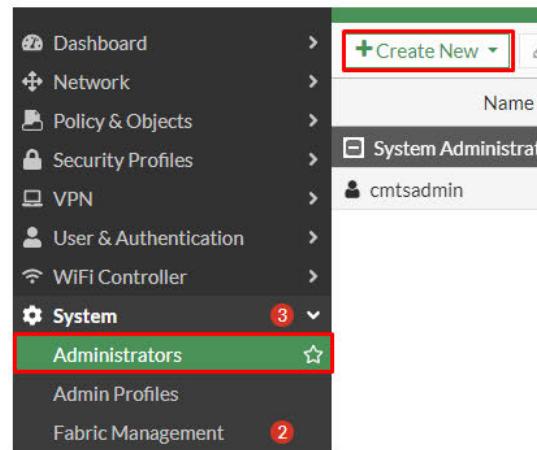
Name	Bozo_Admin		
Comments	0/255		
Access Permissions			
Access Control	Permissions	Set All ▾	
Security Fabric	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="checkbox"/> Read/Write		
FortiView	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="checkbox"/> Read/Write		
User & Device	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="checkbox"/> Read/Write		
Firewall	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="checkbox"/> Read/Write	<input checked="" type="checkbox"/> Custom	
Log & Report	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="checkbox"/> Read/Write	<input checked="" type="checkbox"/> Custom	
Network	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="checkbox"/> Read/Write	<input checked="" type="checkbox"/> Custom	
System	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="checkbox"/> Read/Write	<input checked="" type="checkbox"/> Custom	
Security Profile	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="checkbox"/> Read/Write	<input checked="" type="checkbox"/> Custom	
VPN	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="checkbox"/> Read/Write		
WAN Opt & Cache	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="checkbox"/> Read/Write		
WiFi & Switch	<input type="radio"/> None <input checked="" type="radio"/> Read <input checked="" type="checkbox"/> Read/Write		
Permit usage of CLI diagnostic commands <input checked="" type="checkbox"/>			
<input type="checkbox"/> Override Idle Timeout			

Now we can see that Bozo_Admin is a new profile

Bozo_Admin
prof_admin
super_admin

Next I will create a new User & will give him the new Bozo_Admin profile

Doing this by going to System/Administrators/Create New



Here I'll give the new user bozo, Bozo_Admin permissions

The screenshot shows the "New Administrator" configuration page:

- Username:** Bozo (highlighted with a red box)
- Type:** Local User (highlighted with a green box)
- Password:** (redacted)
- Confirm Password:** (redacted)
- Comments:** Write a comment... (Bozo_Admin)
- Administrator profile:** Bozo_Admin (highlighted with a red box)
- Force Password Change:** Off (radio button)
- Two-factor Authentication:** Off (radio button)
- Restrict login to trusted host:** Off (radio button)
- Restrict admin to guest account:** Off (radio button)

A note at the bottom states: "Password must conform to the following rule" with two options: "8 Minimum length" and "Cannot reuse old passwords".

And we can see that Bozo has the appropriate Profile & permissions

Bozo		Bozo_Admin
cmtsadmin		super_admin

Now I will login with Bozo to check if everything is working properly

The screenshot shows a left sidebar menu and a right-hand list panel. The sidebar includes options like Dashboard, Network, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi Controller, System (selected), Administrators (highlighted in green), Admin Profiles, Fabric Management, Settings, HA, SNMP, Replacement Messages, FortiGuard, Feature Visibility, Certificates, Security Fabric, and Log & Report. The right panel shows a 'System Administrator' list with a single entry: 'Bozo'. A red box highlights the 'Bozo' name in the list.

Bozo is logged in and has all the functions and features that a super_admin has using the new Bozo_Admin profile

Next I'll create a new profile for IT with view only permissions for these interfaces

.Policy, logs, VIPS, interfaces :

I'll go to System/AdminProfiles/Create New & Create a new profile for IT
Named IT_Profile

Name	IT_Profile		
Comments	0/255		
Access Permissions			
Access Control	Permissions Set All ▾		
Security Fabric	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input type="radio"/> Read/Write
FortiView	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input type="radio"/> Read/Write
User & Device	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input type="radio"/> Read/Write
Firewall	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input type="radio"/> Read/Write
Log & Report	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input type="radio"/> Read/Write
Network	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input type="radio"/> Read/Write
System	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input type="radio"/> Read/Write
Security Profile	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input type="radio"/> Read/Write
VPN	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input type="radio"/> Read/Write
WAN Opt & Cache	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input type="radio"/> Read/Write
WiFi & Switch	<input type="radio"/> None	<input checked="" type="radio"/> Read	<input type="radio"/> Read/Write

I gave the new IT_Profile read only permissions for Policy,Logs,VIPs,Interfaces

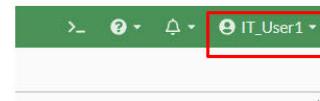
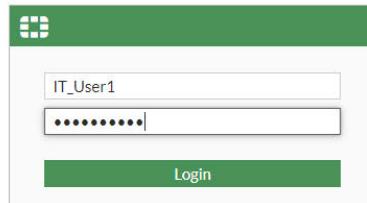
Next step I'll create three new users named IT_User1, IT_User2, IT_User3

The screenshot shows a user creation interface. The 'Username' field contains 'IT_User3'. The 'Type' dropdown is set to 'Local User', with other options like 'Match a user on a remote server group', 'Match all users in a remote server group', and 'Use public key infrastructure (PKI) group' available. The 'Password' and 'Confirm Password' fields both contain masked text. Below these fields is a note: 'Password must conform to the following rules:' followed by two items: '8 Minimum length' and 'Cannot reuse old passwords'. The 'Comments' field has the placeholder 'Write a comment...'. The 'Administrator profile' dropdown is set to 'IT_Profile'. At the bottom, there's a 'Force Password Change' checkbox with an information icon and a toggle switch.

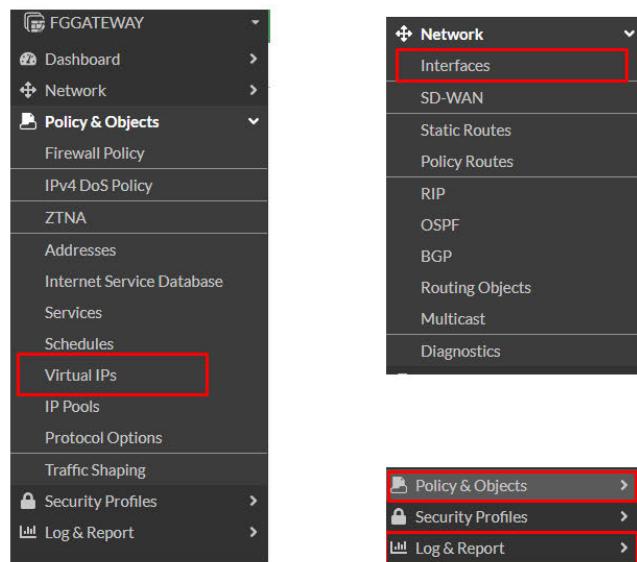
I have created three new users for IT and gave them the IT_Profile permissions

IT_User1		IT_Profile
IT_User2		IT_Profile
IT_User3		IT_Profile

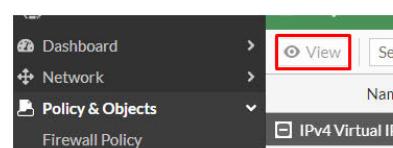
Now I will logon with IT_User1 and check if he only has the View Only permissions for the specific interfaces I've selected



And here we can see that it's working as intended, IT_User1 has read only permissions for Policy,Logs,VIPs,Interfaces



We can see that he has view only permissions



Part 2: Password Policy

A strong password policy for FortiGate management is crucial to prevent unauthorized access.

It's important to protect sensitive information, mitigate threats like brute-force attacks, meet compliance requirements, foster user accountability, and enhance overall security.

Next I will create a new Password Policy that consists of the following Parameters

- At least 8 letters
- At least 2 unique symbols
- At least 2 large letters
- At least 1 small letter
- At least 1 number

I'll go to System/Settings/Password Policy & enter the required parameters & click Apply

Password Policy	
Password scope	Off Admin IPsec Both
Minimum length	8
Minimum number of new characters	0
Character requirements	<input checked="" type="checkbox"/>
Upper case	2
Lower case	1
Numbers (0-9)	1
Special	2
Password expiration	<input type="checkbox"/>

Now my password policy is hardened and my network is safer

Part 3: VPN Configuration

Using a VPN with FortiGate encrypts your internet connection, protecting data from interception. It also masks your IP address for anonymity and enables secure remote access to corporate networks, enhancing overall security.

SSL VPN tunnel mode in FortiGate creates a secure, encrypted connection between a user's device and the corporate network. It encrypts data transmission, ensuring privacy and preventing eavesdropping.

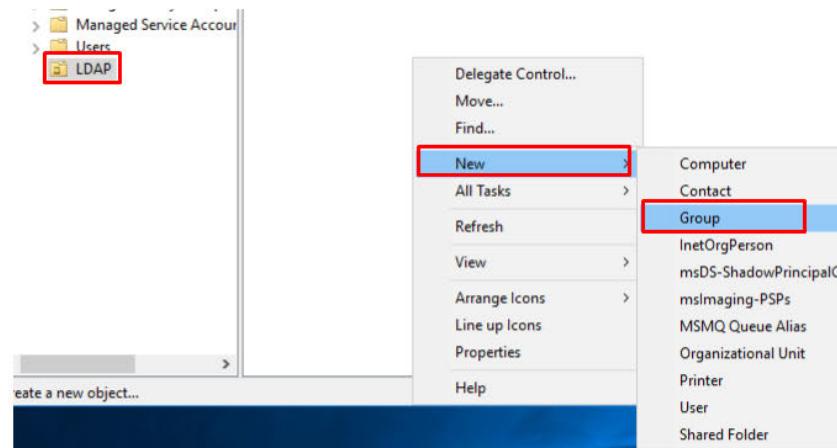
This mode allows secure access to internal resources remotely, enhancing security for remote workers and ensuring confidentiality of sensitive information.

I'll start by configuring SSLVPN Tunnel Mode:

First I'll start a new group named LDAP_Sales in my AD Machine (AtlasAD)
I'll connect to the Atlas_AD using the remote desktop Application



I'll go to Active Directory users & computers and create a new group named LDAP_Sales

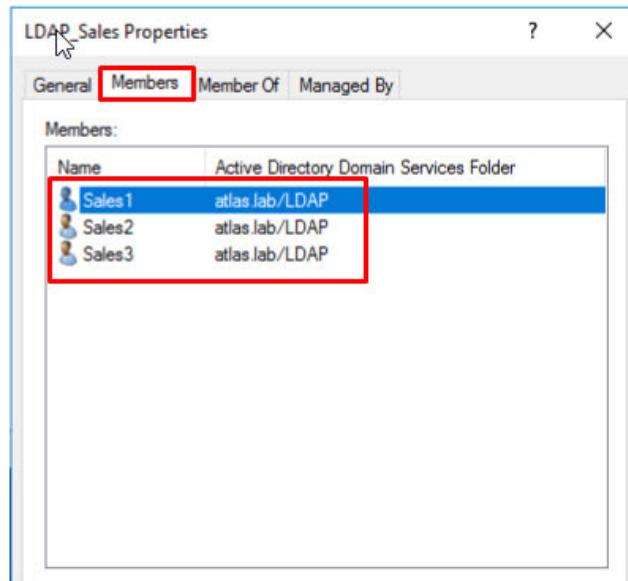


Name	Type	Description
LDAP_Sales	Security Group...	

Now I'll create 3 new users and put them in the LDAP_Sales group

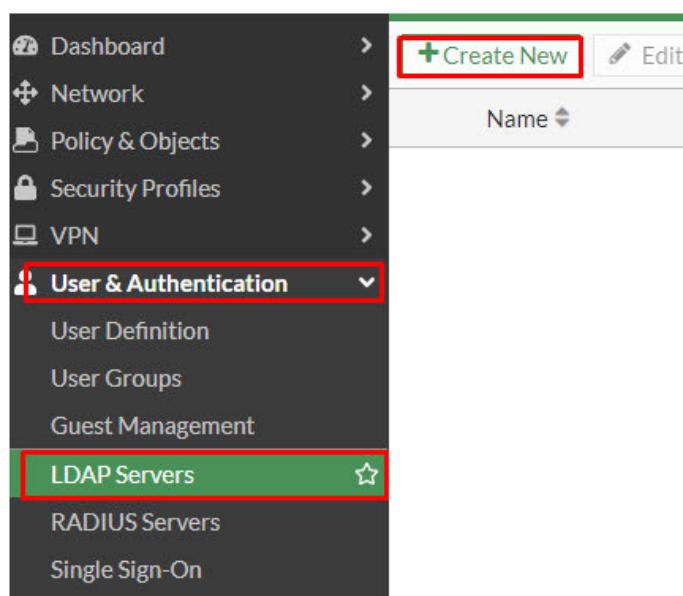
Name	Type	Description
Sales1	User	
Sales2	User	
Sales3	User	

And now we can see that LDAP_Sales group has three new users



Now I'll start configuring LDAP on FG

I'll go to Users & Authentications> LDAP Servers>Create New



I'll enter the relevant information for my LDAP Server

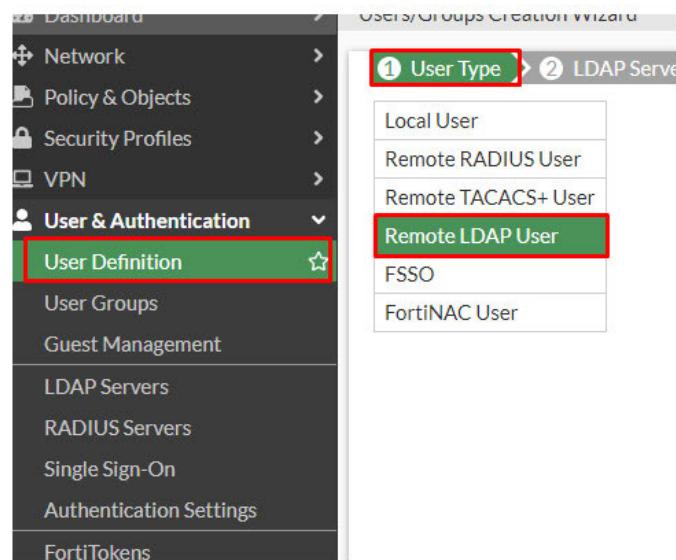
Edit LDAP Server

Name	LDAP
Server IP/Name	10.76.11.200
Server Port	389
Common Name Identifier	cn
Distinguished Name	dc=atlas,dc=lab
Exchange server	<input type="checkbox"/>
Bind Type	Simple <input type="radio"/> Anonymous <input checked="" type="radio"/> Regular
Username	atlasadmin@atlas.lab
Password	***** <input type="password"/>
Secure Connection	<input type="checkbox"/>
<input type="button" value="Test Connectivity"/>	
<input type="button" value="Test User Credentials"/>	

Now I have connection to the LDAP server

Name	LDAP
Server IP/Name	10.76.11.200
Server Port	389
Common Name Identifier	cn
Distinguished Name	dc=atlas,dc=lab
Exchange server	<input type="checkbox"/>
Bind Type	Simple <input type="radio"/> Anonymous <input checked="" type="radio"/> Regular
Username	atlasadmin@atlas.lab
Password	***** <input type="password"/> Change
Secure Connection	<input type="checkbox"/>
Connection status	Successful
<input type="button" value="Test Connectivity"/>	
<input type="button" value="Test User Credentials"/>	

Next I'll go to LDAP User Creation & select Remote LDAP User



Select the appropriate server



Now I'll be adding the 3 Sales users to be Remote Users

The screenshot shows the LDAP search results for the 'Sales' users. The results table has columns for ID and Name. The rows for 'Sales1', 'Sales2', and 'Sales3' are highlighted with a red box. Below the table, there are buttons for '+ Add Selected' and '- Remove Selected'.

ID	Name
Sales1	Sales1
Sales2	Sales2
Sales3	Sales3

We can see them Active as LDAP

Name	Type
Sales1	LDAP
Sales2	LDAP
Sales3	LDAP
guest	LOCAL

I'll also create more users using a script that I'll put in the C drive on the AtlasAD
This method is easier and way faster for bulk creating users

```

1 New-ADOrganizationalUnit -Name "FG-Users" -Path "DC=atlas,DC=lab"
2 $Users = Import-Csv -Path "C:\UserList.csv"
3 foreach ($User in $Users)
4 {
5     $DisplayName = $User.'Firstname' + " " + $User.'Lastname'
6     $UserFirstname = $User.'Firstname'
7     $UserLastname = $User.'Lastname'
8     $OU = $User.'OU'
9     $SAM = $User.'SAM'
10    $UPN = $User.'SAM' + "@" + $User.'Maildomain'
11    $Description = $User.'Description'
12    $Password = $User.'Password'
13    $Server = 'atlas.lab'
14    New-ADUser -Name "$DisplayName" -DisplayName "$DisplayName" -
15

```

Albert Einstein	LDAP
DefaultAccount	LDAP
Dudu Aharon	LDAP
Eyal Golan	LDAP
Guest	LDAP
Johann Sebastian Bach	LDAP
Leonardo Da Vinci	LDAP
Mc Manzur	LDAP
Pablo Picasso	LDAP
Salvador Dali	LDAP

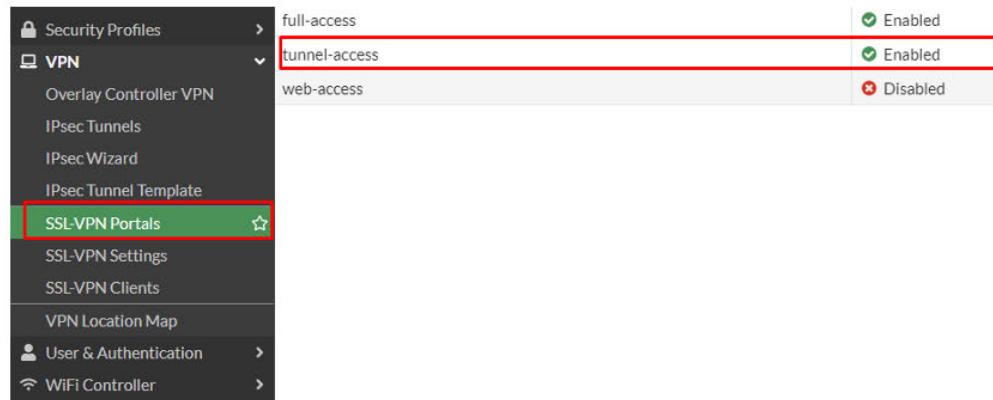
Name	Type
Albert Einstein	User
Dudu Aharon	User
Eyal Golan	User
Johann Sebastian Bach	User
Leonardo Da Vinci	User
Mc Manzur	User
Pablo Picasso	User
Salvador Dali	User
Vincent Van Gogh	User
Wolfgang Amadeus Mozart	User

I'll add them to the LDAP_Sales Group as well

In the next step I'll configure a new SSLVPN Tunnel Portal & than I'll configure a separate web access portal

- Tunnel Access: Provides full network access to remote users, allowing them to access resources as if they were physically connected to the network.
- Web Access: Offers limited access to specific web-based applications or services without providing full network access. Typically used for accessing web-based tools or services securely.

VPN>SSLVPN>Tunnel Access



I'll also give the a source IP Pool

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 policy will be directed over the SSL-VPN tunnel.

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

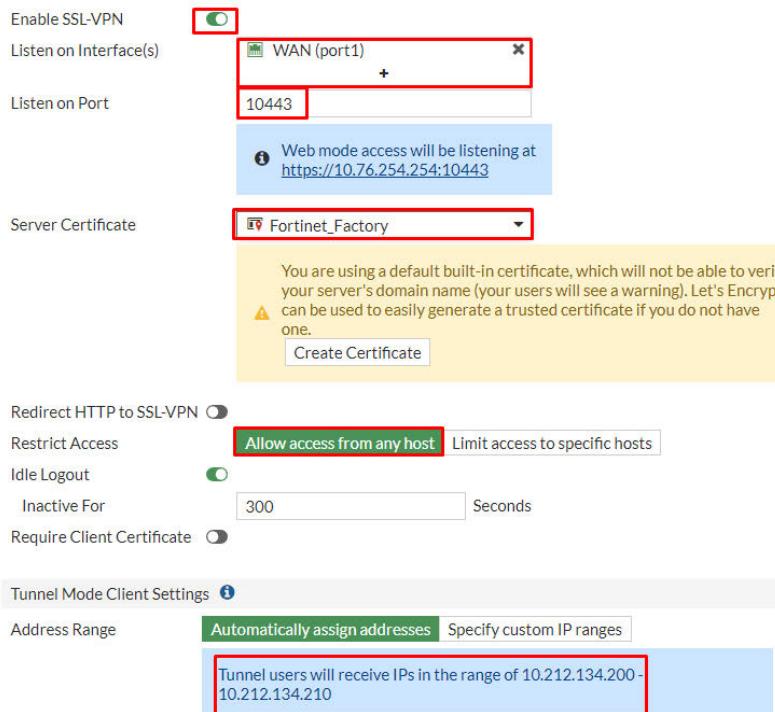
Routing Address Override:

Source IP Pools: SSLVPN_TUNNEL_ADDR1

Tunnel Mode Client Options

Allow client to save password

Next I will go the the SSL-VPN Settings & configure to enable & listen on Port 10433
Also to allow access from any host



Now I'll give the LDAP_Sales group the tunnel-access portal



Now I'll configure the IP range by going to VPN>SSLVPN Portal>Tunnel Access

New Address

Name	Net_10.189.1.0
Color	<input type="button" value="Change"/>
Type	Subnet
IP/Netmask	10.189.1.0/24
Interface	<input type="button" value="LAN (port2)"/>
Static route configuration	<input type="checkbox"/>

Routing Address Override

Net_10.189.1.0	<input type="button" value="X"/>
<input type="button" value="+"/>	

Source IP Pools

SSLVPN_TUNNEL_ADDR1	<input type="button" value="X"/>
<input type="button" value="+"/>	

Go into the VPN settings and configure the connection of the portal with the Users

New Authentication/Portal Mapping

Users/Groups	<input type="button" value="LDAP_Sales"/>	<input type="button" value="X"/>
Portal	tunnel-access	<input type="button" value="▼"/>

Authentication/Portal Mapping	
<input type="button" value="Create New"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Send SSL-V"/>	
Users/Groups	Portal
LDAP_HR	web-access
<input type="button" value="LDAP_Sales"/>	tunnel-access
All Other Users/Groups	web-access

Next step I'll create a new policy

Name	SSL-VPN access
Incoming Interface	SSL-VPN tunnel interface (ssl.root)
Outgoing Interface	LAN (port2)
Source	SSLVPN_TUNNEL_ADDR1 LDAP_Sales
IP/MAC Based Access Control	
Destination	Net_10.189.1.0
Schedule	always
Service	ALL
Action	<input checked="" type="button"/> ACCEPT <input type="button"/> DENY

Now I'll try to connect using FortiClientVPN



I'll name it and put in the public WAN address, Port will be customized

Edit VPN Connection

VPN	SSL-VPN	IPsec VPN	XML
Connection Name	Sales		
Description			
Remote Gateway	20.163.248.237		
	<input checked="" type="checkbox"/> Customize port 9443		
	<input type="checkbox"/> Enable Single Sign On (SSO) for VPN Tunnel		
Client Certificate	None		
Authentication	<input checked="" type="radio"/> Prompt on login <input type="radio"/> Save login <input type="checkbox"/> Enable Dual-stack IPv4/IPv6 address		

Enter the Credentials

VPN Name	Sales
Username	Albert Einstein
Password	*****

Connect

Click Yes on the Security Alert



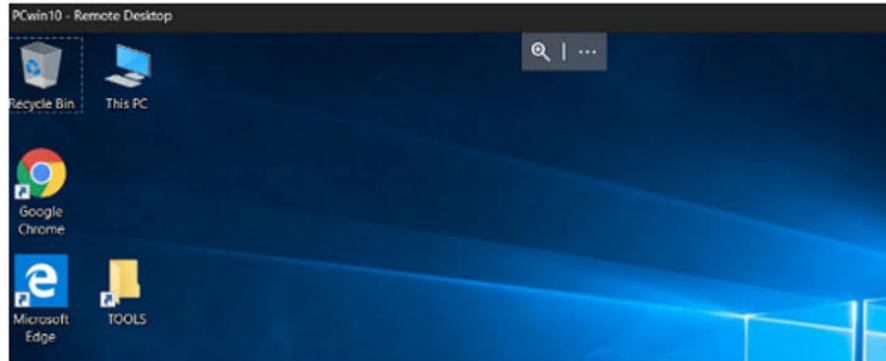
The connection is a success!



VPN Name Sales
IP Address 10.212.134.200
Username Albert Einstein
Duration 00:00:11
Bytes Received 0 KB
Bytes Sent 12.11 KB

Disconnect

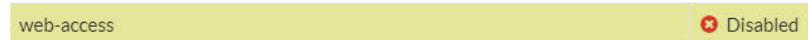
Now I'll test remote desktop connection



Remote is successful!

Next step is the SSLVPN Web Access Mode

I'll create a new Bookmark in the default FortiGate WebAccess Portal

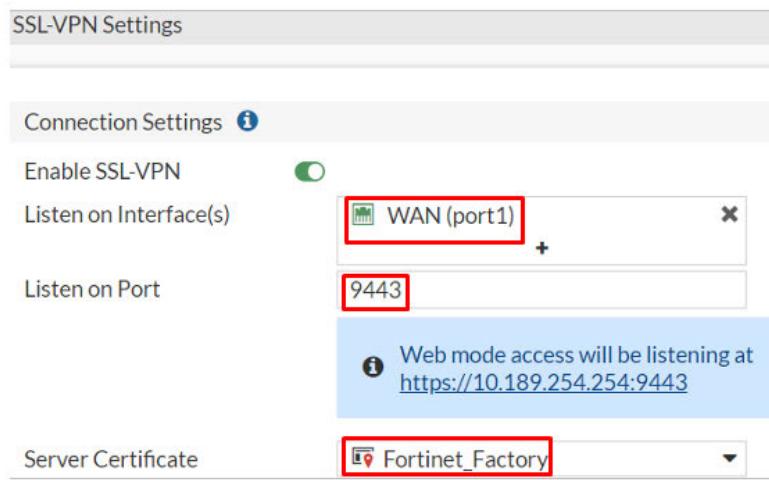


I'll create a new Bookmark using the RDP Type

Predefined Bookmarks

		Create New	 Edit	 Delete
		Name 	Type 	
Name	PC			
Type	RDP			
Host	10.189.1.10			
Port	3389			
Description	PC			
Single Sign-On	<input checked="" type="button" value="Disable"/> <input type="button" value="SSL-VPN Login"/>			
Username				
Password				
Color depth	<input type="radio" value="8 Bit"/> 8 Bit <input checked="" type="radio" value="16 Bit"/> 16 Bit <input type="radio" value="32 Bit"/> 32 Bit			
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"/>			

I'll go to the SSLVPN Settings and configure the fortiGate interface to listen on 9443



Now I'll create a new group named LDAP_HR with three users and attach them to the portal, and another local user named AD_FG for authentication

Edit User Group	
Name	LDAP_HR
Type	Firewall
Members	<ul style="list-style-type: none"> AD_FG Pablo Picasso Salvador Dali Vincent Van Gogh

New Authentication/Portal Mapping	
Users/Groups	<ul style="list-style-type: none"> LDAP_HR
Portal	web-access

Here we can see that LDAP_HR are no using the web-access portal

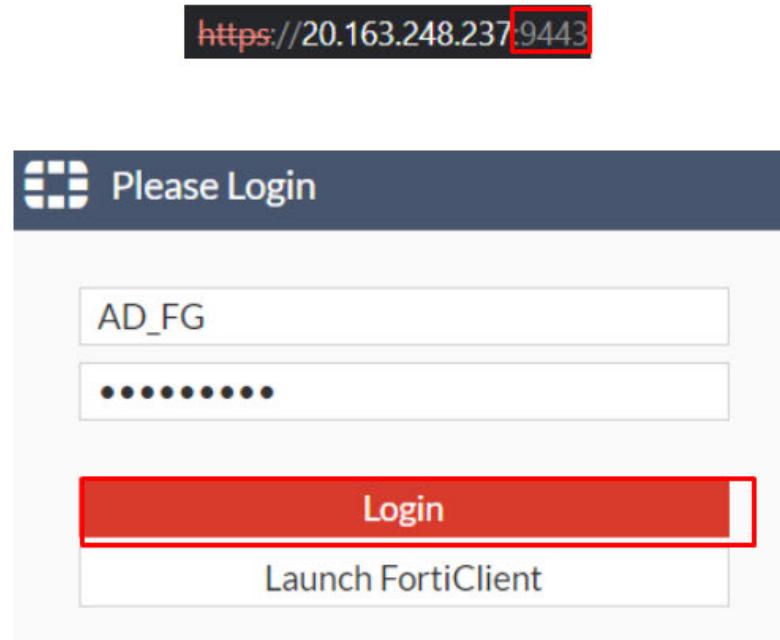
		+ Create New	Edit	Delete	Send SSL-VPN Configuration
Users/Groups		Portal			
	LDAP_HR		web-access		

Now I'll create a policy that will allow a connection to the portal

New Policy

Name	SSL-VPN_Access_WB
Incoming Interface	SSL-VPN tunnel interface (ssl.root)
Outgoing Interface	LAN (port2)
Source	SSLVPN_TUNNEL_ADDR1 LDAP_HR
IP/MAC Based Access Control	
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY

Now I'll test connectivity with a local user to see if it works



I'm in and can see the configured bookmark



SSL-VPN Portal

Download FortiClient ▾

Bookmarks



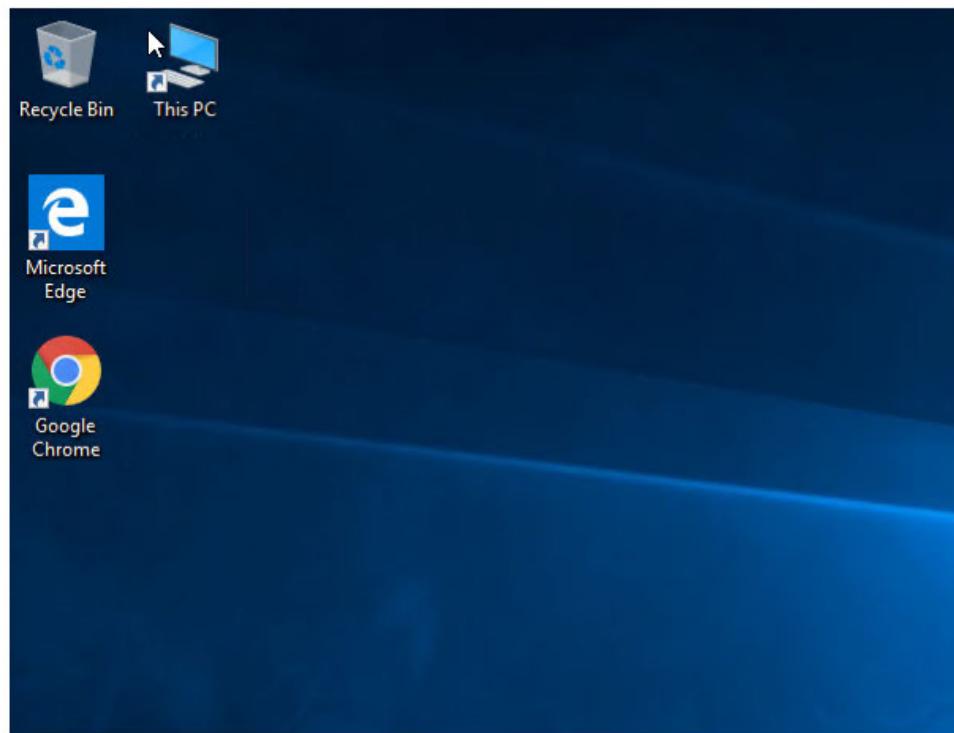
I'll click on it and use the cmtadmin user to get in

Please enter your credential

User name:

Password:

Success!



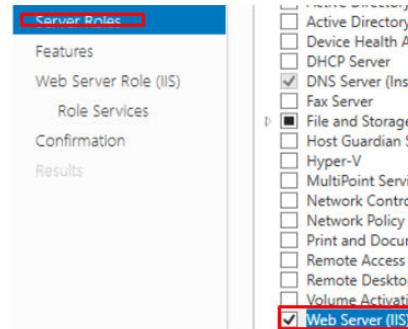
Part 4: VIP

VIP (Virtual IP) in FortiGate lets you map an external IP to an internal resource, making internal servers accessible from the internet without exposing their actual IP addresses.

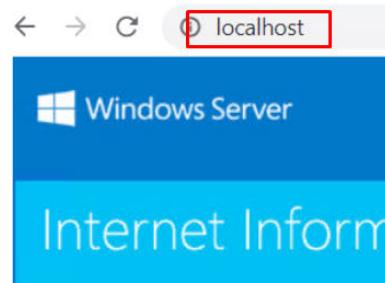
Benefits include server accessibility, load balancing, and enhanced security.

You use VIP for hosting servers, PAT, port forwarding and ensuring high availability. Configure VIP objects, firewall policies, and NAT rules to set it up securely.

I'll start by going the Atlas AD server and installing the IIS feature



After installing I'll check /localhost to see if this worked locally



It works, Now after installing IIS I'll publish a VIP and test if it's possible to reach it from outside network

I'll name the VIP, give it the port that it needs to reach (WAN)

In a normal scenario I'll need to give an external IP but because this is a lab simulation I'll need to give the GWFW address because it maps to the outside address of the WAN.

In a real world scenario this usually be replaced with an ISP given public address
I'll also do Port Forwarding, mapping the external 8080 port to an internal 80 port

Edit Virtual IP

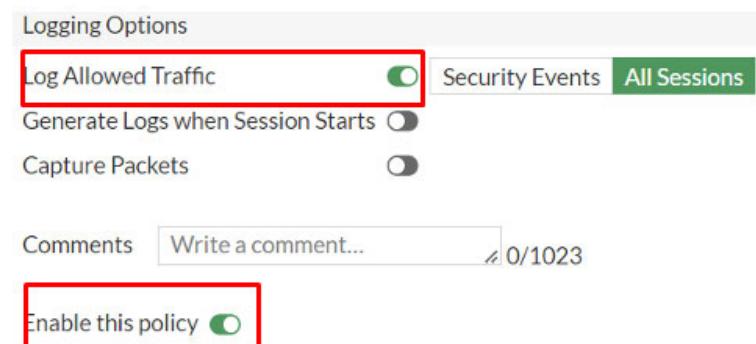
VIP type	IPv4
Name	atlasAD_iis_WB
Comments	Write a comment...
Color	Change
Network	
Interface	WAN (port1)
Type	Static NAT
External IP address/range	10.189.254.254
Map to	IPv4 address/range
	10.189.11.200
Optional Filters	
Port Forwarding	
Protocol	TCP
Port Mapping Type	One to one
External service port	8080
Map to IPv4 port	80

Now I'll create a new policy that will allow traffic to go outside the network

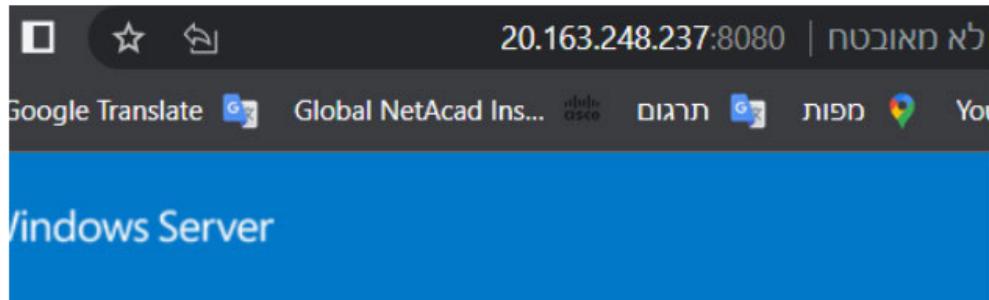
Edit Policy

Name	EXT_TO_AtlasAD_IIS
Incoming Interface	WAN (port1)
Outgoing Interface	LAN (port2)
Source	all
IP/MAC Based Access Control	
Destination	atlasAD_iis_WB
Schedule	always
Service	HTTP
Action	ACCEPT DENY
Inspection Mode <input checked="" type="radio"/> Flow-based <input type="radio"/> Proxy-based	

Additionally I'll enable logs and activate all sessions to make sure that every action is recorded and monitored, this gives more security but also more load on the machine



Now I'll check if outside connectivity is working using the configured 8080 port



Its working!

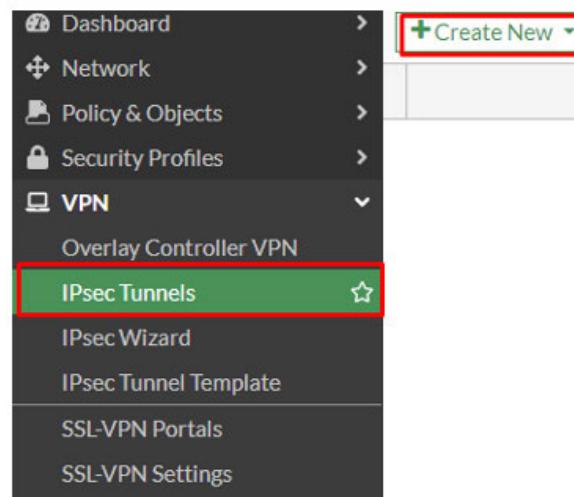
Part 5: IP SEC

IPsec (Internet Protocol Security) is crucial for securing communications over untrusted networks like the internet.

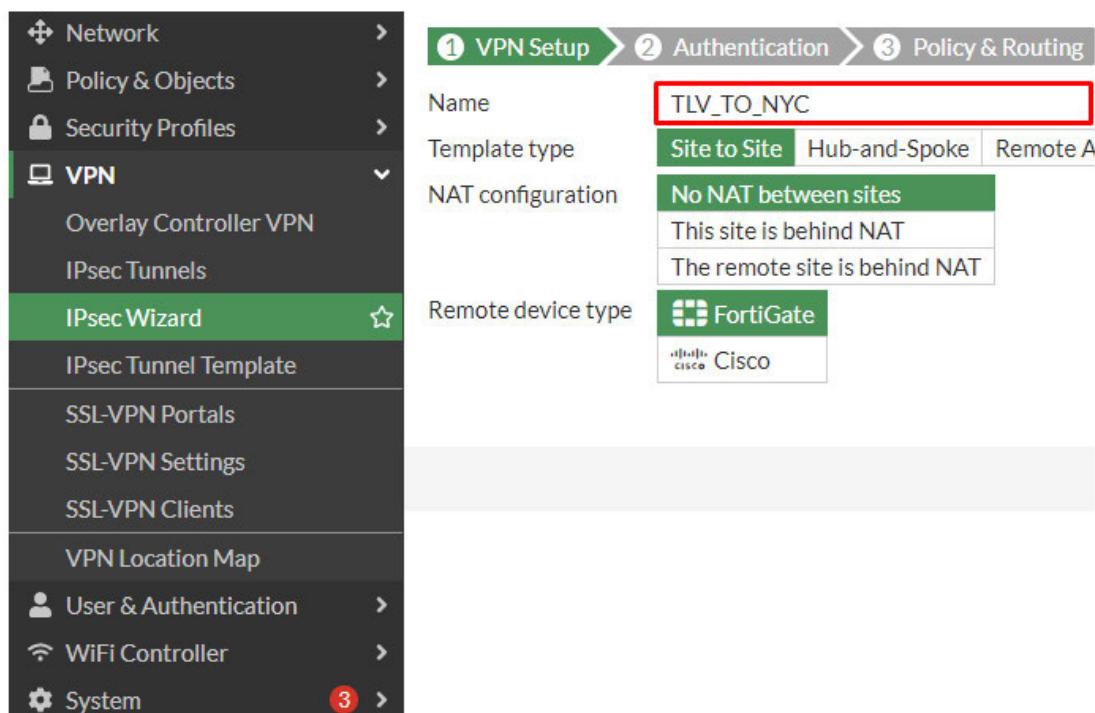
It ensures data confidentiality, integrity, and authentication. IPsec is used for secure remote access, site-to-site connectivity, and offers enhanced security, scalability, cost-effectiveness, flexibility, and interoperability.

I'm going to create an IP SEC connection with another classmate, we'll be synchronizing our actions on both sides.

We'll start by creating a new IPsec tunnel



I'll name it



We'll both use an agreed upon Pre-shared Key on both sides

The screenshot shows the configuration interface for step 2 of the IPsec Wizard. On the left, a sidebar lists various VPN-related options. The 'IPsec Wizard' option is highlighted with a red box. The main panel displays the 'Authentication' configuration steps:

- IP Address:** Dynamic DNS (highlighted with a red box)
- Remote IP address:** 40.71.97.44
- Outgoing Interface:** WAN (port1) (highlighted with a red box)
- Authentication method:** Pre-shared Key (highlighted with a red box)
- Pre-shared key:** A masked password field containing '*****'.

Below the configuration fields, a note states: "Password must conform to the following rules:" followed by a list of eight rules:

- ① Lower Case Letters
- ② Special Characters
- ① Numbers (0-9)
- ② Upper Case Letters
- ⑧ Minimum length
- ~ Cannot reuse old passwords

Now we'll configure both remote and local subnets and select the LAN interface

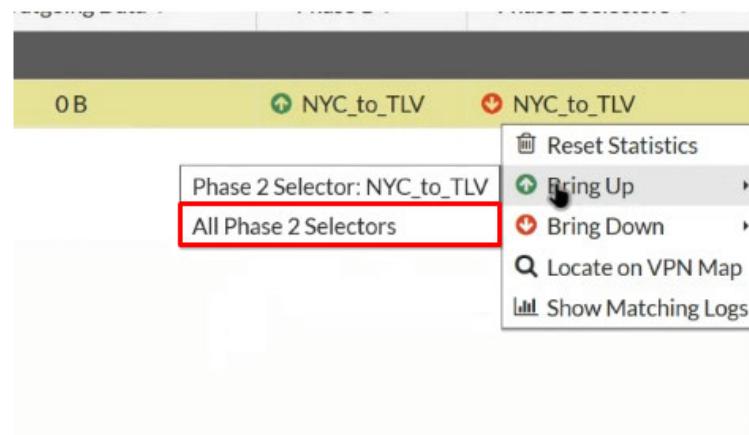
The screenshot shows the configuration interface for step 3 of the IPsec Wizard. The sidebar again highlights the 'IPsec Wizard' option. The main panel displays the 'Policy & Routing' configuration steps:

- Local interface:** LAN (port2)
- Local subnets:** Two entries: 10.171.1.0/24 and 10.171.11.0/24 (both highlighted with a red box).
- Remote Subnets:** Two entries: 10.76.1.0/24 and 10.76.11.0/24 (both highlighted with a red box).
- Internet Access:** Options: None, Share Local, Use Remote (None is selected).

Here we can see the summary of the VPN

Object Summary	
Phase 1 interface	TLV_TO_NYC
Local address group	TLV_TO_NYC_local
Remote address group	TLV_TO_NYC_remote
Phase 2 interface	TLV_TO_NYC
Static route	static
Blackhole route	static
Local to remote policies	vpn_TLV_TO_NYC_local
Remote to local policies	vpn_TLV_TO_NYC_remote

Now we'll bring up Phase 2 Selectors



I'll create a policy that will allow ping

The screenshot shows a configuration window for a firewall policy. On the left, there are several dropdown menus and input fields:

- Name: vpn_NYC_to_TLV_local_0
- Incoming Interface: LAN (port2)
- Outgoing Interface: NYC_to_TLV
- Source: NYC_to_TLV_local
- Destination: NYC_to_TLV_remote
- Schedule: always
- Service: PING
- Action: ACCEPT (selected)

Below these, there are tabs for "Inspection Mode" (Flow-based is selected) and "Firewall/Network Options". To the right, a "Select Entries" dialog box is open, showing a list of entries:

- ping (highlighted with a red border)
- SERVICE (1)
- Network Services (1)
- PING

I'll create a policy that will allow RDP

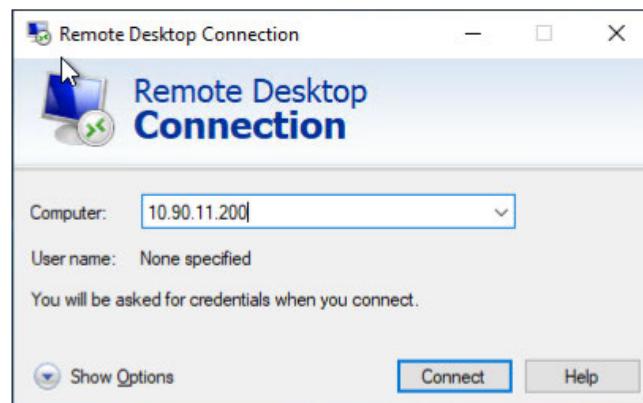
The screenshot shows a configuration window for a firewall policy. On the left, there are several dropdown menus and input fields:

- Name: vpn_NYC_to_TLV_remote_0
- Incoming Interface: NYC_to_TLV
- Outgoing Interface: LAN (port2)
- Source: NYC_to_TLV_remote
- Destination: NYC_to_TLV_local
- Schedule: always
- Service: ALL
- Action: ACCEPT (selected)

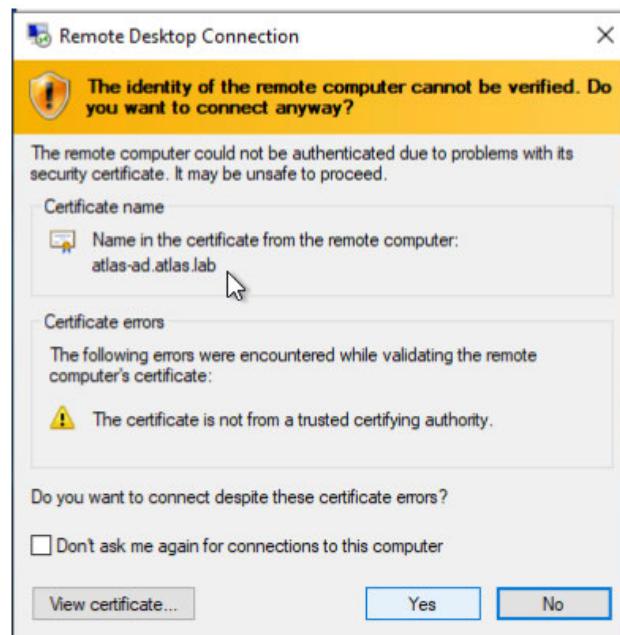
Below these, there are tabs for "Inspection Mode" (Flow-based is selected) and "Firewall/Network Options". Under "Firewall/Network Options", there are sections for NAT (disabled) and Protocol Options (PROT default). To the right, a "Select Entries" dialog box is open, showing a list of entries:

- rdp (highlighted with a red border)
- SERVICE (1)
- Remote Access (1)
- RDP

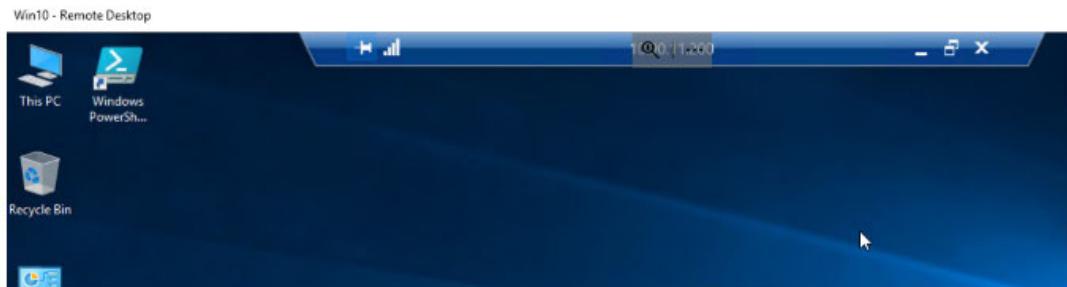
Now I'll test the RDP



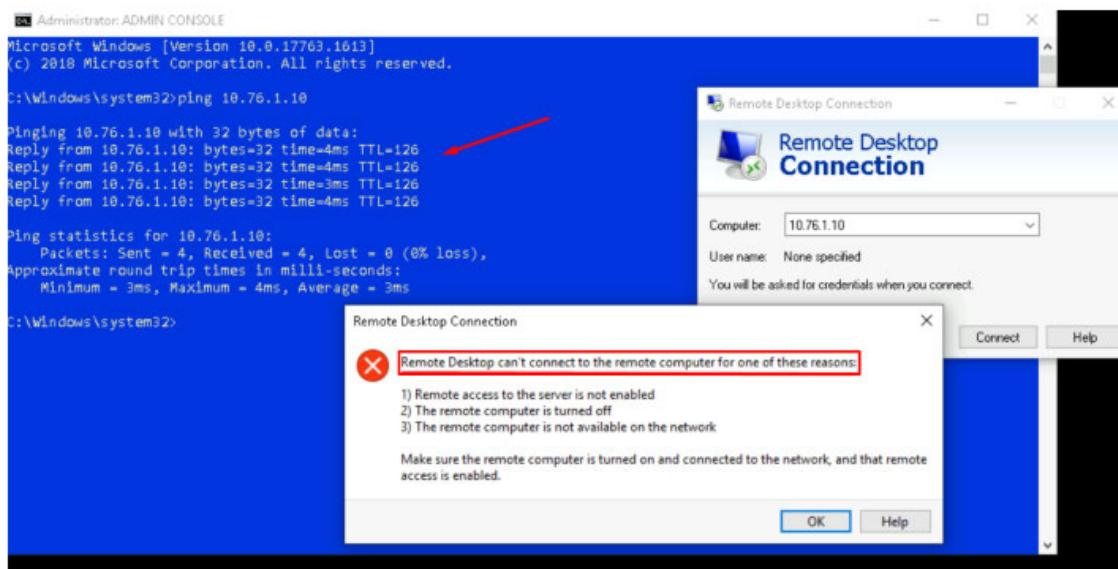
Allow to Proceed



Here we can see that the RDP connection is a success



We can also see that on the other side the user cannot use RDP while he can ping



Part 6: Inspection

Inspection in FortiGate is vital for analyzing network traffic and enforcing security policies.

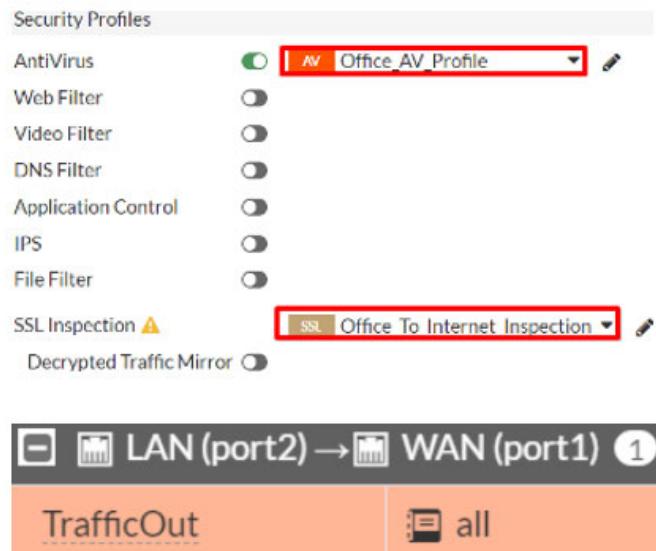
It detects and blocks threats, filters content, controls applications, and ensures compliance. It offers benefits like threat prevention, optimized performance, and customizable security measures.

I'll start by creating a new profile for Inspection, with full SSL inspection mode. I'll select multiple clients, Full SSL Inspection, I'll also download a FortiGate certificate

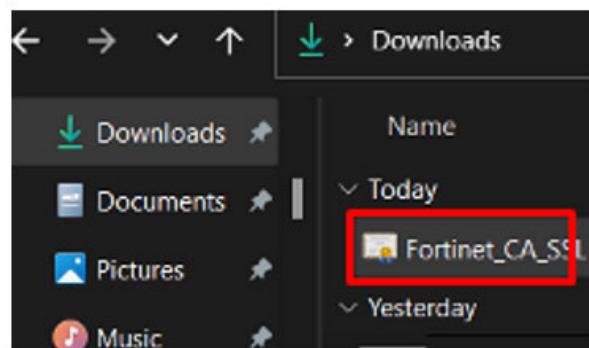
The screenshot shows the configuration of a new SSL/SSH Inspection Profile named "Office_To_Internet_Inspection". The "SSL Inspection Options" section is highlighted, showing the following settings:

- Enable SSL inspection of: **Multiple Clients Connecting to Multiple Servers**
- Protecting SSL Server
- SSL Certificate Inspection: **Full SSL Inspection** (selected)
- CA certificate: **Fortinet_CA_SSL** (selected)
- Blocked certificates: **Allow** (selected)
- Untrusted SSL certificates: **Allow** (selected)
- Server certificate SNI check: **Enable** (selected)

Now I'll go to the firewall policy, and configure the Profile with the existing Traffic Out policy.



Now I'll copy the certificate to windows 10 and install it



Next I'll go to the Certificate Import Wizard and Select local machine

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate lists from your disk to a certificate store.

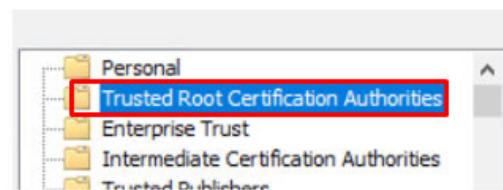
A certificate, which is issued by a certification authority, is a confirmation of the identity of a user or computer and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

Current User
 Local Machine

To continue, click Next.

Select the Trusted Authorities



We can see the Certificate information here

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- 2.23.140.1.2.2

* Refer to the certification authority's statement for details.

Part 7: Web Filter

The web filter feature in FortiGate helps organizations control web traffic by blocking access to inappropriate or malicious websites based on predefined policies.

It enhances security, promotes productivity, ensures compliance, and offers customizable filtering options for tailored control.

Proxy-based filtering in FortiGate routes web traffic through a proxy server for detailed inspection and control. It enhances security by blocking malicious content, improves performance through caching, and offers granular access control.

It ensures compliance and scalability while providing robust protection against web-based threats.

I'll start by creating a new Profile named Office_Web_Filter and make it Proxy Based

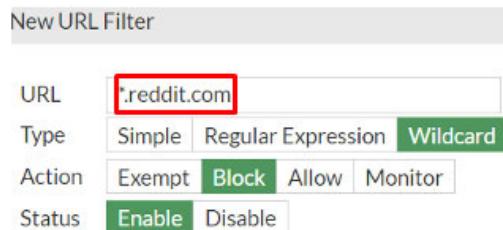
New Web Filter Profile

Name	Office_Web_Filter
Comments	Write a comment...
Feature set	Flow-based Proxy-based

Next I'll deny access to Reddit.com, also to the Shopping and Job Search categories
I'll start by disabling fortyguard filter



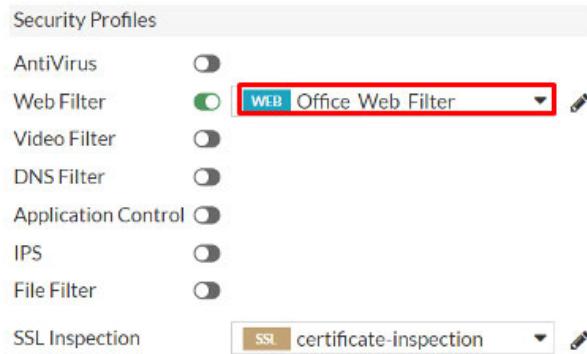
Now I'll put in a URL filter and type in the reddit domain so all variations will be blocked



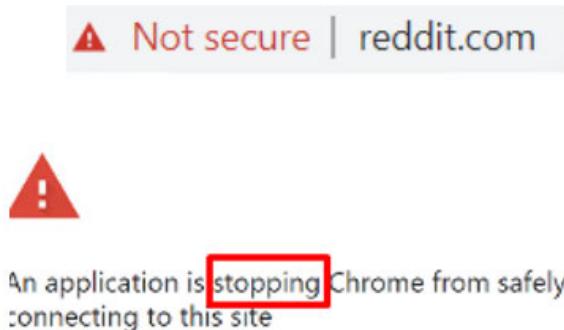
Now I'll go to the traffic out interface and change to proxy based inspection



Now I'll add in the Office_Web_Filter and apply



Let's test with one of the users to see if reddit is blocked



It's blocked, Next step I'll be blocked shopping to everyone but one user
I'll also block job searching for everyone

I'll start by making a group for the one user that will have access to shopping

New User Group

Name	Allow Shopping
Type	Firewall
	Fortinet Single Sign-On (FSSO)
	RADIUS Single Sign-On (RSSO)
	Guest
Members	Albert Einstein x

I'll turn on fortiguard

FortiGuard Category Based Filter

Resize to Contents

Contains Does Not Contain Regex

Job Search	1
Shopping	1

For Shopping we'll select "authenticate" and for Job Searching we'll select "Block"

FortiGuard Category Based Filter

Name	Action
General Interest - Personal 2/35	
Job Search	Block
Shopping	Authenticate

2/93

In the next page I'll select the group that can use shopping

Edit Filter

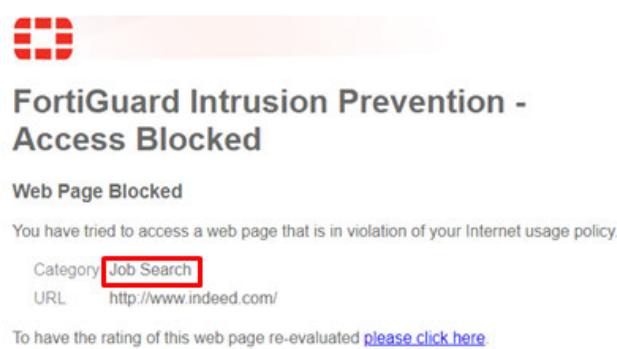
Warning Interval	0	hour(s)	5
Selected User Groups	<input checked="" type="checkbox"/> Allow Shopping ×		
OK			

Now I'll try amazon.com



I can see that now there's an option to override with the right credentials

Now let's test job search



We can see that its blocked!

Part 8: DNS Filter

DNS filtering in FortiGate involves intercepting DNS queries and applying filtering policies to block access to malicious or inappropriate websites based on predefined criteria.

It enhances security by preventing access to malicious domains, improves productivity by blocking non-business-related sites, and ensures compliance with regulatory requirements.

DNS filtering offers customizable filtering options and provides visibility into DNS traffic for effective monitoring and management of web usage.

I'll start by creating a new Profile named Office_DNS_Filter, also activating the Botnet C&C requests to block portal which will redirect and block all C&C type requests

New DNS Filter Profile

Name	Office_DNS_Filter
Comments	Comments 0/255
Redirect botnet C&C requests to Block Portal	<input checked="" type="checkbox"/>

Next I'll block facebook.com by creating a new Domain filter

Create Domain Filter

Domain	*.facebook.*		
Type	Simple	Reg. Expression	Wildcard
Action	Redirect to Block Portal		
Status	Enable	Disable	

Now let's test if Facebook.com is blocked from WIN10



This site can't be reached

The connection was reset.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnos

ERR_CONNECTION_RESET

And its blocked, which is great because Facebook sucks

Part 9: Antivirus Profile

The antivirus (AV) profile in FortiGate detects and blocks malware threats in network traffic, safeguarding against viruses, trojans, and ransomware.

It provides real-time protection for email and web traffic, automatically updates to combat new threats, and ensures minimal performance impact.

The AV database in FortiGate is a repository of signatures and definitions used to identify and block malware threats. It's regularly updated to detect new viruses, trojans, and other malicious software, ensuring effective protection against evolving threats.

I'll start by creating a new Flow-Based profile named Office_AV_Profile

The screenshot shows the 'New AntiVirus Profile' configuration window. At the top, there is a 'Name' field containing 'Office_AV_Profile' with a red border around it. Below it is a 'Comments' field with a placeholder 'Write a comment...' and a character count of '0/255'. Underneath these are two buttons: 'Block' and 'Monitor', with 'Block' being the selected option. The 'Feature set' section has two options: 'Flow-based' (selected) and 'Proxy-based', with 'Flow-based' also having a red border. At the bottom, there is a section titled 'Inspected Protocols' containing checkboxes for various protocols: HTTP, SMTP, POP3, IMAP, FTP, and CIFS. All checkboxes are checked.

I'll apply the rule on the existing interface/policy trafficOut



To test I'll disable all existing profiles except SSL

The screenshot shows the 'Security Profiles' settings. Under 'SSL Inspection', the 'Office_AV_Profile' is selected and highlighted with a red border. Other profiles like 'Web Filter', 'Video Filter', 'DNS Filter', 'Application Control', 'IPS', and 'File Filter' are listed below it. At the bottom, there are buttons for 'SSL' (selected), 'Office_To_Internet_Inspection', and 'Decrypted Traffic Mirror'.

Now I'll check if the added Virus test files are blocked by the new AV Profile

The screenshot shows the 'Blocking URL's' interface. It lists several URLs under the 'Simple' type, all of which are set to 'Block' and 'Enable'. One specific URL, 'wildfire.paloaltonetworks.com/publicapi/test/apk', is highlighted with a red box. Below this, a 'High Security Alert' message is displayed, stating: '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"'.

	Type	Action	Status
wildfire.paloaltonetworks.com/publicapi/test/apk	Wildcard	Block	Enable
wildfire.paloaltonetworks.com/publicapi/test/macros	Simple	Block	Enable
wildfire.paloaltonetworks.com/publicapi/test/apk	Simple	Block	Enable
wildfire.paloaltonetworks.com/publicapi/test/macros	Simple	Block	Enable

URL: http://wildfire.paloaltonetworks.com/publicapi/test/apk
 Quarantined File Name: [disabled]
 Reference URL: http://www.fortinet.com/virus-Android%2FPaloAlto_Test_Apk_File

Success, its blocking the PaloAlto virus test files as intended

Part 10: IPS Profile

An IPS (Intrusion Prevention System) profile in FortiGate detects and blocks network-based attacks in real-time.

Its benefits include preventing known and zero-day attacks, offering customizable protection, and providing real-time response to threats.

IPS profiles ensure comprehensive coverage and integrate threat intelligence for effective network security.

I'll start by creating a new profile named Office_IPS_Profile

Going to Security Profiles > intrusion Prevention > Create New

The screenshot shows the FortiGate configuration interface for creating a new IPS profile. At the top, there are fields for 'Name' (set to 'Office_IPS_Profile') and 'Comments' (with a placeholder 'Write a comment...' and a character count of '0/255'). Below these is a toggle switch for 'Block malicious URLs'. The main area is titled 'IPS Signatures and Filters' and contains a table with columns 'Details', 'Exempt IPs', 'Action', and 'Packet Logging'. A message 'No results' is displayed below the table. At the bottom, there is a section for 'Botnet C&C' with options 'Scan Outgoing Connections to Botnet Sites', 'Disable', 'Block' (which is highlighted with a red border), and 'Monitor'.

I'll create a new policy & activate the two security profiles SSL+IPS

New Policy

Name	IPS_Office
Incoming Interface	WAN (port1)
Outgoing Interface	LAN (port2)
Source	all
IP/MAC Based Access Control	all
Destination	all
Schedule	always
Service	ALL
Action	ACCEPT

Inspection Mode: Flow-based (selected) | Proxy-based

Security Profiles:

- AntiVirus: Off
- Web Filter: Off
- DNS Filter: Off
- Application Control: Off
- IPS: On, Profile: Office_IPS_Profile
- File Filter: Off
- SSL Inspection: On, Profile: Office_SSL
- Decrypted Traffic Mirror: Off

Now to test this, I will see if it's getting blocked from WIN10 by taking one of the addresses from the botnet Database

Botnet C&C IP Definitions			
IP	Port	Protocol	
1.9.167.36	60,489	TCP	KillNet

① 1.9.167.36



This site can't be reached

The connection was reset.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)
- [Running Windows Network Diagnostics](#)

ERR_CONNECTION_RESET

Its working as intended!

Part 11: Application Control

Application control in FortiGate allows administrators to monitor and manage the use of applications on the network.

It enables the identification and control of applications, offering benefits such as regulating bandwidth usage, enhancing security by blocking unauthorized applications, and enforcing policies to ensure compliance.

Application control ensures efficient network resource allocation, reduces the risk of data breaches, and helps organizations maintain control over their network environment.

I'll go to Security Profiles > Application Signatures and add TeamViewer

Application Signature 3/2413			
✓	Teamviewer	Remote.Access	Client-Server
✓	Teamviewer_CallReceive	Remote.Access	Client-Server
✓	Teamviewer_CallRequest	Remote.Access	Client-Server

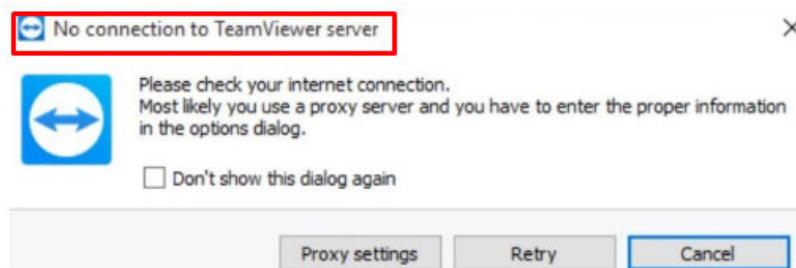
Next I'll create a new profile named Office_Application_Control

The screenshot shows a user interface for creating a new security profile. At the top, there is a blue header bar with the text "93 Cloud 0 policies". Below this, there are two input fields: "Name" and "Comments". The "Name" field contains the text "Office_Application_Control", which is highlighted with a red rectangular border. The "Comments" field has a placeholder "0/255".

And I'll block Remote Access



Now I'll test on WIN10 to see if the new settings are working as intended



We can see that there's no connection to TeamViewer Server
Now I'll add a 2 day quarantine on anybody using TeamViewer

Add New Override

Type Application Filter

Action Quarantine (Expires 2 Day(s))

Add All Results teamviewer

	Name	Category
<input checked="" type="checkbox"/>	Application Signature 3/24/13	
<input checked="" type="checkbox"/>	Teamviewer	Remote.Access
<input checked="" type="checkbox"/>	Teamviewer_CallReceive	Remote.Access
<input checked="" type="checkbox"/>	Teamviewer_CallRequest	Remote.Access

Save the changes and try to use TeamViewer

FortiGate Application Control

Application Blocked

You have attempted to use an application that violates your Internet usage policy.

Application TeamViewer
Category Remote.Access
URL https://www.teamviewer.com/

And its blocked, working as intended