קורס למתחילים בסייבר

CSPP

מבואות סייבר

ניהול רשתות ובקר SOC

FortiGate Project

Tables Of Content

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

Project Sources: Google, Class Recordings, ChatGPT, Bard, SeeSecurity Books

Part 1: User Management

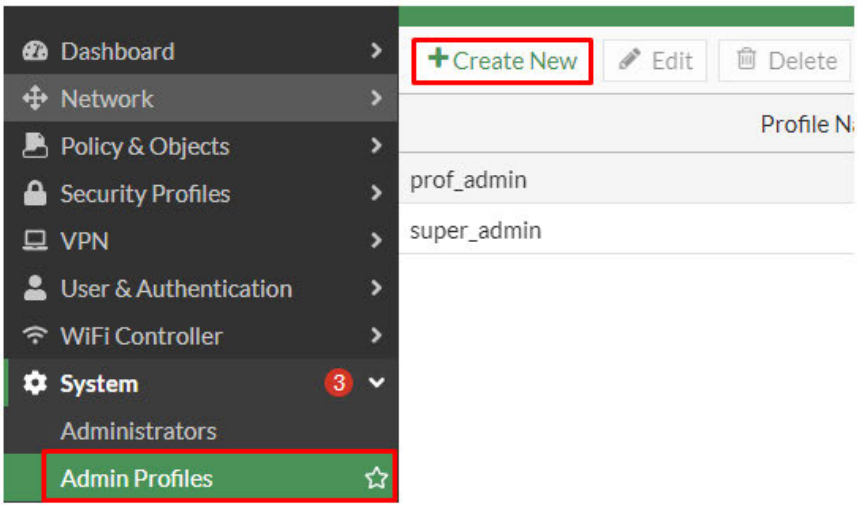
User management in FortiGate involves verifying user identities, defining access policies, enforcing security measures, monitoring user activity, and centralized administration.

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

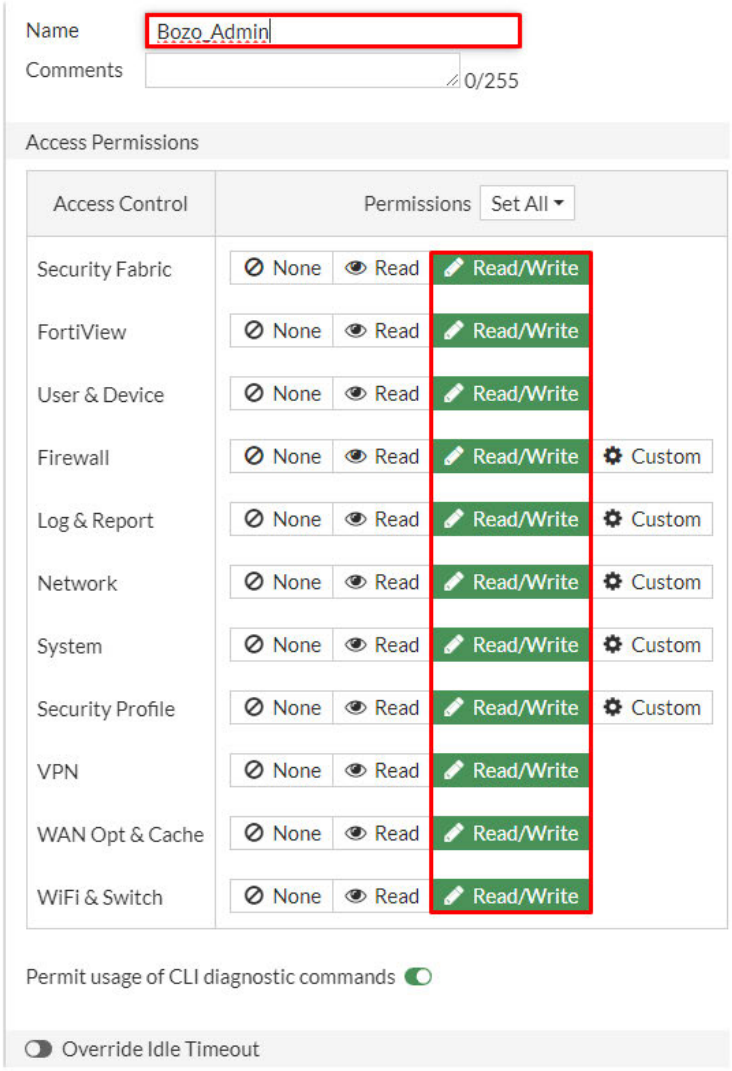
In order to connect to the FortiGate dash board I'll enter the WAN IP

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



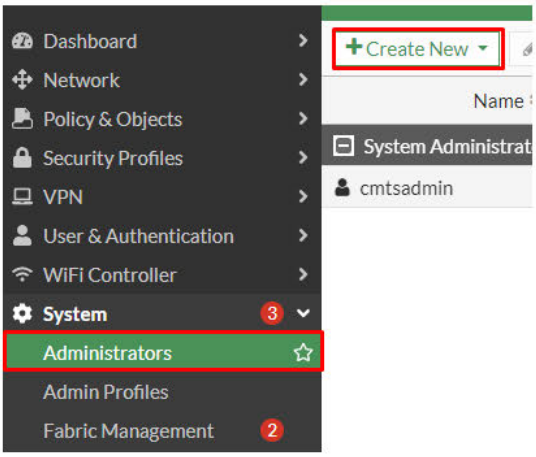
I'll give Bozo_Admin super_admin permissions



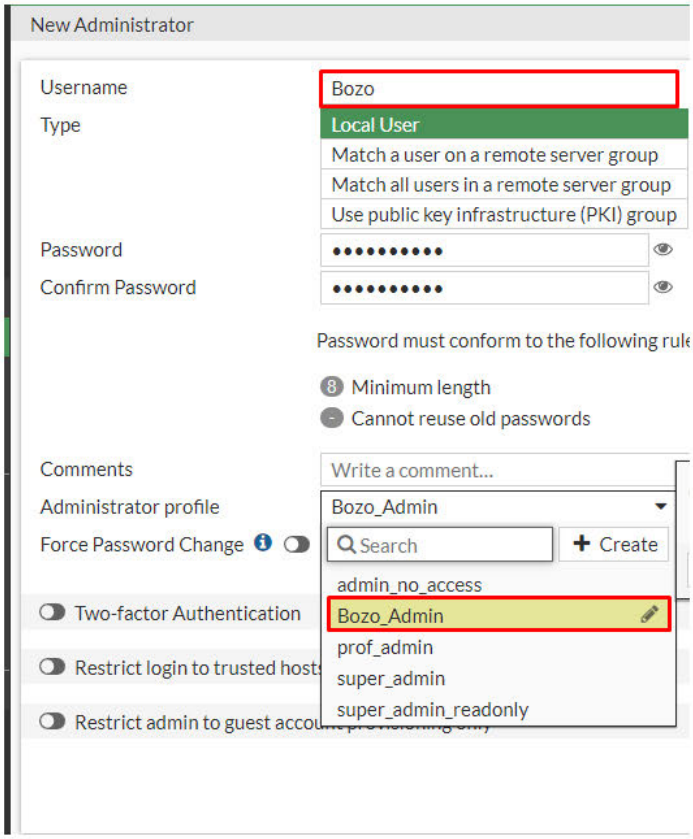
Now we can see that Bozo_Admin is a new profile

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

Doing this by going to System/Administrators/Create New



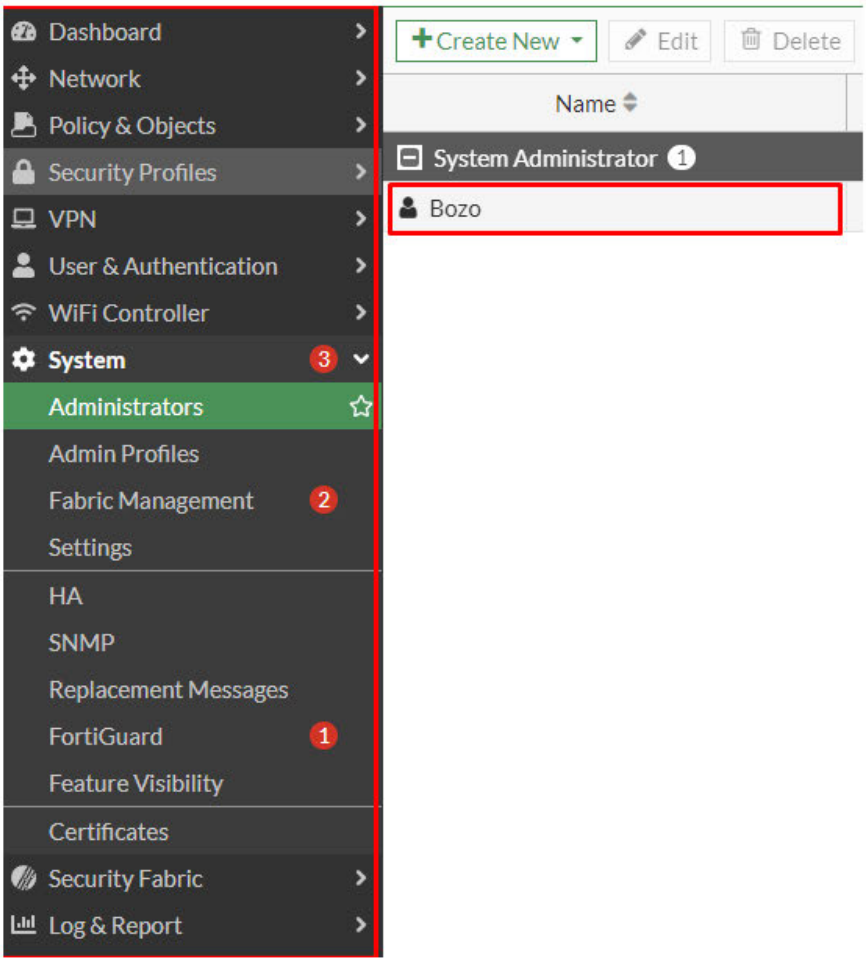
Here I'll give the new user bozo, Bozo_Admin permissions



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

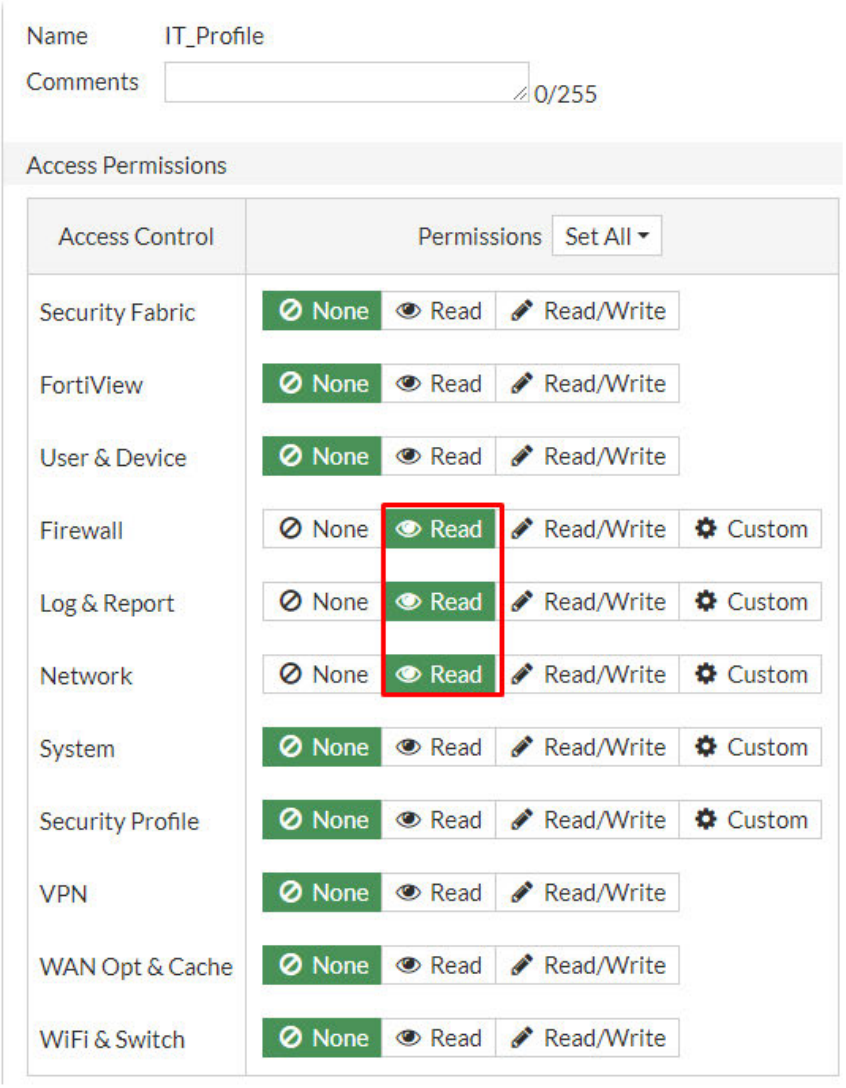


Bozo is logged in and has all the functions and features that a super_admin has using the new Bozo_Admin profile

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

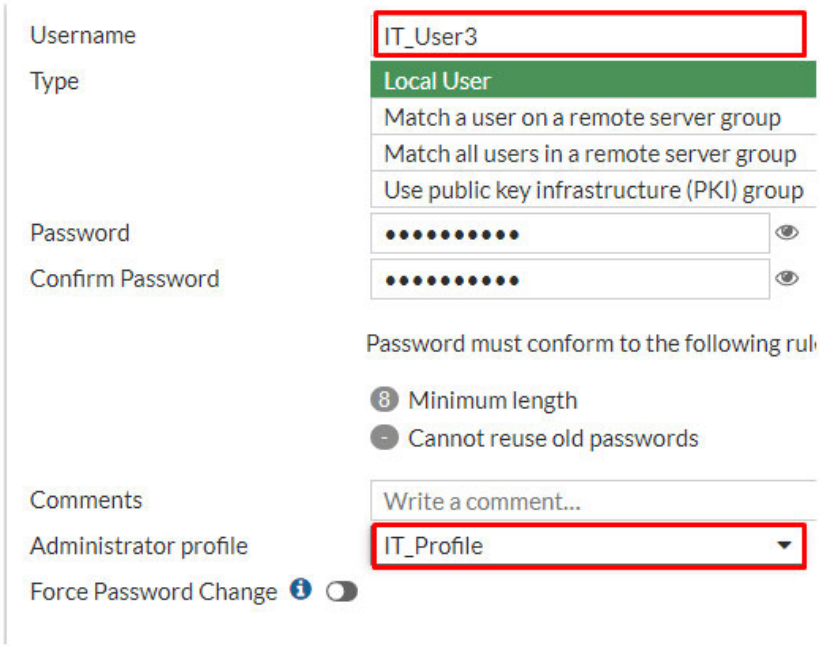
.Policy, logs, VIPS, interfaces :

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



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

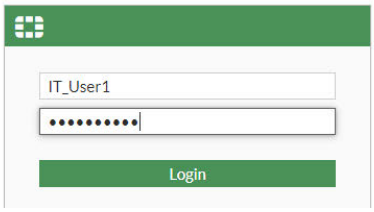
Next step I'll create three new users named IT_User1, IT_User2, IT_User3

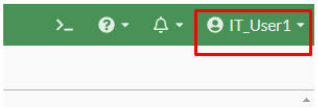


I have created three new users for IT and gave them the IT_Profile permissions

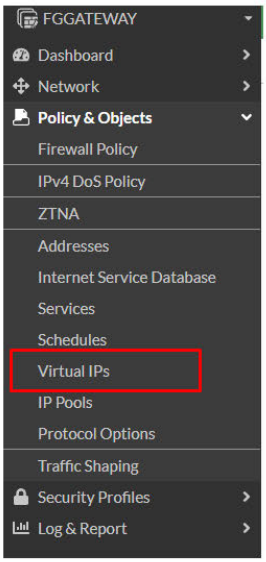
IT_User1		IT_Profile
IT_User2		IT_Profile
IT_User3		IT_Profile

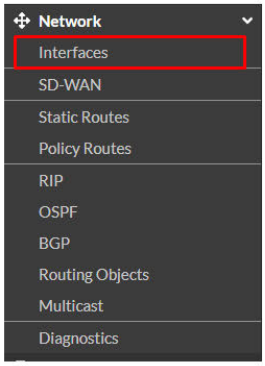
Now I will logon with IT_User1 and check if he only has the View Only permissions for the specific interfaces I've selected

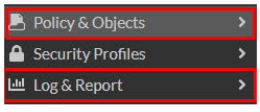




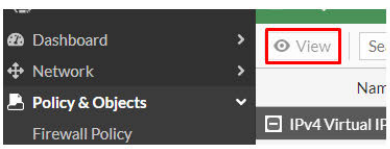
And here we can see that it's working as intended, IT_User1 has read only permissions for Policy,Logs,VIPs,Interfaces







We can see that he has view only permissions



Part 2: Password Policy

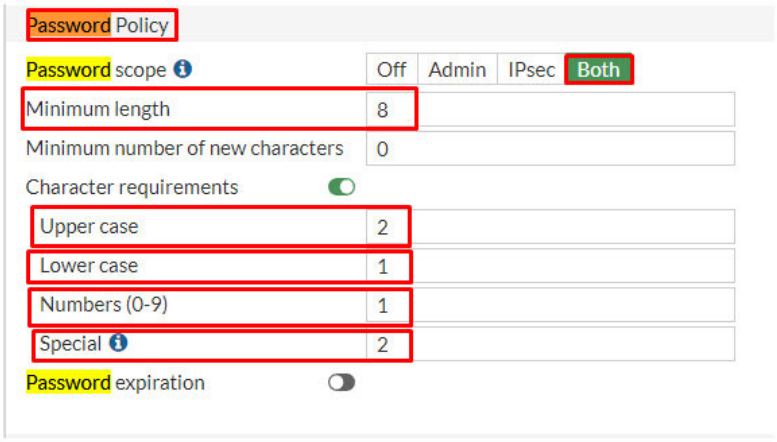
A strong password policy for FortiGate management is crucial to prevent unauthorized access.

It's important 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 these 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



Now my password policy is hardened and my network is safer

Part 3: VPN Configuration

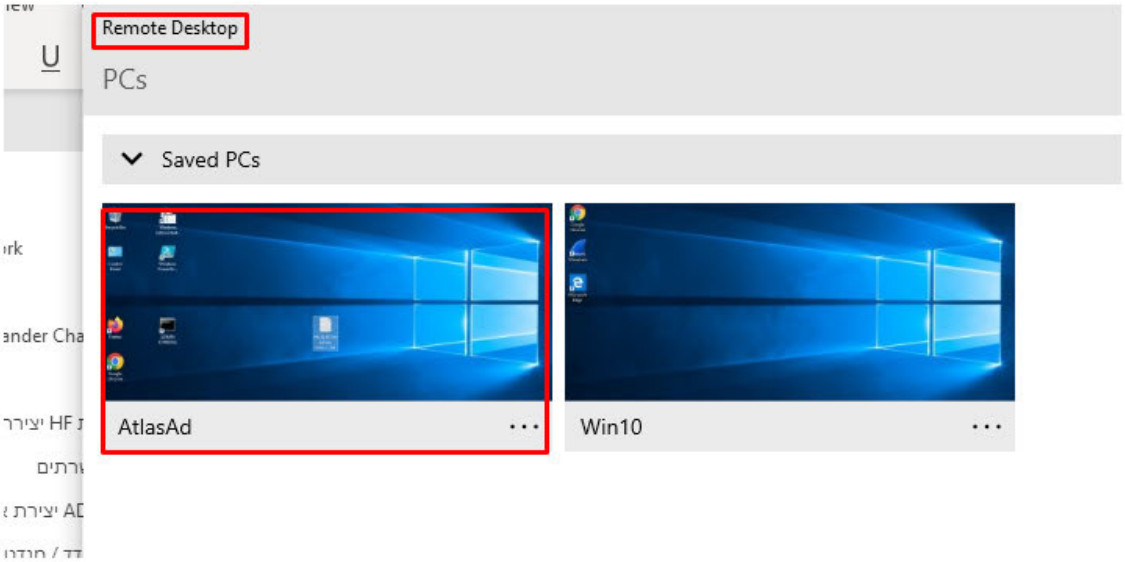
Using a VPN with FortiGate encrypts your internet connection, protecting data from interception. It also masks your IP address for anonymity and enables secure remote access to corporate networks, enhancing overall security.

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.

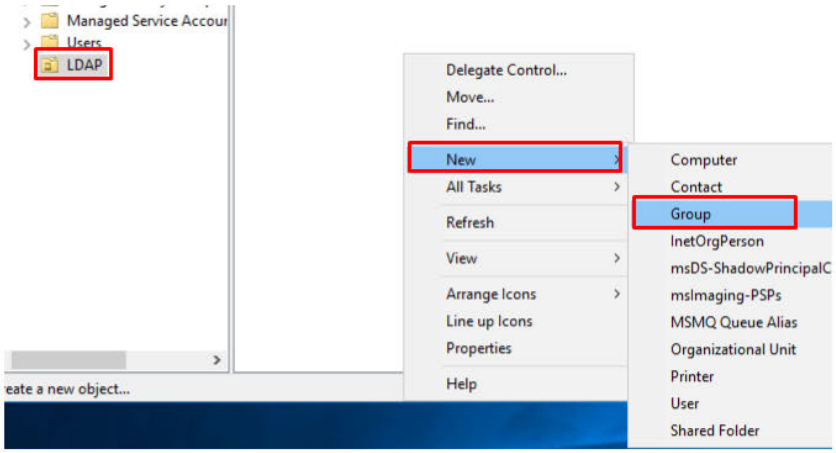
This mode allows secure access to internal resources remotely, enhancing security for remote workers and ensuring confidentiality of sensitive information.

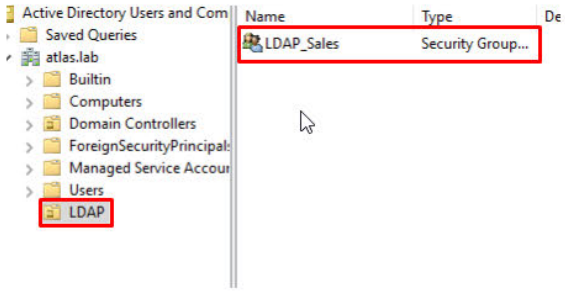
I'll start by configuring SSLVPN Tunnel Mode:

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

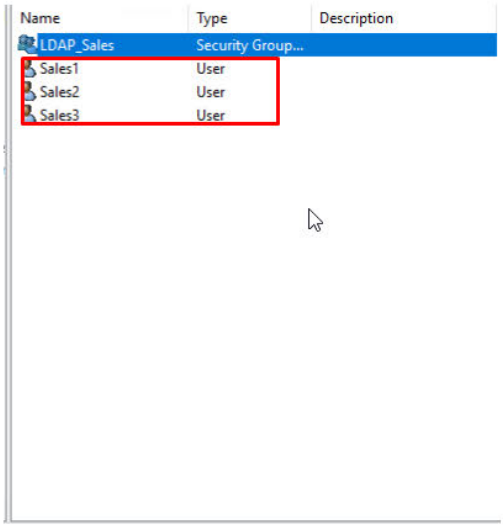


I'll go to Active Directory users & computers and create a new group named LDAP_Sales

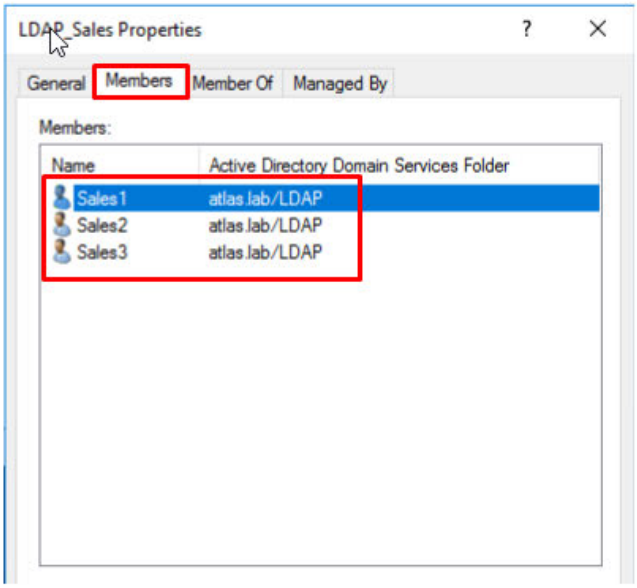




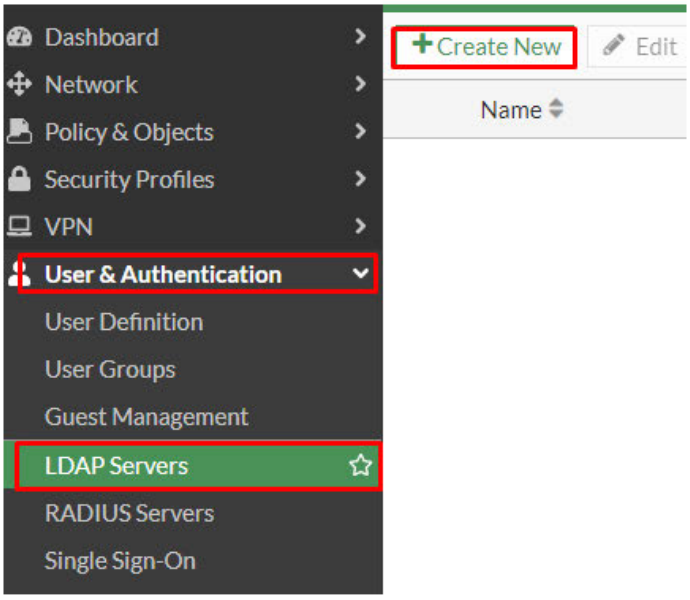
Now I'll create 3 new users and put them in the LDAP_Sales group



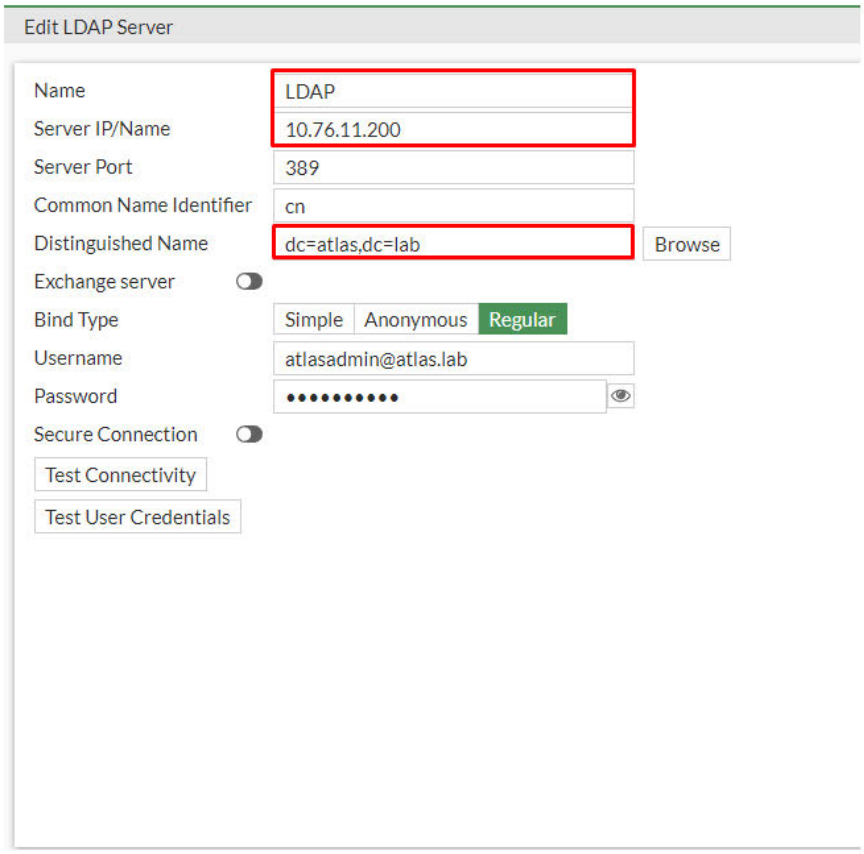
And now we can see that LDAP_Sales group has three new users



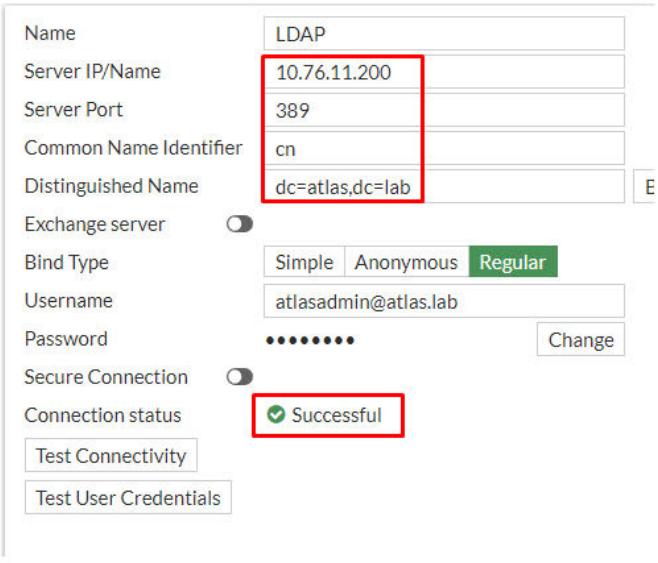
Now I'll start configuring LDAP on FG
I'll go to Users & Authentications> LDAP Servers>Create New



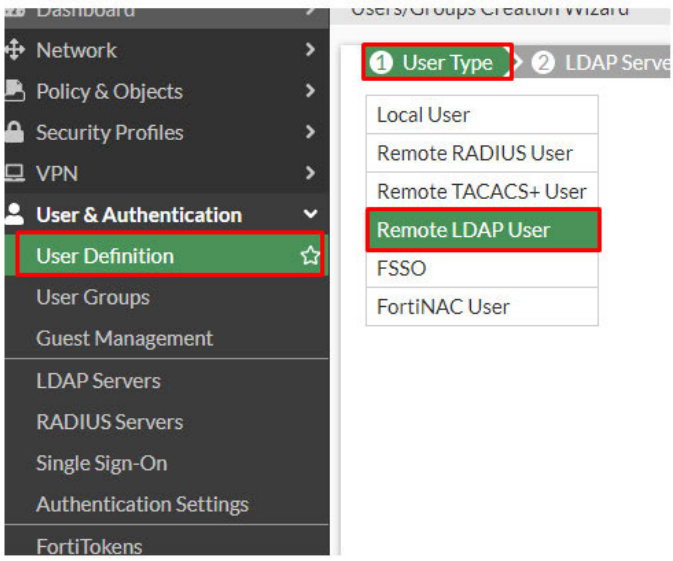
I'll enter the relevant information for my LDAP Server



Now I have connection to the LDAP server

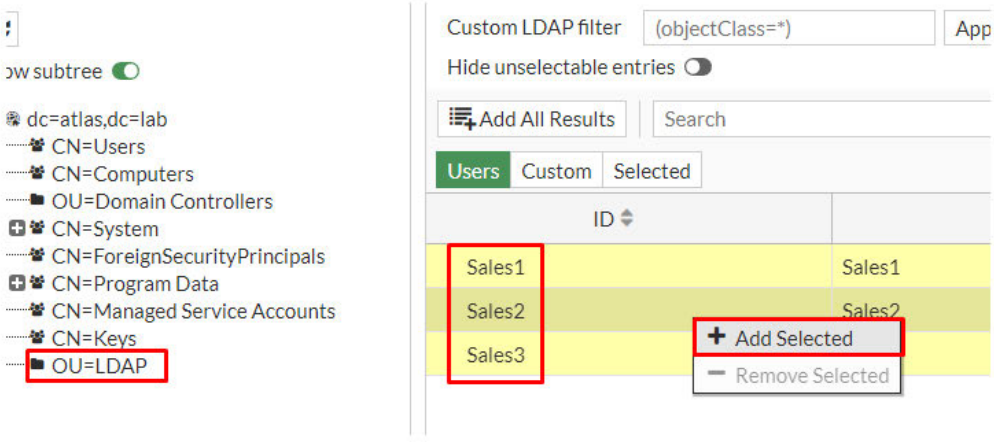


Next I'll go to LDAP User Creation & select Remote LDAP User

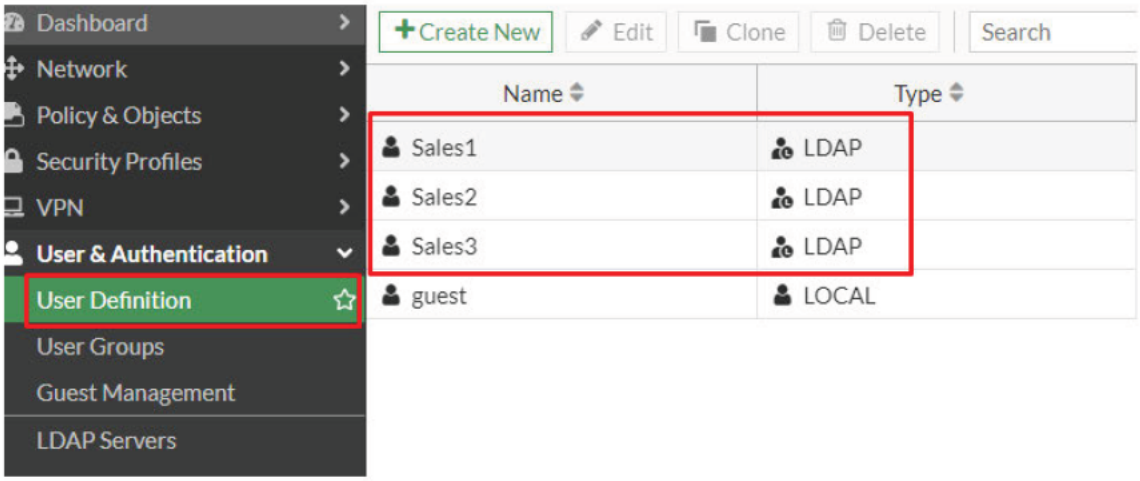


Select the appropriate server

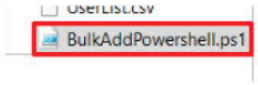
Now I'll be adding the 3 Sales users to be Remote Users



We can see them Active as LDAP

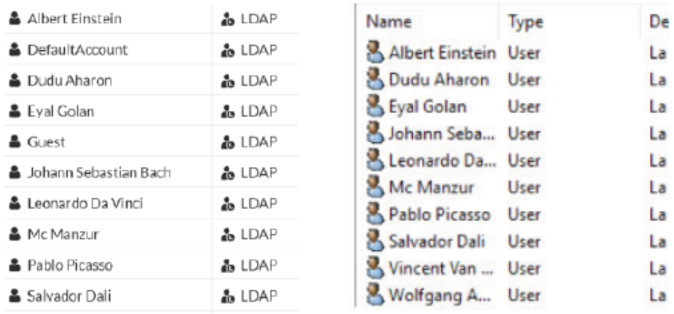


I'll also create more users using a script that I'll put in the C drive on the AtlasAD
This method is easier and way faster for bulk creating users




```
New-ADOrganizationalUnit -Name "FG-Users" -Path "DC=atlas,DC=lab"

$Users = Import-Csv -Path "C:\UserList.csv"
foreach ($User in $Users)
{
    $Displayname = $User.'Firstname' + " " + $User.'Lastname'
    $UserFirstname = $User.'Firstname'
    $UserLastname = $User.'Lastname'
    $OU = $User.'OU'
    $SAM = $User.'SAM'
    $UPN = $User.'SAM' + "@" + $User.'Maildomain'
    $Description = $User.'Description'
    $Password = $User.'Password'
    $server = 'atlas.lab'
    New-ADUser -Name "$Displayname" -DisplayName "$Displayname" -
```

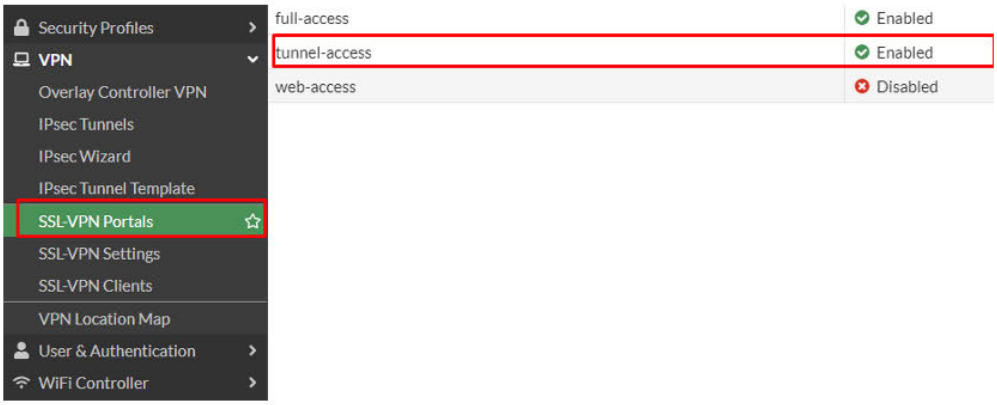


I'll add them to the LDAP_Sales Group as well

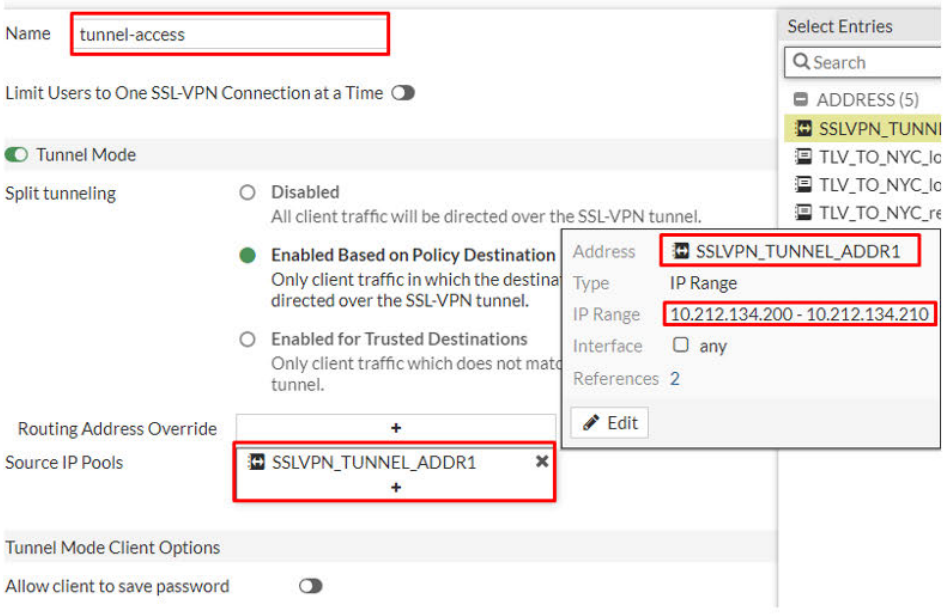
In the next step I'll configure a new SSLVPN Tunnel Portal & than I'll configure a separate web access portal

- 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.

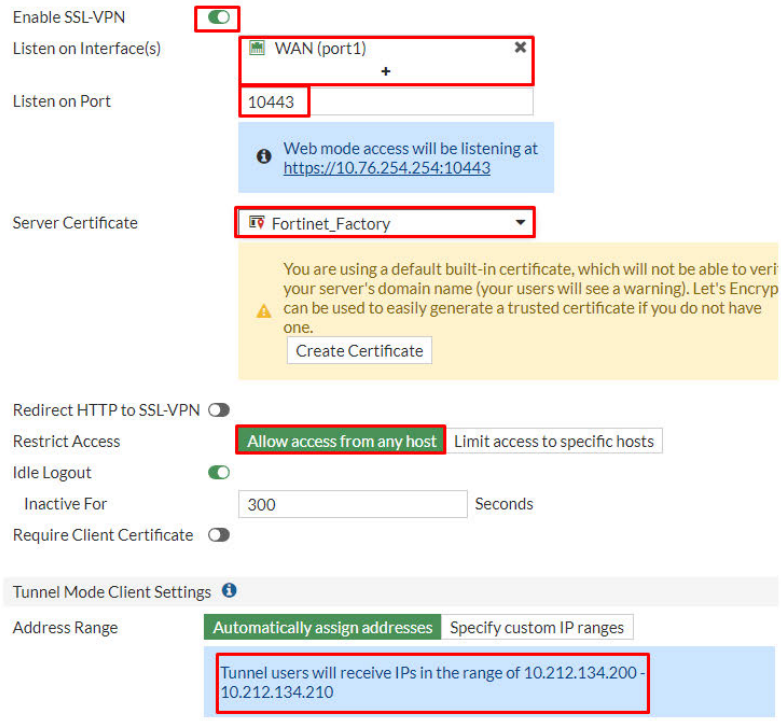
VPN>SSLVPN>Tunnel Access



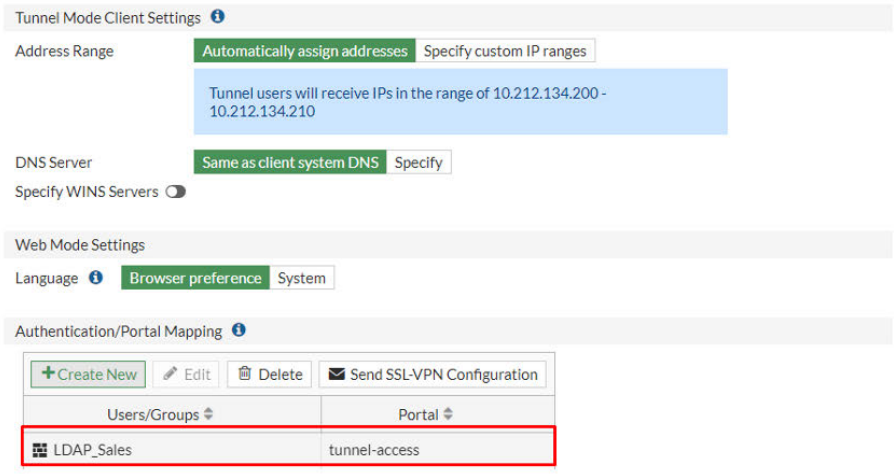
I'll also give the a source IP Pool



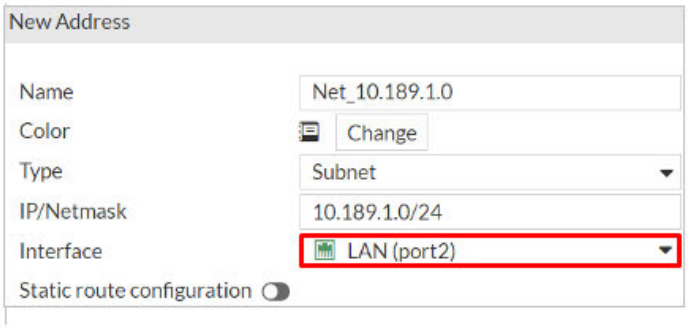
Next I will go the the SSL-VPN Settings & configure to enable & listen on Port 10433
Also to allow access from any host



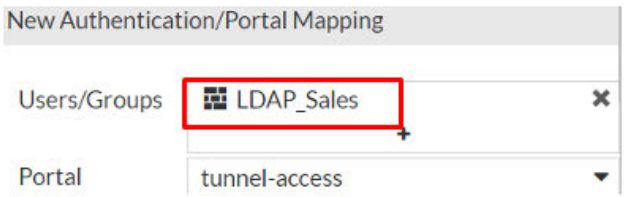
Now I'll give the LDAP_Sales group the tunnel-access portal

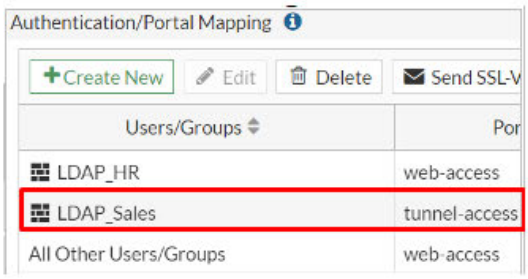


Now I'll configure the IP range by going to VPN>SSLVPN Portal>Tunnel Access

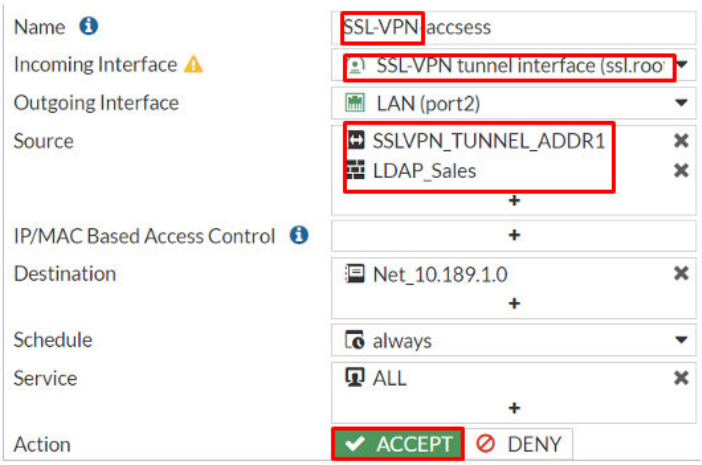


Go into the VPN settings and configure the connection of the portal with the Users



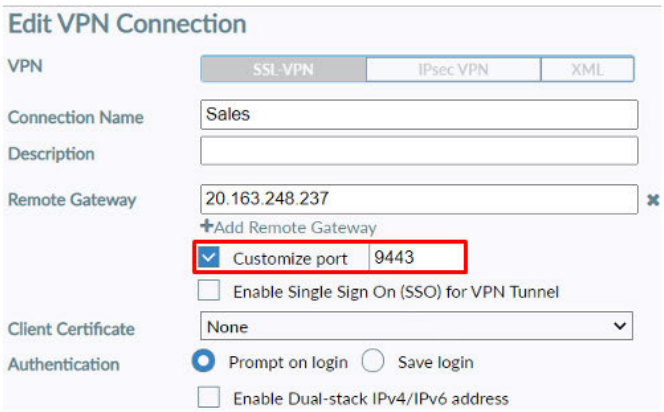


Next step I'll create a new policy

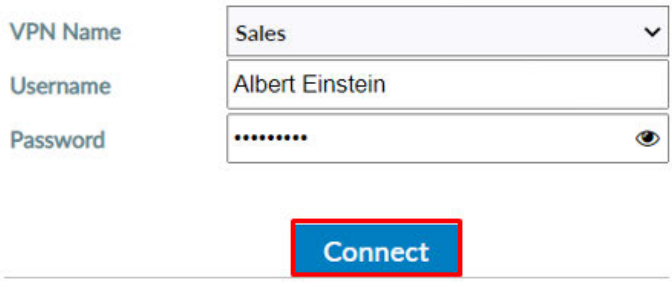


Now I'll try to connect using FortiClientVPN

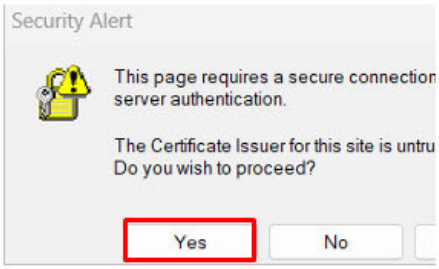
I'll name it and put in the public WAN address, Port will be customized



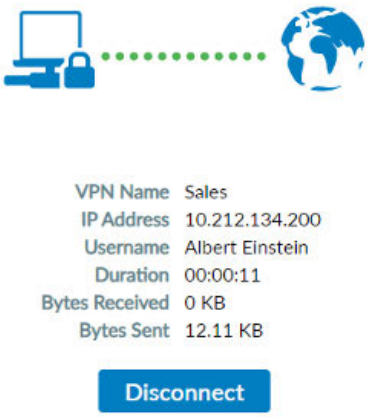
Enter the Credentials



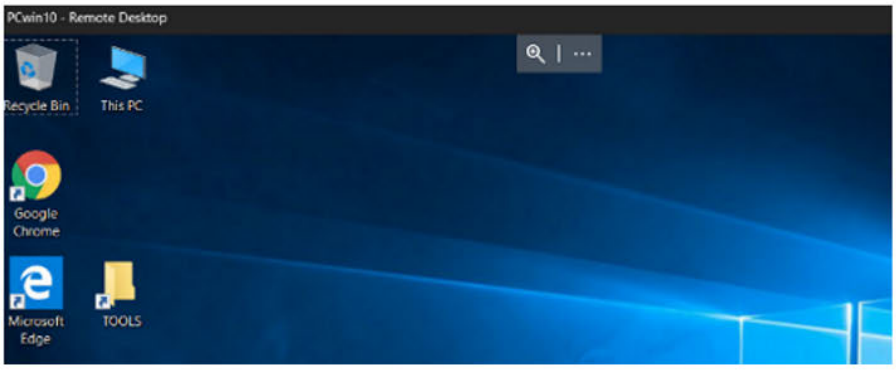
Click Yes on the Security Alert



The connection is a success!



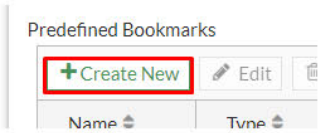
Now I'll test remote desktop connection

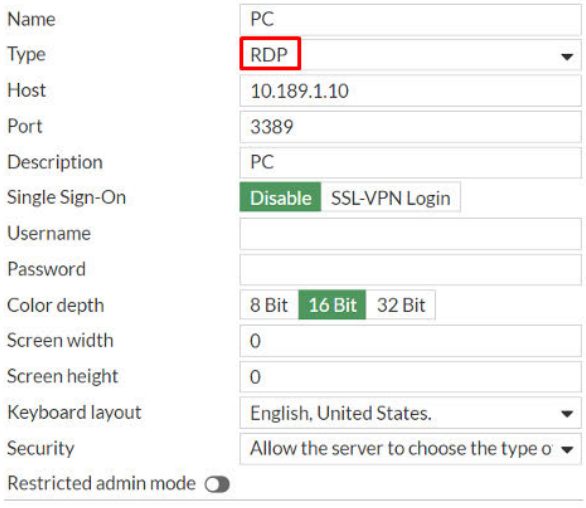


Remote is successful!
Next step is the SSLVPN Web Access Mode

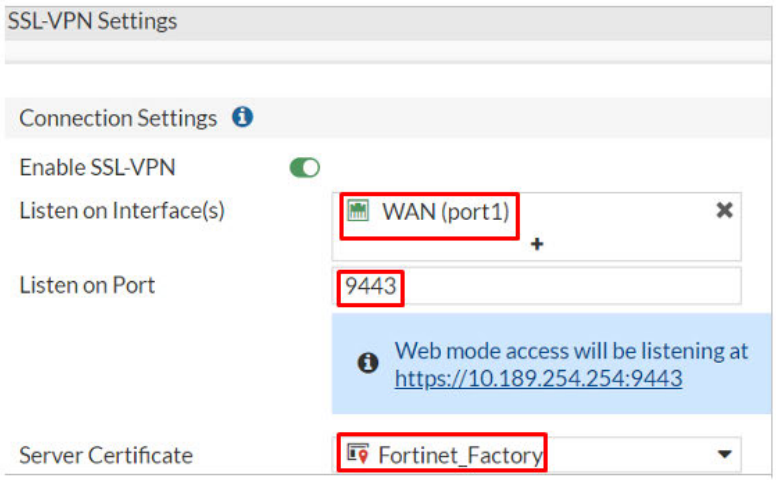
I'll create a new Bookmark in the default FortiGate WebAccess Portal

I'll create a new Bookmark using the RDP Type

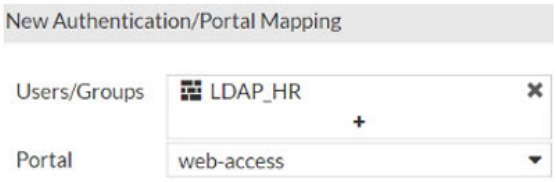




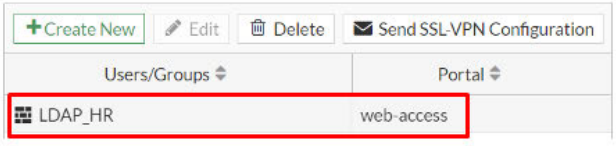
I'll go to the SSLVPN Settings and configure the fortiGate interface to listen on 9443



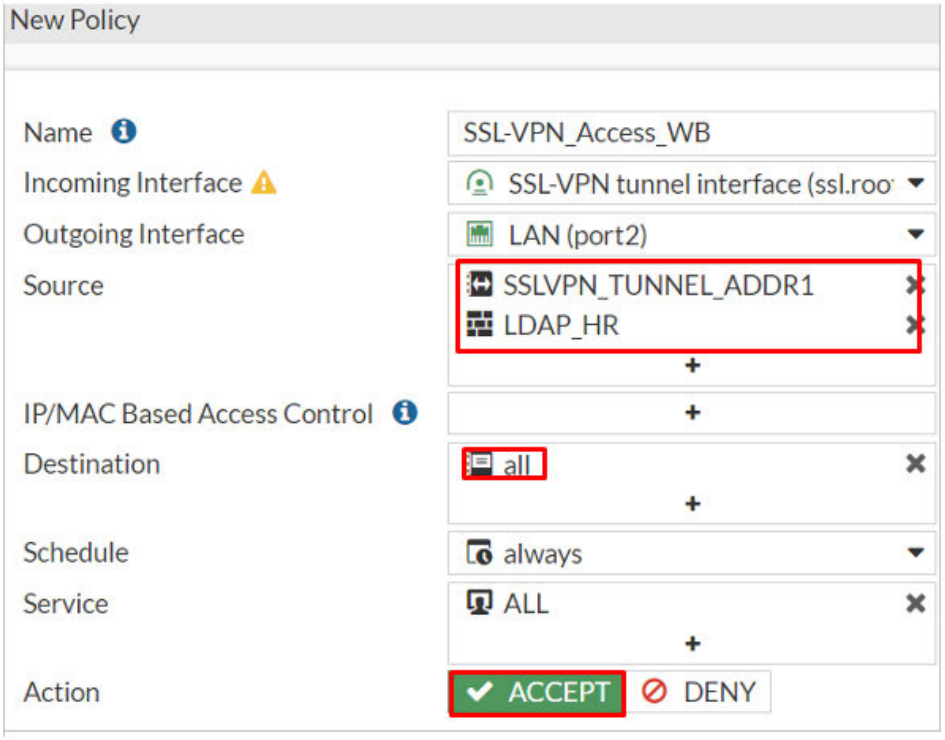
Now I'll create a new group named LDAP_HR with three users and attach them to the portal, and another local user named AD_FG for authentication



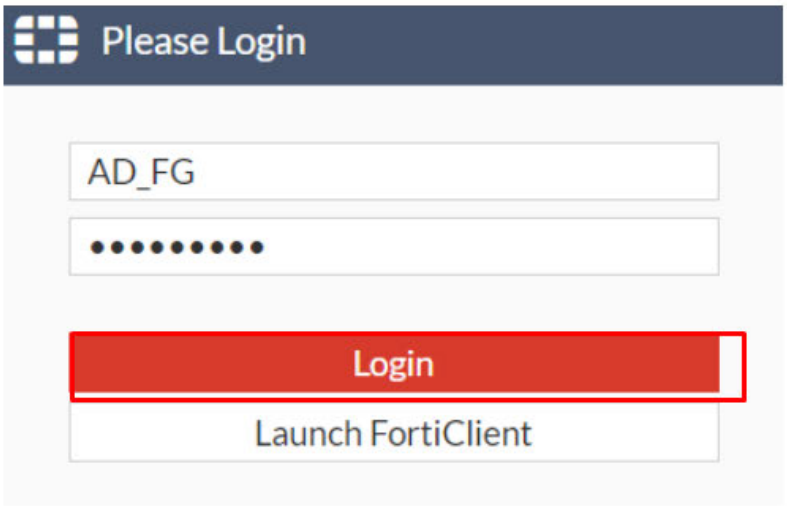
Here we can see that LDAP_HR are no using the web-access portal



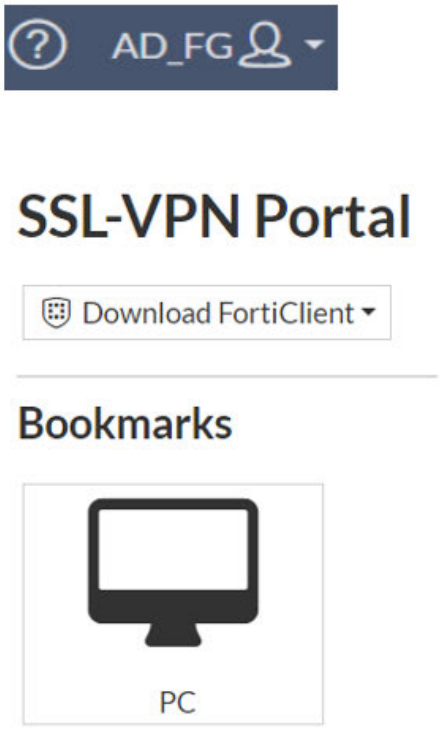
Now I'll create a policy that will allow a connection to the portal



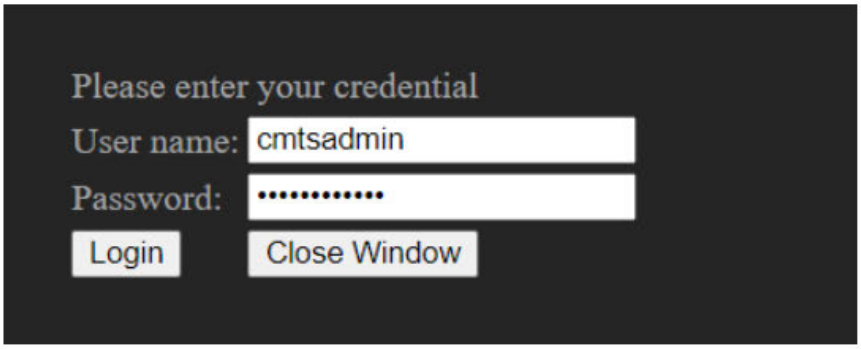
Now I'll test connectivity with a local user to see if it works



I'm in and can see the configured bookmark



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



Success!

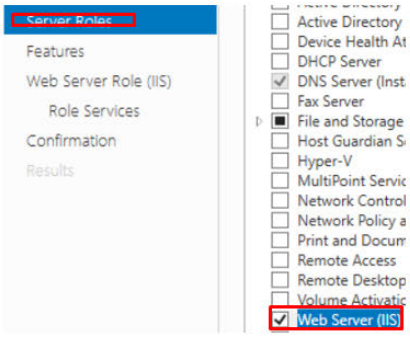
Part 4: VIP

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.

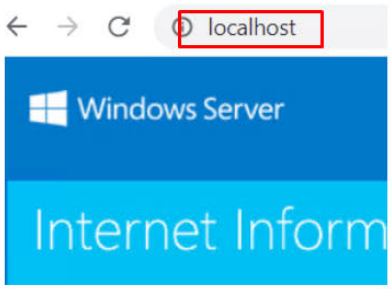
Benefits include server accessibility, load balancing, and enhanced security.

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



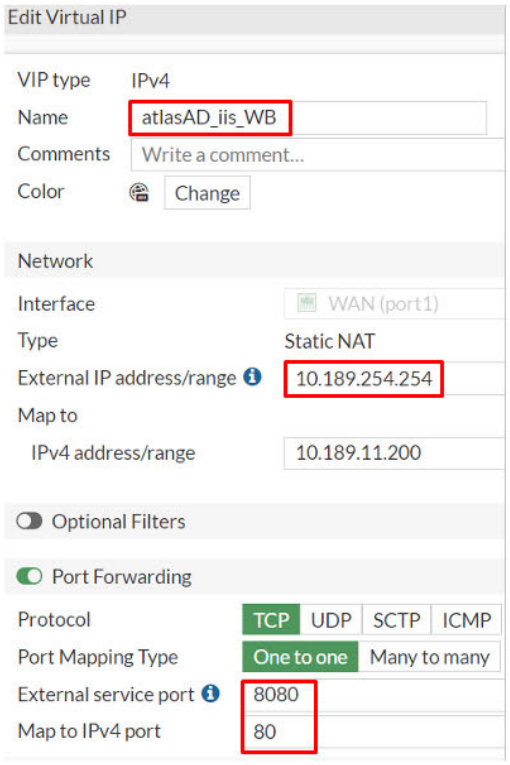
After installing I'll check /localhost to see if this worked locally



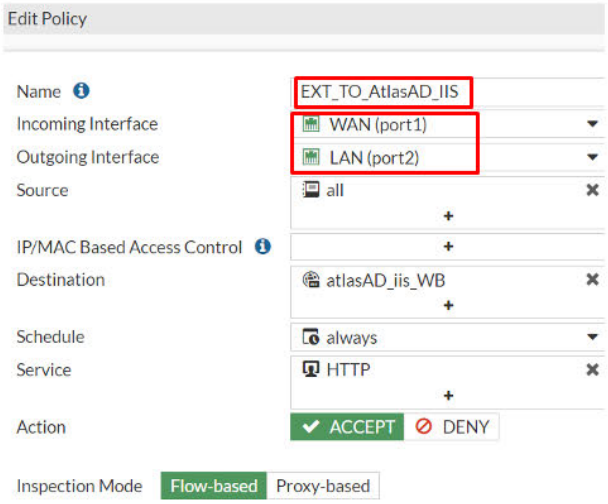
It works, Now after installing IIS I'll publish a VIP and test if it's possible to reach it from outside network

I'll name the VIP, give it the port that it needs to reach (WAN)
In a normal scenario I'll need to give and 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.

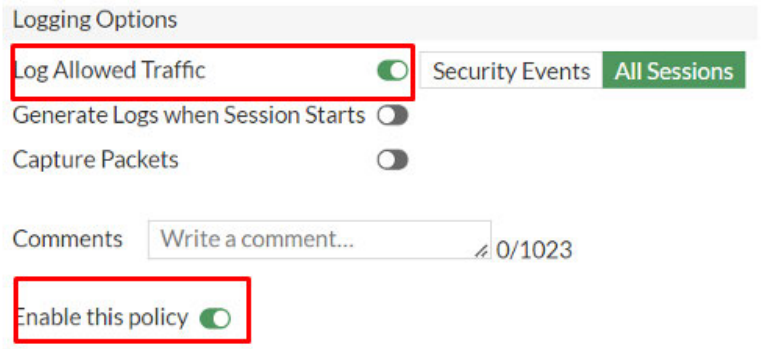
In a real world scenario this usually be replaced with an ISP given public address
I'll also do Port Forwarding, mapping the external 8080 port to an internal 80 port



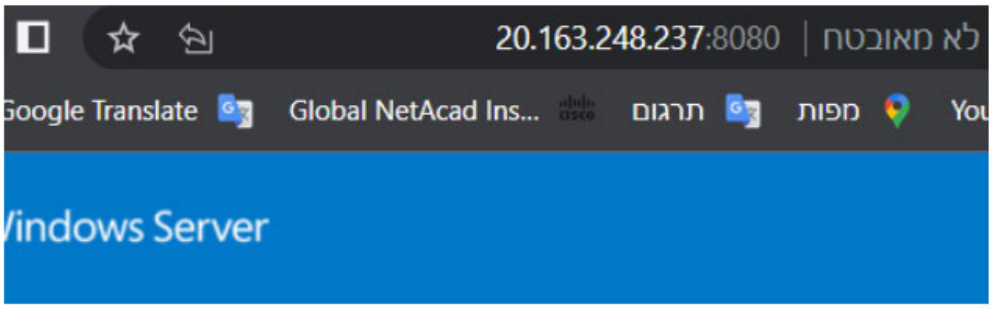
Now I'll create a new policy that will allow traffic to go outside the network



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!

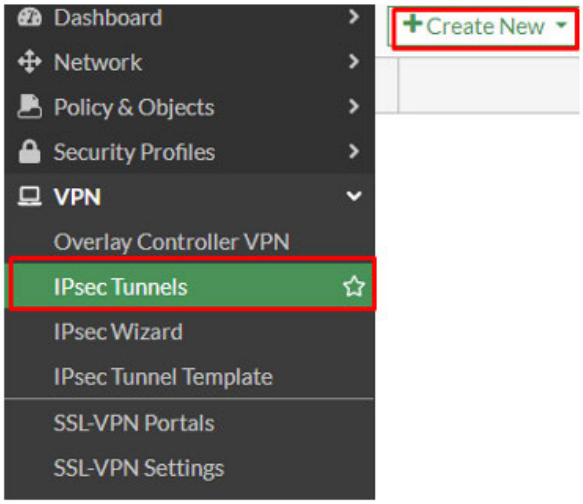
Part 5: IP SEC

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

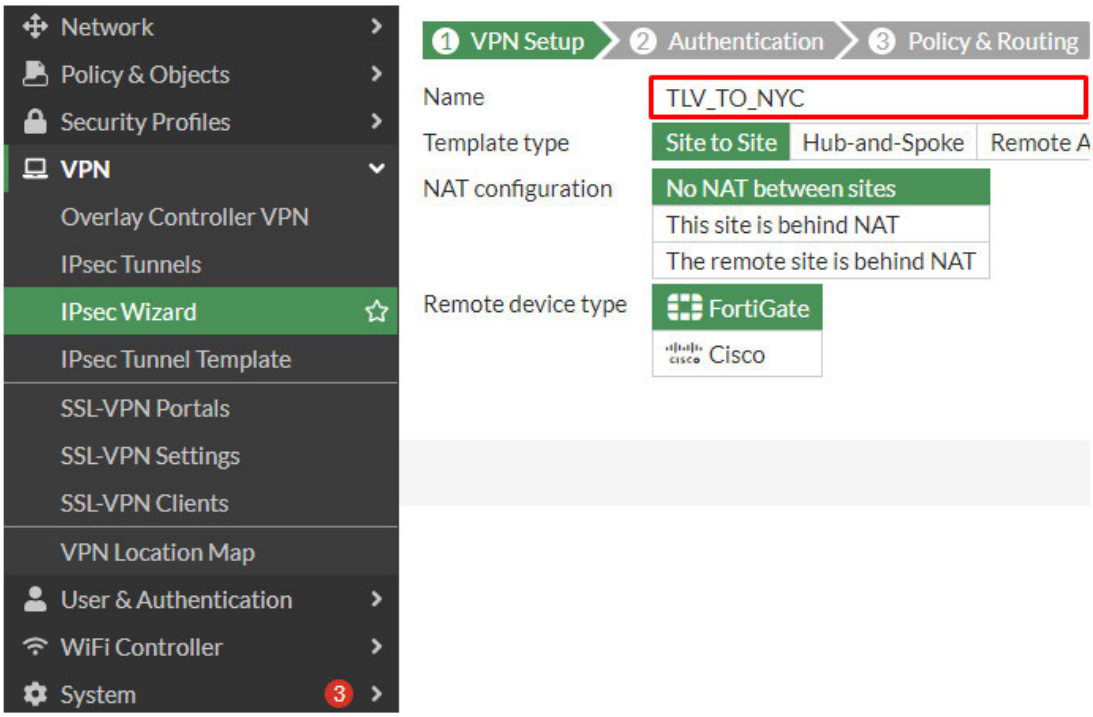
It ensures data confidentiality, integrity, and authentication. IPsec is used for secure remote access, site-to-site connectivity, and offers enhanced security, scalability, cost-effectiveness, flexibility, and interoperability.

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

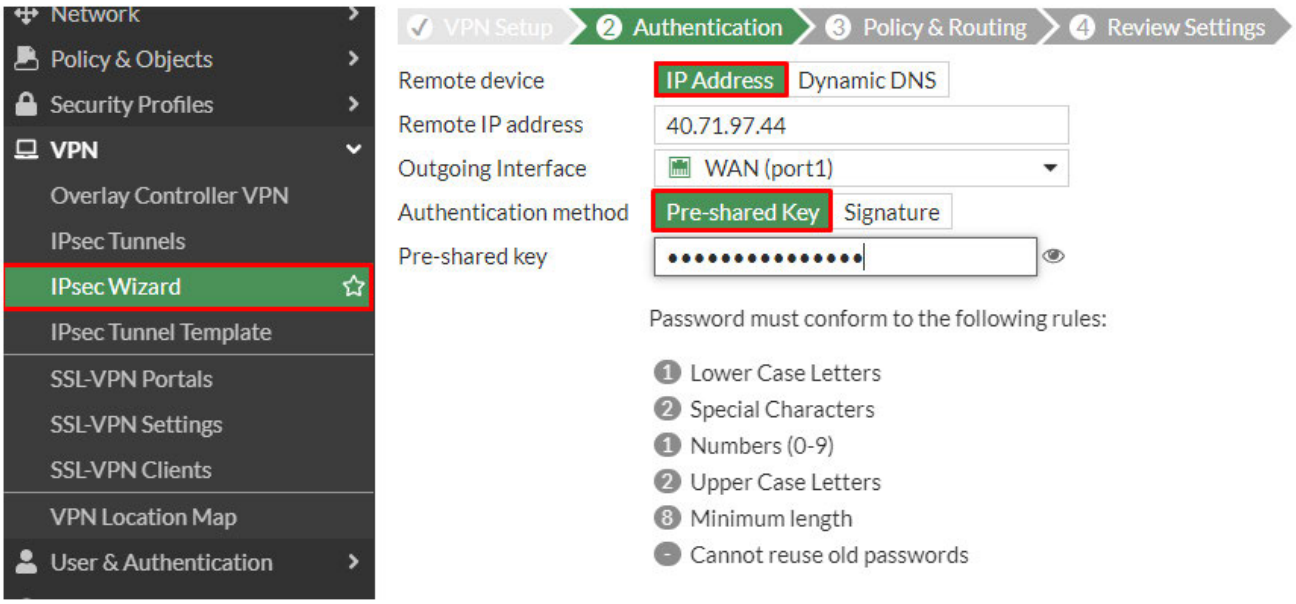
We'll start by creating a new IPsec tunnel



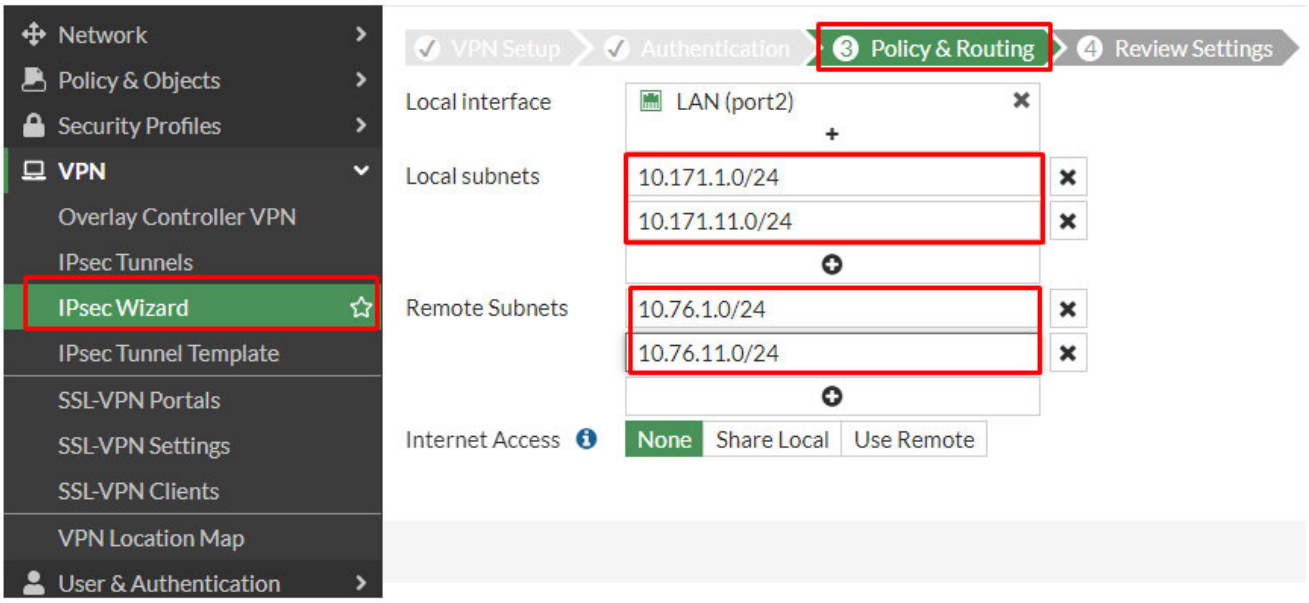
I'll name it



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



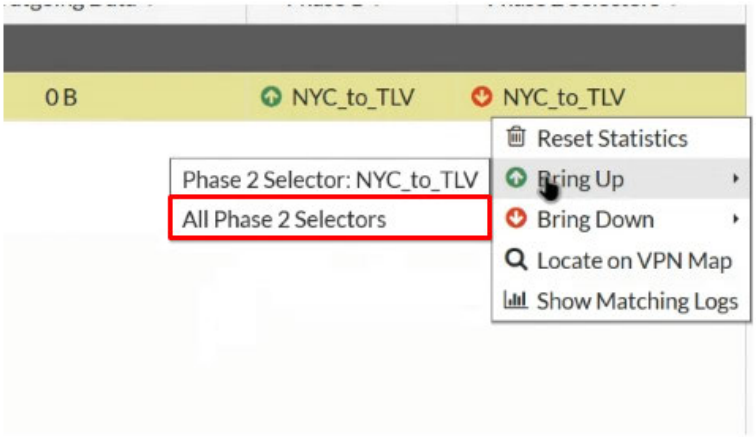
Now we'll configure both remote and local subnets and select the LAN interface



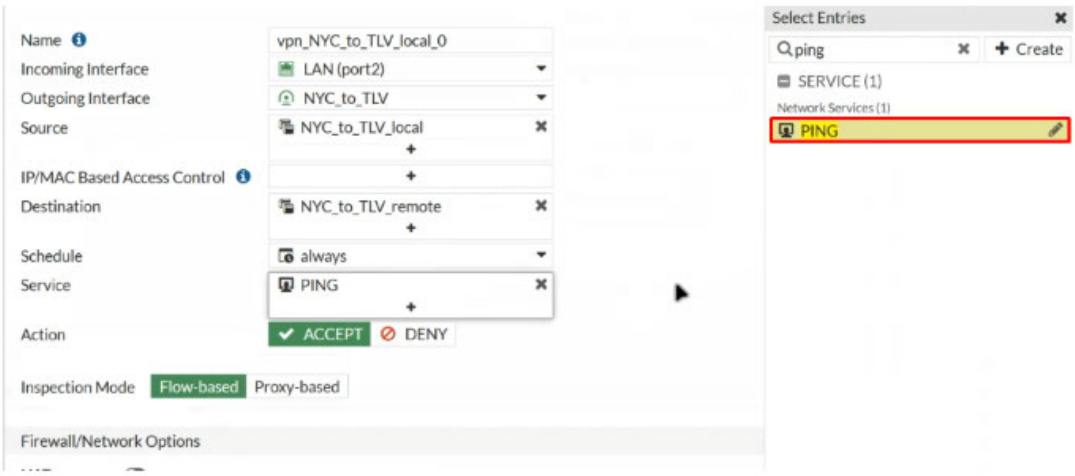
Here we can see the summary of the VPN

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

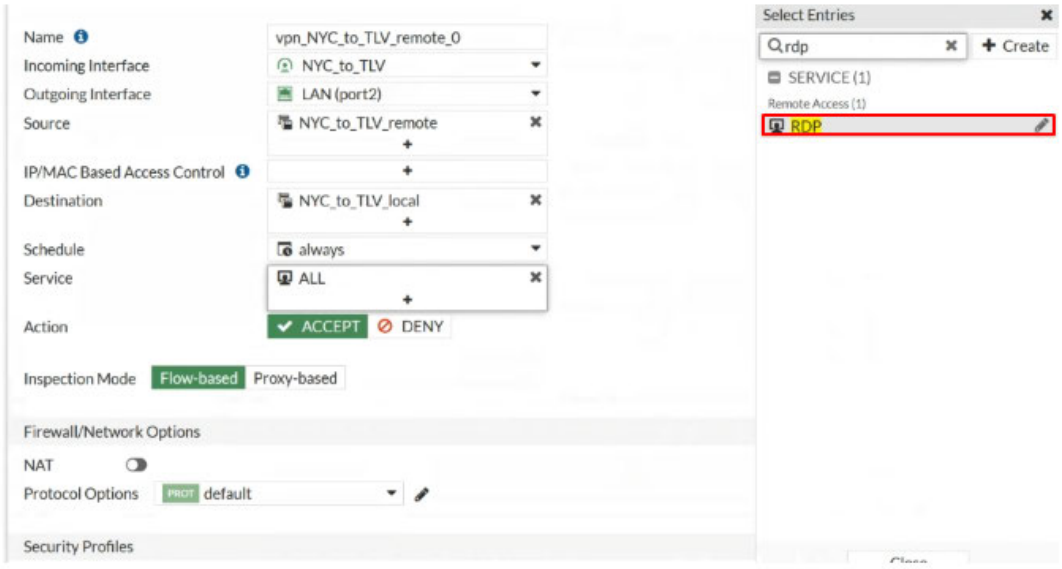
Now we'll bring up Phase 2 Selectors



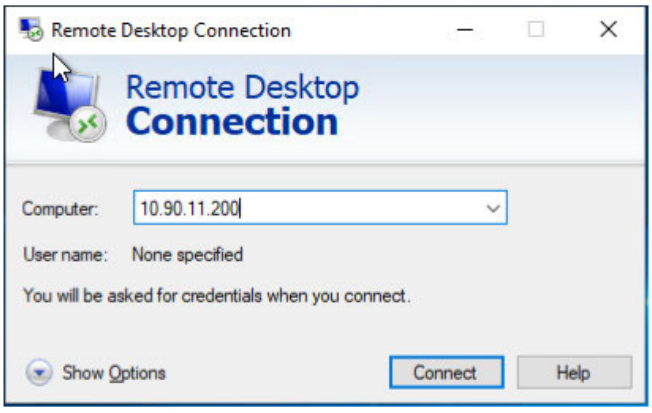
I'll create a policy that will allow ping



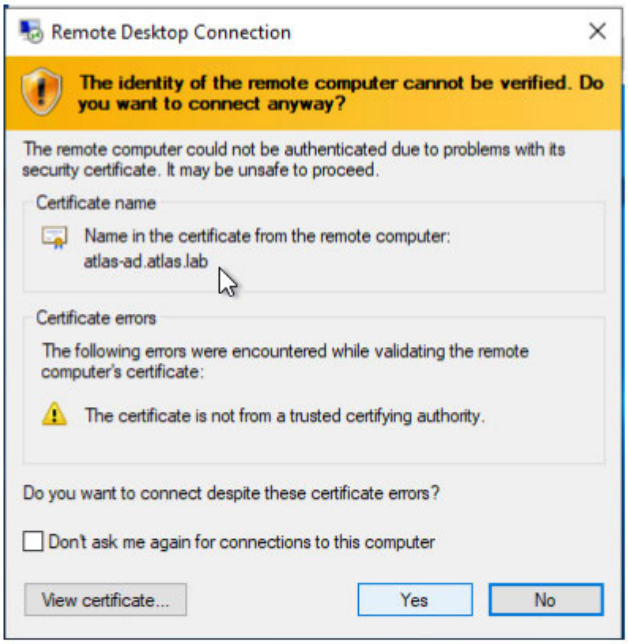
I'll create a policy that will allow RDP



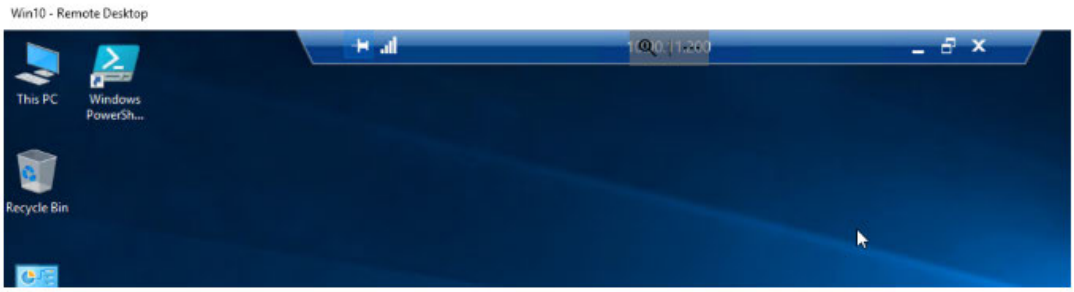
Now I'll test the RDP



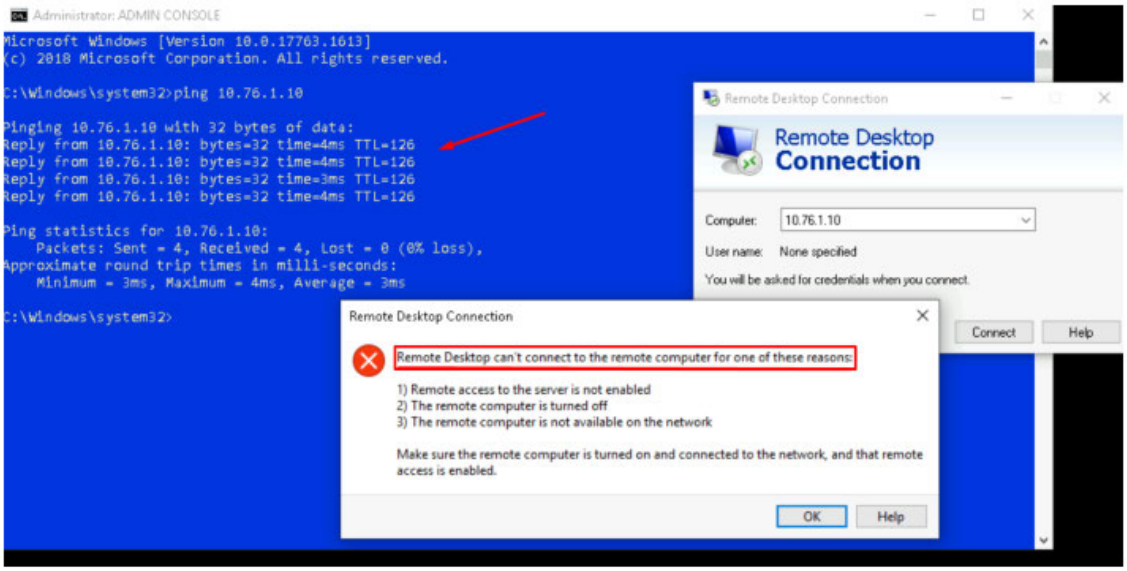
Allow to Procced



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

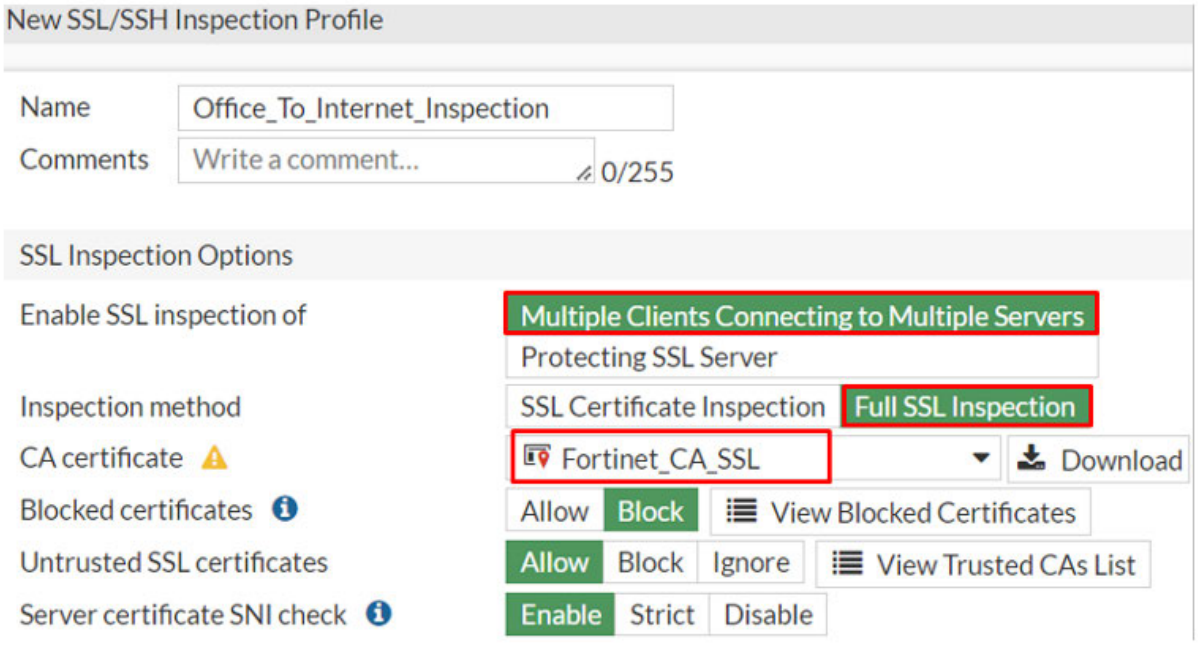


Part 6: Inspection

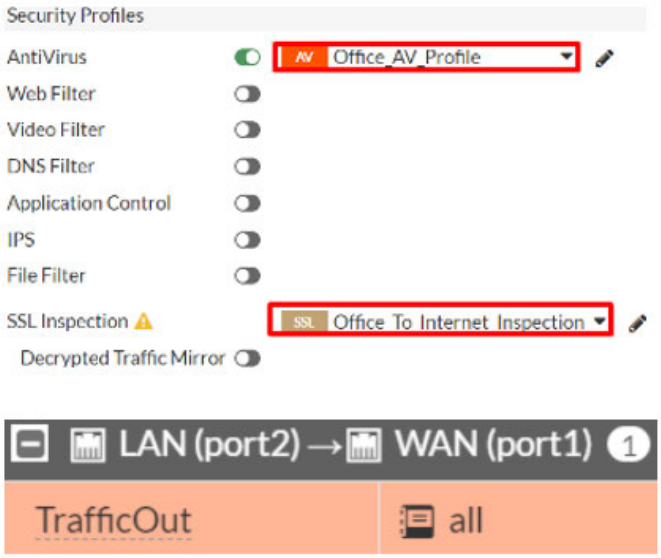
Inspection in FortiGate is vital for analyzing network traffic and enforcing security policies.

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

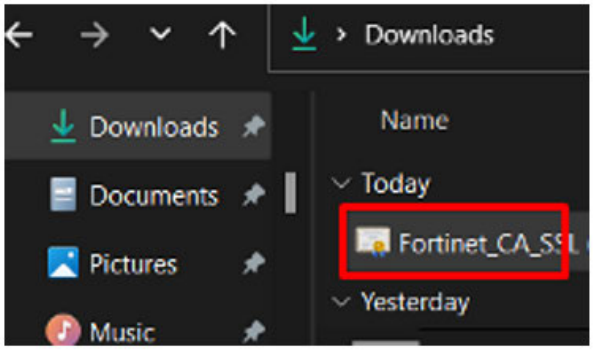
I'll start by creating a new profile for Inspection, with full SSL inspection mode. I'll select multiple clients, Full SSL Inspection, I'll also download a FortiGate certificate



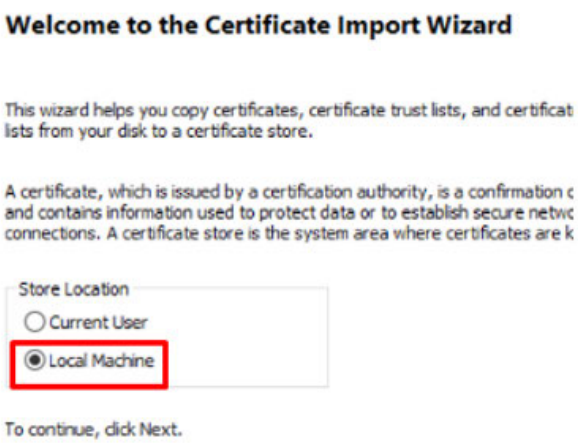
Now I'll go to the firewall policy, and configure the Profile with the existing Traffic Out policy.



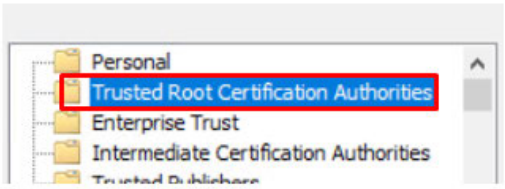
Now I'll copy the certificate to windows 10 and install it



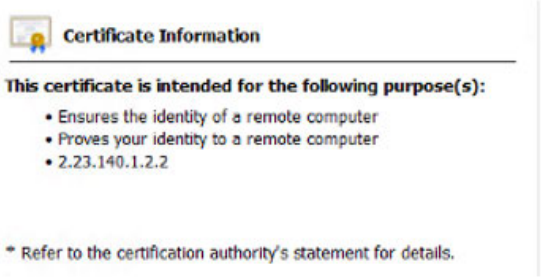
Next I'll go to the Certificate Import Wizard and Select local machine



Select the Trusted Authorities



We can see the Certificate information here



Part 7: Web Filter

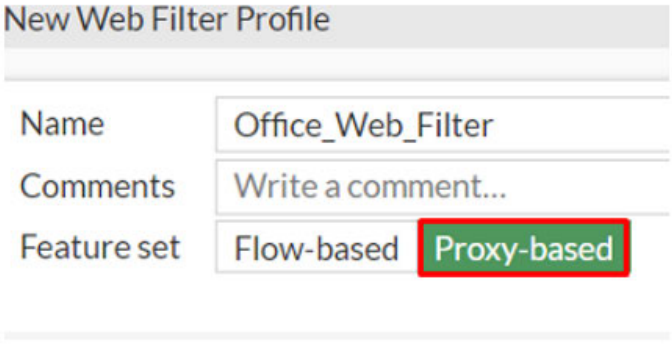
The web filter feature in FortiGate helps organizations control web traffic by blocking access to inappropriate or malicious websites based on predefined policies.

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.

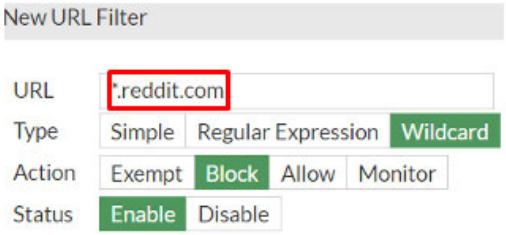
I'll start by creating a new Profile named Office_Web_Filter and make it Proxy Based



Next I'll deny access to Reddit.com, also to the Shopping and Job Search categories

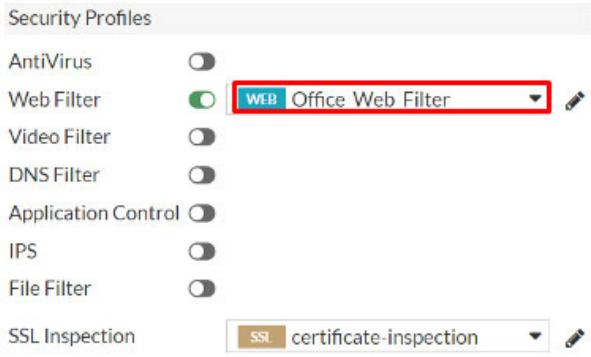
I'll start by disabling fortyguard filter

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

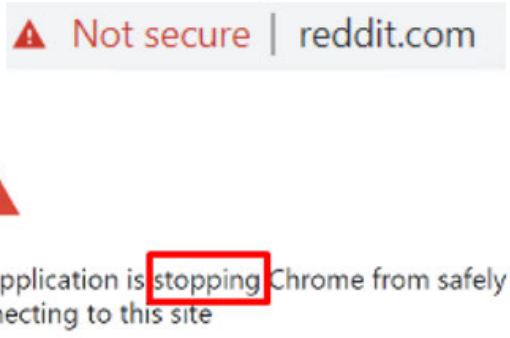


Now I'll go to the traffic out interface and change to proxy based inspection

Now I'll add in the Office_Web_Filter and apply

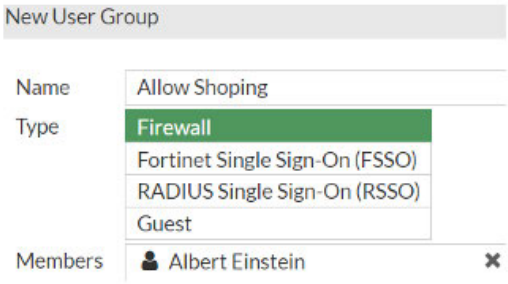


Let's test with one of the users to see if reddit is blocked

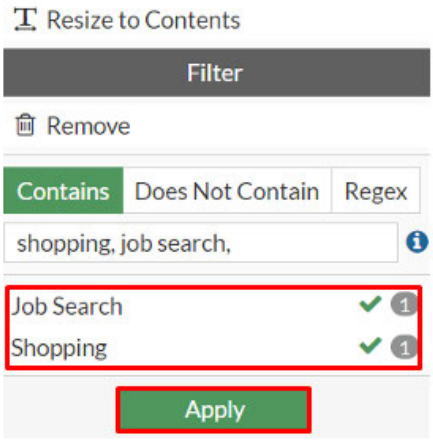


It's blocked, Next step I'll be blocked shopping to everyone but one user
I'll also block job searching for everyone

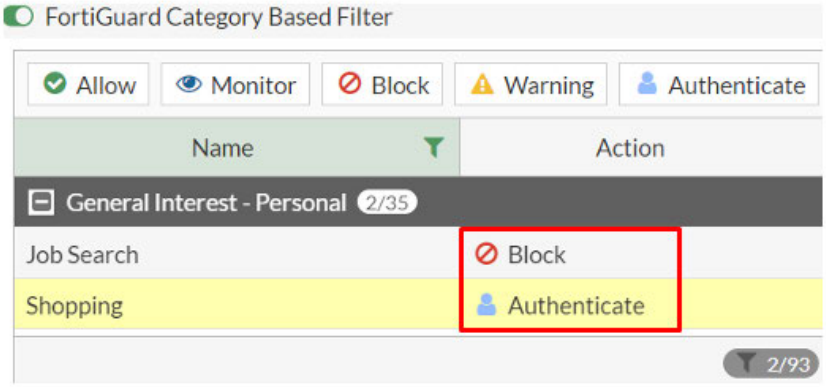
I'll start by making a group for the one user that will have access to shopping



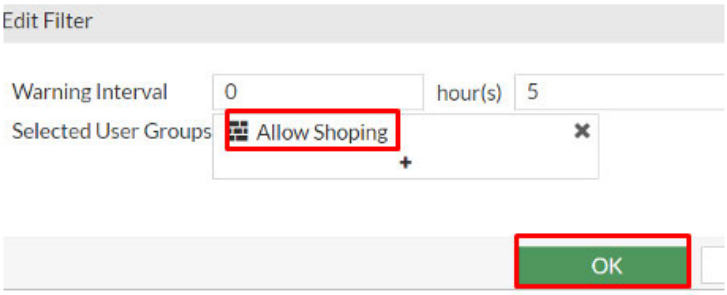
I'll turn on fortiguard



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



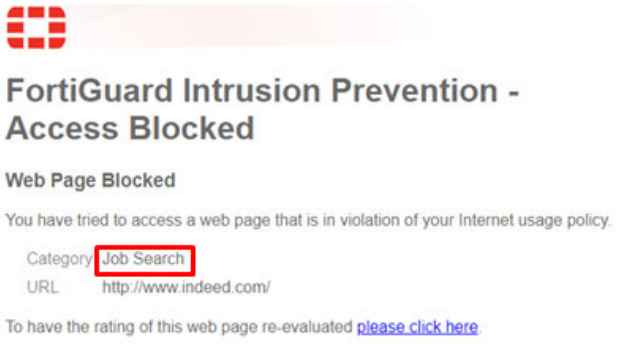
I the next page I'll select the group that can use shopping



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!

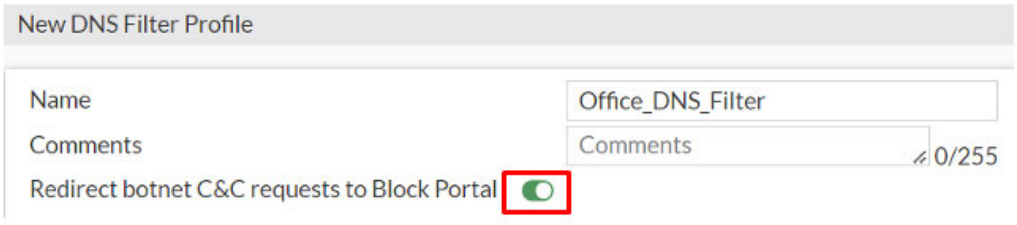
Part 8: DNS Filter

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

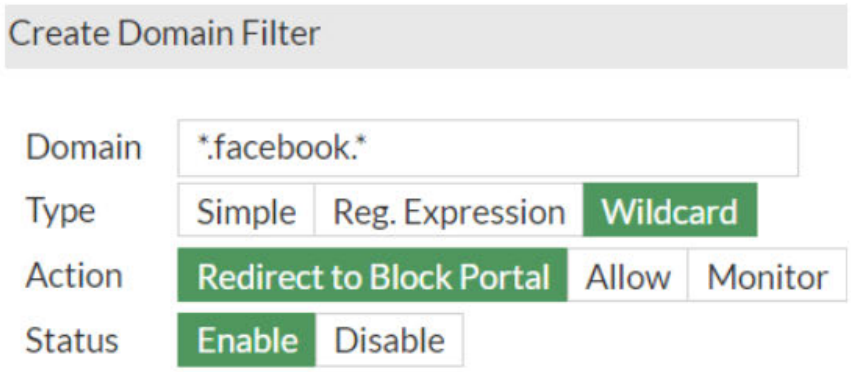
It enhances security by preventing access to malicious domains, improves productivity by blocking non-business-related sites, and ensures compliance with regulatory requirements.

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

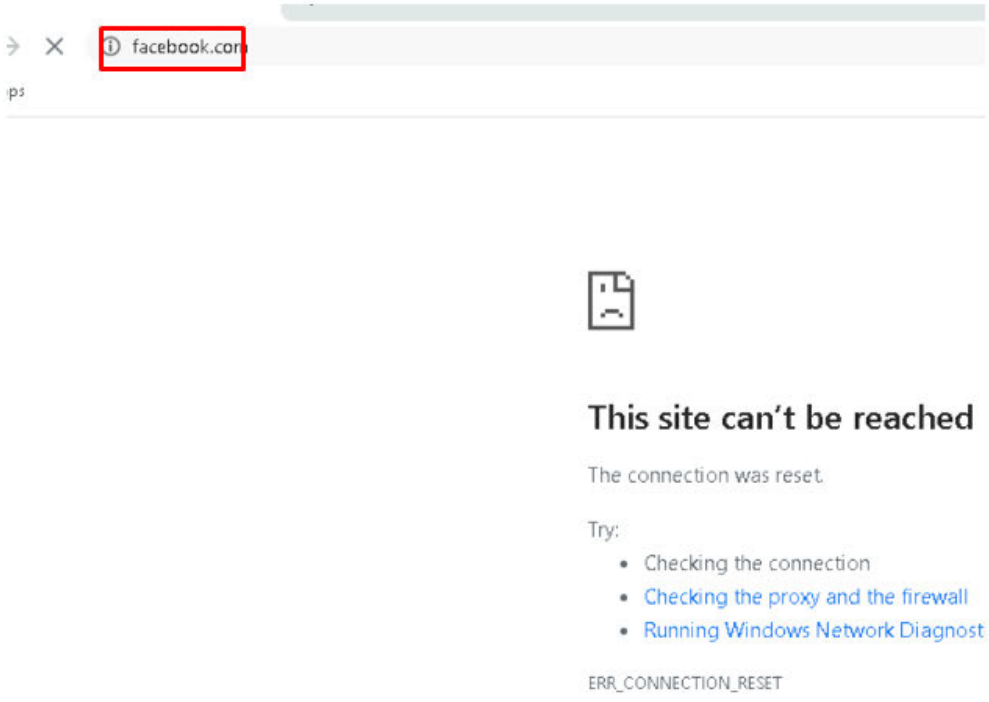
I'll start by creating a new Profile named Office_DNS_Filter, also activating the Botnet C&C requests to block portal which will redirect and block all C&C type requests



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



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



And its blocked, which is great because Facebook sucks

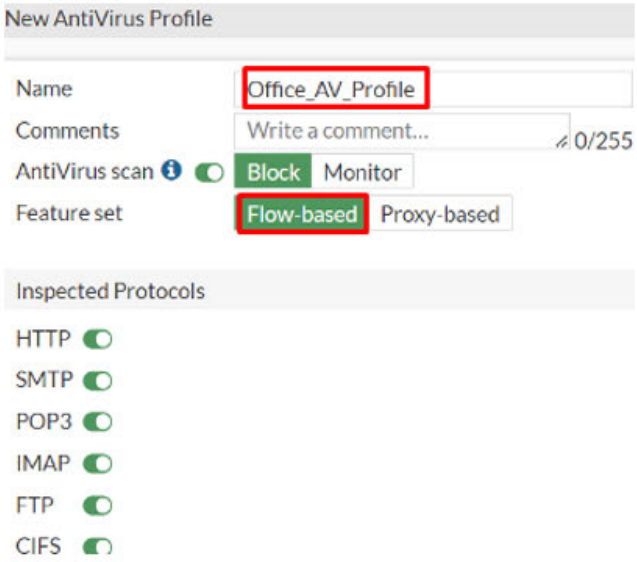
Part 9: Antivirus Profile

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.

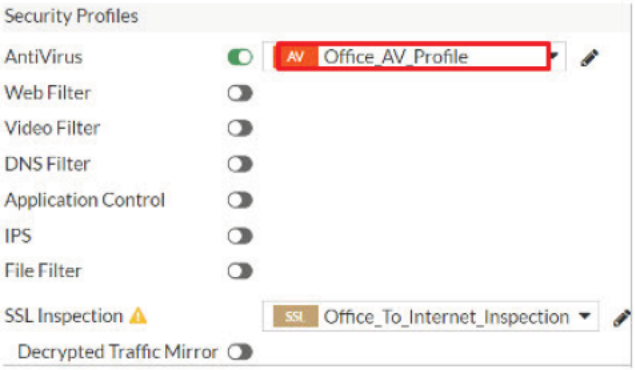
The AV database in FortiGate is a repository of signatures and definitions used to identify and block malware threats. It's regularly updated to detect new viruses, trojans, and other malicious software, ensuring effective protection against evolving threats.

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

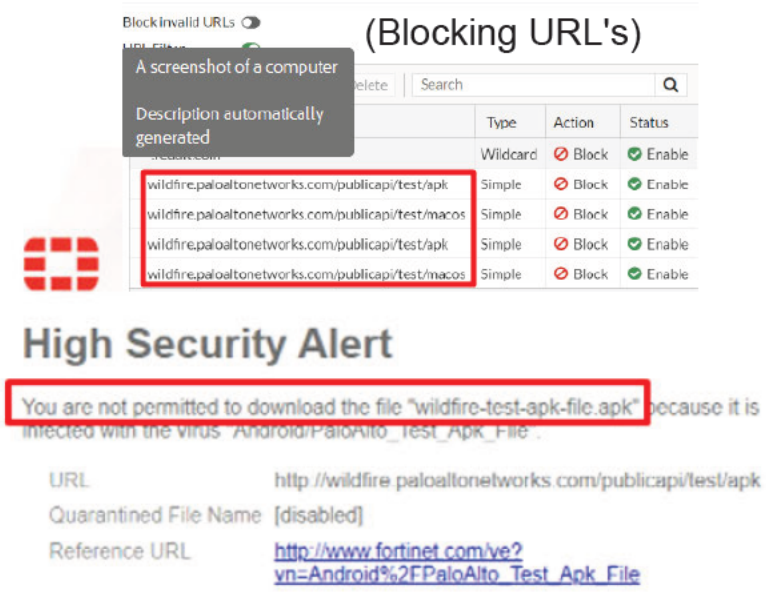


I'll apply the rule on the existing interface/policy trafficOut

To test I'll disable all existing profiles except SSL



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



Success, its blocking the PaloAlto virus test files as intended

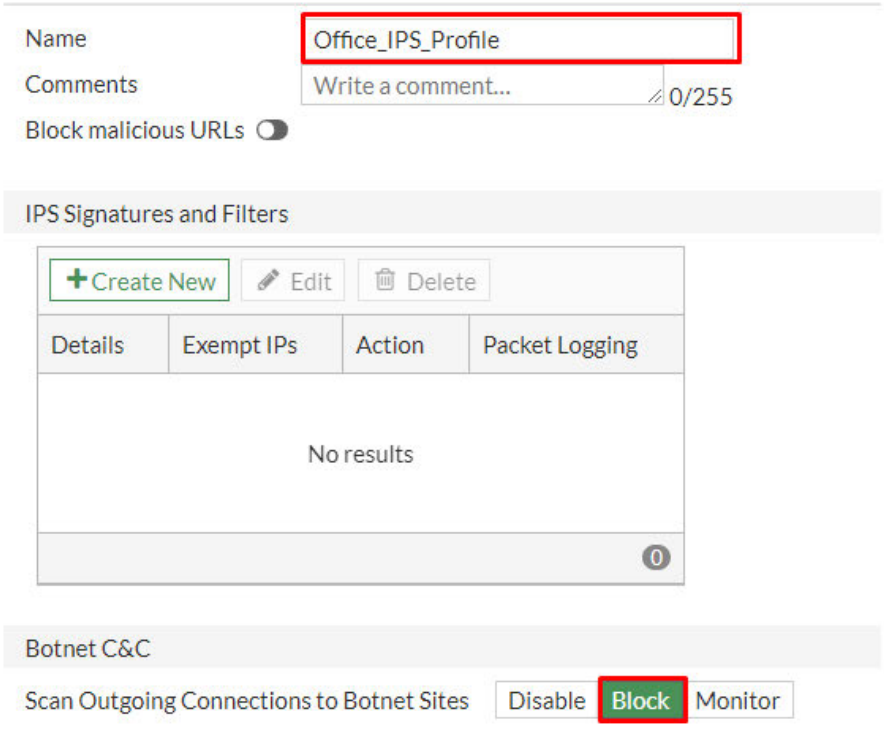
Part 10: IPS Profile

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

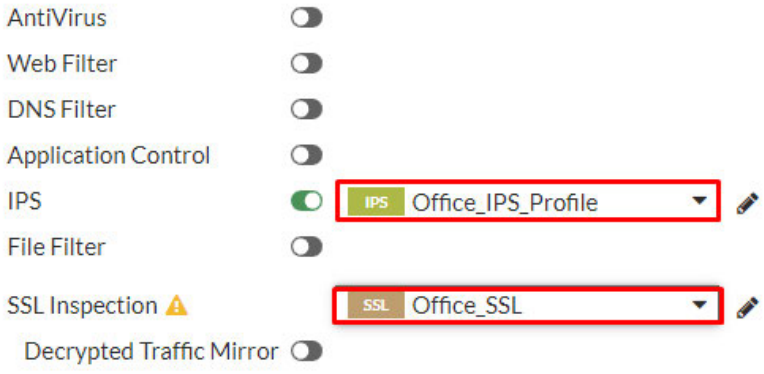
Its benefits include preventing known and zero-day attacks, offering customizable protection, and providing real-time response to threats.

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



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

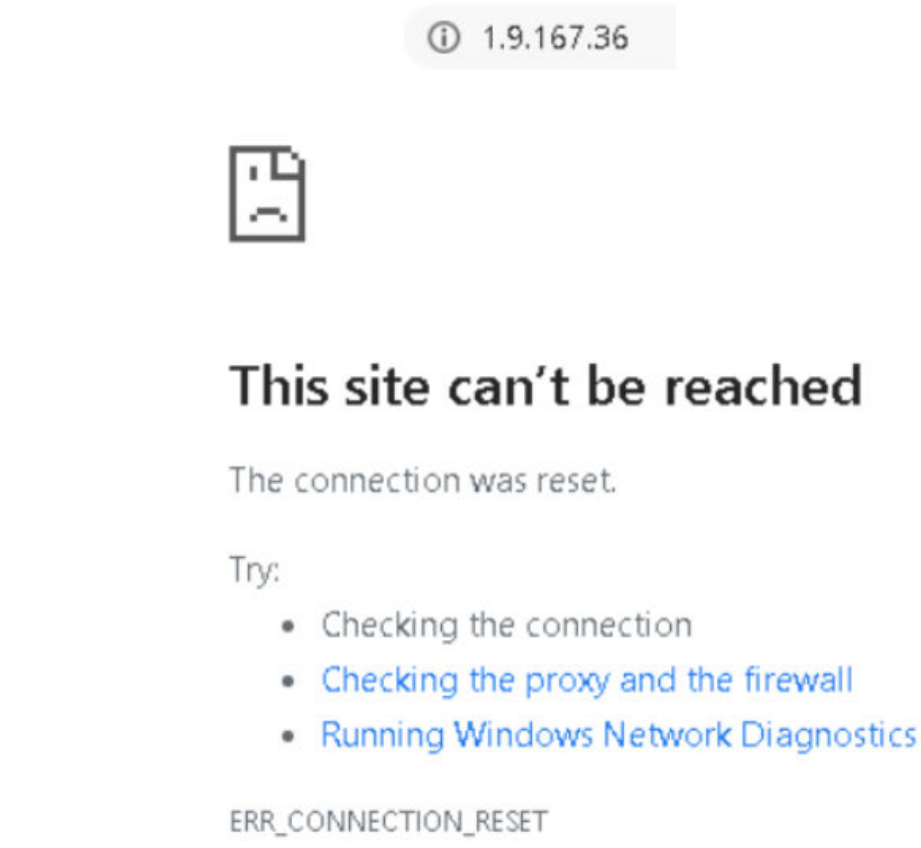


Now to test this, I will see if it's getting blocked from WIN10 by taking one of the addresses from the botnet Database

Botnet C&C IP Definitions

Search

IP	Port	Protocol	
1.9.167.36	60,489	TCP	KillNet



Its working as intended!

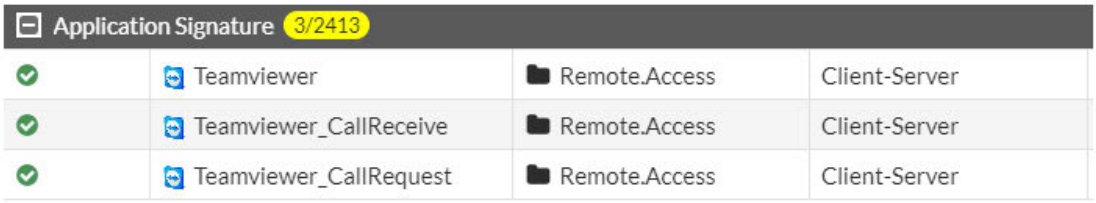
Part 11: Application Control

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

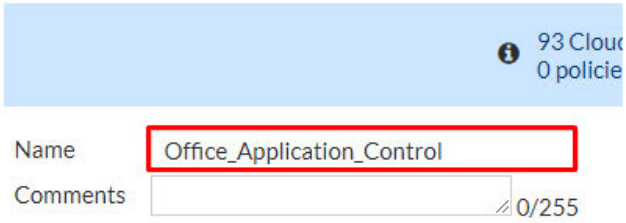
It enables the identification and control of applications, offering benefits such as regulating bandwidth usage, enhancing security by blocking unauthorized applications, and enforcing policies to ensure compliance.

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

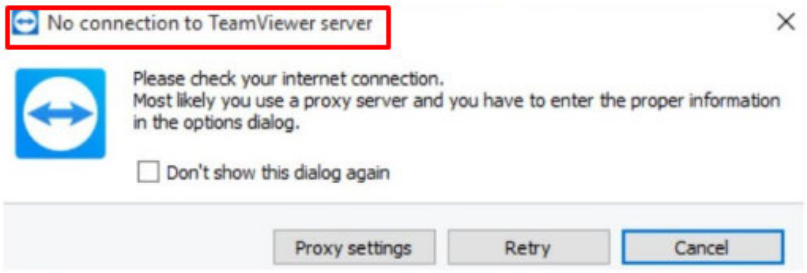


Next I'll create a new profile named Office_Application_Control

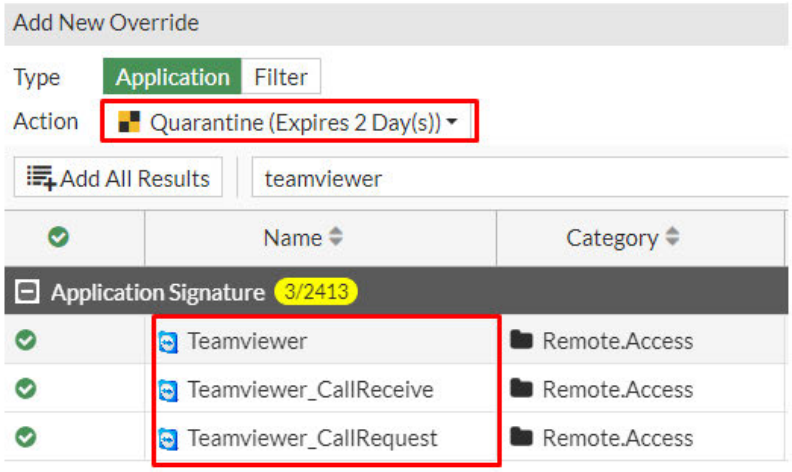


And I'll block Remote Access

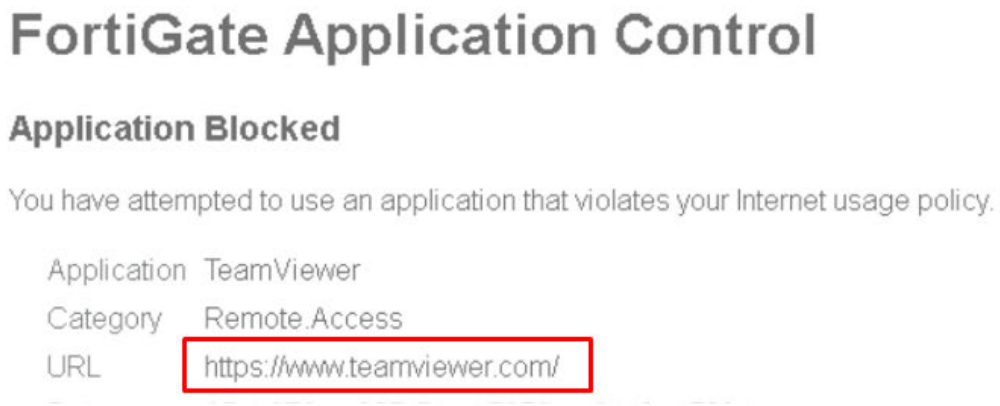
Now I'll test on WIN10 to see if the new settings are working as intended



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



Save the changes and try to use TeamViewer



And its blocked, working as intended